



# SQL安全审计

## - PostgreSQL hook实践

金华峰@莲子数据

Email: [aida@lotuseed.com](mailto:aida@lotuseed.com)

# 数据库安全审计现状



# 数据库安全审计现状

- 数据库安全审计系统
  - 主要用于**监视**并记录对**数据库服务器**的各类操作行为，通过对**网络数据**的分析，实时地、智能地解析对数据库服务器的各种操作，并记入审计数据库中以便日后进行查询、分析、过滤，实现对目标**数据库系统**的用户操作的监控和审计。
- 数据库审计产品
  - Imperva
  - Guardium
  - ...



# SQL安全审计

- 以PostgreSQL扩展形式存在:

```
CREATE EXTENSION safe_audit;
```

扩建好扩展即可使用!

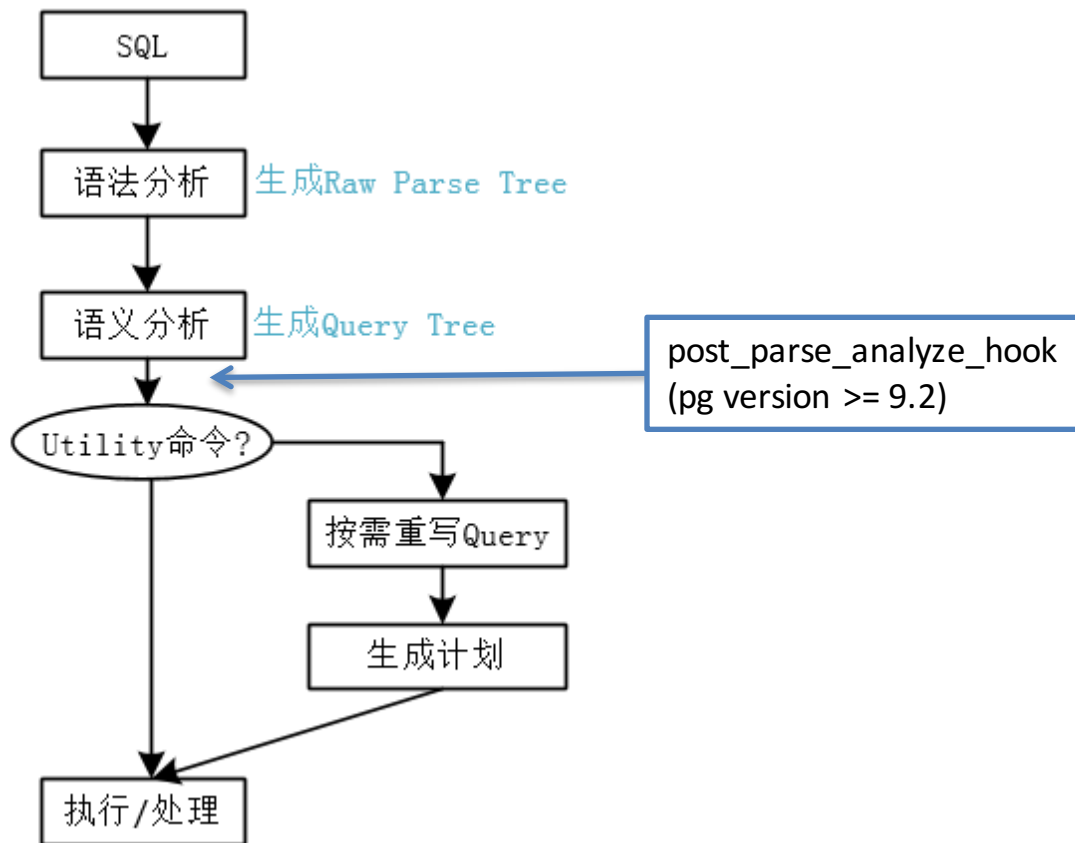
默认模式: lotus;

包含对象:几个审计表以及提供的相关操作函数等等。

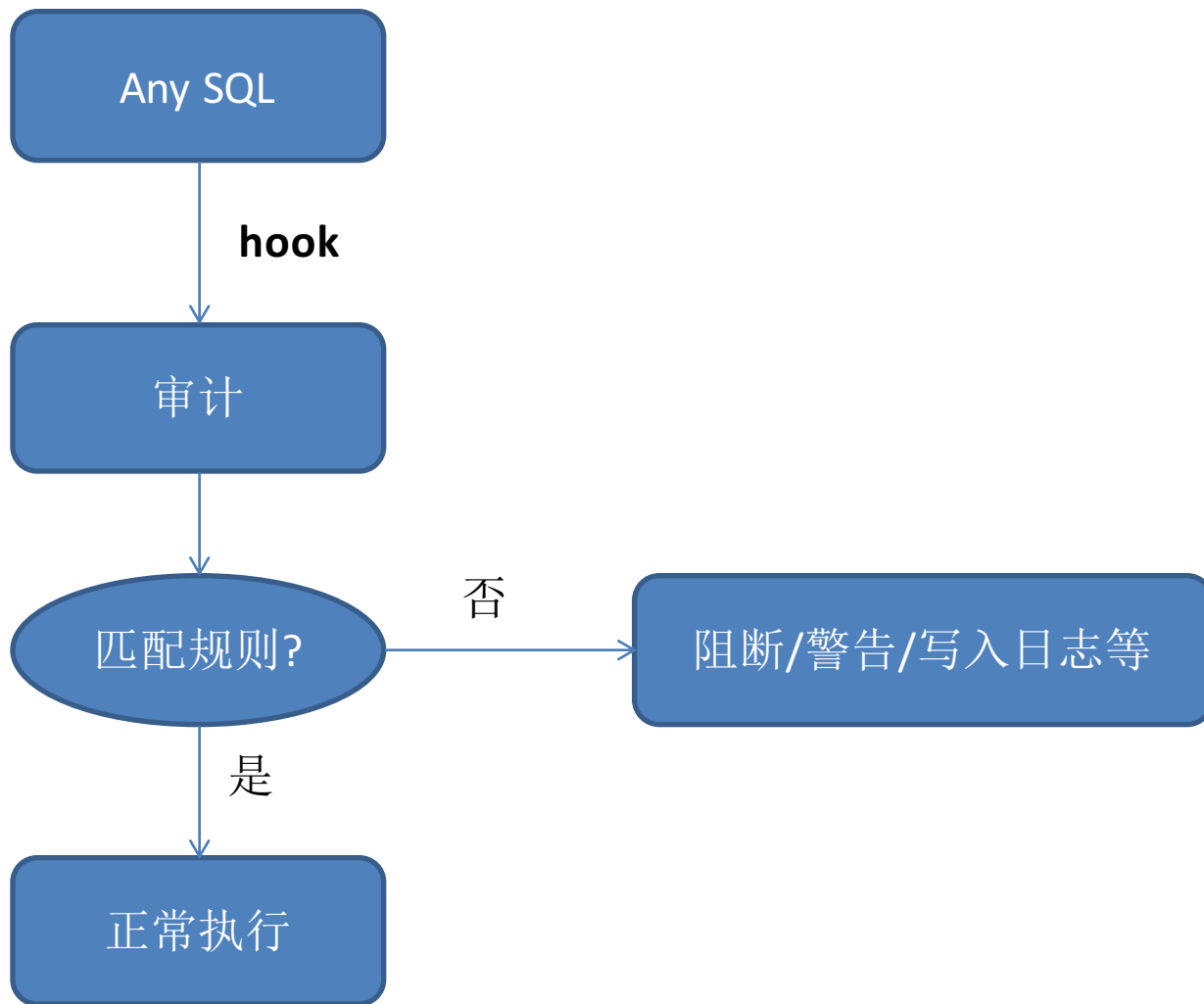
- 高效、不错漏



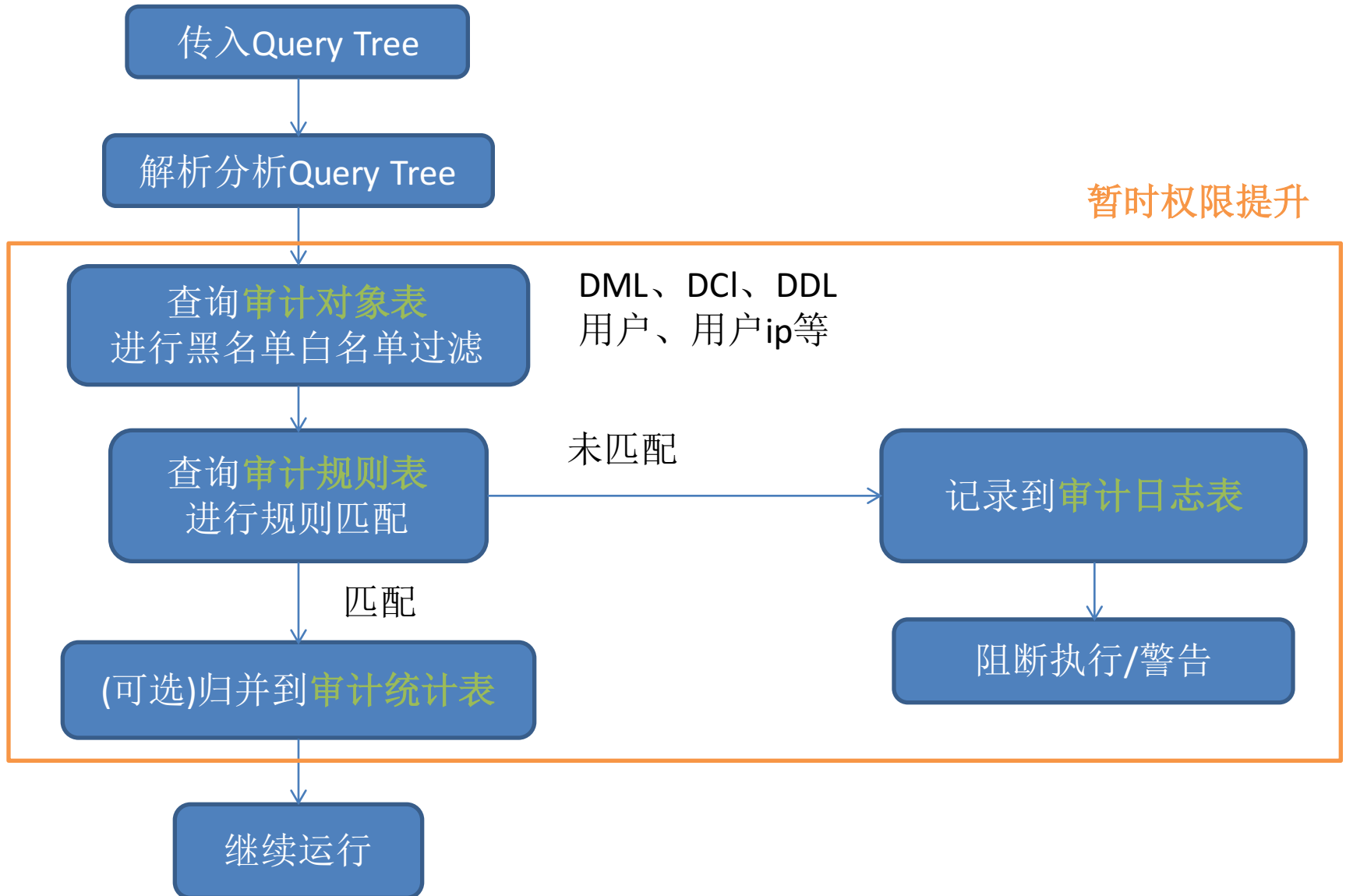
# SQL一般处理流程



# 大致总流程



# 审计流程



# 规则的产生

## 审计对象表:

由管理员/审计人员手动设置要审计/排除的语句类型, 审计/排除的用户, 源ip等。

## 审计规则表:

1. 安装扩展时, 默认会插入一些必要的和额外的规则。
2. 在审计写模式状态(全局/session)时, 由所有输入的SQL产生。
3. 管理员手动插入规则。
4. 管理员批量导入规则(之后需刷新规则)。





# 控制审计状态

1. postgresql.conf中控制全局审计状态，如审计开关。
2. 数据库级：
  - 如：ALTER DATABASE xxx SET safe\_audit.enable TO ON;
3. 用户级：
  - 如：ALTER USER xxx SET safe\_audit.enable TO ON;
4. 临时：
  - 在一个session或连接中临时设置审计状态。



# 审计规则

- 审计规则可分等级

等级1 - 最严格，输入的就是唯一允许的

规则源	<code>select 1+1;</code>
不允许	<code>select 1+2;</code>

等级2 - 值无关

规则源	<code>select * from t where id &gt; 1 AND id &lt; 100;</code>
允许	<code>select * from t where id &gt; 50 AND id &lt; 500;</code>
不允许	<code>select * from t where id &gt; 50;</code>
不允许	<code>select * from t2 where id &gt; 1 AND id &lt; 100;</code>

可细分：操作符无关、顺序无关等



# 审计规则

- 审计规则可分等级

等级3 - 对象无关

OID无关

字段名无关

表名无关

...

.....

根据需要，可定制审计规则来将等级不断细分。



# 审计规则表结构

- 分析Query Tree，提取必要元数据信息，产生一个顺序无关、规则等级无关的Audit String。
- 保存由Query Tree缩减变换过来的Query String， Audit String、元数据信息、**当前规则等级**。并根据Audit String做哈希，取部分哈希值作为索引字段(id)。规则表根据需要附加额外的字段，如规则插入时间、插入者、enable状态，一些额外标志(编码/压缩方法、是否哈希碰撞)等等。

id(索引)	元数据	标志	query string	audit string	enable	规则等级	原始SQL	.....
--------	-----	----	--------------	--------------	--------	------	-------	-------



# 审计规则表结构

- 进行规则匹配时，由当前的Query Tree产生Audit String，取其哈希值索引查询审计规则表。

1. 未查询到 -> 阻断/警告/记录

2. 查询到 -> 根据元数据信息判断是否匹配规则

无法直接判断 -> 根据元数据信息、当前的以及记录里存储的Query String、规则当前等级生成它们的Rule String，比较Rule String看是否匹配。

若匹配 -> 做匹配后操作。

若不匹配 -> 阻断/警告/记录



# 审计统计表

- 用于统计已匹配的规则，如记录匹配次数、最新匹配时间、最新匹配用户/IP、最新匹配原始查询等等。
- 由于PostgreSQL的MVCC特性，频繁地更新可能会导致审计效率降低，审计统计表大小膨胀。
  - 安全审计提供选项允许：  
尽可能 **Update In Place**.  
这将打破MVCC特性，但对审计表来说是允许的!



# 其他

- 丰富的函数用于导入/导出/备份/恢复、验证、重写审计表。
- 分析审计统计表、日志表给出分析报告。
- 可分割审计多条SQL和函数内部SQL。





产品系列: 移动app数据分析系统  
产品系列: LotuseeData大数据平台  
数据服务: 莲子大数据分析服务  
官 网: [www.lotuseed.com](http://www.lotuseed.com)  
Email: [support@lotuseed.com](mailto:support@lotuseed.com)  
[hr@lotuseed.com](mailto:hr@lotuseed.com)

微信号: qq19483741  
手机号: 13306815522





# Thanks!

## Q & A