資料庫稽核與應用實務

國立空中大學管理與資訊學系副教授兼系主任
國立空中大學資訊科技中心主任
郭秋田 博士

2015/11/27

電子資料保護基本概念

- 電子資料形式
  - 檔案格式
  - 資料庫資料
- 檔案資料保護
- 資料庫資料保護

資料庫與應用系統管理問題

- 缺乏系統弱點補強
  - 易遭入侵
- 未作存取稽核
  - 合法使用者執行非授權指令
  - 帳號密碼管理薄弱，遭盜用偽冒
- 應用程式撰寫問題
  - 查詢語言寫法不當

資料庫與應用系統管理強化作為

- 強化系統安檢掃瞄或滲透測試
  - 網站主機、網站應用程式、資料庫
  - 定期實施
  - 依結果加以修補補強
- 啟動資料庫稽核機制
  - 儲存所有存取記錄、定期稽查
- 資料庫加密

資料庫加密安全問題

- 影響資料庫效能
- 需要改寫應用程式
- 或調整資料庫
- 對於擁有資料庫存取權限者無效
- 防止無權限者讀取資料

資料庫稽核

- 透過稽核的方法來嚇阻不當存取的發生或當發現不當存取時，可以在有效的時限內進行必要的因應措施
- 資料庫稽核和資料庫加密的不同
  - 資料庫加密透過將資料加密的方式直接防止資料的洩密
  - 資料庫稽核是透過事前嚇阻、事中及時發現並進行阻斷、以及事後分析追查來因應可能的資安事件

資料庫稽核模式

- 本機監控模式
  - 在資料庫本機安裝稽核監控的模組
  - 可記錄所有資料庫活動外
  - 可適時地偵測出異常的活動進而將其中止
  - 會影響系統效能
  - 侵入式導入，有風險

資料庫稽核模式

- 網路監控模式
  - 利用網路監聽的方式，記錄監控資料庫的活動
  - 透過獨立的設備介接聽取資料庫和外部的網路通訊活動
  - 完全不會影響到資料庫的效能
  - 無法監控到本機的操作
  - 不只可以記錄資料庫的網路活動，亦可在偵測到異常行為發生時，透過發送阻斷的網路封包來達到中止異常活動的效果

網路監控v.s代理程式

	網路監控	代理程式
佈署方式	使用網路設備資源	使用資料庫伺服器資源
本機登入	無法監控，仍須代理程式(Telnet*)	可監控
資料庫交易量增加	無影響	有影響
資料庫伺服器增加	可監控	無法監控
單一超高交易量資料庫	可分散處理	無法分散處理

資料庫稽核導入要點

評估關鍵	監視系統
佈署架構彈性與安全性	安裝監視系統會不會危及建築主結構？ 調整監視系統會不會影響建築物使用？
是否可以全面監控 資料庫存取活動	監視系統是否沒有死角？
是否可以儲存 所有資料庫稽核記錄	監視系統一天只能錄2小時？！ （個資法舉證：5年）
分析資料庫稽核記錄的 效能與易用性	我要看二樓的四號攝影機！
導入成本與效益 （採購成本、管理成本）	監視系統很貴嗎？

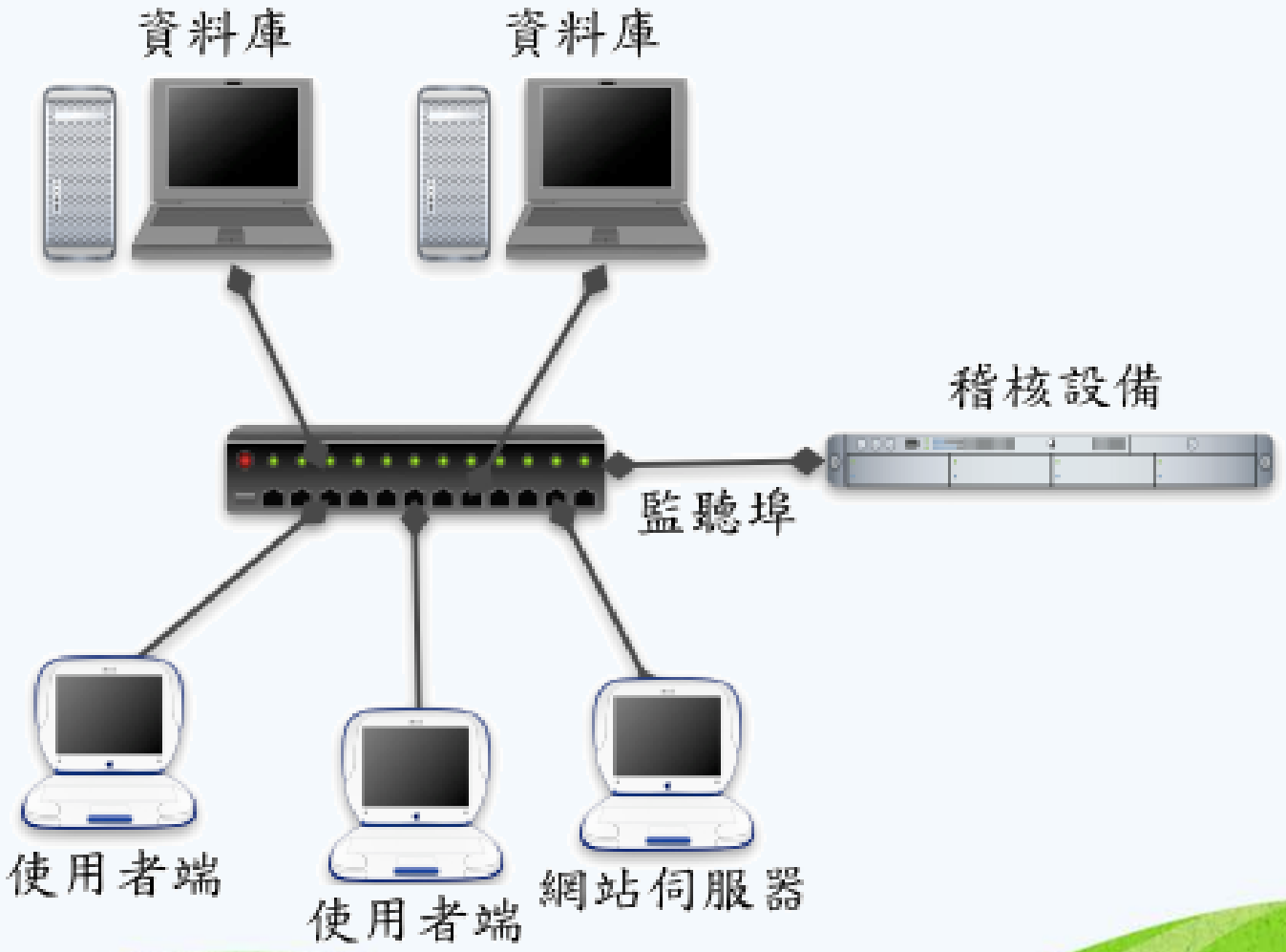
網路型資料庫稽核系統

工具特色	存取行為風險模式 智慧型情報中心
操作性	自動偵測資料庫與物件 自動學習模式 關聯式分析
支援資料庫種類	Oracle, MS SQL, DB2* DB Agents*
資料庫活動分析	1.資料庫使用者、資料庫物件、SQL語法 2.人事時地物
異常行為分析	•政策模式 •行為模式 •風險模式
分析與報表界面	•關聯式分析界面-可由人事時地物任一角度切入 •所見即得報表系統-能分析就能訂閱報表 •支援多國語系，全球唯一全中文化介面

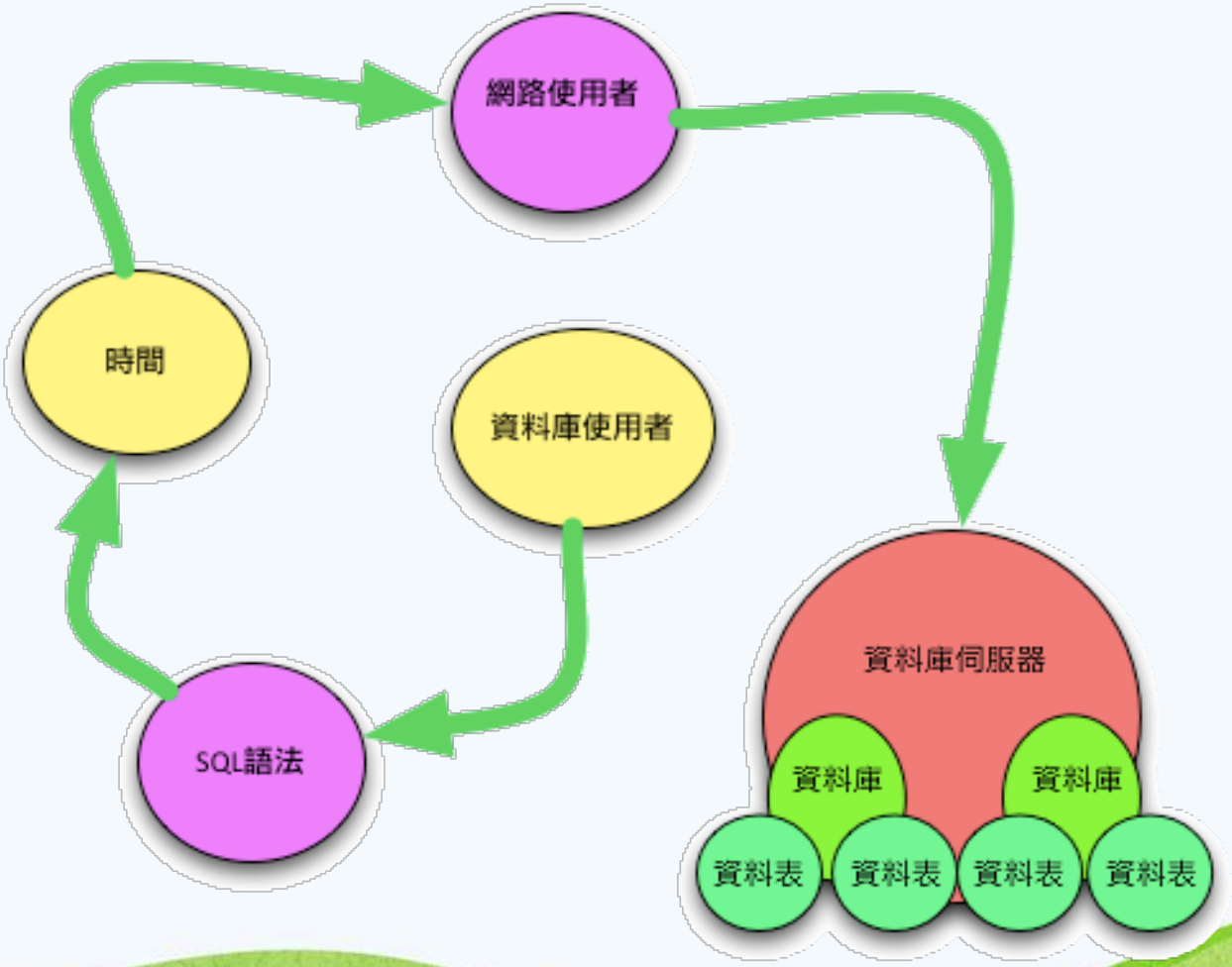
資料庫稽核機制導入程序

- 部署架構-初次導入建議以網路監控模式
- 導入程序
  - 監控與資產探索
  - 規則設定
  - 稽核追蹤

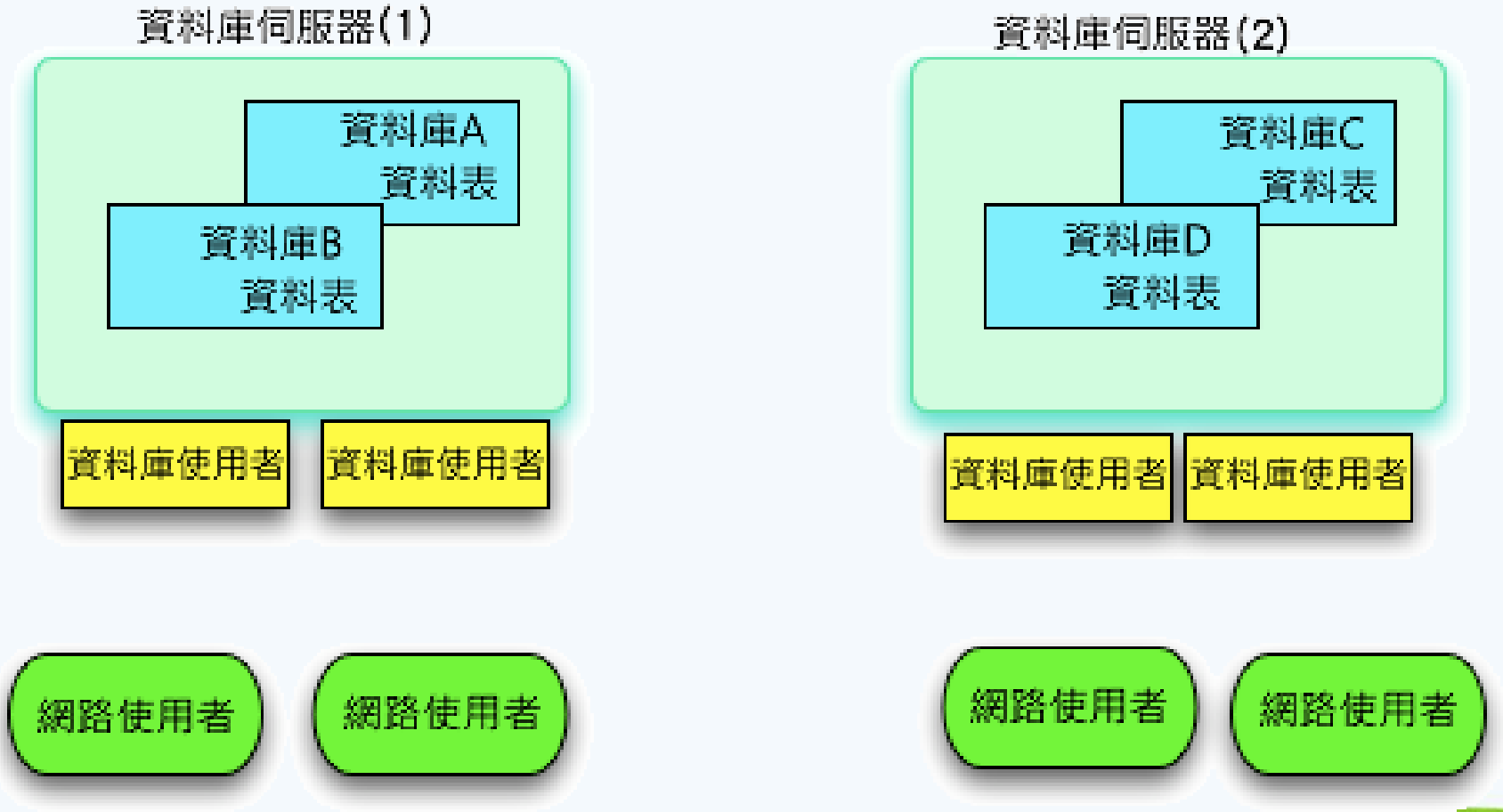
網路監控模式部署架構



資料庫稽核五元素



分析資料庫物件


資料庫伺服器(1)
資料庫A
資料表
資料庫B
資料表
資料庫使用者
資料庫使用者
資料庫伺服器(2)
資料庫C
資料表
資料庫D
資料表
資料庫使用者
資料庫使用者
網路使用者
網路使用者
網路使用者
網路使用者

資訊資產總覽


資產資訊
資料庫伺服器
NO 主機名稱 埠號 資料庫# 資料庫使用者#
1 192.168.48.137 1433 0 1
2 192.168.48.223 1521 2 16
資料庫伺服器
資料庫
NO 資料庫名稱 資料表# 預存程式#
1 noud01 69 0
2 Uncertain-192.168.48.223 157 0
資料庫
資料表
NO 資料表名稱
1 AUTT010
2 AUTT015
3 AUTT019
4 AUTU002
5 CCST010
6 CGUT001
7 CGUT002
資料表
資料庫使用者
NO 使用者名稱
1 nou
2 noudbo
3 scott
4 system
5 Uncertain-192.168.48.122
6 Uncertain-192.168.48.123
7 Uncertain-192.168.48.132
資料庫使用者
預存程式
NO 預存程式名稱
預存程式

存取政策設定

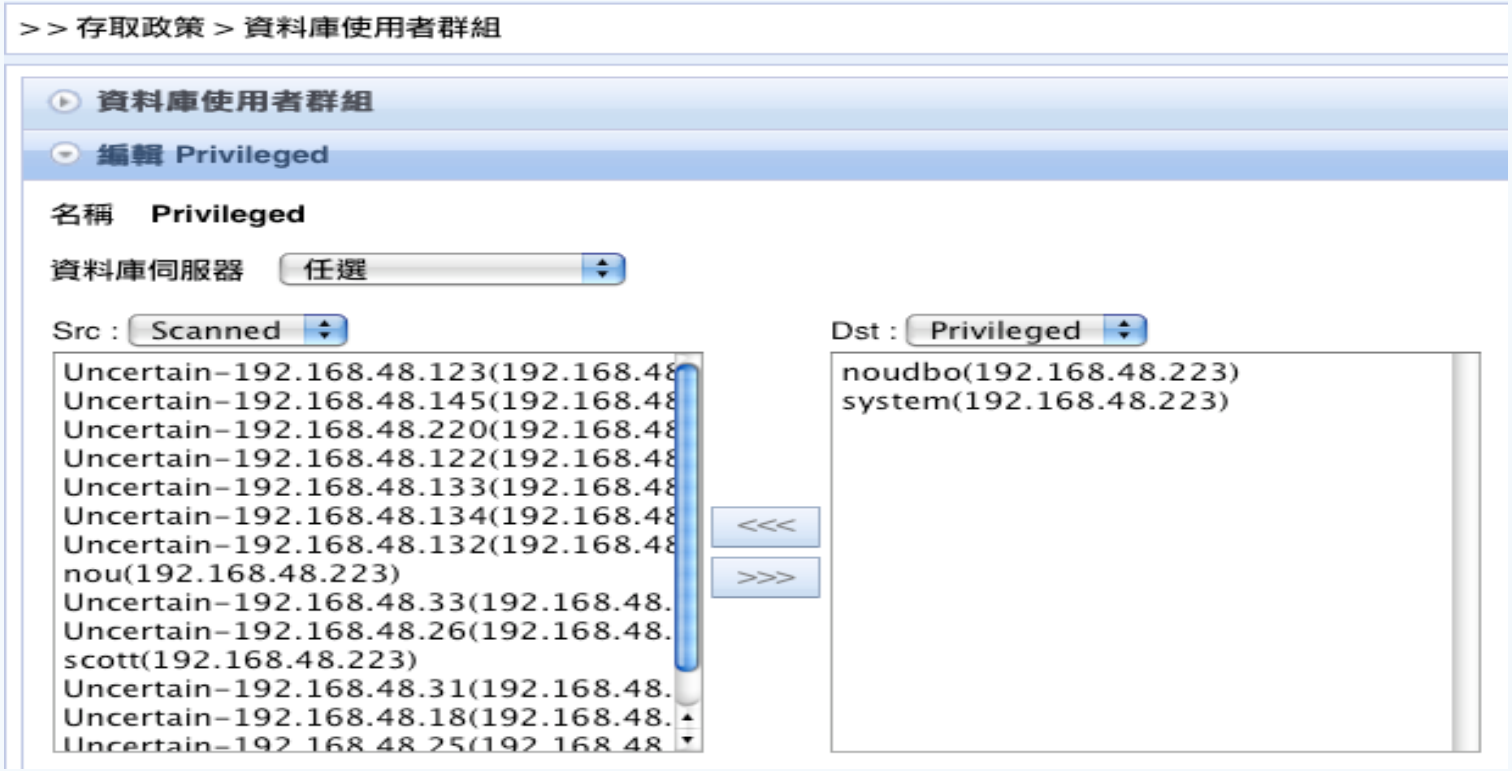
>> 存取政策 > 存取規則

存取規則

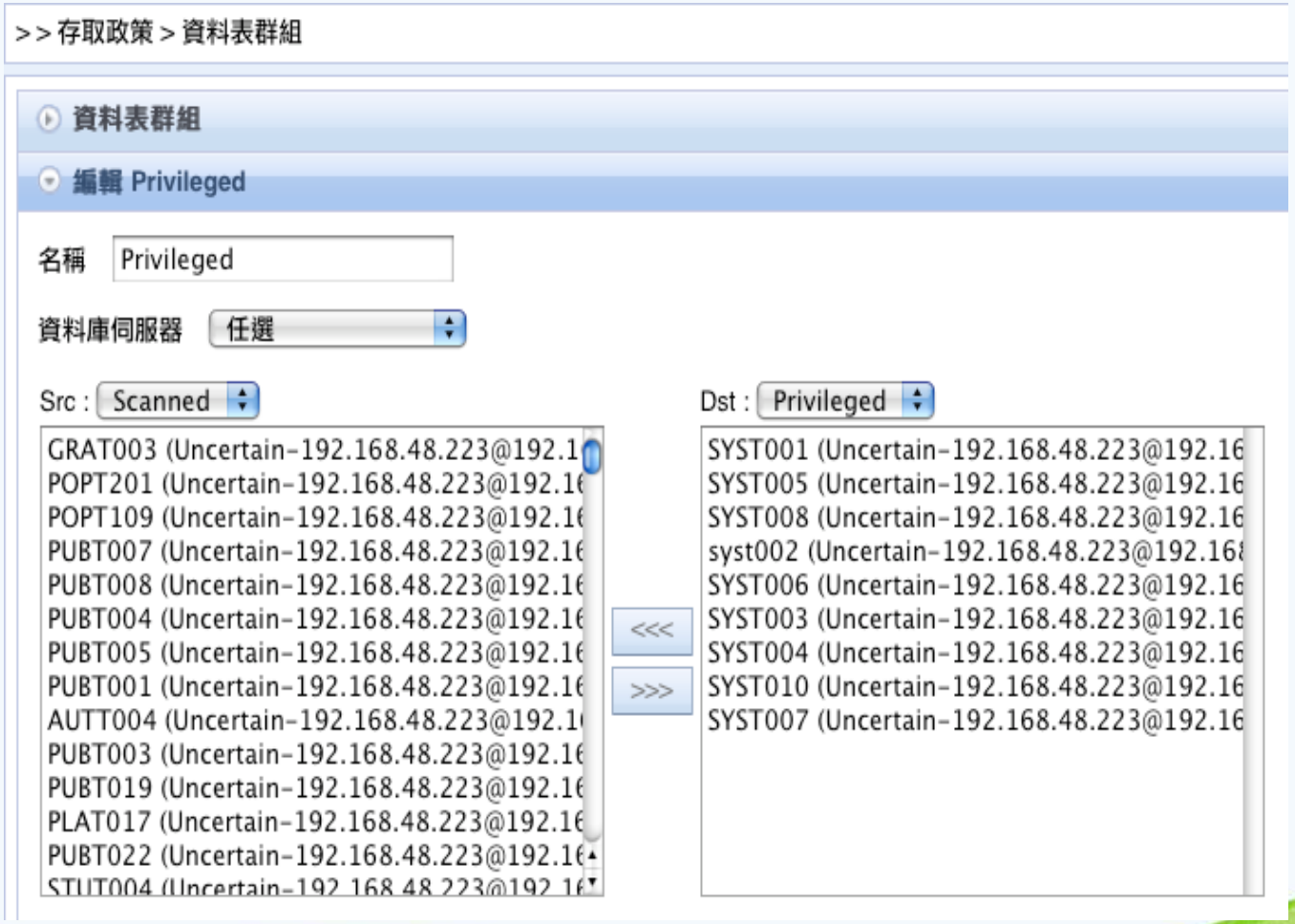
	修改	排序	名稱	資料庫伺服器	資料庫物件群	資料庫使用者群	SQL 指令群	網路使用者群	時間區段	執行動作
☑	✎ 🗑	1	Critical Access	任選	Scanned	Privileged	任選	任選	任選	Alert
☑	✎ 🗑	2	SQL Admin	任選	任選	Scanned	ADMIN	任選	任選	Alert
☑	✎ 🗑	3	Privileged Table	任選	Privileged	Scanned	任選	任選	任選	Audit
☑	✎ 🗑	4	Privileged User	任選	任選	Privileged	任選	任選	任選	Audit
☑	✎ 🗑	5	Night time	任選	任選	任選	任選	任選	Night Time	Audit
☑	✎ 🗑	6	anything	任選	任選	任選	任選	任選	任選	Audit

新增

使用者群組


>> 存取政策 > 資料庫使用者群組
資料庫使用者群組
編輯 Privileged
名稱 Privileged
資料庫伺服器 任選
Src : Scanned
Uncertain-192.168.48.123(192.168.48
Uncertain-192.168.48.145(192.168.48
Uncertain-192.168.48.220(192.168.48
Uncertain-192.168.48.122(192.168.48
Uncertain-192.168.48.133(192.168.48
Uncertain-192.168.48.134(192.168.48
Uncertain-192.168.48.132(192.168.48
nou(192.168.48.223)
Uncertain-192.168.48.33(192.168.48.
Uncertain-192.168.48.26(192.168.48.
scott(192.168.48.223)
Uncertain-192.168.48.31(192.168.48.
Uncertain-192.168.48.18(192.168.48.
<<<
>>>
Dst : Privileged
noudbo(192.168.48.223)
system(192.168.48.223)

資料表群組


>> 存取政策 > 資料表群組
資料表群組
編輯 Privileged
名稱
Privileged
資料庫伺服器
任選
Src :
Scanned
GRAT003 (Uncertain-192.168.48.223@192.1
POPT201 (Uncertain-192.168.48.223@192.16
POPT109 (Uncertain-192.168.48.223@192.16
PUBT007 (Uncertain-192.168.48.223@192.16
PUBT008 (Uncertain-192.168.48.223@192.16
PUBT004 (Uncertain-192.168.48.223@192.16
PUBT005 (Uncertain-192.168.48.223@192.16
PUBT001 (Uncertain-192.168.48.223@192.16
AUTT004 (Uncertain-192.168.48.223@192.1
PUBT003 (Uncertain-192.168.48.223@192.16
PUBT019 (Uncertain-192.168.48.223@192.16
PLAT017 (Uncertain-192.168.48.223@192.16
PUBT022 (Uncertain-192.168.48.223@192.16
<<<
>>>
Dst :
Privileged
SYST001 (Uncertain-192.168.48.223@192.16
SYST005 (Uncertain-192.168.48.223@192.16
SYST008 (Uncertain-192.168.48.223@192.16
syst002 (Uncertain-192.168.48.223@192.168
SYST006 (Uncertain-192.168.48.223@192.16
SYST003 (Uncertain-192.168.48.223@192.16
SYST004 (Uncertain-192.168.48.223@192.16
SYST010 (Uncertain-192.168.48.223@192.16
SYST007 (Uncertain-192.168.48.223@192.16

行為規則-門檻值設定

>>行為政策 > 行為規則

行為規則

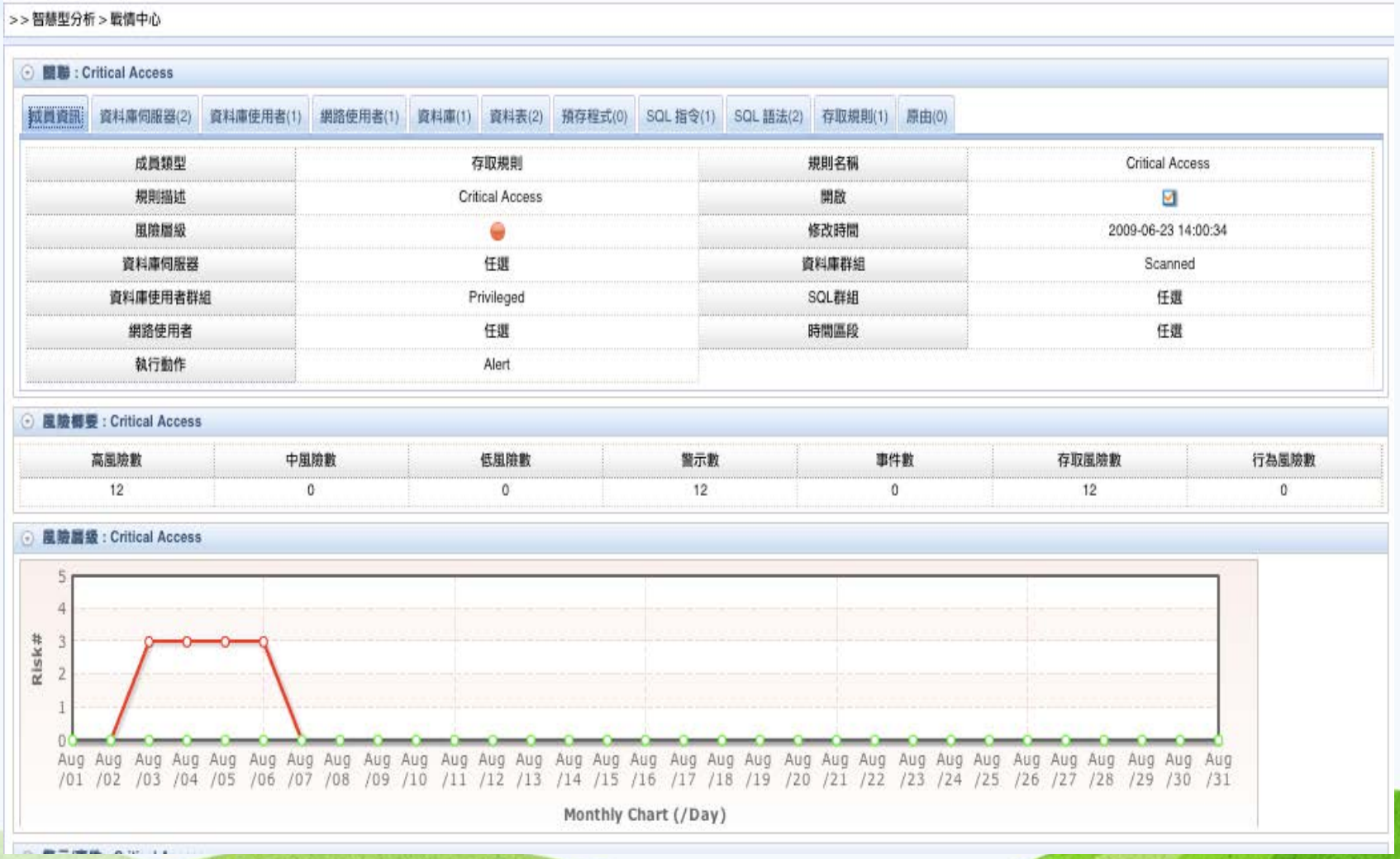
每日計數	行為型別	檔案名稱	客制檔案	低風險上限值	高風險上限值	執行動作
初用-SQL Statement數	資料庫	Default		100	500	Alert
原始資料數	資料庫	Default		500	3000	Audit
Record數	資料庫	Default		1000	5000	Alert
SQL Select數	資料庫	Default		1000	10000	Alert
SQL Admin數	資料庫	Default		500	5000	Alert

5 / 1 1

紀錄觀察分析


存取政策: 每月
Risk#
5
4
3
2
1
0
Aug /01 Aug /02 Aug /03 Aug /04 Aug /05 Aug /06 Aug /07 Aug /08 Aug /09 Aug /10 Aug /11 Aug /12 Aug /13 Aug /14 Aug /15 Aug /16 Aug /17 Aug /18 Aug /19 Aug /20 Aug /21 Aug /22 Aug /23 Aug /24 Aug /25 Aug /26 Aug /27 Aug /28 Aug /29 Aug /30 Aug /31
Monthly Chart (/Day)
High
存取政策: 存取規則
High Risk#
15
12
9
6
3
0
12
0
0
0
Critical Access
Privileged Table
Night time
anything

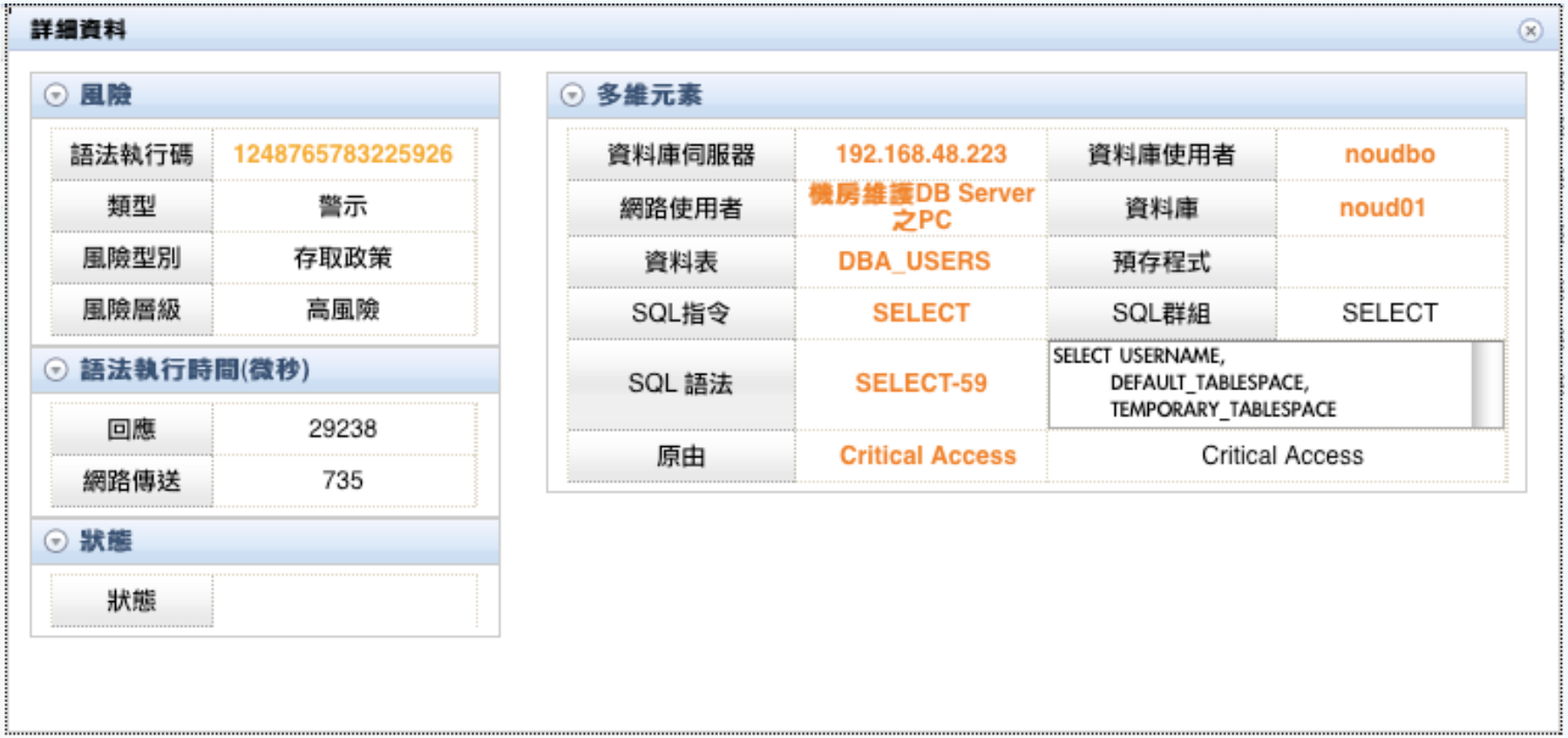
紀錄觀察分析


>> 智慧型分析 > 戰情中心
: Critical Access
成員資訊
資料庫伺服器(2)
資料庫使用者(1)
網路使用者(1)
資料庫(1)
資料表(2)
預存程式(0)
SQL 指令(1)
SQL 語法(2)
存取規則(1)
原由(0)
成員類型
存取規則
規則名稱
Critical Access
規則描述
Critical Access
開啟
風險層級
修改時間
2009-06-23 14:00:34
資料庫伺服器
任選
資料庫群組
Scanned
資料庫使用者群組
Privileged
SQL群組
任選
網路使用者
任選
時間區段
任選
執行動作
Alert
: Critical Access
高風險數
中風險數
低風險數
警示數
事件數
存取風險數
行為風險數
12
0
0
12
0
12
0
: Critical Access
Risk#
0
1
2
3
4
5
Aug /01
Aug /02
Aug /03
Aug /04
Aug /05
Aug /06
Aug /07
Aug /08
Aug /09
Aug /10
Aug /11
Aug /12
Aug /13
Aug /14
Aug /15
Aug /16
Aug /17
Aug /18
Aug /19
Aug /20
Aug /21
Aug /22
Aug /23
Aug /24
Aug /25
Aug /26
Aug /27
Aug /28
Aug /29
Aug /30
Aug /31
Monthly Chart (/Day)

紀錄觀察分析


>> 智慧型分析 > 警示管理
2009-08-03 00:00:00 ~ 2009-08-03 23:59:59
警示管理
狀態 原由 資料庫伺服器 資料庫使用者 網路使用者 SQL指令 結束時間
Critical Access 192.168.48.223 noudbo 機房維護DB Server之PC SELECT 2009-08-03 17:04:25
Critical Access 192.168.48.223 noudbo 機房維護DB Server之PC SELECT 2009-08-03 17:04:25
Critical Access 192.168.48.223 noudbo 機房維護DB Server之PC SELECT 2009-08-03 17:04:24
資料庫: 過多的SQL Select數 192.168.48.223 nou 網路書店 SELECT 2009-08-03 11:02:35
資料庫: 過多的資料庫筆數 192.168.48.223 nou 網路書店 SELECT 2009-08-03 10:21:53
資料庫: 過多的SQL Select數 192.168.48.223 nou 網路書店 SELECT 2009-08-03 01:40:50
6 / 1 1
條件
時間
過濾條件
政策型別 : 任選
風險層級 : 任選
資料庫伺服器 : 任選
網路使用者 : 任選
SQL指令 : 任選
語法執行碼 :
執行

紀錄觀察分析



詳細資料

風險

語法執行碼	1248765783225926
類型	警示
風險型別	存取政策
風險層級	高風險

語法執行時間(微秒)

回應	29238
網路傳送	735

狀態

狀態	

多維元素

資料庫伺服器	192.168.48.223	資料庫使用者	noudbo
網路使用者	機房維護DB Server之PC	資料庫	noud01
資料表	DBA_USERS	預存程式	
SQL指令	SELECT	SQL群組	SELECT
SQL 語法	SELECT-59	SELECT USERNAME, DEFAULT_TABLESPACE, TEMPORARY_TABLESPACE	
原由	Critical Access	Critical Access	

觀察結果


>> 智慧型分析 > 風險圖
存取政策: 每月
Risk#
7,000
5,600
4,200
2,800
1,400
0
Aug/01 Aug/02 Aug/03 Aug/04 Aug/05 Aug/06 Aug/07 Aug/08 Aug/09 Aug/10 Aug/11 Aug/12 Aug/13 Aug/14 Aug/15 Aug/16 Aug/17 Aug/18 Aug/19 Aug/20 Aug/21 Aug/22 Aug/23 Aug/24 Aug/25 Aug/26 Aug/27 Aug/28 Aug/29 Aug/30 Aug/31
Monthly Chart (/Day)
High
Medium
Low
存取政策: 存取規則
All Risk#
18K
14.4K
10.8K
7.2K
3.6K
0
17.63K
Night time

觀察結果

>> 智慧型分析 > 戰情中心

關聯 : Night time

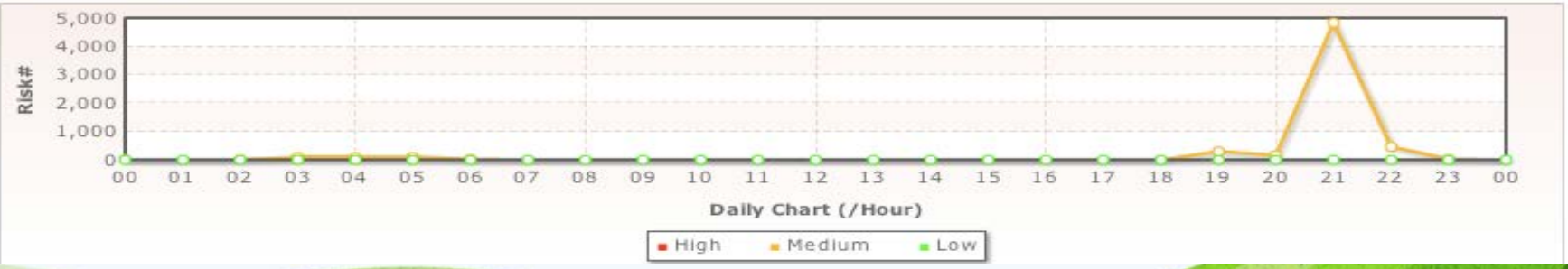
成員資訊 | 資料庫伺服器(2) | 資料庫使用者(1) | 網路使用者(6) | 資料庫(1) | 資料表(39) | 預存程式(0) | SQL 指令(4) | SQL 語法(64) | 存取規則(1) | 原由(0)

成員類型	存取規則	規則名稱	Night time
規則描述	night time access	開啟	☑
風險層級		修改時間	2009-07-24 16:05:48
資料庫伺服器	任選	資料庫群組	任選
資料庫使用者群組	任選	SQL群組	任選
網路使用者	任選	時間區段	Night Time
執行動作	Audit		

風險摘要 : Night time

高風險數	中風險數	低風險數	警示數	事件數	存取風險數	行為風險數
0	6107	0	0	6107	6107	0

風險層級 : Night time



觀察結果

>> 智慧型分析 > 戰情中心

關聯 : Night time

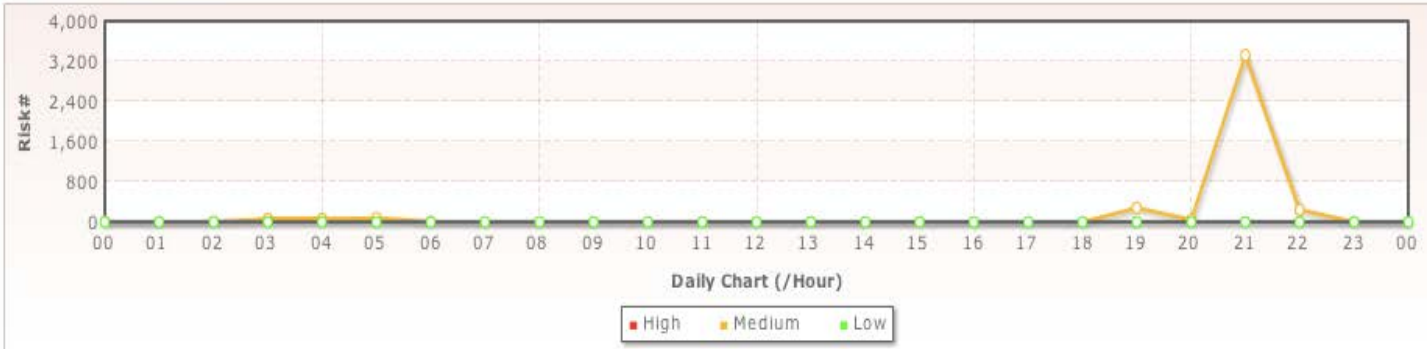
成員資訊 | 資料庫伺服器(1) | 資料庫使用者(1) | 網路使用者(6) | 資料庫(1) | 資料表(28) | 預存程式(0) | SQL 指令(4) | SQL 語法(43) | 存取規則(1) | 原由(0)

NO	網路使用者	IP 位址	網路使用者
1	內網AP server1	192.168.48.122	Scanned
2	內網AP server2	192.168.48.123	Scanned
3	外網AP server1	192.168.48.132	Scanned
4	外網AP server2	192.168.48.133	Scanned
5	機房維護DB Server 之PC	192.168.48.155	Scanned
6	網路書店	192.168.48.220	Scanned

風險概要 : Night time

高風險數	中風險數	低風險數	警示數	事件數	存取風險數	行為風險數
0	4116	0	0	4116	4116	0

風險層級 : Night time



觀察結果


>> 智慧型分析 > 戰情中心
2009-08
關聯 : DROP TABLE
成員資訊
資料庫伺服器(1)
資料庫使用者(1)
網路使用者(1)
資料庫(1)
資料表(1)
預存程式(0)
SQL 指令(1)
SQL 語法(1)
存取規則(1)
原由(0)
成員類型
SQL指令
名稱
DROP TABLE
群組
DEFINE
檔案
DEFINE
風險概要 : DROP TABLE
高風險數
中風險數
低風險數
警示數
事件數
存取風險數
行為風險數
0
0
1
0
1
1
0
風險層級 : DROP TABLE
Risk#
Monthly Chart (/Day)
High
Medium
Low
條件
時間
過濾條件
政策型別 : 任選
事件類型 : 任選
圖表橫軸 : 資料庫指令
縱軸 : All Risk#
資料庫伺服器 :
192.168.48.223
SQL指令 :
DROP TABLE
執行

觀察結果


>> 智慧型分析 > 事件列表
2009-08-03 11:40:00 ~ 2009-08-03 11:44:59
事件列表
事件類型
原由
資料庫伺服器
資料庫使用者
網路使用者
SQL指令
結束時間
anything
192.168.48.223
nou
192.168.48.18
DROP TABLE
2009-08-03 11:42:41
1 / 1
1
條件
時間
過濾條件
政策型別 : 任選
風險層級 : 任選
事件類型 : 任選
資料庫伺服器 :
任選
網路使用者 :
任選
SQL指令 :
DROP TABLE
語法執行碼 :
執行

觀察結果

詳細資料

風險

語法執行碼	1248765783111368
類型	一般事件
風險型別	存取政策
風險層級	低風險

語法執行時間(微秒)

回應	699273
網路傳送	0

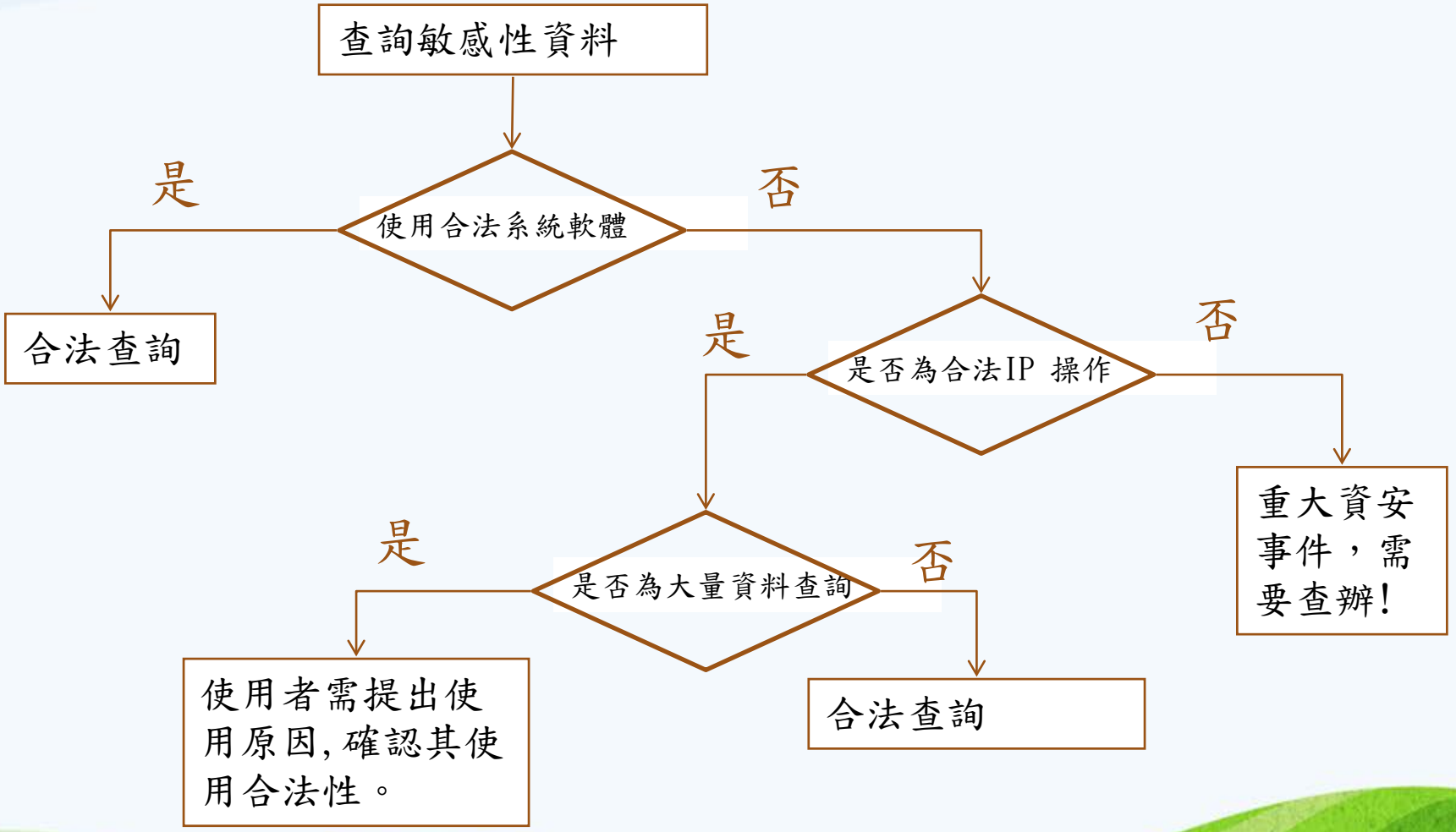
多維元素

資料庫伺服器	192.168.48.223	資料庫使用者	nou
網路使用者	192.168.48.18	資料庫	noud01
資料表	SOLT003	預存程式	
SQL指令	DROP TABLE	SQL群組	DEFINE
SQL 語法	DROP TABLE-826	drop table SOLT003	
原由	anything	anything	

資料庫稽核常發現的問題

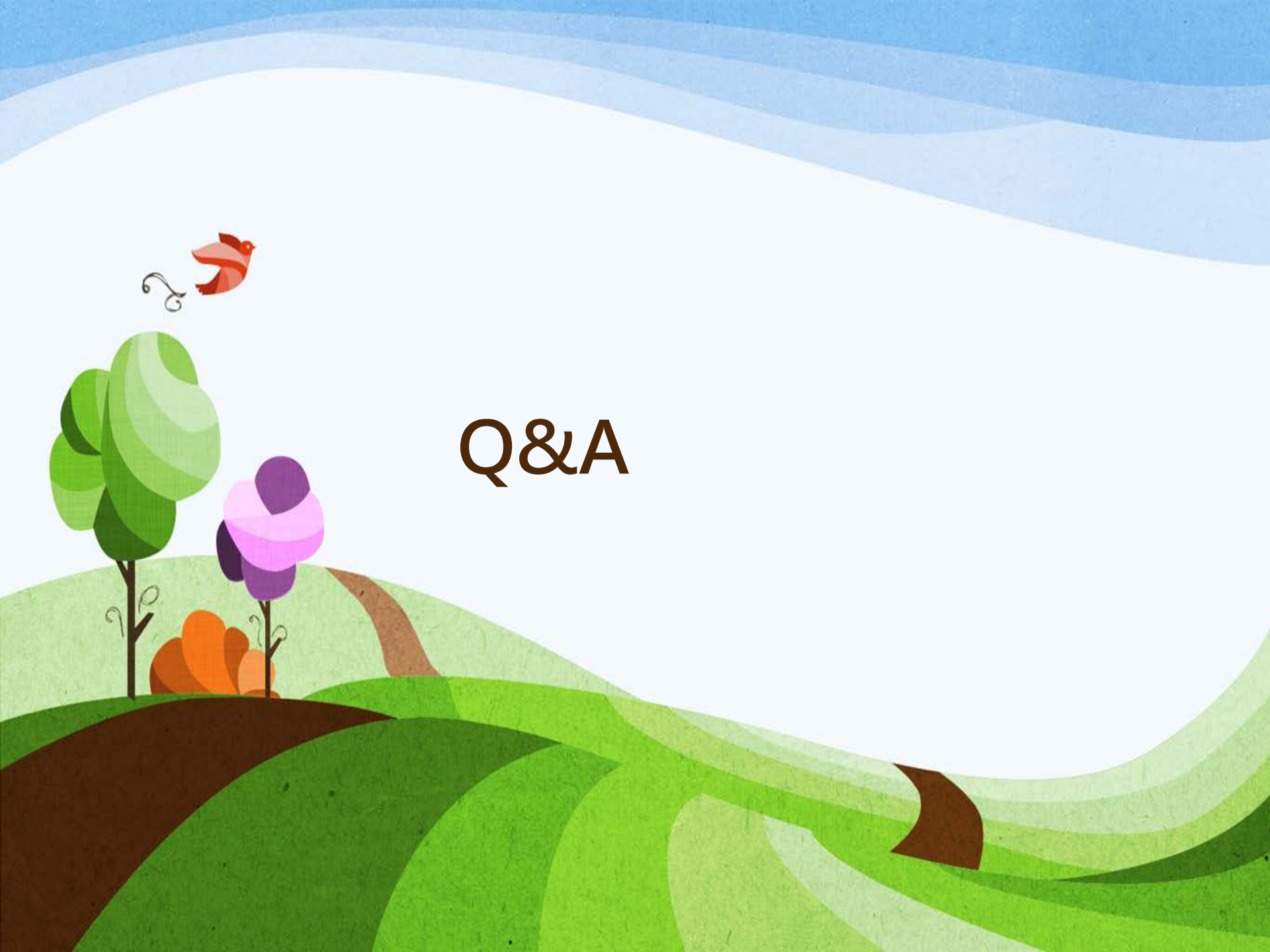
- 敏感性tables存取
- 大量資料存取
- 資料庫物件異動
- 資料庫權限授予
- 應用程式所造成資料庫的錯誤
- 失敗的連線 (Fail Login)
- 過慢的SQL語句
- SQL client直接連線

敏感性資料稽核事件處理流程例



資安管理稽核表

稽核日期:	稽核人員:
稽核事項:	
操作語法:	
稽核事件: □敏感性資料查詢異動 □ 資料庫權限授予 □ 非法帳號使用 □ 非法IP 使用 □不當語法操作 □ 資料表格異動	
操作人員:	操作日期:
原因:	
直屬主管簽名:	操作人員簽名:
稽核主管簽名:	稽核人員簽名:


Q&A