设置 FortiDB 审计与监控

说明：

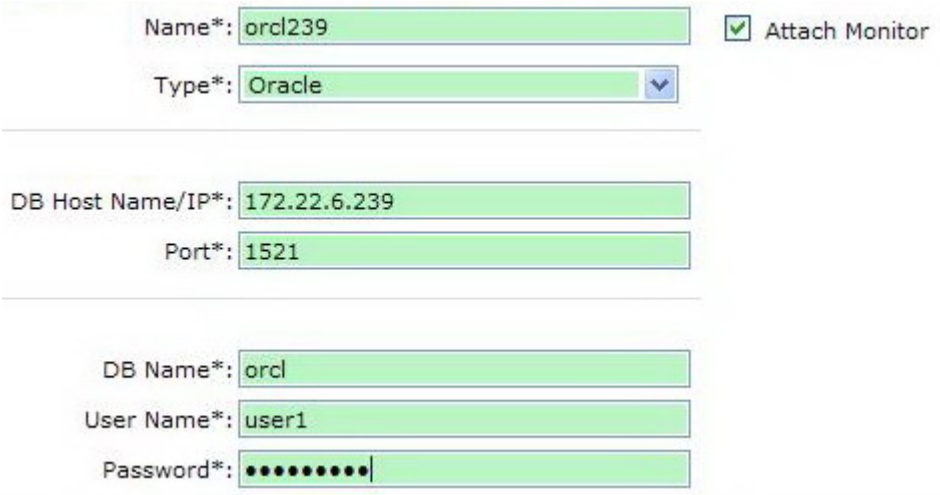
本文档针对 FortiDB 审计与监控配置进行说明。FortiDB 可以对登陆到数据库的用户行为进行 100%记录，并对违反规则的动作产生告警，告警信息基于四个 W（谁、在哪里、在何时、做了什么）原则呈现。FortiDB 还可以把告警信息生成审计报告，从而帮助数据库管理员实现对数据库的审计功能。

环境介绍：

本文使用 FortiDB1000B 做演示。本文使用的系统版本为 4.0。本文以 Oracle 10g 为例说明漏扫过程。

步骤一：配置目标数据库

在左侧菜单 Target Management—Targets 中点击 Add 按钮，填写目标数据库信息



勾选 Attach Monitor 启用审计功能

Name：目标数据库名称，自定义一个名称

Type：数据库类型，本例为 Oracle

DB Host Name/IP：目标数据库 IP 地址，本例为 172.22.6.239

Port：目标数据库端口，默认是 1521

DB Name：数据库实例名，一个数据库软件可以开多个实例，FortiDB 认为一个实例就是一个目标数据库

User Name：连接到目标数据库的用户名

Password：连接到目标数据库的密码

以上信息可以让数据库管理员协助完成。

点击左下角的 Test Connection 按钮测试连接。在左上角出现 • Success 表明连接正确，否则会出现红色报错信息。点击右下角的 Save 按钮保存信息。

步骤二：配置审计策略

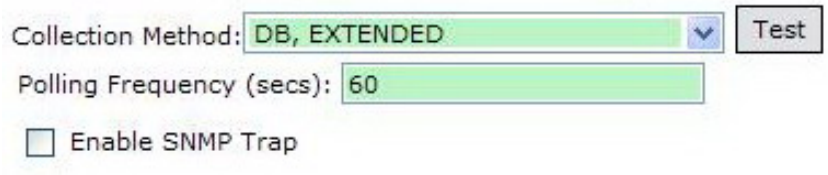
在 MA Policy Management—Policies 中选中所有策略

点击下面的 Enable 按钮启用策略，然后到第二页重复上述操作。

注：出厂配置时审计的所有预定义策略都是关闭的，需将其全部启用，以后就可以直接使用了。

步骤三：执行数据库审计

在 Data Activity Monitoring—Monitors 中点击目标数据库名称 orcl239



Collection Method：取得数据方法，选择 DB,EXTENDED。

Polling Frequency：取得数据的时间间隔，默认 60 秒

点击 Test 按钮测试目标数据库的审计功能是否开通。在左上角出现 • Success 表明审计开通，否则会出现红色报错信息。点击右下角的 Save 按钮保存信息。

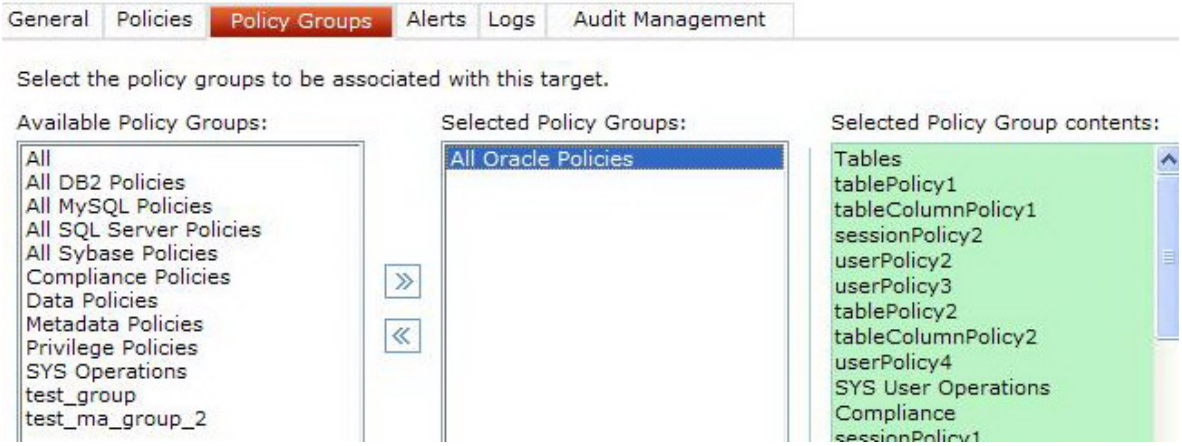
如何开启数据库审计和 FortiDB 连接到数据库的账户权限说明：

本步骤需要数据库管理员协助完成，在 FortiDB 管理员手册中有详细说明，参见

http://docs.fortinet.com/fdb/fortidb-user-guide.pdf

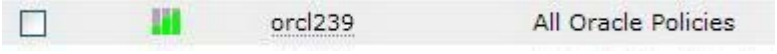
在手册的 Target Management—Required Settings for Monitoring Target Database 目录下，从 66 页到 82 页，有详细介绍。

在 Data Activity Monitoring—Monitors 中点击目标数据库名称 orcl239。点击 Policy Groups 按钮，从 Available Policy Groups 中选择 All Oracle Policies，将它移动到 Selected Policy Groups 中，点击右下角的 Save 按钮保存信息。



在 Data Activity Monitoring—Monitors 中勾选目标数据库 orcl239，点击下面的 Start Monitoring 按钮开始审计，

审计开始后小图标会变成绿色，如下图



步骤四：查看审计告警

在 Data Activity Monitoring—Monitors 中点击目标数据库名称 orcl239。在 Alerts 菜单中可以看到告警日志

测试：本例测试 FortiDB 预定义的表监控功能。

表监控：监控用户对表的增加、删除和修改（重命名，增加或删除列）操作并产生告警。

测试时 SGATEST 用户在 DALIAN2 表中增加了一列 COLUMN2，下面是 FortiDB 监控到的告警：

Alert ID:	7773
Target Name:	orcl239
Policy Name:	Tables
Rule Violations:	Metadata Activity checked: Create Table, Alter Table, Drop Table
Severity:	MIN
Action:	Alter Table
OS User:	dalian
DB User:	SGATEST
Login Name:	SGATEST
Object:	orcl.SGATEST.DALIAN2
Return Code:	0
SQL Statement:	ALTER TABLE DALIAN2 ADD ("COLUMN2" NUMBER)
Location:	computer Terminal: UNKNOWN
Timestamp:	2010.04.13 - 15:49:22.247
Application:	Not available

步骤五：导出审计报告

在 Report Management—Pre-Defined MA Reports 中可以看到审计报告。

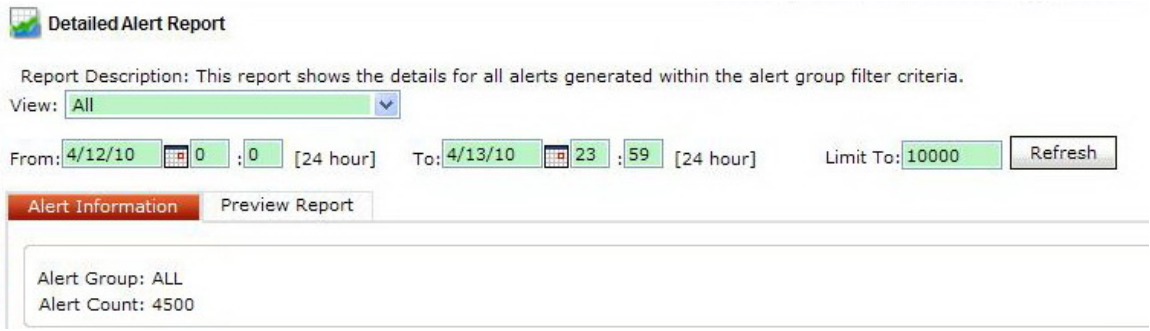
FortiDB 预定义了一些报告内容：

Detailed：给出所有违反审计规则的告警信息详细描述

Summary：给出所有违反审计规则的告警信息汇总描述

Statistical：给出所有违反审计规则的告警状态信息汇总描述

点击 Detailed，可以看到所有告警的个数，本例为 4500



点击 Preview Report 按钮查看详细信息

下面点击 Export 可以导出报告，支持的格式为 PDF，Excel，Tab，CSV

报告样例

下面是导出的审计报告部分信息

Database:orcl
Host:172.22.6.239

ID	Severity	Policy Name	Object	Timestamp	Description	
7775	MIN	Tables	orcl.SGATEST.DALIAN3	2010.04.13 - 16:03:23.595	OS User	dalian
					DB User	SGATEST
					Login Nm	SGATEST
					Grantee	
					Err Code	0
					Location	computer Terminal: UNKNOWN
					Application	Not available
					Rule Violations	Metadata Activity checked: Create Table, Alter Table, Drop Table
					SQL Statement	ALTER TABLE DALIAN3 RENAME TO DALIAN2
7774	MIN	Tables	orcl.SGATEST.DALIAN2	2010.04.13 - 15:57:54.278	OS User	dalian
					DB User	SGATEST
					Login Nm	SGATEST
					Grantee	
					Err Code	0
					Location	computer Terminal: UNKNOWN
					Application	Not available
					Rule Violations	Metadata Activity checked: Create Table, Alter Table, Drop Table
					SQL Statement	ALTER TABLE DALIAN2 RENAME TO DALIAN3

Database:orcl
Host:172.22.6.239

ID	Status	Severity	Policy	Action	Rule Violations	Timestamp
7775		MIN	Tables	Alter Table	Metadata Activity checked: Create Table, Alter Table, Drop Table	2010.04.13 - 16:03:23.595
7774		MIN	Tables	Alter Table	Metadata Activity checked: Create Table, Alter Table, Drop Table	2010.04.13 - 15:57:54.278
7773		MIN	Tables	Alter Table	Metadata Activity checked: Create Table, Alter Table, Drop Table	2010.04.13 - 15:56:52.143
7772		MIN	Tables	Create Table	Metadata Activity checked: Create Table, Alter Table, Drop Table	2010.04.13 - 15:54:47.996
7771		INF	tablePolicy1	Select	Suspicious Database User: SGATEST, Suspicious Location: computer	2010.04.13 - 15:49:39.890
7770		INF	tablePolicy1	Select	Suspicious Database User: SGATEST, Suspicious Location: computer	2010.04.13 - 15:49:39.888
7769		INF	tablePolicy1	Select	Suspicious Database User: SGATEST, Suspicious Location: computer	2010.04.13 - 15:49:39.888