Information Management

IBM Data Management

IBM Guardium
資料庫安全稽核管理

Guardium 報表範例說明
Guardium 與AP整合範例說明

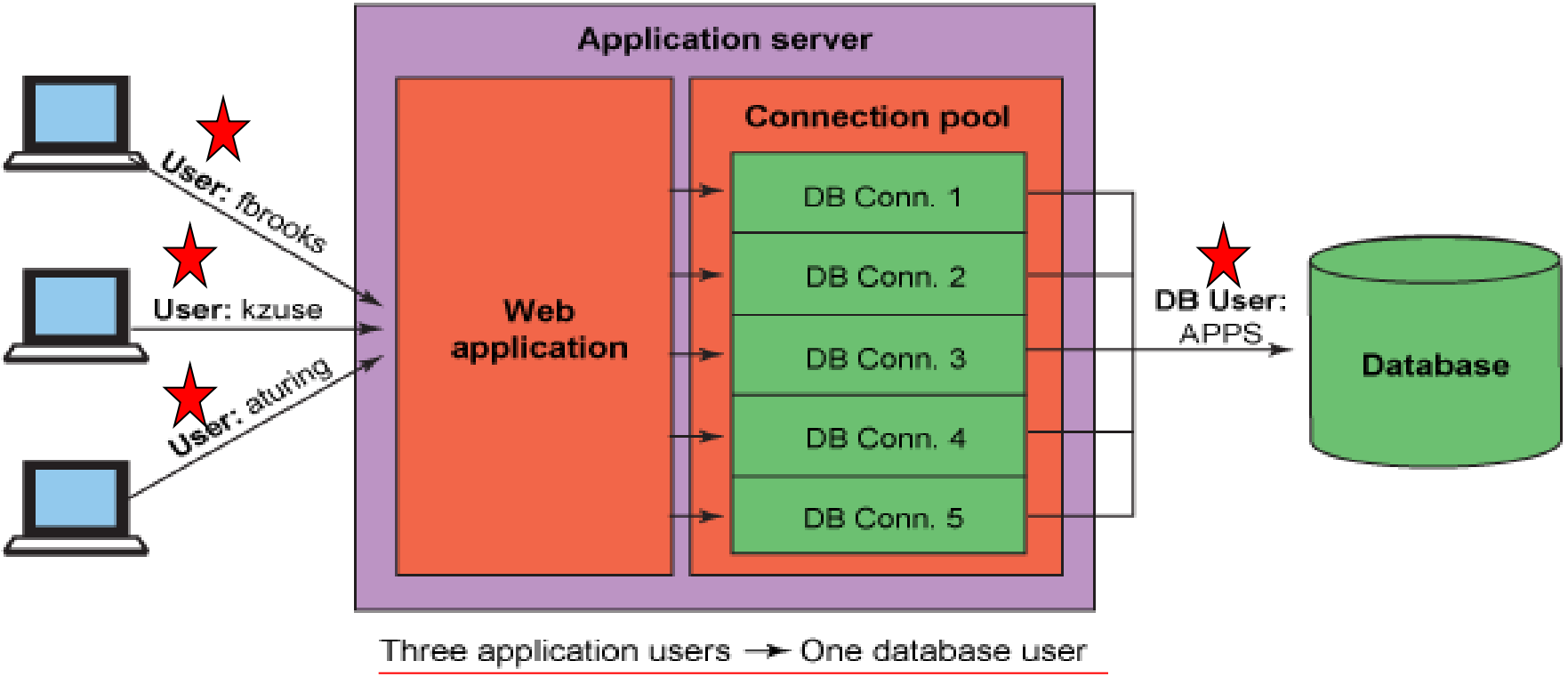
凱信資訊股份有限公司

Guardium
SAFEGUARDING DATABASES | AN IBM COMPANY

應用程式 使用者稽核說明

- 報表範例
- 作法說明
- 需AP人員配合修改Guardium API 說明

現行應用程式終端使用者稽核的困難與問題.



應用程式終端使用者稽核的困難與問題：
在三層式的架構下，應用系統伺服器是使用“連接池”中的DB User來使用資料庫中的資料。所以從DBA的角度上，無法得知真正的使用者AP User。
需求：可以得到AP User與所執行的SQL指令間的關聯

應用程式使用者追蹤稽核報表範例

查詢語法

使用的
應用系統名稱+
模組功能名稱

test

Start Date: **2012-10-18 01:18:13** End Date: **2012-10-18 01:19:13**
Aliases: **OFF** DB_Username: **LIKE %**

Timestamp	Client IP	Server IP	Source Program	DB User Name	Full Sql	Event Type	Event Value Str	App User Name	Total access
2012-10-18 01:19:33.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.21	Ferrero	1
2012-10-18 01:19:32.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.21	Ferrero	1
2012-10-18 01:19:31.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.21	Ferrero	1
2012-10-18 01:18:57.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.18	Chloe	2
2012-10-18 01:18:55.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.18	Chloe	1
2012-10-18 01:18:20.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.12	Jackal	3
2012-10-18 01:18:19.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.12	Jackal	5
2012-10-18 01:18:18.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.12	Jackal	5
2012-10-18 01:18:17.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.12	Jackal	2
2012-10-18 01:18:16.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.12	Jackal	1
2012-10-18 01:18:02.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.7	Kappa	4
2012-10-18 01:18:01.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.7	Kappa	5
2012-10-18 01:18:00.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.7	Kappa	4
2012-10-18 01:17:59.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.7	Kappa	5
2012-10-18 01:17:58.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.7	Kappa	3
2012-10-18 01:17:57.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.7	Kappa	5
2012-10-18 01:17:56.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.7	Kappa	5
2012-10-18 01:17:55.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.7	Kappa	5
2012-10-18 01:17:53.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.7	Kappa	1
2012-10-18 01:17:38.0	10.1.3.31	10.1.3.31	JAVAW.EXE	SA	select * from Customer	投資人查詢系統_查詢委託功能	102.1.1.1	Jerry	4

Records 1 to 20 of 41

登入 IP

登入 帳號

作法:透過呼叫 Guardium API 來追蹤終端使用者身份

1. Guardium API 提供了簡單的“無操作 no-operation”呼叫 – Dummy SQL。
2. 應用程式中需要存取資料庫前，可呼叫這些 API 向 Guardium 發出信號，並將相關資訊帶入Guardium，例如使用者帳號名稱。
3. Guardium 在收到API 之 Start 和 Released 命令之間，都將該資料庫連接的所有行為和該事件相關聯。
4. 需AP人員配合修改程式。

需AP人員配合修改呼叫 Guardium API 方法說明

Guardium 在收到 GuardAppEvent:Start 和 GuardAppEvent:Released

命令之間，都將該資料庫連接的所有行為和該事件相關聯。

應用程式 程式碼:

1. **透過 GuardAppEvent:Start..等 API， 設置應用程式使用者和事件**
2. **中間為 應用程式 操作資料庫之SQL Statement**
3. **透過 GuardAppEvent:Released API，清除應用程式使用者和事件**

注意事項:
應用程式 SQL connection 如果中斷(Close) ,
需重新呼叫 GuardAppEvent:Start API.

Guardium API 詳細使用方法

啟用語法：

- SELECT ‘ GuardAppEvent:Start’ ,
  ‘ GuardAppEventUserName:參數’ ,
  ‘ GuardAppEventType:參數’ ,
  ‘ GuardAppEventStrValue:參數’
  FROM location

參數為需要帶入Guardium 的資訊
(見下一頁)

Location 需視不同資料庫型態而調整 (見下二頁)

- **中間為應用程式操作資料庫之SQL Statement**

結束語法：

- SELECT ‘ GuardAppEvent:Released’
  FROM location

Location 需視不同資料庫型態而調整 (見下二頁)

要帶入Guardium API 之參數說明

- 帶入Guardium API 之AP 參數，目的為做為追蹤終端使用者身份與查詢資料之用途，並將呈現於Guardium 稽核報表之對應欄位:
- AP 資訊 帶入Guardium API 的參數 :

Guardium API	參數 (要帶入的資訊)
GuardAppEventUserName	登入系統之使用者 帳號(ID)
GuardAppEventType	使用者所使用的 應用系統名稱_模組功能名稱
GuardAppEventStrValue	使用者 IP 位址

FROM location 不同的資料庫有不同格式：

- **Oracle: FROM DUAL**

  SELECT ‘ GuardAppEvent:Start’ , ….. FROM **DUAL**

  SELECT ‘ GuardAppEvent:Released’ FROM **DUAL**

- **MS SQL**、**MySQL和Sybase** 沒有 Dummy Table, 只需 把 Select 後面的 From location 去掉即可.

  SELECT ‘ GuardAppEvent:Start’

  SELECT ‘ GuardAppEvent:Released’

- DB2: FROM SYSIBM.SYSDUMMY1
- INFORMIX: FROM SYSTABLES

```
try {
    //ConnectionStart
    DriverManager.registerDriver(new com.ibm.db2.jcc.DB2Driver());
    Connection conn= DriverManager.getConnection(jdbc_url, jdbc_user, jdbc_password);
    PreparedStatement pstmt = null;
```

Connection Start

```
    //GuardiumSqlStart
    String UserID = "Steven";
    String SystemName = "人員管理系統";
    String ModuleName = "資訊修改模組";
    String IPAddr = "192.168.30.27";

    String GuardiumSql = "SELECT ?, ?, ?, ? ";
    pstmt = conn.prepareStatement(GuardiumSql);
    pstmt.setString(1, "GuardAppEvent:Start");
    pstmt.setString(2, "GuardAppEventUserName:" + UserID);
    pstmt.setString(3, "GuardAppEventType:" + SystemName + "_" + ModuleName);
    pstmt.setString(4, "GuardAppEventStrValue:" + IPAddr);
    pstmt.executeUpdate();
    pstmt.close();
```

Guardium Sql Start

```
    //MainSql
    String updateSql = "UPDATE DM_PERSONS SET USERNAME=?, NAME=?, EMAIL=?, SMS=?, LEVEL=?, PASSWORD=? WHERE PERSON_ID=?";
    pstmt = conn.prepareStatement(updateSql);
    pstmt.setString(1, USERNAME);
    pstmt.setString(2, NAME);
    pstmt.setString(3, EMAIL);
    pstmt.setString(4, SMS);
    pstmt.setInt(5, Integer.valueOf(LEVEL));
    pstmt.setString(6, PASSWD);
    pstmt.setInt(7, Integer.valueOf(PERSON_ID));
    pstmt.executeUpdate();
    pstmt.close();
```

Main Sql

```
    //GuardiumSqlEnd
    GuardiumSql = "SELECT 'GuardAppEvent:Released' ";
    pstmt = conn.prepareStatement(GuardiumSql);
    pstmt.executeUpdate();
    pstmt.close();
```

Guardium Sql End

```
    //ConnectionEnd
    conn.close();
```

Connection End

各系統程式語言(客戶需提供)

範例：

系統名稱	Web Application Server	程式語言 (Java, .net, …)
abcv系統	IBM Websphere Application Server	Java
對內服務系統	IIS	ASP
資服資訊公司管理系統對內、對外	Tomcat	ASP, JSP, JAVA
監視系統	IIS	ASP, c++, c#
外部人員出勤系統	IIS	.net
統計報表系統	MS iis 6.0	.net(c#)
保單查詢系統	IIS 6.0	.NET
財會系統	IIS	.NET, ASP