In this appendix, we will cover the following topics:

- ▶ IBM Infosphere Guardium Database Security
- Oracle Database Firewall
- Oracle Audit Vault

# **IBM Infosphere Guardium Database Security**

A Database Activity Monitor (DAM) is a non-intrusive system that implements real time monitoring and alerting for various databases.

Non-intrusive monitoring systems are implemented by the vendor at the network communication and database shared memory level, and therefore a direct connection to the database to query or look for audit information is not required.

Generally these systems may have additional protection and prevention capabilities such as blocking unauthorized access to data or blocking access to data which is violating a defined access policy (for example, do not run a query more than three times in a minute).

## **Guardium security life cycle**

The Guardium life cycle can be summarized as follows:

• **Discover and classify**: Discover all databases, applications, and clients. Discover and classify sensitive data.

- Access and harden: Vulnerability assessment, configuration assessment, behavioral assessment, create baseline, configuration lock-down, and change tracking.
- Monitor and enforce: Non-intrusive monitoring, policy-based actions, anomaly detection, real-time prevention, and granular access controls.
- Audit and report: Centralized governance, compliance reporting, sign-off management, automated escalations, secure audit warehouse, data mining for forensics, and long-term retention.

### Installation and configuration

Guardium is generally recommended to be installed on a dedicated system or is usually delivered as appliances. The installation kit consists of a customized Linux and application package. It is important to remember to have allocate sufficient free space on the installation drive (about 180 GB free space, or else the installation will fail). The installer will remove and will use all available space.

1. Insert the CD or mount the installation kit if you install Guardium on virtual machines. The installation will start by creating the storage layout followed by the Linux and Guardium packages installation, as shown in the following screenshot:



2. When installation of the packages is completed, you'll need to introduce temporary user passwords for CLI, ADMIN, and ADMIN\_MGM users. These passwords will be changed at the first login. If you do not change the password for the user **CLI** during installation, the default temporary password guardium will be used.



3. Enter a temporary password for the user **GUI ADMIN**.

			•
Please enter	GUI ADM a password: (ther	IN password e will be no feedback)	]
	< 0K >	<cancel></cancel>	-

4. Enter a temporary password for the user **ACCESS MANAGER**.

			<b>N</b>
Please enter	ACCESS MANA a password: (there	NGER password : will be no feedback)	
		<cancel></cancel>	-

5. For a standalone installation, chose the default option, Collector, otherwise if you want to run Guardium as an aggregator choose **No**.

	Aggreg	fator			1
Please press this machine	YES to proceed an AGGREGATOR.	with the	default,	NO to make	
					-
	< Yes >	< No	>		

6. At this moment we have finished installing Guardium. The system will reboot automatically. Next, we will proceed to the network configuration phase. Connect as the **cli** user with the password guardium. At this step, it is mandatory to change the password.





```
7. Configure the IP address and network mask:
   store network interface ip <your ip>
   store network interface mask <your ip's corresponding mask>
   SQL Guard 8.0 ------
  Unauthorized access is prohibited
   -----
   INIT: Id "0" respawning too fast: disabled for 5 minutes
   SOL Guard 8.0 ------
   Unauthorized access is prohibited
   L
_____
  guard login: cli
   guarPassword:
   ogin incorrect
  login: cli
   Password:
   Welcome cli - this is your first login in this system.
  Your password has expired.
Changing password for 'cli'.
  Enter current password:
  Enter new password:
   Re-enter new password:
                                                                k
   Setting default expiration period to 90 days.
  guard.yourcompany.com> store network interface ip 10.241.132.20
   This change will take effect after the next reboot.
   ok
  guard.yourcompany.com> store network interface mask 255.255.2
   This change will take effect after the next reboot.
   ok
  guard.yourcompany.com>
```

8. To make these values active, and persistent we have to reboot the system. In the CLI command prompt execute the following command:

restart system

5 —

#### **Deployment and configuration of S-TAP agents**

Database and system monitoring is performed by using and deploying agents on each database server host. These agents have the generic name of S-TAP. Installation and configuration of these agents can be made using an interactive installer. After the agents are deployed and are communicating with the Guardium server they can be configured remotely from the administration console local S-TAPs as follows:

As the user root starts the S-TAP installer:



- Next the installer will perform the installation of all the libraries. The last step is the configuration of the S-TAP init file. S-TAP configuration is contained in a file named s-tap.init. The installer will open this file for the purpose of editing with vi and this will require to set all the mandatory parameters.
- To verify and check that the agents are running and communicating with the Guardium server, log in to the Guardium console, check the status of agents. Their status should be green in the console.

# Performing a vulnerability assessment

Usually performing a vulnerability assessment is one of the first few steps for securing and defending a database. There are many types of vulnerabilities based on bugs or incorrect configuration.

 To perform a vulnerability assessment we must connect to the administration console and navigate to **Tools** and in the **Config & Control** panel click on the **Security Assessment Builder** link, as shown in the following screenshot:

	Daily Monitor   Guardium Monitor   Tap Monitor   Incident Management
onfig & Control	Security Assessment Builder
ccess Map Builder/Viewer	Security Assessment Finder
lert Builder	A
lias Builder	
udit Process Builder	
udit Process To-do List	
uto-discovery Configuration	
aseline Builder	
AS Host Config	
AS Template Set Config	
Classification Policy Builder	
lassification Process Builder	
atasource Definitions	
aroup Builder	
olicy Builder	
'ortlet Editor	
rivacy Set Builder	
ecurity Assessment Builder	New
ime Period Builder	Run Once Now View Results
Joluo Chango Audit DR Croation	User-defined tests
alue change Audit DB creation	Query-based Tests CAS-based Tests
alue Change Audit DB Update & Upload	
alue Change Audit DB Creaton 'alue Change Audit DB Update & Upload 'alue Change Auditing Builder	
'alue Change Audit DB Cleanon 'alue Change Audit DB Update & Upload 'alue Change Auditing Builder Vorkflow Builder	
ande Change Audit DB Greaton 'alue Change Audit DB Update & Upload 'alue Change Auditing Builder Vorkflow Builder	
ande Change Audit DB Greaton 'alue Change Audit DB Update & Upload 'alue Change Auditing Builder Vorkflow Builder	
alue Change Audit DB Update & Upbad 'alue Change Audit DB Update & Upbad 'alue Change Auditing Builder Vorkflow Builder	

2. We must first define the source on which we will run the security assessment. The configuration of a data source is straightforward. In our case, we have the following configuration. In this panel we can test whether we can connect. We have used the system user. If the network data is ready to go, click on the **Apply** button, as shown in the following screenshot:

Datasource Definition	<u> </u>	
Name	HACKDB SEC ASSESSMENT	
Database Type	Oracle (DataDirect)	
Severity classification	HIGH 🗢	
Description		
Share Datasource		
Authentication		
Save Password		
Login Name	system	
Password		
Location		
Host Name/IP	10.241.132.80	
Port	1521	
Service Name	HACKDB	
Informix Server		
Schema		
Connection Property		
Custom Uri		
CAS		
Database Instance Account		
Database Instance Directory		
Roles		
lo roles have been assigned t	o this datasource Roles	
Add Com	nents Test Connection Apply Back	
	( the second sec	

- 8 -

3. Our configured data source will appear as the target for the security assessment, then click on the **Apply** button, as shown in the following screenshot:

ystem View Administration Console To	ols 🖉 Daily Monitor 🛛 Guardium Me	onitor Tap Monitor Inc	cident Management		
Config & Control	Security Assessment Builder				
Access Map Builder/Viewer	Security Assessment Builder				?
Alert Builder	Description	HACKDB_SECASSESS	IENT		
Alias Builder	Observed Test Parameters:				
Audit Process Builder	Period From	NOW -1 DAY		$\overline{\bigcirc}$	
Audit Process To-do List	То	NOW	) 🖬	$\overline{\bigcirc}$	
Auto-discovery Configuration	Client IP or IP subnet		(0	ptional)	
Baseline Builder	Server IP or IP subnet		(0	ptional)	
CAS Host Config	Datasources				
CAS Template Set Config		Name	Туре	Host UserNan	ne
Classification Policy Builder	ACKDB_SEC_ASSESSME	NT_ORACLE(Security A	ssessment) ORACLE 10	.241.132.80 system	
Classification Process Builder				Add Datasource	
Datasource Definitions	Doles				
Group Builder	No Polos have been assigned t	a this Cosurity Assocs	mont Dalas		
Policy Builder	No Roles have been assigned t	o uns security Assessi	Roles		
Portlet Editor	Revert Apply	Configure Test	s CAS Supp	ort Back	
Privacy Set Builder					_
Security Assessment Builder					
Time Period Builder					
Value Change Audit DB Creation					
Value Change Audit DB Update & Upload					
Value Change Auditing Builder					
Workflow Builder					

4. Next choose the vulnerabilities to be checked. In the **Test available for addition** option, check the option **All**. Then click on the **ORACLE** tab and select all the vulnerabilities from the list box found on this panel and click on the **Add Selections** button. Click on the **Select All** button and click on **Save**. This is shown in the following screenshot:

System View	Administration Console Tool	ls 🧷 Daily Monitor 🛛	Guardium Monitor Tap Monitor In	cident Management			
Config & Co	ntrol	Security Assessment Bu	ilder				
Access Map	Builder/Viewer	Assessment Test S	elections				?
Alert Builder		Tests for Security A	ssessment HACKDB_SECASSES	SMENT			
Alias Builder		Select All	Unselect All De	lete Selected			
Audit Proces	s Builder	Type	Test Na	me		Tuning	Â
Audit Proces	is To-do List	ORACLE TRA	CE FILES PUBLIC Is False		CONF M	linor (n/a)	=
Auto-discove	ery Configuration		IN RESTRICTIONS Is On		CONF M	laior (n/a)	
CAS Heat Or	oer		ss To The UTL EILE Package in	restricted		aior (n/a)	
CAS Templa	te Set Confin					ajor (n/a) .	
Classification	a Policy Builder	ORACLE Adm	inistrative privilege assignm	ent		ajor (n/a):	
Classification	Process Builder	ORACLE CON	NECT_TIME is limited		Enter ma	ximum allowed value.	
Datasource	Definitions		DED SESSION limited		CONF C	autionary 5,000,000	
Group Builde	er	V ORACLE CFO	PER_SESSION Innited		Enter ma	ximum allowed value.	-
Policy Builde	r	Tests available f	or addition () Predefined () Q	uery based 🔿 CVE 💿 Al			
Portlet Editor							
Privacy Set I	Builder	[Observed] DB2	INFORMIX MS SQL SERVER M	YSQL NETEZZA ORACLE	POSTGRESQL	BASE TERADATA	
Security Ass	essment Builder						
Time Period	Builder	lests marks with an a	sterisk (*) require specific CAS monito	ing running on the Datasource	(s) tested		
Value Chang	e Audit DB Creation	no more tests o	f this type found / available 🔺				
Value Chang	e Audit DB Update & Upload						
Value Chang	e Auditing Builder						
Workflow Bu	ider						
		L	~	Add Selections			

-10-

5. A page will appear with our security assessment defined. Click on the **Run Once Now** button to perform a security assessment.

IBM° Info	Sphere™ Guardium®								
System View	Administration Console	Тоо	ls 🧷	Daily Monitor	Guardium Monitor	Tap Monitor	Incident Management	t	
Config & Co	introl		Secur	ity Assessment	Builder				
Access Map	Builder/Viewer		Sec	urity Assess	ment Finder			6	2
Alert Builder			HA	CKDB_SECASS	ESSMENT			4	
Alias Builder									
Audit Proces	ss Builder								
Audit Proces	ss To-do List								
Auto-discov	ery Configuration								
Baseline Bui	ilder								
CAS Host C	onfig								
CAS Templa	ate Set Config								
Classificatio	n Policy Builder								
Classificatio	n Process Builder								
Datasource	Definitions								
Group Builde	er								
Policy Builde	er								
Portlet Edito	r								7
Privacy Set	Builder			New	Madifu	afiaura Tasta	Commont	Clana Delete	
Security Ass	sessment Builder			New		ingure rests		Cione Delete	
Time Period	Builder						Run Once Now	View Results	
Value Chang	ge Audit DB Creation		Use	er-defined test	s				
Value Chang	ge Audit DB Update & Uplo	ad				Q	uery-based Tests	CAS-based Tests	
Value Chang	ge Auditing Builder						,		2
Workflow Bu	rilder								
Report Build	ling								

The result for the security assessment with details and scores is generated as follows:

Textubite Society Associations: B AucCosta, SECASSES SEMANT Association and AucCosta, SECASSES SEMANT Association and AucCosta AucCosta AucCosta AucCosta AucCosta Costa AucCosta Aucc	The in the intervention of the process and the process and the intervention of the int	Deventional HDF
Tests passive $32\%'$	Table is name free you can address problems within your analogness to it what you down you for a second sec	
Exercise technique entre d'une le la sessione de access de la des de la de de de de la des des provients again reprover. Eler is his conversion a la reducia la de Roccas en de Diorne, si no traga administrativa produid esc conder al male gina resource si en aut tech contra a de sub- tection de la desta de la de Roccas de la desta de la de	an and a start and a start and	a com
Result Service         Data         Main         Carrier Main         Carrier Main           Data         Main         Carrier Main         Carrier Main         Carrier Main           Administration 19         Main         Carrier Main         Carrier Main         Carrier Main           Contracting 19         Main         Carrier Main         Carrier Main         Carrier Main           Contracting 19         Main         Strate         Strate         Strate           Weinit         29         Strate         Strate         Strate           Weinit         29         Strate         Strate         Strate           Weinit         29         Strate         Strate         Strate		
Assessment Text Results Konservath atter results	Showing 274 of 274 ref	alter (0 filtered)
Test / Celescurce	Besult	
PR A String FARTS_LODE_ATTREPS tare tended Tour starty GARTOUSTOUS_CONE_CONE_CONE_CONE_CONE_CONE_CONE_CONE	Fail Like years (ACID TURKE, PROFIL) lead permanent ALLIL (CORL, PUTTHER'S Institut or antibutine bard and Personnabative: The FALLID (CORL, ATTIVITY) personals is reset Alight rules of the Light despite and subscribed control for an UNITY and the permanent and rule in the permanent scale of interference and rules and subscribed on the PALLID (CORL, ATTIVITY) and the permanent scale of interference and rules and the permanent scale of the PALLID (CORL, ATTIVITY) and the permanent scale of interference and rules and the permanent scale of the PALLID (CORL, ATTIVITY) and the permanent scale of interference and rules and the permanent scale of the PALLID (CORL, ATTIVITY) and the permanent scale of the the permanent scale of the PALLID (CORL, ATTIVITY) and the permanent scale of the the permanent scale of the permane	ia inying te gan Laccount

Perform the necessary correction as the security assessment report advises and repeat the assessment until you have a 100 percent score.

# **Oracle Database Firewall**

Oracle Database Firewall monitors traffic at network level using SQL grammar-based technology. In practice, it dissects the network packet and checks the SQL statements issued by the clients. It is a heterogeneous technology with support for monitoring DB2, MS SQL, MySQL, and Sybase databases. Depending on the traffic registered in a period of time, policies can be defined using a tool called **Oracle Firewall Analyzer**. The definition of policies is largely based on baselines. We may have white lists, black lists, and exceptions. **White listed statements** are a category of statements that may pass from clients to servers without any restriction. **Black listed statements** are a category of statement that may not pass and that are blocked by Oracle Database Firewall. **Exceptions** are a category of statements that can be exempted from a policy.

Policies can also be associated with additional inspection criteria such as the time of day, IP address, and username in order to generate more complex policies when needed.

Traffic can be monitored by interposing an Oracle Database Firewall between a client and a server (in-line monitoring) by using bridged or proxy traffic sources or by using network taps (out of band monitoring). Monitoring can be made either in passive mode, Database Activity Monitor (DAM) mode, reactive mode, or Database Policy Enforcement (DPE) mode. There is also support for remote monitoring using monitoring agents and local connections for statements issued locally using local agents.

Along with monitoring capabilities, Oracle Database Firewall provides real-time alerting and reporting capabilities and provides built-in custom modules to verify compliance with regulatory requirements such as **Sarbanes-Oxley (SOX) Act**, **Payment Card Industry Data Security Standard (PCI DSS)**, and **Health Insurance Portability and Accountability Act (HIPAA)**.

#### Installation and configuration

Oracle Database Firewall consists of a custom installation of Oracle Enterprise Linux infrastructure, ODF packages, customized WebLogic application server, and a database which is used as a repository for items such as policies, rules, and exceptions. For a more complex installation where we want to use more than one Database Firewall environment it is recommended to install the Oracle Database Firewall Management server used for centralized management. Depending on the current network configuration in your organization you can decide on the type of monitor configuration to use. We used a configuration with three network cards, one dedicated to ODF management and two for implementing bridged network configuration. In a bridged network configuration all traffic from clients will pass through the network devices configured on ODF machine. We used something similar with the following setup described at this link.



The installation kit for version 5.1 used in our description consists of the following:

- Oracle Linux Release 5 Update 5 for x86 (32 Bit) DVD
- Oracle Database Firewall Management Server 5.1 (ISO)
- Oracle Database Firewall 5.1 Disc 1 (ISO)
- Oracle Database Firewall 5.1 Disc 2 (ISO)
- ► Oracle Database Firewall 5.1 Disc 3 (ISO)
- Oracle Database Firewall Utilities 5.1 (ISO)

The installation and configuration steps are as follows:

- 1. On the dedicated server for DBF, insert Disc 1 and boot from it. If you want to install Oracle Firewall Management server, insert this disc.
- 2. After the system is booted it will require the disc with **Oracle Enterprise Linux** (**OEL**). It will perform the creation of the layout and install the core Linux system.
- 3. Next Disc 2 and Disc 3 will be required and the installation will continue.
- 4. Finally Disc 1 will be required again and the installation will finalize with configuration steps.
- 5. Next we have to configure the IP address for Oracle Database Firewall and the gateway if it is the case:

Network Settings Console	
<mark>Current settings</mark> IP Address: 10.241.132.200 Network Mask: 255.255.255.0 Default Gateway: 10.241.132.1	
Change	
IP Address Network Mask <u>-Default Gateway</u>	

## Adding and configuring protection for databases

From the client host, open a browser and type the DBF management host and port number (the default is 80) and log in as an admin user with an admin temporary password. At this step a password change is required.



#### **Traffic source configuration**

Navigate to the **System** tab. In the left-hand side panel, click on the **Networks** link and add the available network card to **Network 0** and check the **Bridge Enabled** option as follows:

System:	Management Int	erface						
Manage <u>NetwÖrk</u> Services	Settings IP Address	192.168.1.200	Device MAC Address 00.0c.29.4c.46.25	Bus Info 0000-02-03-0	Identifier 79c970 IPCnet32 LANCE1	Manufacturer Advanced Micro	Link	
Status Email Configuration Date and Time	Gateway	192.168.1.254 dbfw000c294cf611	Proxy Ports Traffic Source Id	Port	Enabled	Devices [AMD]	1	
Keyboard Public Keys Management Server			There are no traffic p	roxy ports assigne	d.			
Logs:	Traffic Sources							
Manage System Events Traffic Log Files	Network 0	Remove ]	Devices MAC Address	Bus Info	Identifier	Manufacturer	Link	
Administration Changes Repair	Network Mask	255 255 255 0	00.0c.29.4c.f6.11	0000.02.01.0	79c970 [PCnet32 LANCE]	Advanced Micro Devices [AMD]		Remove ]
Connectors:	MAC Address	00.0c.29.4c.f6.1b	00:0c:29:4c:f5:1b	0000:02:02.0	79c970 [PCnet32 LANCE]	Advanced Micro		Remove ]
Syslog ArcSight SIEM	Bridge Enabled	2				neures (vaup)		

#### Adding protected database

Navigate to the **Monitoring** tab. In the left-hand side panel, select **Protected Databases** and click on **Create**. Enter **Name** as **HACKDB\_ORCL**, the protected database configuration **Database Type** as **Oracle**, add **Address** and **Port Number** and click on the **Save** Button, as shown in the following screenshot:

CIUNCLE				
racle Database Firew	all Administration Console			
Ionitoring	Add Protected Database			
nforcement Points:	Settings			
List Create Tasks	Name	HACKDB_ORCL		
trotected Databases: List Create	Description (Optional)		*	
olicies:	Database Type	Oracle *		
List Upload	Address	192.168.1.90		
	Port Number	1521		
				Sage Cancel



15 -

#### **Creating enforcement point**

The enforcement points are the databases to be protected and monitored.

1. Navigate to the **Monitoring** tab. In the **Enforcement Points** panel, click on the **Create** link. Name the enforcement point as **HACKDB\_ORCL\_ENF**, as shown in the following screenshot, and click on **Next**:

ORACLE	Dashboard Monitoring	Reporting	Archiving	System
Oracle Database Firewall	Administration Console			
Monitoring	Enforcement Point Wizard: St	ep 1		
Enforcement Points: List Create	1 2 3	••• 4		
Tasks	Specify enforcement point details:			
Protected Databases:	Name: HACKDB_ORCL_ENF			
List Create	Use a builtin enforcement point:			
Policies: List	<ul> <li>Monitor locally (80 available</li> </ul>	)		
Upload	Netst			

2. Chose the protection point defined before HACKDB\_ORCL and click on Next:

ORACLE	Dashboard	Monitoring	Reporting	Archiving	System
racle Database Firewall	Administration Co	nsole			
Ionitoring	Enforcement Poi	nt Wizard: Step	2		
nforcement Points: List Create	1 2	••• 3 •	•• 4		
Tasks	Select a protected	database:			
rotected Databases:	Protected Databas	e: Oracle	- HACKDB ORCL	•	
List Create	Specify the details	of the protected da	tabases you wish to	monitor:	
olicies:	Name:				
List	Database Type:	Oracl		]	
Upload	Address		Port		Resolved Address
					Add
					Draviaua Nort
opodu	Address		Port		Resolved Address Add Previous

3. Choose the monitoring mode – **Database Policy Enhancement (DPE)** and from the available policies select **unique-nomask.dna** and click on **Next**, as shown in the following screenshot:

Enforcement	Point Wizard: Step 3	
Enlorcemen	T one wizard. Step 5	
1	2 ••• 3 ••• 4	
Specify the m	onitoring mode and policy to use for monitoring:	
Monitoring Mode:	<ul> <li>Database Policy Enforcement (DPE)</li> <li>Database Activity Monitoring (DAM)</li> </ul>	
Policy:	Name	Description
	logall-nomask.dna	Log all statements for offline analysis without masking data (Note: if this policy is applied, it can use significant amounts of st you select this policy)
	💿 logall.dna	Log all statements for offline analysis (Note: if this policy is applied, it can use significant amounts of storage for the logged data
	logsample.dna	Log a sample of statements for offline analysis (Note: if this policy is applied, although it will store less statements than loggir the logged data)
	passall.dna	Pass all statements
	policy1.dna	
	unique-nomask.dna	Log examples of statements for offline analysis covering each distinct source of traffic in the statements (Note: if this policy is statements, it can still use significant amounts of storage for the logged data. Sensitive information may be logged if you sele
	◎ unique.dna	Log examples of statements for offline analysis covering each distinct source of traffic (Note: if this policy is applied, although use significant amounts of storage for the logged data)
	Browse	l l

4. Now a summary will be displayed, as we do not have another traffic source defined while **Network 0** is the default one. Finally, click on **Finish**. At this moment our database starts being monitored.

ORACLE.	Dashboard	Monitoring	Reporting	Archiving	System		
Oracle Database Firewa	II Administration C	Console					
Monitoring	Enforcement P	Enforcement Point Wizard: Step 4					
Enforcement Points: List Create Tasks	1 ····	2 • • • 3 •	••• 4	ith the following detai	Is will be created:		
Protected Databases: List Create	Name: Database Type:		I I	HACKDB_ORCL_ENF			
Policies:	Protected Databa	ase Name:					
List Upload	Protected Databa	ase Addresses:		Address Port 192.168.1.90 1521			
	Monitoring Mode		I	DPE			
	Policy:			unique-nomask.dna			
				Pr	evious Finish		



Verify that Oracle Database Firewall monitors the traffic from client host connect to server database server **HACKDB**. To check that our connection is monitored, navigate to the **System** tab. In the **Network Traffic** panel, click on the **Network traffic**: link. Try to issue some statements against the server. From the **Level of details** panel, select **Packet content** and select **Network 0** from **Network**. Issue a statement and click on the **Show Traffic** button. With this, we should see the packet's content as shown in the following screenshot:

2							
Adminis	tration C	onsole					
Matura	els Troffi o						
Netwo	IK ITAIIIC						
Filter		Show all	oracle - HACKDB	•	C:\Windows\system	n32\cmd.exe - sqlplus hr/hr@hackdb	
Level	of details	<ul> <li>Only where database</li> <li>Summary</li> <li>Packet content</li> </ul>			Stiles Sullivan Sully Taylor Taylor	Stephen Martha Patrick Jonathon Winston	
Durati	ion	12 - seconds			Tobias Tucker Tuvault	Sigal Peter Oliver	
Netwo	ork	Management			LAST_NAME	FIRST_NAME	
Show	w <sub>o</sub> Traffic	Network 0			Urman Vargas Vishney Vollman Walsh	Jose Manuel Peter Clara Shanta Alana	
Netwo	ork traffic	*			Weiss Whalen Zlotkey	Matthew Jennifer Eleni	
21:48:1 Ack=1	13.952502 1 Win=253 Le	192.168.1.10 -> 192.168.1 en=299	.220 TCP 49255 > micromus	e-Im [PSH, ACK] Seq=	107 rows selecte	ed.	
0000 0 0010 0 0020 0	00 0c 29 4c 01 53 05 05 01 dc c0 67	f6 11 00 0c 29 2e fe 43 0 40 00 80 06 70 69 c0 a8 05 fe 5f 9b 6e 32 6c 9d b	8 00 45 00)L)CE. 01 0a c0 a8S@pi 2 6e 50 18gn2lnP.		SQL> 1 1* select last SQL>	t_name,first_name from employees	
0030 0	) 0 fd 33 e8 ( 11 69 32 fe f	00 00 01 2b 00 00 06 00	00 00 00 00				
0050 0	0 00 00 03	5e 33 61 80 00 00 00 00	00 00 fe ff^3a				
0060 ff	f ff 0d 00 00	ουυυυτεπππππ 00 fe ff ff ff ff ff ff ff fe ff .	····~				
0080 ff 0090 0	ffffffffff00 00 00 00 00	0 00 00 00 01 00 00 00 00 00 00 00 00 00	0 00				
00a0 0	00 00 00 00	00 00 fe ff ff ff ff ff ff 00 0	00				
00c0 ff	f ff ff ff ff ff fe	ffffffffffff0000					
00d0 0 00e0 ff	00 00 00 00 f ff ff ff ff ff 00	00 00 fe ff ff ff ff ff ff ff fe ff 0 00 00 00 00 00 00 00 00 00	0 00				
00f0 0	0 00 00 00 0	00 00 00 00 00 00 00 00 00	00 00 00 00				
0110 6	61 6d 65 2c	66 69 72 73 74 5f 6e 61	6d 65 20 66 ame,first_name	f			
0120.7	72.6f.6d 20.6	65.6d.70.6c.6f.79.65.65.7	3.01.00.00rom employees.				

17 –

# **Using Oracle Firewall Analyzer**

**Oracle Firewall Analyzer** is a standalone tool which is designated to create and modify custom policies. The following steps will help you to install and use Oracle Firewall Analyzer.

1. On the windows client, install Oracle Firewall Analyzer and launch it. From the **New** menu, click on **New Model** and select **Train on Log Data** and click on the **Change...** button, as shown in the following screenshot:

Data Advanced			
Irain on Log Dat	a		
Protected Db:	<none selected=""></none>	Change	
Start Date:	<none selected=""></none>		
End Date:	<none selected=""></none>		
🔿 Train on File			
File:	<none selected=""></none>		Browse
Database Type	e: Orade	Ŧ	

- 18

2. Add **Traffic Log Server** which is the same IP used during the installation of Oracle Database Firewall. Next log in with the Oracle Database Firewall credentials as follows and click on **OK**, as shown in the following screenshot:

1	Fraffic Log Server:	
New _	IP Address: Change	23
Da	Protected Database:	
©	Traffic Log Server       IP Address:       192.168, 1.200       S       Login       Username:       admin       Password:       •••••••       Train       Ø No       QK       Cancel	]
	Advanced: Exception matches Invalid statements	

19 -

3. After the connection is established, click on the **Train** button. We should then see the captured statements issued in the logging interval, as shown in the following screenshot:

e View Update Annotate Tools	Window Help			
mmary Details Baceline Properties An	alueie Towalid SOL			
ceptions	alysis Invalid Sige			Unassigned: 0
				Passed: 0
data to display.				Warned: 0
				Blocked: 0
				New Group
tement Class Distribution				Data manipulation
				Data manipulation:
				Data definition:
				Data control:
📕 Data Manipulation Read Only 📕 D	ata Manipulation 📒 Data Definitio	n 📃 Data Control 📕 Procedural 📕 Transaction 📕 Con	mposite Containing Transaction 🗌 Composite	Procedural: Transaction
and the probability of the				Transaction.
eat Seventy Distribution				Assign Threat Severit
				Unassigned: 10
				Insignificant: 0
				Minor: 0
	· · · ·			
Unassigned In:	significant <u>Minor</u>	Moderate Ma	jor <u>Catastrophic</u>	Moderate: 0
Unassigned In:	significant Minor	Moderate Ma	jor <u>Catastrophic</u>	Moderate: 0 Major: 0
Unassigned In:	significant Minor	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Assign Policies
Unassigned In:	significant Minor	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Assign Policies Unassigned: 10
Unassigned Ins	significant Minor	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Assign Policies Unassigned: 10 Passed: 0
Unassigned In	significant Minor	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Assign Policies Unassigned: 10 Passed: 0 Warned: 0
Unassigned In:	significant Minor Minor Pass	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Assign Policies Unassigned: 10 Passed: 0 Warned: 0 Blocked: 0
Unassigned In on Distribution Unassigned etty Policy Rules	significant Minor	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Lnassigned: 10 Passed: 0 Warned: 0 Blocked: 0 Passed: 0
Unassigned In:	Pass	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Assign Policies Unassigned: 10 Passed: 0 Blocked: 0 Blocked: 0
Unassigned In: on Distribution Unassigned etty Policy Rules Novelty rules that use Match Any Table	significant Minor	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Assign Policies Unassigned: 10 Passed: 0 Bioked: 0 Bioked: 0 Mannoushe Bellow
Unassigned In: on Distribution Unassigned eity Policy Rules Novelty rules that use 'Match Any Table' Novelty rules that use 'Match All Tables'	Pass	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Assign Policies Unassigned: 10 Passed: 0 Blocked: 0 Blocked: 0 Blocked: 0 Inew Novelty Policy.
Unassigned In on Distribution Unassigned etly Polcy Rules Novethy rules that use Match Air Tables'	Pass	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Assign Policies Unassigned: 10 Passed: 0 Warned: 0 Biocked: 0 Biocked: 0 Biocked: 0
Unassigned In on Distribution Unassigned Unassigned Verty Policy Rules Novelty rules that use Match All Tables' Novelty rules that use Match All Tables'	Pass	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Assign Policies Unassigned: 10 Pased: 0 Warned: 0 Biocked: 0 Biocked: 0 New Novelty Policy.
Unassigned In on Distribution Unassigned Vinassigned Voveity rules that use 'Match All Tables' Noveity rules that use 'Match All Tables' ault Rule for Baseline Anomalies	Pass	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Lassign Policies Unassigned: 10 Pasaed: 0 Warned: 0 Biocked: 0 Biocked: 0 New Novelty Policy.
Unassigned In on Distribution Unassigned ethy Policy Rules Novelty rules that use Match Any Table Novelty rules that use Match All Tables' ault Rule for Baseline Anomalies	Pass	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Lassign Policies Unassigned: 10 Passed: 0 Biocked: 0 Biocked: 0 Mew Novelty Policy. Action: Unassig Threat: Unassig Logical Level: Unassig
Unassigned In on Distribution Unassigned Unassigned Unassigned Unassigned Novelty rules that use Match Air Tables Novelty rules that use Match Air Tables Novelty rules that use Match Air Tables fault Rule for Baselne Anomalies Anomaly Default Rule Default Rule	significant Minor	Moderate Ma	jor Catastrophic Block b	Moderate: 0 Major: 0 Linesigned: 10 Pasaed: 0 Warned: 0 Biodxed: 0 Biodxed: 0 Biodxed: 0 Action: Linesig Logging Level: Linesig Logging Level: Unasig
Unassigned In Unassigned Unassigned Unassigned Unassigned Velty Polcy Rules Novelty rules that use 'Match Any Table' Novelty rules that use 'Match All Tables' Fault Rule for Baseline Anomalies Fault Rule Faul	Pass	Moderate Ma	jor Catastrophic Catastrophic Block b	Moderate: 0 Major: 0 Lassign Policies Unassigned: 10 Passed: 0 Biocked: 0 Biocked: 0 New Navelty Policy. New Navelty Policy. Trreat: Unassig Logging Level: Unassig Logging Level: Unassig
Unassigned In on Distribution Unassigned etly Polcy Rules Novethy rules that use Match Any Tables Novethy rules that use Match All Tables' ault Rule for Baseline Anomalies ault Rule for Baseline Anomalies Unable Default Rule Cefault Rule	Pass	Moderate Ma	jor Catastrophic	Moderate: 0 Major: 0 Assign Policies Unassigned: 10 Passed: 0 Biocked: 0 Biocked: 0 New Novelty Poley. Action: Unassig Logging Level: Unassig Options

4. Navigate to the **Baseline** tab and click on the **select last\_name**, **first\_name from employees** statement. Select **Action** as **Block**, **Logging Level** as **Always**, and **Threat Severity** as **Major**, and change **Substitute Statement** to **select 1 from dual**, and then click on **OK**, as shown in the following screenshot:

\_\_\_\_20

#### - Appendix

mmary Detail	s Baseline p	roperties Ana	alysis Invalid SO											
lected Profile: I	Background.	Ordered by Id (	(asc).											
00346311														4
Î	Action 🔽	Logging 🔽	Threat 🗸	Stat	ement	Count	IpAddr	esses 🔻	Tables	~	Columns 🔽	Users 🔽	StatementType	✓ Client
653935213	Unassigned	Unassigned	Unassigned	select user from du	al		1 192.168.1.10	)	DUAL	_		hr	Data Manipulation Read On	ly sqlplus.ex
1110951003	🛕 Unassigned	Unassigned	Unassigned	select Cluster Pro	nerties					X	1	hr	Data Manipulation Read On	ly sqlplus.ex
1145983085	Unassigned	Unassigned	Unassigned	begin o							,	hr	Procedural	sqlplus.ex
1784145203	Unassigned	Unassigned	Unassigned	begin Statement:	select last_n	ame,first_name fro	m employees			~		hr	Procedural	sqlplus.ex
2750366510	C Unassigned	Unassigned	Unassigned	extrac								hr	Transaction	sqlplus.ex
3200346311	Unassigned	Unassigned	Unassigned	select						Ψ.	ST_NAME, LAS	hr	Data Manipulation Read On	ly sqiplus.ex
3310634856	Unassigned	Unassigned		select	atten Disale		-			_	RIBUTE, CHAP	nr	Data Manipulation Read On Data Manipulation Read On	iy sqipius.ex
3418778580		Unassigned		begin c	BIOCK	* after	1	staten	nents per minut	-	KIDUTE, CHAP	hr	Procedural	salplus.ex
3522986933	Unassigned	Unassigned		begin								hr	Procedural	cololus ex
				V Substit	ute Statement: Notes	select 1 from du	ual	_		4				
					OK	Cancel	Apply	) [ +	lelp					

5. Next, go back to main menu and click on **Assign Threat Severities**. At this point we are able to save the model and the policy.

tatement Class Distribution	nly 🔲 Data Manipulation 🚺	Data Definition 🔲 Data Cont	irol 📕 Procedural 🖬 Tran	saction Composite Contai	ning Transaction Composite	Data manipulatio (read only:) Data manipulatio Data definition: Data control: Procedural: Transaction:	
Unassigned ction Distribution	Insignificant	Minor	Moderate	Major	Catastrophic	Unassigned: 9 Insignificant: 0 Minor: 0 Moderate: 0 Major: 1 Assigb Pr	Nicies
Unassigned	Pass		Warn	Bio	<u>ck</u>	Unassigned: 9 Passed: 0 Warned: 0 Blocked: 1	
Novelty Policy Rules Novelty rules that use 'Match A Novelty rules that use 'Match A	Any Table' All Tables'	*****	11.22 - Ann 18. M. S MAR - A. M. M.	******	11 11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Passed: 0 Blocked: 0 New Novelty	Policy

6. From the New menu, click on Save the model as test policy and Export policy as testpolicy.dna.



- Next we will proceed to upload the new policy in Oracle Database Firewall. Navigate to the **Monitoring** tab, in the **Policies** panel, and click on the **Upload** link. Select **testpolicy.dna** and click on **Save**.
- 8. Navigate to Enforcement Points and click on the List link. HACKDB\_ORCL\_ENF will be listed, click on the Settings button. Next, from the Policies panel, select testpolicy.dna and click on Save to enforce the defined policies with OFA and ensure that in the Appliance Mode, Database Policy Enforcement (DPE) is checked (in DAM mode only monitoring is performed, no reactive measure are applied such as statement blocking). This is shown in the following screenshot:

Enforcement Points:	Monitoring Setti	ngs	
List			
Create	Protected Database	Oracle - HACKDB_ORC	CL ▼
Tasks	Traffic Sources:		
Protected Databases:	Traine Sources.	Enable Network In	terface
List		V Networ	rk 0
Create			
Policies:	Database	Activate Database R	esponse Monitorina
List	Response:		
Upload	Database Interrogation:	Activate Database In	terrogation
	Remote Monitor:	CACTIVATE Remote Mor	nitor
	Local Monitor:	Activate Local Monit	lor
	SPA:	Activate Stored Proc	edure Auditing
	URA:	Activate User Role A	uditing
	Appliance Mode:	● Database Policy Enfo ○ Database Activity Mo	orcement (DPE) onitoring (DAM)
	Policy:	Oracle	
		Name	Description
		logall-nomask.dna	Log all statements for offline analysis without masking data (Note: if this policy is applied, it can use sig
		logall.dna	Log all statements for offline analysis (Note: if this policy is applied, it can use significant amounts of sto
		logsample.dna	Log a sample of statements for offline analysis (Note: if this policy is applied, although it will store less s
		🔘 passall.dna	Pass all statements
		policy1.dna	
Advantation of the state of the state		estpolicy.dna	

9. Now the enforcement point will be reconfigured and the current monitored connection will be dropped.





23 –

10. Reconnect to the HACKDB database and reissue **select last\_name**, **first\_name from employees** to verify that the current policy is blocking the statement, shown as follows:



11. Navigate to the Oracle Database Firewall console's main page. The following screenshot shows the blocked statement listed:

ruoio Butubase i liewa		
Threat Status: OK	Throughput Status: OK	Traffic Snapshot at 2012-06-19 22:26
Known Blocked: Unseen Blocked: Known Warned: Unseen Warned:	2 Statement Rate: 0 Total Statements: 21 (In Last Hour)	Filter (no filter active) Warned and blocked statements 2012-06-19 18:26:59 - 2012-06-19 21:26:59
Quick Start		13
( Monitor datab	ases 🔹 System settings	00 103 1942 195 304 303 305
Top Ten Threats (Last We	ek)	Throughput [statements/sec] 2012-06-19 18:27:02 - 2012-06-19 21:27:02
Count     Status     Statement       2     A     select Mgt name	Seen         Log Level         Source         Destination           .f         yes         always         192.168.1.10         192.168.1.90	u
Enforcement Points		43 <b>0</b> 113 <sup>1</sup> 1440 1449 2013 2031 213 <sup>1</sup>
Name	Appliance IP Address	Number of statements [statements/second] 2012-06-19 18:27:02 - 2012-06-19 21:27:02
HACKDB_ORCL_ENF	Local 127.0.0.1	19
		HI
		Most blocked clusters (last hour)

# **Oracle Audit Vault**

Oracle Vault addresses the problem of centralization, separation, and protection of audit trails and provides real-time alerting and reporting capabilities. As we mentioned in *Chapter 8, Tracking and Analysis – Database Auditing,* it is imperative to collect audit information in a location where it cannot be tampered with.

Audit Vault has heterogeneous database support. In addition to Oracle, Audit Vault offers the ability to collect audit data from DB2, MS SQL, and Sybase. It's good to know that Oracle Audit Vault does not implement or alter audit procedures on the database. It is solely based on traditional methods of defining the methods by using the standard audit and fine grained auditing.

The Audit Vault database used is architecturally designed to be a warehouse. In a large organization that has a need to audit many databases, the audit data volume generated can be significant and the Audit Vault database must be able to handle the volume of data being generated. It is therefore important to install Oracle Audit Vault on a dedicated powerful server. On the other hand AV offers a variety of reporting methods. Since the audit information must be protected, the Audit Vault database is configured with the Oracle Database Vault product.

The Audit Vault environment consists of an audit server, audit agents, and collectors.

## Installation and configuration

The following steps will present how to install and perform an initial configuration of AV:

 Launch the installer and select the Create and configure Audit Vault option and click on Next, as shown in the following screenshot:

ý Í	Configure Security Updates	Select any of the following installation options. <ul> <li>Greate and configure Oracle Audit Vault</li> </ul>
	Installation Type	Install Oracle Audit Vault software only
Ý	Basic Installation	
þ	Prerequisite Checks	
ģ	Summary	
ģ	Install Product	
9	Finish	

2. Navigate to **Audit Vault Details**, and you will have to configure the audit vault administrator, audit vault auditor, oracle vault owner, and account manager usernames and credentials.

Configure Security Updates	Enter the Administrato Vault Auditor user to p	r user name and password provide separation of dutie	l. You can optionally choo s between account and au	se to create a separate Audit dit management.
Installation Option	A <u>u</u> dit Vault Admin	avadmin		
Grid Installation Options	Password	*****	<u>C</u> onfirm Password	******
Product Languages	✓ Cr <u>e</u> ate a Separate A	udit Vault Auditor		
Installation Location	Audit <u>V</u> ault Auditor	avaudit		
Audit Vault Details	Password		Confirm Password	******
Memory Options Management Options	Enter the Database Vau separate Database Vau policy management.	uit Owner user name and p ilt Account Manager to pro	assword. You can optiona vide separation of duties	Ily choose to create a between account and security
Database Storage	Database Vault <u>O</u> wner	dvowner		
Backup and Recovery	Pa <u>s</u> sword	*****	Conf <u>i</u> rm Password	*****
Schema Passwords	🗸 Crea <u>t</u> e a Separate D	atabase Vault Account Mar	nager	
Operating System Groups	Account <u>M</u> anager	dvacctmgr		
Summary	Pass <u>w</u> ord	*****	 Confi <u>r</u> m Passwor@	*******
Install Product				
Einish				

3. When at **Management Options**, depending on your local configuration, you can select **Use an existing Oracle Enterprise Management Grid Control for database management** or **Use Oracle Enterprise Manager Database Control for database management**.

A Installation Option	You can use Oracle Enterprise Manager 11g Grid Control to manage each Oracle Database 11g centrall or manage each database locally using Oracle Enterprise Manager 11g Database Control. For Grid
Installation Type	Control, specify the Oracle Management Service to manage your database.
Crid Installation Options	Select the management options for your instance.
Product Languages	
Installation Location	O Use an existing Oracle Enterprise Manager <u>G</u> rid Control for database management.
Audit Vault Details	
Database Identifiers	Management Service: No Agent found.
Memory Options	
Management Options	Use Oracle Enterprise Manager Database Control for database management
Database Storage	Se of alle Enterprise Manager Database control for database in anagement.
Backup and Recovery	
Schema Passwords	
Operating System Groups	
Prerequisite Checks	
J Summary	

- 26 -

4. Navigate through all the steps and finalize the installation:

Configure Security Updates	The installation of Oracle Audit Vault was successful.
Installation Option	Note:
Installation Type	Audit Vault 10.3.0.0.0 URL:
Grid Installation Options	https://oraaudva.1156/av
Product Languages	Enterprise Manager Database Control URL - (avdb) : https://oraaudva:1158/em
Installation Location	
Audit Vault Details	
Database Identifiers	
Memory Options	
Management Options	
Database Storage	
Backup and Recovery	
Schema Passwords	
Operating System Groups	
Prerequisite Checks	
Summary	
Install Product	
Finich	

## **Deploying and configuring agents and collectors**

In order to communicate with a Oracle Database Vault repository, a set of collectors, and an Oracle Audit Vault, an agent must be deployed on each host.

1. Copy the agent installation kit on each source database host. Launch the installer and configure the password, the port, and the connection string for the connection to the central repository.

Oracle	Audit Vault Agent Installation - Ag	gent Details 📃 🗶
Oracle Audit ' Agent Details	Vault Agent Installation	108
Each Audit Vault Agent i path for the location whe and the connect string fo	s identified by an unique Agent Name. Spec ere the Agent installation will take place, the or the Audit Vault Server.	ify the name of the Agent, the Agent user name and password,
Audit Vault Agent Name	avagnt	]
Audit <u>V</u> ault Agent Home	/u01/app/oracle/product/11.2.0/avagent	t Browse
Agent <u>U</u> ser Name:	avagnt	]
Agent User Password:	****	]
Audit Vault Server Con	nection Information:	
Connect String:	oraaudva:1521:avdb	(Hostname:Port:Service Name)
		Product Languages
Help	Back Next	(Install Cancel
ORACLE		

- 2. Complete the installation and proceed to configuration.
- 3. On a server host, define the agent for audit collection as follows:

[oracle@oraaudva Disk1]\$ avca add_agent -agentname avagn	t
-agenthost nodeorcl1	
Enter agent user name: avagnt	
Enter agent user password:	
Re-enter agent user password:	
Agent added successfully.	

28

- 4. On the client database, create a user av\_collector for audit trail collection and grant collector privileges as follows: SQL> create user av\_collector identified by "gY5+TY?z2\$5"; User created. SQL> SQL> @/u01/app/oracle/product/11.2.0/avagent/av/scripts/streams/ source/zarsspriv.sql av\_collector setup Granting privileges to AV COLLECTOR ... Done.
- 5. On the audit vault host, verify if the source database is enabled for the audit trail collection:

```
[oracle@oraaudva Disk1]$ avorcldb verify -src
nodeorcl1:1521:HACKDB -colltype ALL
Enter Source user name: av_collector
Enter Source password: gY5+TY?z2$
source HACKDB verified for OS File Audit Collector collector
source HACKDB verified for Aud$/FGA_LOG$ Audit Collector collector
parameter _JOB_QUEUE_INTERVAL is not set; recommended value is 1
parameter UNDO_RETENTION = 900 is not in recommended value range
[3600 - ANY_VALUE]
parameter GLOBAL_NAMES = false is not set to recommended value
true
```

 Perform corrections on the source database as instructed by the verification output: SQL> alter system set global\_names=true scope=both;

System altered.

SQL> alter system set undo\_retention=3600 scope=both;

System altered.

SQL> alter system set job\_queue\_interval=1 scope=spfile; System altered.



- 7. Perform a verification again as follows: [oracle@oraaudva Disk1]\$ avorcldb verify -src nodeorcl1:1521:HACKDB -colltype ALL Enter Source user name: av\_collector Enter Source password: source HACKDB verified for OS File Audit Collector collector source HACKDB verified for Aud\$/FGA\_LOG\$ Audit Collector collector source HACKDB verified for REDO Log Audit Collector collector [oracle@oraaudva Disk1]\$
- With this the source database is enabled for collection. Add a source database and a collection agent:

[oracle@oraaudva ~]\$ avorcldb add\_source -src 10.241.132.80:1521:HACKDB -desc HACKDB -srcname HACKDB\_SCHM -agentname avagnt Enter Source user name: av\_collector Enter Source password: Adding source... Source added successfully.

remember the following information for use in avctl Source name (srcname): HACKDB\_SCHM Credential stored successfully. Mapping Source to Agent...

9. If we plan to use OS audit trails then add a collector of type OSAUD as follows:

```
[oracle@oraaudva ~]$ avorcldb add_collector -srcname HACKDB_SCHM
-agentname avagnt -colltype OSAUD -orclhome /u01/app/oracle/
product/11.2.0/dbhome_1
source HACKDB_SCHM verified for OS File Audit Collector collector
Adding collector...
Collector added successfully.
remember the following information for use in avctl
```

```
Collector name (collname): OSAUD_Collector
[oracle@oraaudva ~]$
```

30

10. Add a database audit collector type as follows:

```
[oracle@oraaudva ~]$ avorcldb add_collector -srcname HACKDB_SCHM
-agentname avagnt -colltype DBAUD
source HACKDB_SCHM verified for Aud$/FGA_LOG$ Audit Collector
collector
Adding collector...
Collector added successfully.
```

```
remember the following information for use in avctl
Collector name (collname): DBAUD_Collector
[oracle@oraaudva ~]$
```

11. Add a redo collector as follows:

```
[oracle@nodeorcl1 av]$ /u01/app/oracle/product/11.2.0/avagent/bin/
avorcldb setup -srcname HACKDB_SCHM
Enter Source user name: av_collector
Enter Source password:
adding credentials for user av_collector for connection [SRCDB21]
Credential stored successfully.
updated tnsnames.ora with alias [SRCDB21] to source database
verifying SRCDB21 connection using wallet
```

12. Start the agent on the source database, as follows:

```
[oracle@nodeorcl1 av]$ /u01/app/oracle/product/11.2.0/avagent/bin/
avc
avca avctl
[oracle@nodeorcl1 av]$ /u01/app/oracle/product/11.2.0/avagent/bin/
avctl start_agent -agentname avagnt
Starting agent...
Agent started successfully.
[oracle@nodeorcl1 av]$
```

13. Start the collectors as follows:

```
[oracle@oraaudva ~]$ avctl start_collector -collname OSAUD_
Collector -srcname HACKDB_SCHM
Starting collector...
Collector started successfully.
```

31 -

```
[oracle@oraaudva ~]$ avctl start_collector -collname DBAUD_
Collector -srcname HACKDB_SCHM
Starting collector...
Collector started successfully.
[oracle@oraaudva ~]$
```

## Audit vault administration

In the following section we will summarize the main administrative tasks used with Audit Vault:

Open Audit Vault administration control and log in as the AV administrator (type the password set during installation):

• • • • • • • • •	https://oraaudva:1158/av/	console/logon/logon					
Most Visited 🔻 🗧 Enter	rise Linux 🧧 Linux Technology C.	🔄 Oracle University	🔁 Feature: Faster Linu	OSS from Oracle	🛧 ULN: Login	Oist. sources	S E-Delivery: Enterpr
ORACLE Enterprise Ma	nager 10g						
Login							
rogin							
ogin to Audit Vault							
	No. of Concession, Name	_					
User Name	avadmin	_					
- Password							
Connectives	(1v_00min +)	ogin )					
	-						
pyright © 1996, 2011, Oracle and	or its affiliates. All rights reserved. Oracle is a reg	stered trademark of Oracle Corpo	ration and/or its affiliates. Other name	s may be trademarks of their re	spective owners. Una	uthorized access is strict	ly prohibited.
pyright @ 1996, 2011, Oracle and	or its affiliates. All rights reserved. Oracle is a reg	istered trademark of Oracle Corpo	ration and/or its affiliates. Other name	s may be trademarks of their re	spective owners. Una	uthorized access is strict	ly prohibited.
ayright © 1996, 2011, Cracle and	or its affiliates. All rights reserved. Cracle is a reg	stered trademark of Oracle Corpo	ation and/or its affiliates. Other name	s may be trademarks of their re	spective owners. Una	uthorized access is strict	ly prohibited.
pyright @ 1996, 2011, Oracle and	or its affiliates. All rights reserved. Oracle is a reg	stered trademark of Oracle Corpo	ration and/or its affiliates. Other name	s may be trademarks of their re	spective owners. Una	uthorized access is strict	ly prohibited.
gyright & 1996, 2011, Gracle and	or its affiliates. All rights reserved. Cracle is a reg	stered trademark of Oracle Corpo	otion and/or its affiliates. Other name	s may be trademarks of their re	spective owners. Una	uthorized access is strict	y prohibited
gyright © 1996, 2011, Cracle and	or its afflixies. All rights reserved. Oxcle is a reg	stered trademark of Ciracle Corpo	otion and/or its affiliates. Other name	s may be trademarks of their re	spective owners. Una	uthorized access is strict	y prohibited
pyright © 1996, 2011, Cracle and	ir its affliktes. All rights reserved. Oncle is a reg	stered trademark of Ciracle Corpo	ntion and/or its affiliates. Other name	s may be trademarks of their re	spective owners. Una	uthorized access is strict	y prohibited.
pyright © 1996, 2011, Cracle and	ir its affliktes. All rights reserved. Oncle is a reg	atered teademark of Oracle Corpo	ntion and/or its effiliates. Other name	s may be trademarks of their re	spective owners. Unar	uthorized access is strict	y prohibited
pyright © 1996, 2011, Oracle and	ar its afflikeles. All rights reserved. Oracle is a reg	atered hodemark of Onatle Corpo	nton andie in affiliats. Oher name	s may be trademarks of their re	spective owners. Unar	uthorized access is strict	y probibilist
pyright © 1396, 2011, Oracle arv	or its affiliates. All rights reserved. Oracle is a reg	atend hodenosik of Oracle Corpo	inten ander in afflicers. Other name	s may be trademarks of their re	spective owners. Unar	uthorized acces is strict	y prohibited



Instead of using the command line prompt, you can manage collectors from the **Management** tab and within that **Collectors**, as shown in the following screenshot:

The second seco	sce/avt/AVManagement?tamet_avdb&type_oracle_database	
	serverenangement target av ubatype oracle_uatabase	
Most Visited 🔻 🧧Enterprise Linux 🧧 Linux Technology C 🧧 Oracle U	Jniversity 🥃 Feature: Faster Linu 🔞 OSS from Oracle 🔮 ULN:	: Login Olist sources E-Delivery: En
Audit Vault		
Collectors   Audit Errors   Warehouse		
Database Instance: avth >		
Collectors		
① Information		
The collector, HACKDB_SCHM:DBAUD_Collector, has been started successf	ulty.	
(Pad)(Pad)		
(star) (stop)		
Select Collector	Agent	Audit Source
DBAUD_Collector	avagnt	HACKDB_SCHM
O OSAUD Collector	avagnt	HACKDB_SCHM
		HACKDB SCHM
O REDO Collector	avagnt	

# **Creating additional audit policies**

Audit Vault has the capability to generate scripts for different audit statements which can be applied later on to the source database:

1. Log in as the Audit owner **avaudit**, as shown in the following screenshot:

	Rookurauka Tooia Helb
• • • • • ⊙ •	🏠 🔟 https://oraaudva.1158/av/console/logon/logon
Most Visited • Enter	prise Linux 🧧 Linux Technology C 🧧 Oracle University 🚍 Feature: Faster Linu 💿 OSS from Oracle 🔶 ULN: Login 💿 Dist. sources 💿 E-Delivery: Enterpri
DRACLE Enterprise Ma	snagor 10g
Login	
ogin to Audit vault	
s Hear Name	
* Deseured	
Connect As	
Connectives	(Login)
pyright @ 1996, 2011, Oracle and	size its affiliates. All rights reserved. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Unauthorized access is strictly prohibited.



2. Navigate to the Audit policy tab. The overview page will show you what type of auditing and how many objects or statements are audited:

Audit 9	Settings   Alerts				
Database	Instance: avdb > Audit Settir	ngs >			
НАСКЕ	B SCHM				
Ov	erview Statement C	Object Privilege	FGA	Capture Rule	
Save A	udit Settings				
You ca	in save your work by clickin	ng on the Save All A	udit Settings	s button below. Please note, saving your work does not automatically apply these s	settings to the source database.
			0	Sa	ve All Audit Settings
Apply A	Audit Settings				
You ca	in verify that the audit setting	gs can be successful	ly applied to	o a given source by clicking on Verify. If the DBA for the source has provided you	an account on the source, you can
changes	to a SQL script that you ca	in give the DBA, who	can then a	pply the settings for you.	
Select A	Select None				
Select	Audit Settings Type			In Use	
	Statement			10	
	Object			11	
	Privilege			26	
	FGA			0	
	Capture Rule			0	
	Vorify Export of	Audit Sou	ce User Na	me Provision	
	(Verily) (Export a:	s SQL	Iroo Docour		
		- Addit 30	IICE Passwo		
Conv	udit Settings from Ano	ther Source			
Сору А	n guidht replicate oudit so	tings from one data	one to the	source database to cood it with common cudit estings. You either con use estings	that are already in use in the date
Touca	O A CONTRACTOR AUGILISE	angs nom one data	ase to the :	source database to seed it with continion addit settings. Fou either can use settings	that are already in use in the data
Copy	🔾 Actual (In Use) 🔍 Nee	eaea (Not Yet In Use	) Audit Setti	ngs	
From		Load	)		

 Next navigate to Statements and click on the Create button. The Create Object Audit page will open, then check SELECT in the statement box, select the Object Type as TABLE, Object as HR.DEPARTMENTS, Statement Execution Condition as Both and DML Audit Granularity as SESSION, as shown in the following screenshot:

					mozilla Pire	TOX:	
ile Edit View History Bookr	narks <u>T</u> ools <u>H</u> elp						
🗢 🗣 • 🕲 🙆 🚺	6 https://oraaudva:1158/av/co	nsole/database/avt/AV/	AuditPolicy?target=avdb&t	ype=oracle_database			
Most Visited 👻 🖻 Enterprise L	Jinux 🖲 Linux Technology C	Cracle University	🔁 Feature: Faster Linu	OSS from Oracle	⊕ ULN: Login	Dist. sources	C-Delivery: Enter
DRACLE Enterprise Manager	10g						
Audit Settings   Alerts							
atabase Instance: avdb > Audit Set Create Object Audit	tinas >						
* Statements	SELECT						
Object Type	TABLE						
Object	HR.DEPARTMENTS						
	Roth +						
<ul> <li>Statement Execution Condition</li> </ul>	Court •						
Statement Execution Condition     * DML Audit Granularity	Session \$						

\_\_\_\_34 \_\_

4. Next, we will create a capture rule. Navigate to the **Capture Rule** and set **Capture Rule** to **Table**, set **Table** to **HR.HR\_EMP\_DETAIL\_AUD**, **Capture** to **Both**, and then click on **OK**, as shown in the following screenshot:

<b>U</b>							Mozilla Firef	ох	
<u>F</u> ile <u>E</u> dit <u>V</u> iew	Hi <u>s</u> tory <u>B</u> ool	kmarks <u>T</u> ools <u>H</u>	elp						
\$ ⇒ • €	🏫 🖸 🔇	🚺 https://oraau	dva:1158/av/co	nsole/database/avt/A	/AuditPolicy?target=avdb&t	ype=oracle_database	#		
🛅 Most Visited ▼	Enterprise	Linux 🧧 Linux 1	echnology C	Oracle University	E Feature: Faster Linu	OSS from Oracle	🛧 ULN: Login	Oist. sources	E-Delivery:
ORACLE En Audit Vault	terprise Manago	er 10 <i>g</i>							
Audit Settings	s   Alerts								
Database Instance Create Captu	<u>avdb</u> > <u>AuditS</u> Jre Rule	iettings >							
* Capture Ri * Tat * Captu	ule  Table	Schema GI CDETAILS_AUD DML ® Both	obal		<b>X</b>				
Copyright © 1996, 20	11, Oracle and/or its	affiliates. All rights reserv	ved. Oracle is a registe	red trademark of Oracle Corpo	ration and/or its affiliates. Other name	Home   Audit Rep as may be trademarks of their re	orts   <u>Audit Polic</u> spective owners. Una	cy   <u>Settings</u>   <u>He</u> uthorized access is strict	elp   Logout ly prohibited.
					**************************************				

5. To generate the provisioning script, navigate to the **Overview** tab and click on the **Save All Audit Settings** button, as shown in the following screenshot:

e	Mozilia Firefox
Ele Edit View History Bookmarks Tools Help	
💠 🔅 🕏 🔞 💽 https://oraaudva:1158/av/console/database/avt/AVAuditPolicy?target=avdb&type=oracle_database	
📷 Most Visited 🔻 💽 Enterprise Linux 💽 Linux Technology C 💿 Oracle University 💽 Feature: Faster Linu 🐻 OSS from Oracle	💠 ULN: Login 🛛 🗑 Dist. sources
ORACLE: Enterprise Manager 10g	
Audit Settings   Alerts	
Database Instance: avdb > Audit Settings >	
( ) Information	
The policy has been saved successfully.	
Overview Statement Object Privilege FGA Capture Rule	
Save Audit Settings You can save your work by clicking on the Save All Audit Settings button below. Please note, saving your work does not automatically apply the	ese settings to the source database (Save All Audit Settings)

35 —

6. A script will be generated; select the last two statements and run it on the source database:



## **Using Audit Vault reports**

Audit Vault provides us with the possibility of creating different types of built-in or customized reports, as we will see in the following section.

1. Navigate to the **Audit Reports** tab, as shown in the following screenshot:



- 36

2. To summarize the audit data collected, go to **Activity Overview**. This is an unsorted list of audit events that are captured. This is illustrated in the following screenshot:

								кер	orts - Mozilia	Firer
e <u>E</u> dit	View	Hi <u>s</u> tory	<u>B</u> ookmarks <u>T</u> oo	ls <u>H</u> elp						
•	- 🕅	2	ittps://	oraaudva:5707/av/cons	ole/f?p=7700:15	:2685972581566074:	:::RPT_ID	74167056010678958	}	
Most V	′isited ▼	Ente	rprise Linux 🧧 L	inux Technology C 🤇	Oracle Univers	sity 🧧 Feature: Faste	r Linu	OSS from Oracle	💠 ULN: Login	o Di
			40							
idit Va	ult	erprise m	anager iug							
Default	Reports	Complia	nce Reports   Custo	m Reports   Generated Re	ports   Report Sch	edules   Entitlement Sn	apshots			
Activ	ity Ove	erview								
	-			D	60 20	Create PDF				
P.				Rows		Create PDF				
Ξ 🦷	Event 1	Fime is in	the last 24 hours	🗹 📡						
	<u>So</u> 1	<u>irce</u>	<u>Category</u>	<u>Event</u>	<u>User</u>	<u>Target</u>	<u>Host</u>	<u>Event Time</u> 🔫		
	HACKD	B_SCHM	DATA ACCESS	SELECT	HR	EMPLOYEES	nodeorci1	6/16/2012 1:48:01 PM		
	HACKD	B_SCHM	DATA ACCESS	SELECT	HR	EMPLOYEES	nodeorcl1	6/16/2012 1:47:39 PM		
	HACKD	B_SCHM	USER SESSION	LOGON	HR		nodeorcl1	6/16/2012 1:47:04 PM		
	HACKD	B_SCHM	DATA ACCESS	SELECT	HR	EMPLOYEES	nodeorcl1	6/16/2012 1:46:17 PM		
	HACKD	B_SCHM	USER SESSION	LOGON	HR		nodeorcl1	6/16/2012 1:46:04 PM		
	HACKD	B_SCHM	USER SESSION	SUPER USER LOGON	1			6/16/2012 1:44:39 PM		
	HACKD	B_SCHM	USER SESSION	LOGON	AV_COLLECTOR		nodeorcl1	6/16/2012 1:28:53 PM		
	HACKD	B_SCHM	USER SESSION	LOGON	AV_COLLECTOR		nodeorcl1	6/16/2012 1:28:37 PM		
	HACKD	B_SCHM	USER SESSION	LOGOFF	SMAVRIS		nodeorcl1	6/16/2012 1:23:15 PM		
	HACKD	B_SCHM	OBJECT MANAGEME	INT ALTER TABLE	SMAVRIS	HR_EMP_DETAILS_AUD	nodeorcl1	6/16/2012 1:21:11 PM		
	HACKD	B_SCHM	USER SESSION	LOGON	SMAVRIS		nodeorci1	6/16/2012 1:20:35 PM		
	HACKD	B_SCHM	USER SESSION	LOGOFF	DRAPHEAL		nodeorcl1	6/16/2012 1:20:35 PM		
	HACKD	B_SCHM	OBJECT MANAGEME	INT ALTER TABLE	DRAPHEAL	HR_EMP_DETAILS_AUD	nodeorcl1	6/16/2012 1:20:19 PM		
	HACKD	B_SCHM	OBJECT MANAGEME	INT ALTER TABLE	DRAPHEAL	HR_EMP_DETAILS_AUD	nodeorcl1	6/16/2012 1:18:54 PM		
	HACKD	B_SCHM	USER SESSION	LOGON	DRAPHEAL		nodeorci1	6/16/2012 1:18:43 PM		

You also have the ability to perform compliance reporting. In Audit Vault you have built-in reports for **Credit Card**, **Financial**, and **Health** compliance reports.





# Defining an alert rule

To create an altering condition, navigate to the Audit policy tab and click on **Create Alert Rule**. In this example we will create an alert rule named **delete\_table**. Select the severity level to be **Warning**, **Audit Source Type** to be **HACKDB\_SCH**, **Audit Event Category** to be **DATA ACCESS**. **User** should be set to **HR**, **Table** to **HR.HR\_EMP\_DETAILS\_AUD**, and **Audit Event** to **DELETE**.

File Edit View History Bookmarks Tools Help
4 → . 6 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
📷 Most Visited 🔻 💽 Enterprise Linux 🧧 Linux Technology C 😨 Oracle University 🧧 Feature: Faster Linu 💿 OSS from Oracle 🖓 ULN: Login 💿 Dist. soc
Create Alert Rule
Alert delete_table
Description
0 of 2000 * Alert Severity Warning
* Audit Source Type ORCLDB
Audit Source HACKDB_SCHM
Audit Event Category DATA ACCESS
Specify additional alert conditions in 💿 Basic 🔿 Advanced
Desis Mart Canditian
Dasite Areit Contention Specify when an alert should be raised.
Audit Event DELE IE
Audit Event status
Alert Action
When an alert is raised, take the following actions.
Notification
Template Afert Notification Template      Profile notifications
To alert@orcl1.com Cc Add to List
<u>Profile Name To Cc Template Name</u>
Trouble Ticket Action
* Template 📴 NO Template
Dana

- 38 -