# Welcome

Microsoft TechNet

# 跨平台管理— Microsoft System Center Operations Manager 2007 R2 新功能

詹臺祥昇 Johnson Tan Tai

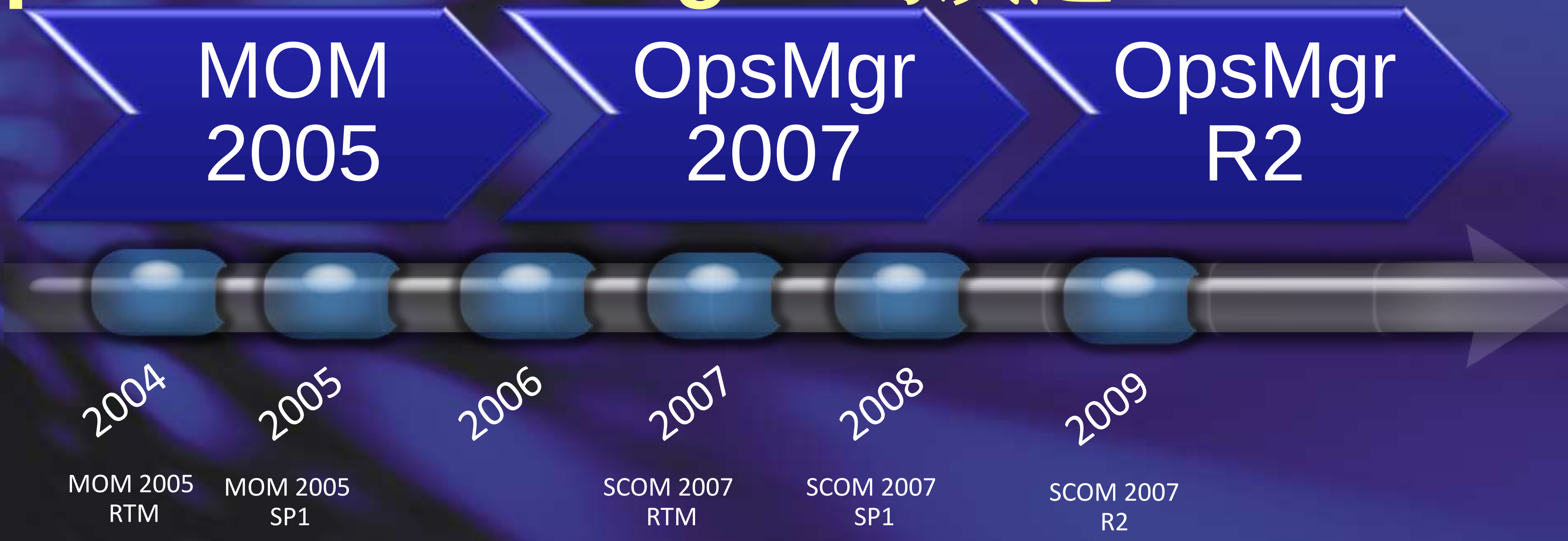
jtantai@microsoft.com

Microsoft Taiwan

# What Will We cover?

- 綜觀System Center Operations Manager 2007 R2
- 跨平台管理
- 服務水平報表
- 存取稽核報表

# Operations Manager 的演進



MOM 2005

OpsMgr 2007

OpsMgr R2

2004

MOM 2005 RTM

2005

MOM 2005 SP1

2006

2007

SCOM 2007 RTM

2008

SCOM 2007 SP1

2009

SCOM 2007 R2

| | MOM 2005 | OpsMgr 2007 | OpsMgr 2007 R2 |
|---|---|---|---|
| 被管理端環境 | 伺服器的角色 | 服務、線上服務的應用程式、線上交易相關服務、用戶端 | 延伸到跨異質平台的環境 |
| 偵測 | State | Health Model | Synthetic Transactions + Health Model |
| 架構 | WS based Tiering and Integration | Model based Management | Model based Management |
| Actions | 工作 | 以知識為管理基礎 | 服務水平回報 |

# Opsmgr 2007 R2的功能

## 集中化安全稽核

- 蒐集與整合安全事件紀錄
- 產出符合稽核的遵循報表
- 預設報表支援客製化

## 主動平台監控

- 跨Linux、UNIX與Windows 平台集中化監控
- 監控重要設定變更狀態
- 監控及管理微軟與其他的虛擬化平台

## 應用程式與服務水平監控

- 應用程式與服務水平監控
- 問題解決知識庫
- 服務水平追蹤與報表產出
- 服務水平監控儀表板

## 跨平台資訊溝通與延伸平台

- 標準的作業系統監控
- 延伸技術支援客製化開發
- 跨平台溝通異質管理平台與Helpdesk

# 其他管理的需求

需要在單一畫面呈現所有平台的監控訊息

- 監控多種作業系統
- 最少的設定
- 支援更多的版本

如何獲得更正確的服務水平訊息

- 服務的關鍵效能指標
- 使用者對IT service 的體驗
- 是否符合與業務單位協定的服務水平
- 易讀的介面

如何減少人力與時間在存取控制的審視報表上

- 帳號登入失敗的統計
- 高權限群組的稽核
- 重要檔案的存取稽核
- 異常登入稽核

# 誰需要Opsmgr 2007 R2?

- 系統管理者

  佈署與管理 Operations Manager 2007

- 營運管理者

  評估IT 服務的監控需求、依據需要設定管理原則

  定義服務水平的目標與建立服務水平儀表板

- **Operator**

  監控所有服務、系統與應用程式，第一線反應服務異常

# Opsmgr 2007 R2如何幫助系統管理者?

- 降低佈署成本與資源
- 降低採購成本與技術門檻
- 增加整合的效益
- 增加問題處理的效率

Microsoft®
System Center
Operations Manager 2007 R2

# Opsmgr 2007 R2如何幫助營運管理者?

- 降低管理範本的成本與資源
- 增加服務水平管理彈性
- 提供整體的服務監控

Microsoft® System Center Operations Manager 2007 R2

Microsoft TechNet

# Opsmgr 2007 R2 如何簡化 Operator 的工作

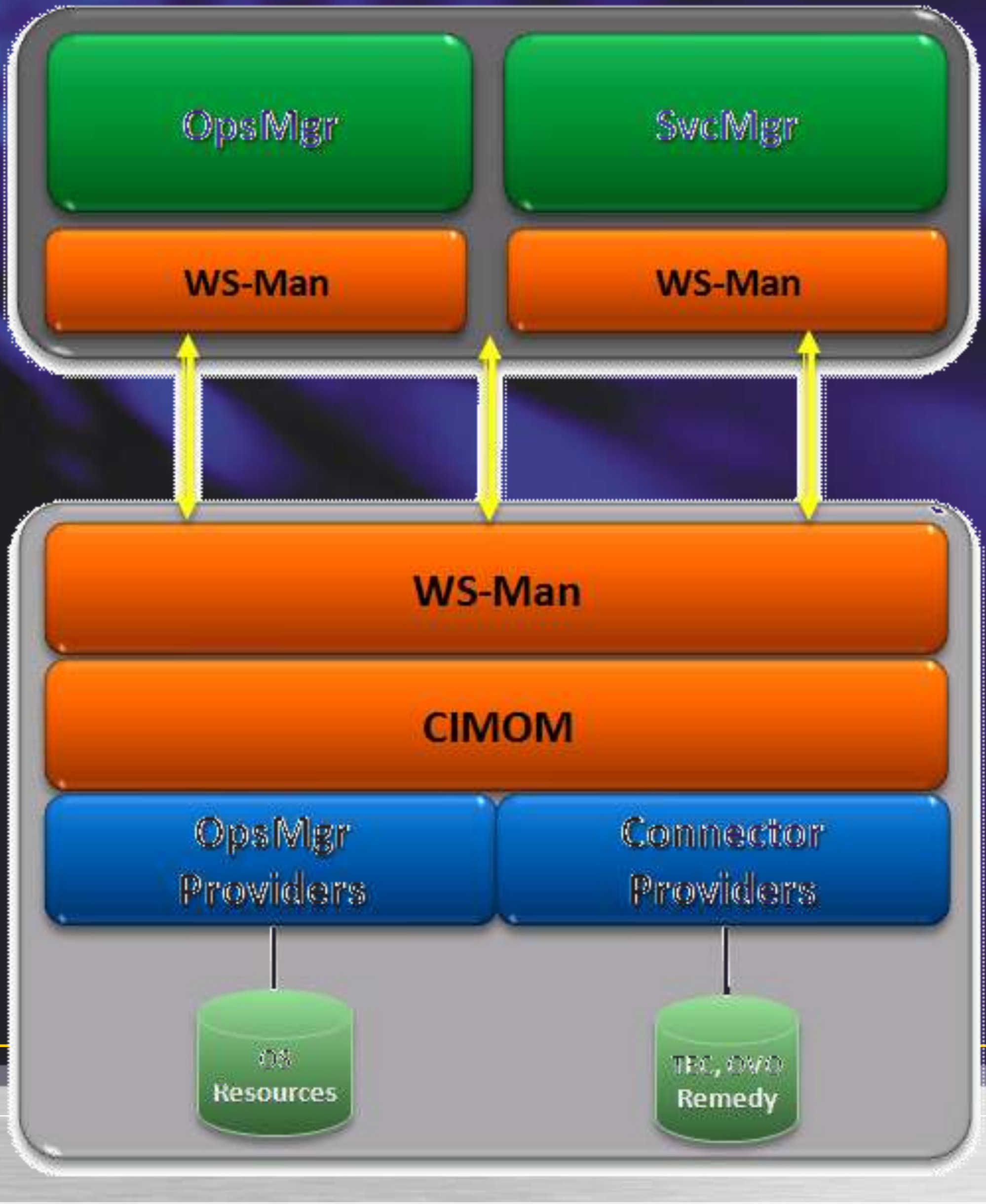
- 提升監控介面的效能
- 網頁管理介面提升管理彈性
- 支援Visio與 SharePoint 整合

LEARNING LIVES HERE

# Opsmgr 2007 R2在異質平台上的管理

Microsoft TechNet

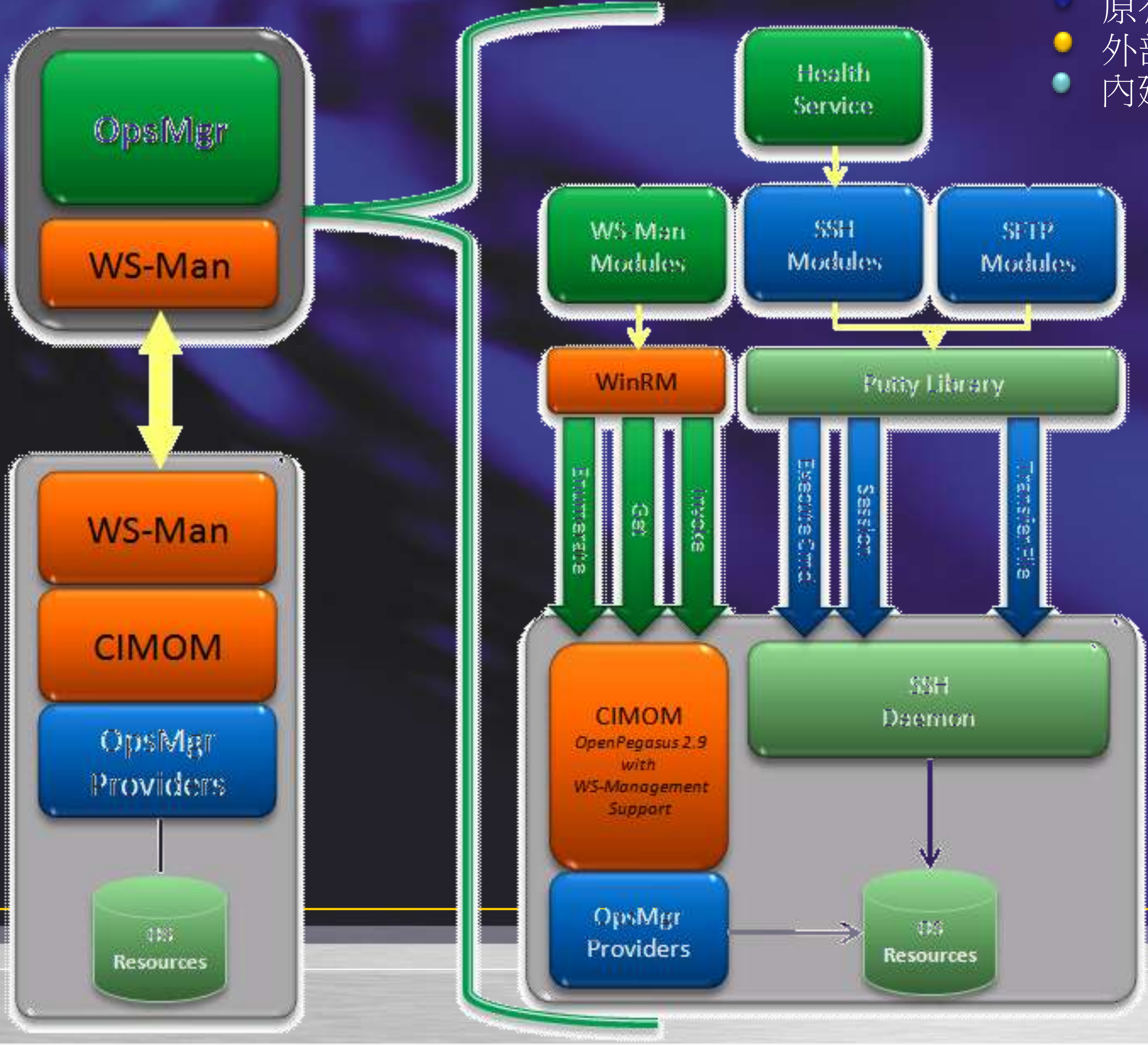
# 架構概觀



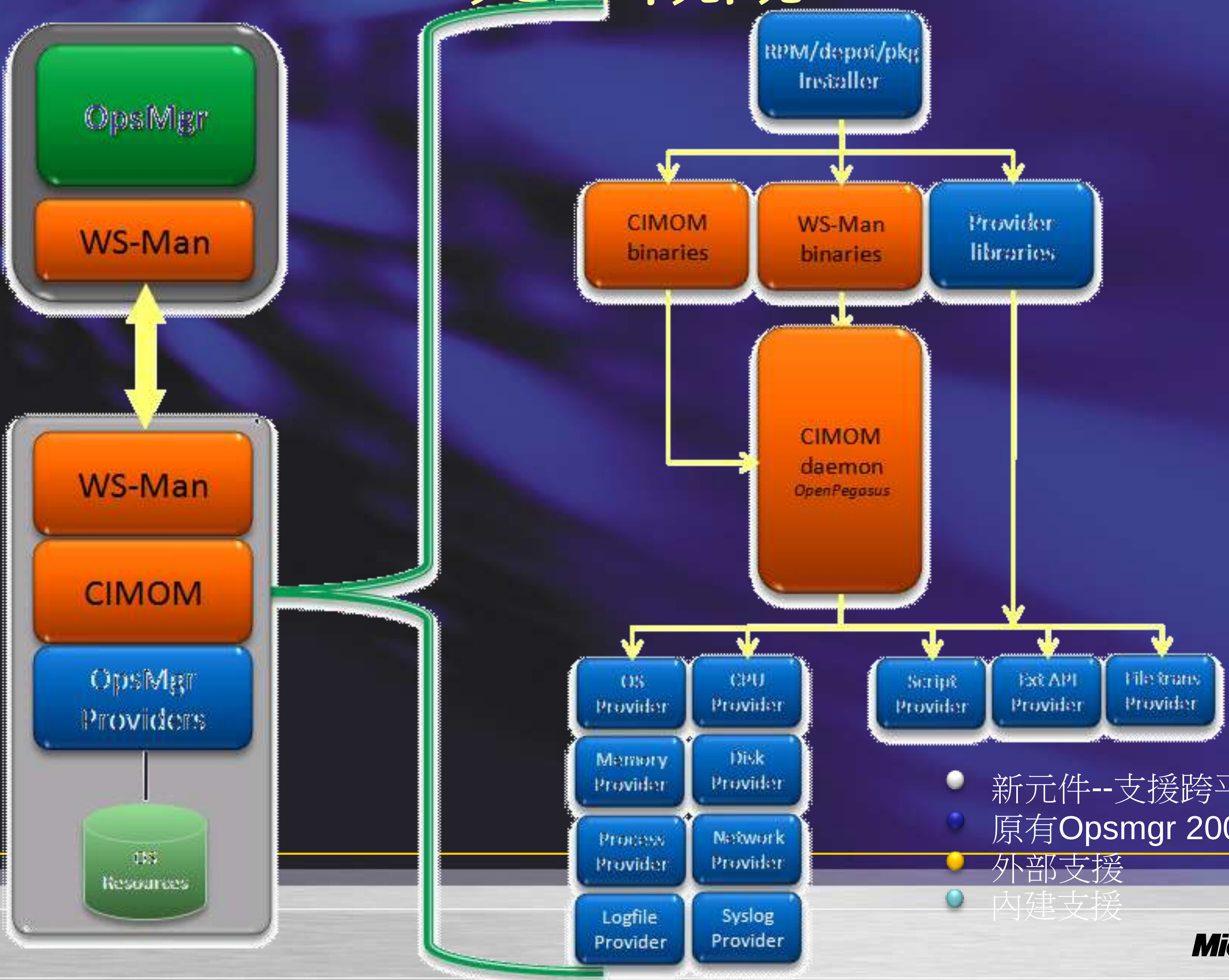
- 新元件--支援跨平台作業系統
- 原有Opsmgr 2007 或SP1的元件
- 外部支援
- 內建支援

# 模組內容

- ● 新元件--支援跨平台作業系統
- ● 原有Opsmgr 2007 或SP1的元件
- ● 外部支援
- ● 內建支援



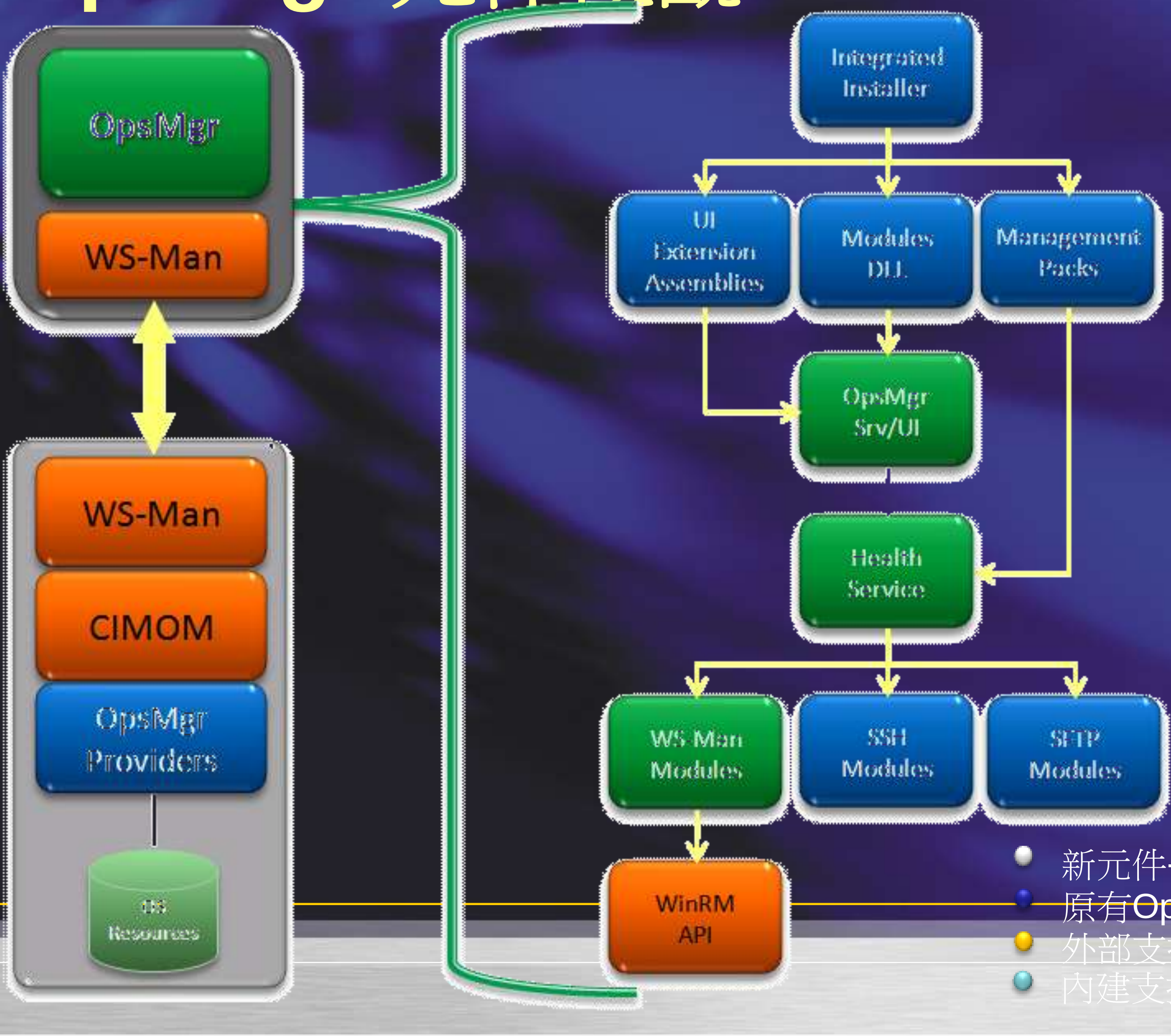
# UNIX/Linux 元件概觀



- 新元件--支援跨平台作業系統
- 原有Opsmgr 2007 或SP1的元件
- 外部支援
- 內建支援

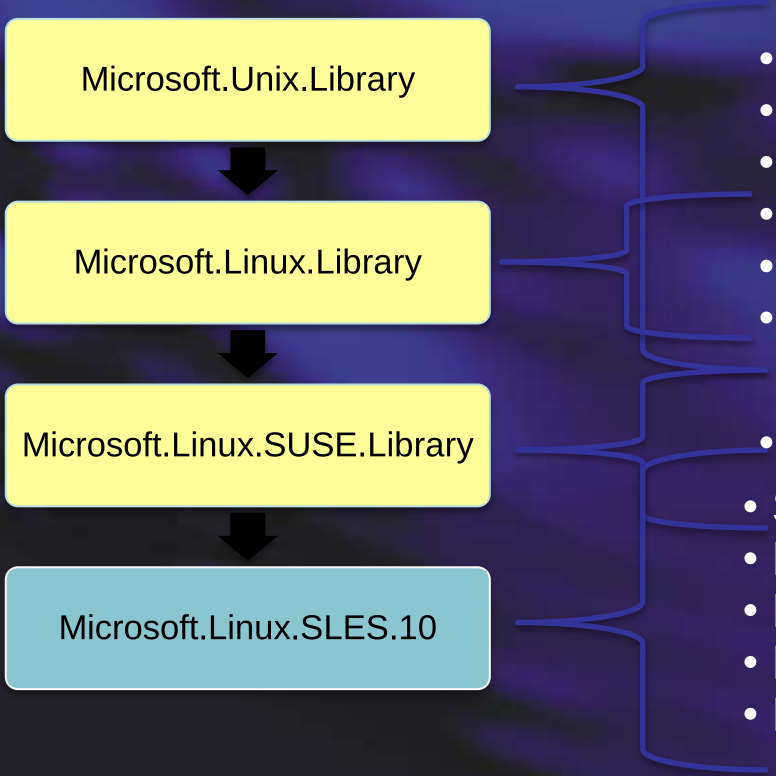
Microsoft TechNet

# Ops Mgr 元件概觀



- ⚪ 新元件--支援跨平台作業系統
- 🔵 原有Opsmgr 2007 或SP1的元件
- 🟡 外部支援
- 🟢 內建支援

# 管理套件的架構



- Unix Object Definitions
- Data Sources (WSMan/SSH/SFTP)
- Probe Actions (WSMan/SSH/SFTP)
- Write Actions (WSMan/SSH/SFTP)
- Linux Object Definitions
- Generic Monitors
- Generic Tasks

- SUSE Linux Object Definitions

- SLES 10 Object Definitions
- Monitors
- Rules
- Diagnostics/Recoveries
- Reports

● Library
● Management Pack

# Opsmgr 2007 R2支援的異質平台

- AIX
  - Version 5.3 (Power)
  - Version 6.1 (Power)
- HP-UX
  - Version 11iv2 (PA-RISC/IA64)
  - Version 11iv3 (PA-RISC/IA64)
- Red Hat Enterprise
- Solaris
  - Version 8 (SPARC)
  - Version 9 (SPARC)
  - Version 10 (SPARC/x86)
- SUSE Linux Enterprise Server
  - Version 9 (x86)
  - Version 10 SP1 (x86/x64)

# 管理套件

- Generic libraries (imported

| Name | Description |
|---|---|
| Microsoft.Unix.Library | Defines all objects, DS, WA, PA for Unix-type systems |
| Microsoft.Unix.Views | Defines all generic views used with Cross Platform |
| Microsoft.Unix.LogFile.Library | Used by Unix/Linux LogFile Management Pack Template |
| Microsoft.Unix.Service.Library | Used by Unix/Linux Service Management Pack Template |

# 管理套件

- OS Type Libraries

| Name | Description |
|---|---|
| Microsoft.AIX.Library.mp | Generic AIX Operating System Library |
| Microsoft.HPUX.Library.mp | Generic HP-UX Operating System Library |
| Microsoft.Linux.Library.mp | Generic Linux Operating System Library |
| Microsoft.Linux.RedHat.Library.mp | Generic Red Hat Operating System Library |
| Microsoft.Linux.SUSE.Library.mp | Generic SUSE Linux Operating System Library |
| Microsoft.Solaris.Library.mp | Generic Solaris Operating System Library |

# 管理套件

- Base OS Management Packs

| Name | Description |
|---|---|
| Microsoft.AIX.5.3.mp | AIX 5.3 Base OS MP |
| Microsoft.AIX.6.1.mp | AIX 6.1 Base OS MP |
| Microsoft.HPUX.11iv2.mp | HP-UX 11iv2 (11.23) Base OS MP |
| Microsoft.HPUX.11iv3.mp | HP-UX 11iv3 (11.31) Base OS MP |
| Microsoft.Linux.RHEL.4.mp | Red Hat Enterprise Linux 4 Base OS MP |
| Microsoft.Linux.RHEL.5.mp | Red Hat Enterprise Linux 5 Base OS MP |
| Microsoft.Linux.SLES.9.mp | SUSE Linux Enterprise Server 9 Base OS MP |
| Microsoft.Linux.SLES.10.mp | SUSE Linux Enterprise Server 10 Base OS MP |
| Microsoft.Solaris.8.mp | Solaris 8 Base OS MP |
| Microsoft.Solaris.9.mp | Solaris 9 Base OS MP |
| Microsoft.Solaris.10.mp | Solaris 10 Base OS MP |

# 預設管理套件支援的平台與版本

- Base OS Management Packs

| Name | Description |
|---|---|
| Microsoft.AIX.5.3.mp | AIX 5.3 Base OS MP |
| Microsoft.AIX.6.1.mp | AIX 6.1 Base OS MP |
| Microsoft.HPUX.11iv2.mp | HP-UX 11iv2 (11.23) Base OS MP |
| Microsoft.HPUX.11iv3.mp | HP-UX 11iv3 (11.31) Base OS MP |
| Microsoft.Linux.RHEL.4.mp | Red Hat Enterprise Linux 4 Base OS MP |
| Microsoft.Linux.RHEL.5.mp | Red Hat Enterprise Linux 5 Base OS MP |
| Microsoft.Linux.SLES.9.mp | SUSE Linux Enterprise Server 9 Base OS MP |
| Microsoft.Linux.SLES.10.mp | SUSE Linux Enterprise Server 10 Base OS MP |
| Microsoft.Solaris.8.mp | Solaris 8 Base OS MP |
| Microsoft.Solaris.9.mp | Solaris 9 Base OS MP |
| Microsoft.Solaris.10.mp | Solaris 10 Base OS MP |

# 跨平台管理的功能

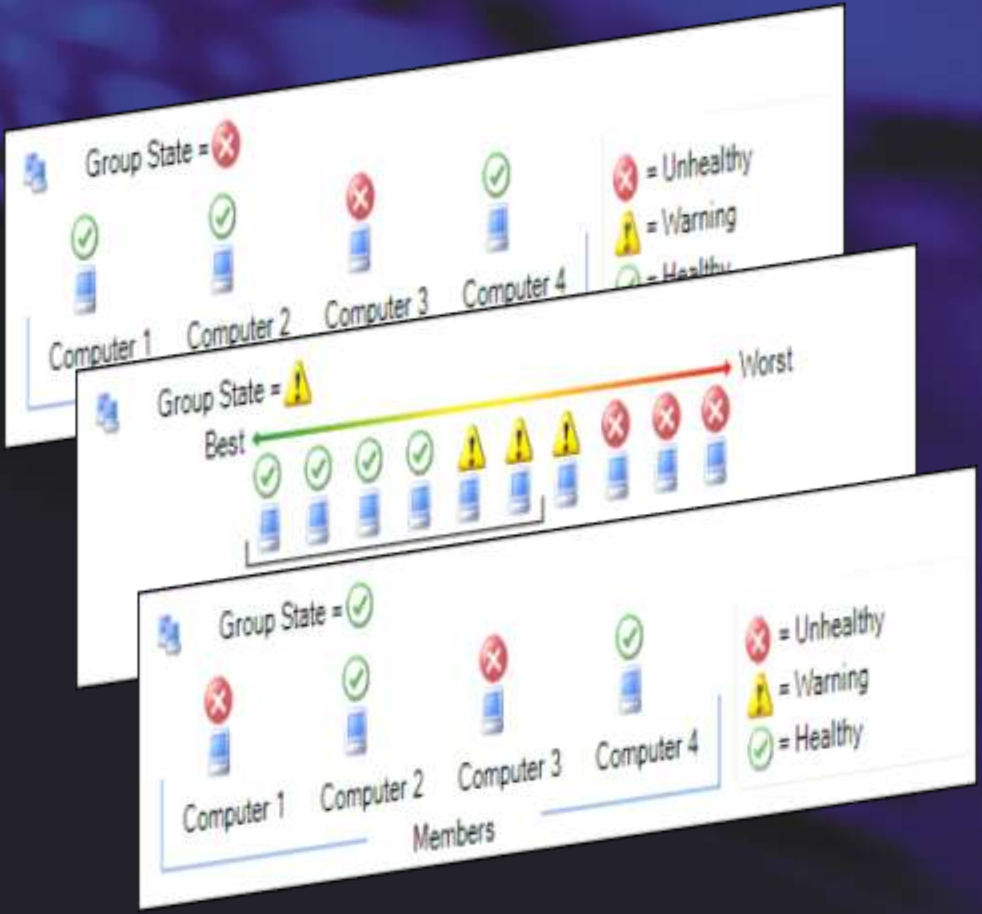
| Feature |
|---|
| Tasks that execute script on non-Windows System and return output to UI |
| Support for customized UI pages for non-Windows templates, monitors etc |
| Support for using non-Windows entities in Distributed Application Designed |
| Reports for data from non-Windows Systems and entities |
| Templates for creating custom monitoring rules and MPs |
| Agent Uninstall |
| Agent Upgrade |
| Fully data driven |

# DEMO

跨作業平台監控

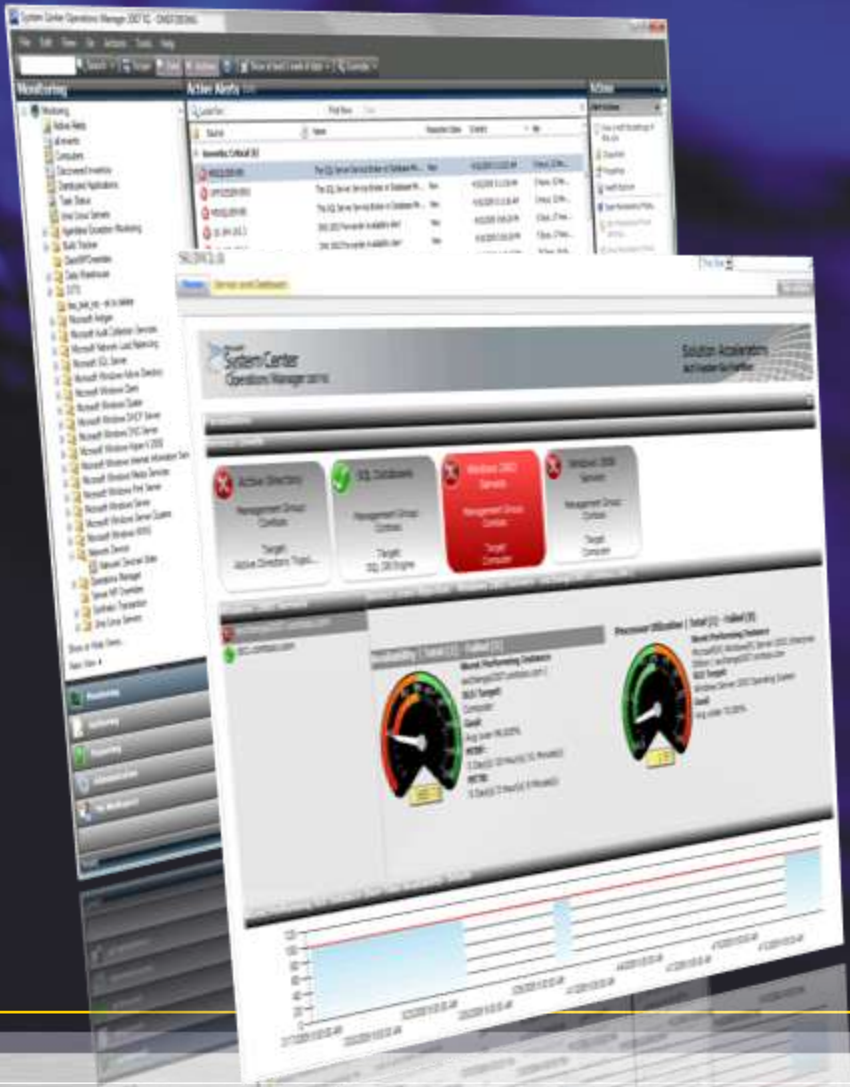
# 服務水平追蹤

# 甚麼是Service Level Tracking?



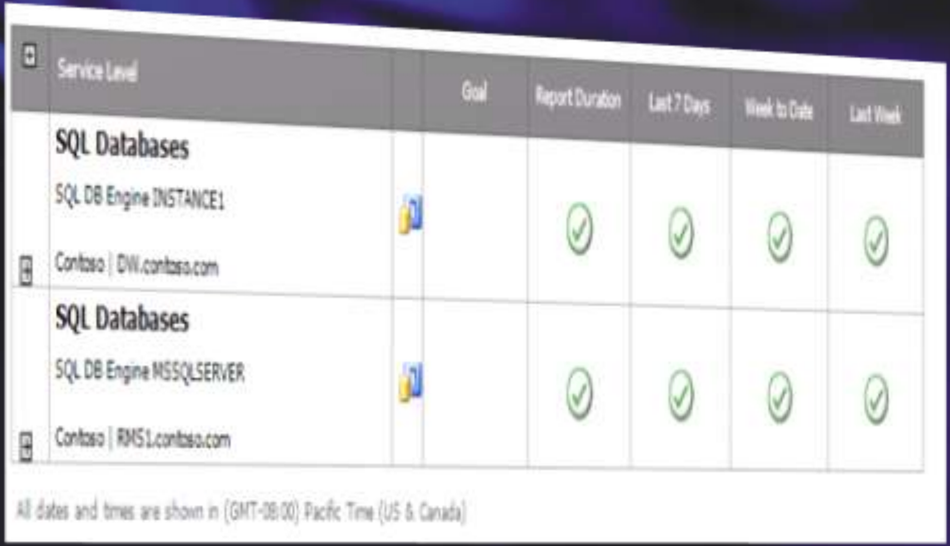
- Opsmgr 2007 R2 內建的功能
- 紀錄服務的水平
- 以”服務”為紀錄目標

# 甚麼是Service Level Tracking?



- 容易閱讀
- 容易產出
- 結合System Center

# Service Level 追蹤

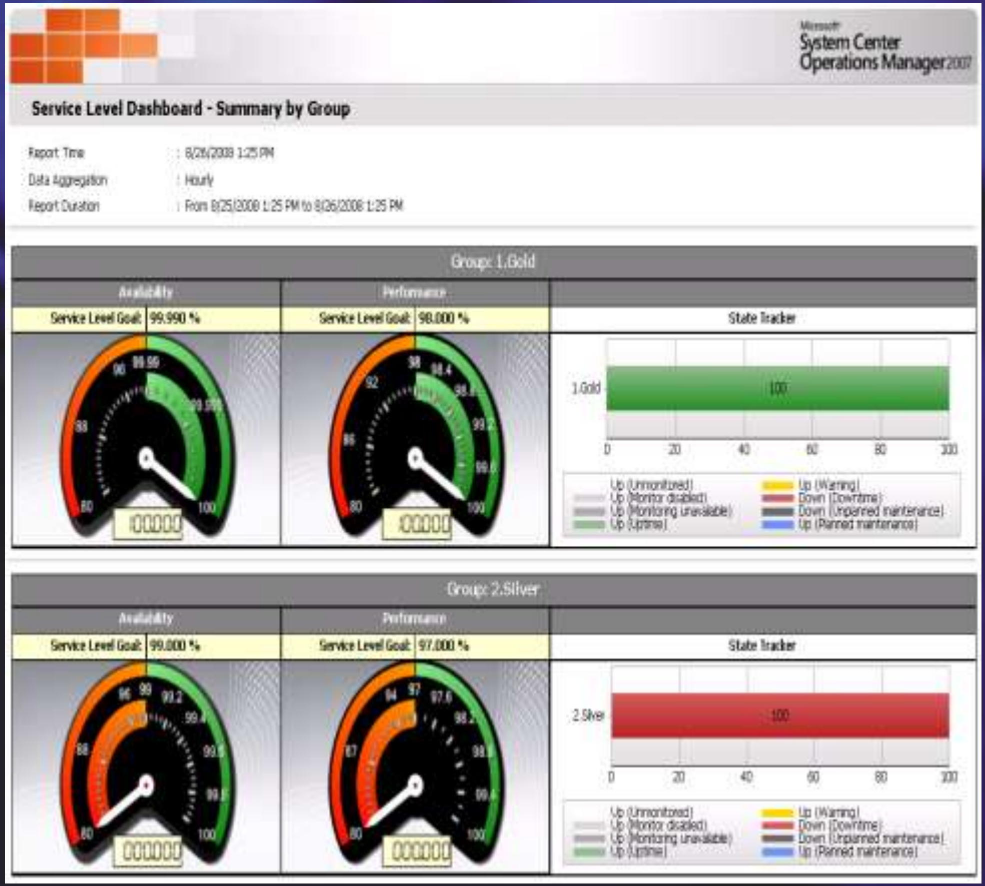


| Service Level | | Goal | Report Duration | Last 7 Days | Week to Date | Last Week |
|---|---|---|---|---|---|---|
| **SQL Databases**<br>SQL DB Engine INSTANCE1<br>Contoso \| DW.contoso.com | | | ✓ | ✓ | ✓ | ✓ |
| **SQL Databases**<br>SQL DB Engine MSSQLSERVER<br>Contoso \| RMS1.contoso.com | | | ✓ | ✓ | ✓ | ✓ |

All dates and times are shown in (GMT-08:00) Pacific Time (US & Canada)

- 支援SQL 報表服務，定期產出報表
- Service Level 是IT服務的關鍵

# Service Level 追蹤



Microsoft System Center Operations Manager 2007

Service Level Dashboard - Summary by Group

Report Time : 8/26/2008 1:25 PM

Data Aggregation : Hourly

Report Duration : From 8/25/2008 1:25 PM to 8/26/2008 1:25 PM

Group: 1.Gold

| Availability | | Performance | | |
|---|---|---|---|---|
| Service Level Goal: | 99.990 % | Service Level Goal: | 98.000 % | State Tracker |

Group: 2.Silver

| Availability | | Performance | | |
|---|---|---|---|---|
| Service Level Goal: | 99.000 % | Service Level Goal: | 97.000 % | State Tracker |

- 儀表板與報表呈現目前的服務水平與預期達到的目標
- 定期產出報表，定期審視
- 支援MOSS Web part

# DEMO

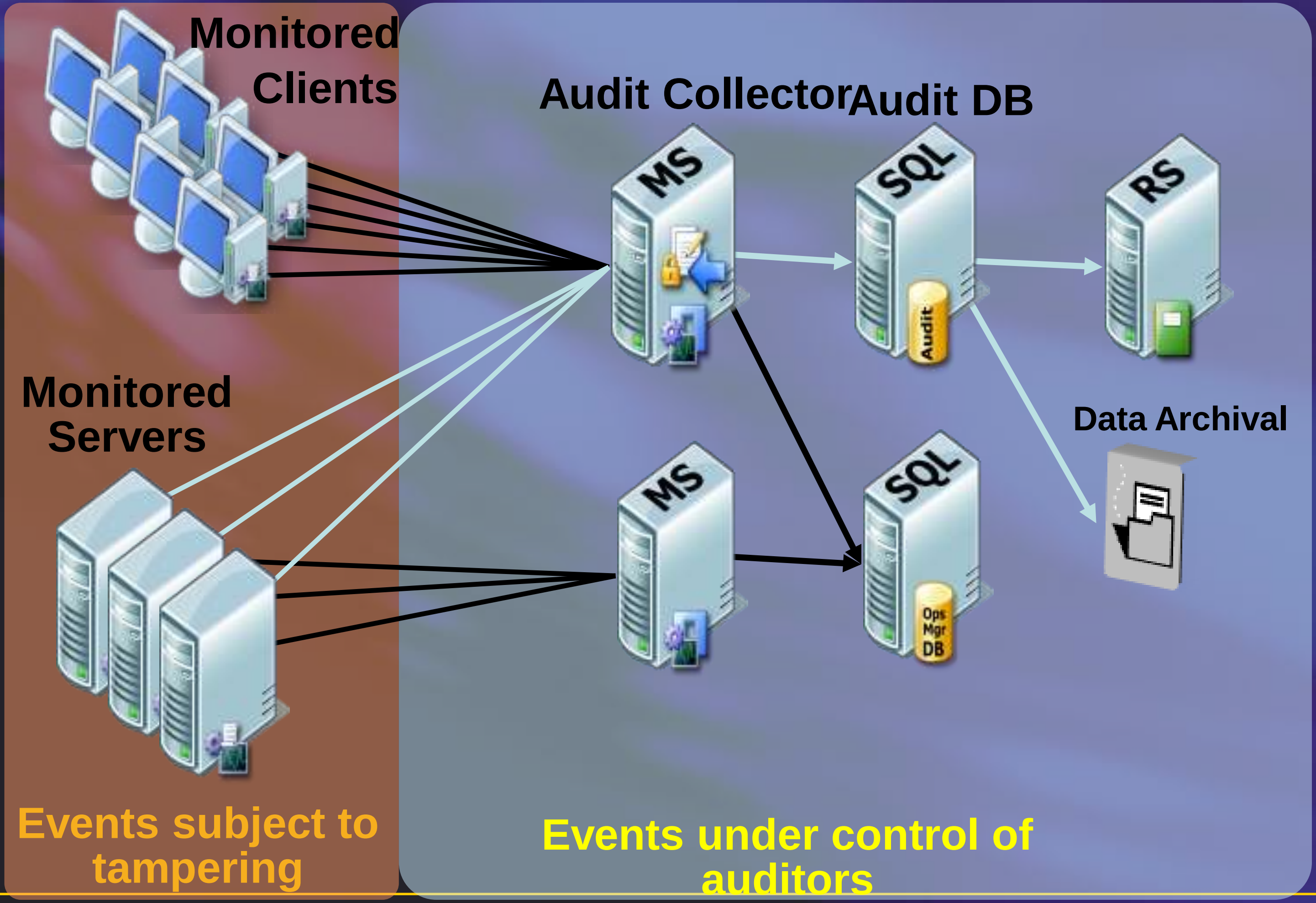
設定服務水平追蹤

# 存取稽核與報表審視

# ACS 基本原理

- 主要設計的原理:
  - 接近即時的匯出安全存取稽核
  - 一致的蒐集原則
  - 減少網路負擔—壓縮、輕量
  - 可延伸架構
  - 效率

# ACS 架構


Monitored Clients
Audit Collector
Audit DB
MS
SQL
RS
Audit
Monitored Servers
Data Archival
MS
SQL
Ops Mgr DB
Events subject to tampering
Events under control of auditors

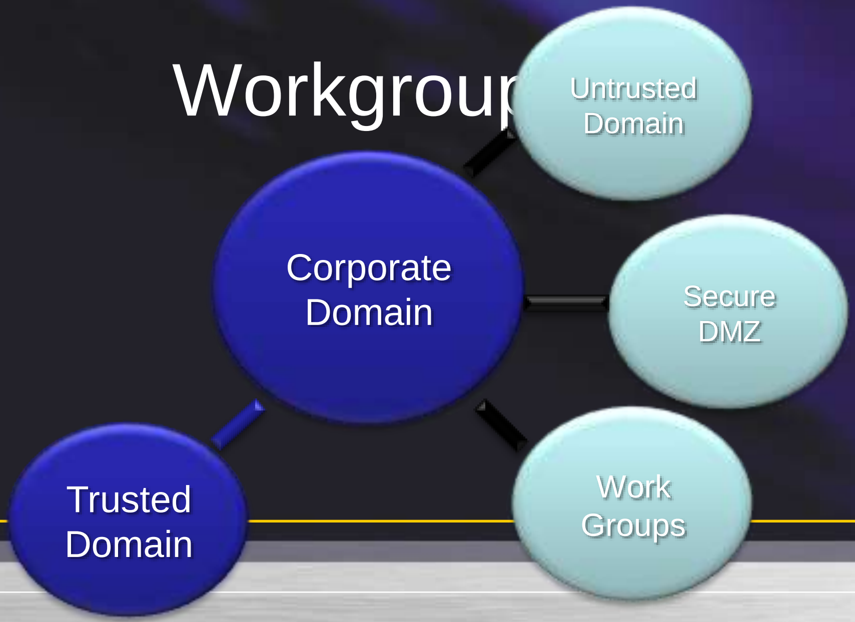
# ACS 主要元件

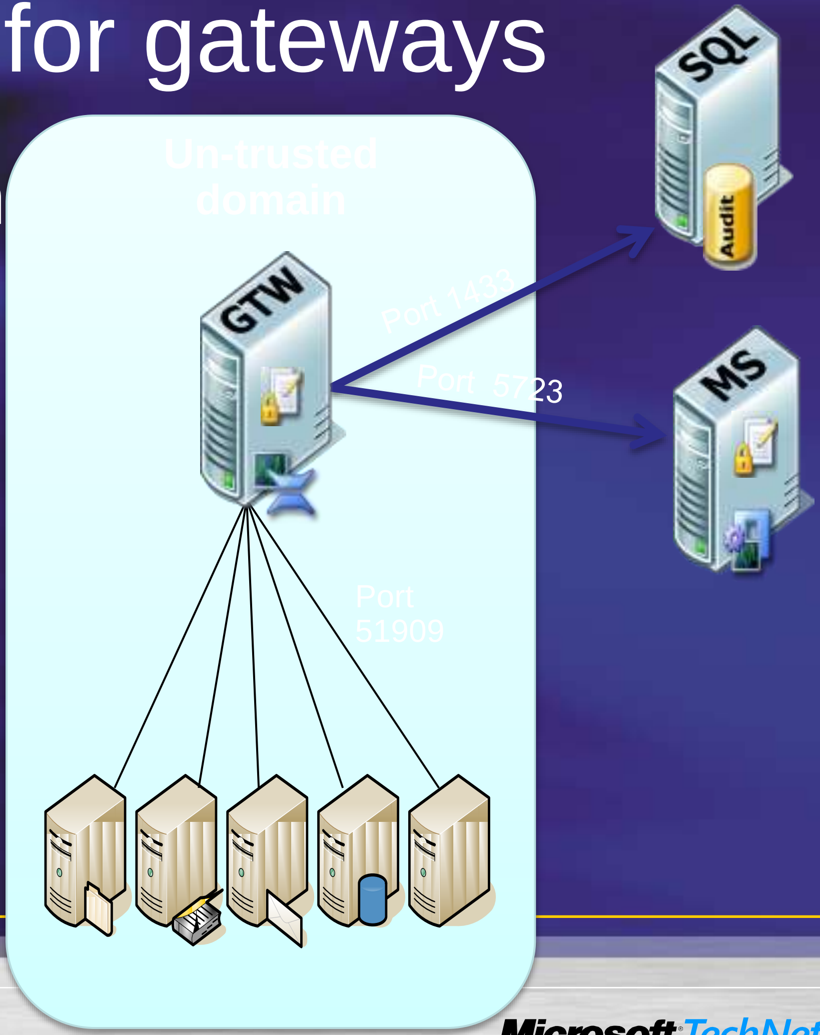
| Roles | Description | Requirements | Security |
|---|---|---|---|
| Forwarder | 蒐集本機的安全事件，即時轉送到 Collector Server | • Windows XP<br>• Win2000 w/SP4<br>• Win2003<br>• Vista<br>• Win2008 | • SLDC compression<br>• 128-bit RC4 encryption<br>• Kerberos if domain-joined<br>• TLS/SSL with certificates<br>• Port 51909 to Collector<br>• Default Network Service Acct. |
| Collector | Collector 負責處裡從Forwarder轉送過來的安全事件，，事件經過濾篩選，儲存在稽核資料庫中 | • Windows Server 2003 or 2008 | • TLS/SSL between Collector & Audit database<br>• Port 1433 inbound to Audit Database |
| Audit Database | Audit database負責集中儲存Collector送進來的事件紀錄，每個Collector 對應一個Audit Database。 | • Windows Server 2003 or 2008<br>• SQL Server 2005 Standard with SP1<br>• *SQL Enterprise and SP2 recommended* | • SQL Security or Windows Integrated Security<br>• End users require db_datareader rights only |
| Report Server | Reporting Server 可以與Audit Database安裝在同一部伺服器，但是為效能考量，建議安裝在獨立伺服器。 | | • SCOM Reporting<br>• SQL 2005 SSRS |

Operations Manager 2007 Supported Configurations
http://technet.microsoft.com/en-us/library/bb309428.aspx

# ACS and Gateways

- Common scenarios for gateways
  - Untrusted forest or dom
  - Secure DMZ
  - Workgrou



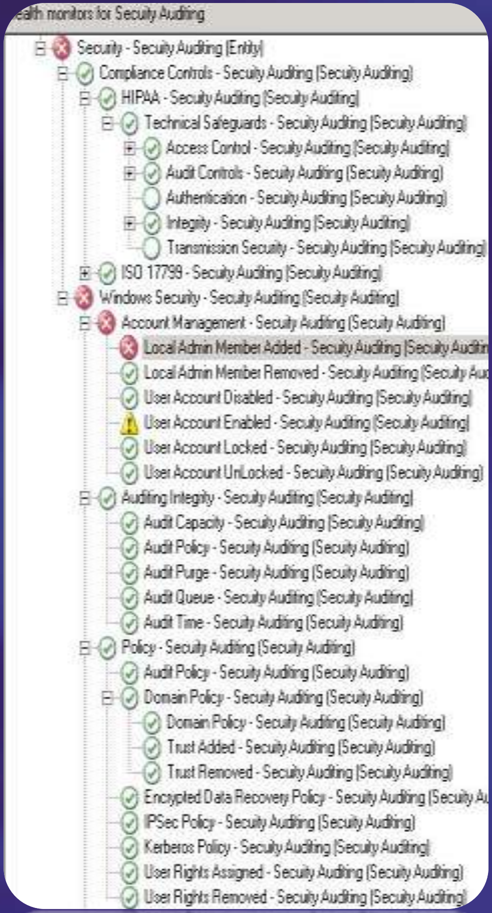


# Security Management

- 反映每天的資安狀態
- 管理套件提供

  監控, 管理原則, 檢視 ..

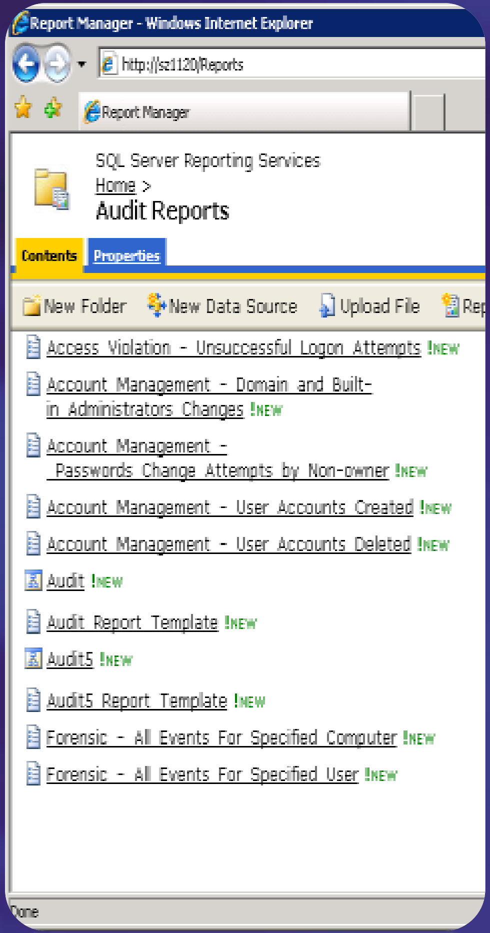
  通知
- 可自行開發管理套件，或是套用協力廠商的現有的支援
- 可從微軟網站下載: Windows Server稽核管理套件



```
ealth monitors for Security Auditing
⊟ ✗ Security - Security Auditing [Entity]
   ⊟ ✓ Compliance Controls - Security Auditing [Security Auditing]
      ⊟ ✓ HIPAA - Security Auditing [Security Auditing]
         ⊟ ✓ Technical Safeguards - Security Auditing [Security Auditing]
            ⊞ ✓ Access Control - Security Auditing [Security Auditing]
            ⊞ ✓ Audit Controls - Security Auditing [Security Auditing]
               ○ Authentication - Security Auditing [Security Auditing]
            ⊞ ✓ Integrity - Security Auditing [Security Auditing]
               ○ Transmission Security - Security Auditing [Security Auditing]
      ⊞ ✓ ISO 17799 - Security Auditing [Security Auditing]
   ⊟ ✗ Windows Security - Security Auditing [Security Auditing]
      ⊟ ✗ Account Management - Security Auditing [Security Auditing]
            ✗ Local Admin Member Added - Security Auditing [Security Auditin
            ✓ Local Admin Member Removed - Security Auditing [Security Au
            ✓ User Account Disabled - Security Auditing [Security Auditing]
            ⚠ User Account Enabled - Security Auditing [Security Auditing]
            ✓ User Account Locked - Security Auditing [Security Auditing]
            ✓ User Account UnLocked - Security Auditing [Security Auditing]
      ⊟ ✓ Auditing Integrity - Security Auditing [Security Auditing]
            ✓ Audit Capacity - Security Auditing [Security Auditing]
            ✓ Audit Policy - Security Auditing [Security Auditing]
            ✓ Audit Purge - Security Auditing [Security Auditing]
            ✓ Audit Queue - Security Auditing [Security Auditing]
            ✓ Audit Time - Security Auditing [Security Auditing]
      ⊟ ✓ Policy - Security Auditing [Security Auditing]
            ✓ Audit Policy - Security Auditing [Security Auditing]
         ⊟ ✓ Domain Policy - Security Auditing [Security Auditing]
               ✓ Domain Policy - Security Auditing [Security Auditing]
               ✓ Trust Added - Security Auditing [Security Auditing]
               ✓ Trust Removed - Security Auditing [Security Auditing]
            ✓ Encrypted Data Recovery Policy - Security Auditing [Security Au
            ✓ IPSec Policy - Security Auditing [Security Auditing]
            ✓ Kerberos Policy - Security Auditing [Security Auditing]
            ✓ User Rights Assigned - Security Auditing [Security Auditing]
            ✓ User Rights Removed - Security Auditing [Security Auditing]
```

# 安全稽核

- 存取稽核的歷史紀錄報表
- 存取行為分析
- 報表提供:
  - 內建可立即套用的表物件
  - 協力廠商加值報表
- Osmgr 2007 R2內建報表



SQL Server Reporting Services
Home >
Audit Reports

- Access Violation - Unsuccessful Logon Attempts !NEW
- Account Management - Domain and Built-in Administrators Changes !NEW
- Account Management - Passwords Change Attempts by Non-owner !NEW
- Account Management - User Accounts Created !NEW
- Account Management - User Accounts Deleted !NEW
- Audit !NEW
- Audit Report Template !NEW
- Audit5 !NEW
- Audit5 Report Template !NEW
- Forensic - All Events For Specified Computer !NEW
- Forensic - All Events For Specified User !NEW

# ACS 預設報表物件

- Forensic_-_All_Events_For_Specified_User.rdl
- Forensic_-_All_Events_With_Specified_Event_ID.rdl
- Planning_-_Event_Counts.rdl
- Planning_-_Event_Counts_by_Computer.rdl
- Planning_-_Hourly_Event_Distribution.rdl
- Planning_-_Logon_Counts_of_Privileged_Users.rdl
- Policy_-_Account_Policy_Changed.rdl
- Policy_-_Audit_Policy_Changed.rdl
- Policy_-_Object_Permissions_Changed.rdl
- Policy_-_Privilege_Added_Or_Removed.rdl
- System_Integrity_-_Audit_Failure.rdl
- System_Integrity_-_Audit_Log_Cleared.rdl
- Usage_-_Object_Access.rdl
- Usage_-_Privileged_logon.rdl
- Usage_-_Sensitive_Security_Groups_Changes.rdl
- Usage_-_User_Logon.rdl
- Access_Violation_-_Account_Locked.rdl
- Access_Violation_-_Unsuccessful_Logon_Attempts.rdl
- Account_Management_-_Domain_and_Built-in_Administrators_Changes.rdl
- Account_Management_-_Passwords_Change_Attempts_by_Non-owner.rdl
- Account_Management_-_User_Accounts_Created.rdl
- Account_Management_-_User_Accounts_Deleted.rdl
- Audit_Report_Template.rdl
- Audit5_Report_Template.rdl
- Forensic_-_All_Events_For_Specified_Computer.rdl

# 稽核規劃

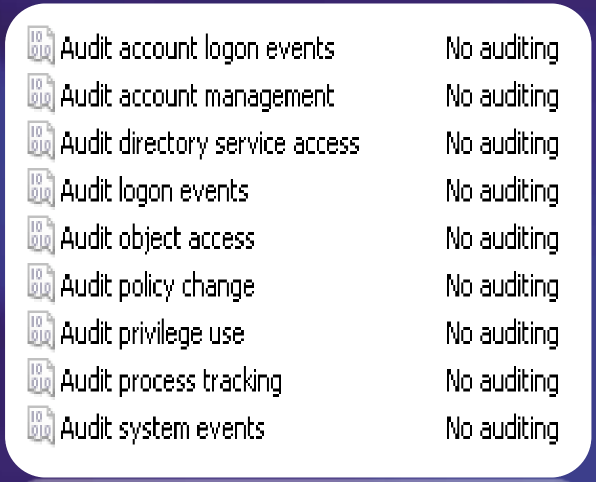
- 制定一致性的稽核政策

決定應該要稽核甚麼

定義可以得到哪些資訊

制定稽核原則與存取控制

蒐集、觸發與分析



| | |
|---|---|
| Audit account logon events | No auditing |
| Audit account management | No auditing |
| Audit directory service access | No auditing |
| Audit logon events | No auditing |
| Audit object access | No auditing |
| Audit policy change | No auditing |
| Audit privilege use | No auditing |
| Audit process tracking | No auditing |
| Audit system events | No auditing |

# 容量規劃

- **Log and Database Drives**

[Average number of disk I/O per event for (transaction log or database file)] *

[Events per second for all computers] * [disk RPM] * 60 sec/minute =

[number of required drives] * 2 (for RAID 1)

| Variable | Value |
|---|---|
| Average number of logical disk I/O per event for transaction log | 1.384 |
| Average number of logical disk I/O per event for database file | 0.138 |
| Events per second for all computers | Estimated by using the script and the To estimate the number of events per second for all computers procedure |
| Disk RPM | Varies, determined by disk device |

# 容量規畫的小訣竅

- Use SQL enterprise
- Document every aspect of your ‘solution’
- Collector ‘load’ will decrease when using “noise filters”
- Separate SQL reporting services server or not?
- Server configuration
    - Use 64-bit
    - Use dedicated hardware / management server
    - Plan your disks for the ACS database

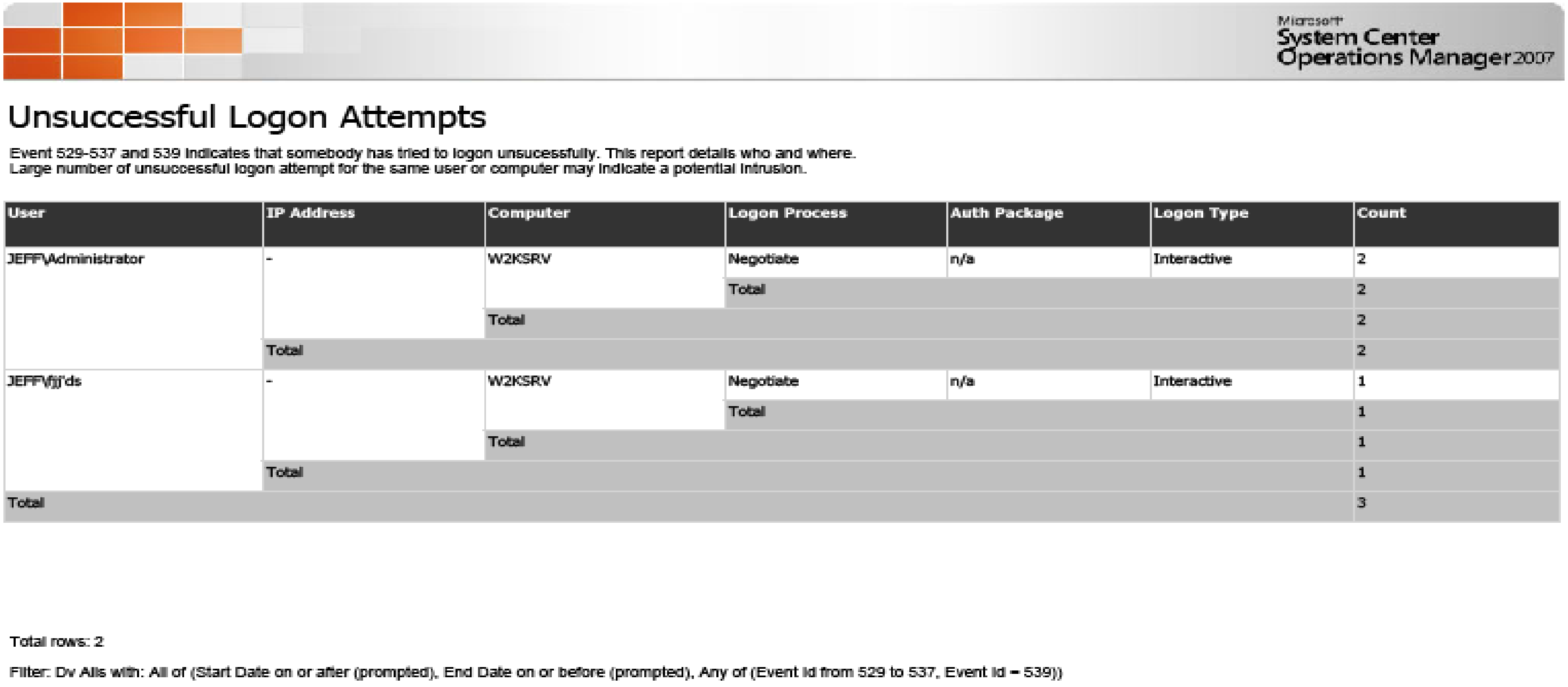
# 強化Opsmgr 2007 R2

- Support for Windows Server 2008 and Windows Server 2008 R2
- New Windows Server 2008 and Windows Server 2008 R2 integrated ACS reports
- Improved report performance
- New multi-staged indexing design that further enhance robustness and performance
- Support for Cross Platform by CY 2H09

# DEMO

稽核報表範本

# 嘗試登入稽核報表



Microsoft System Center Operations Manager 2007

## Unsuccessful Logon Attempts

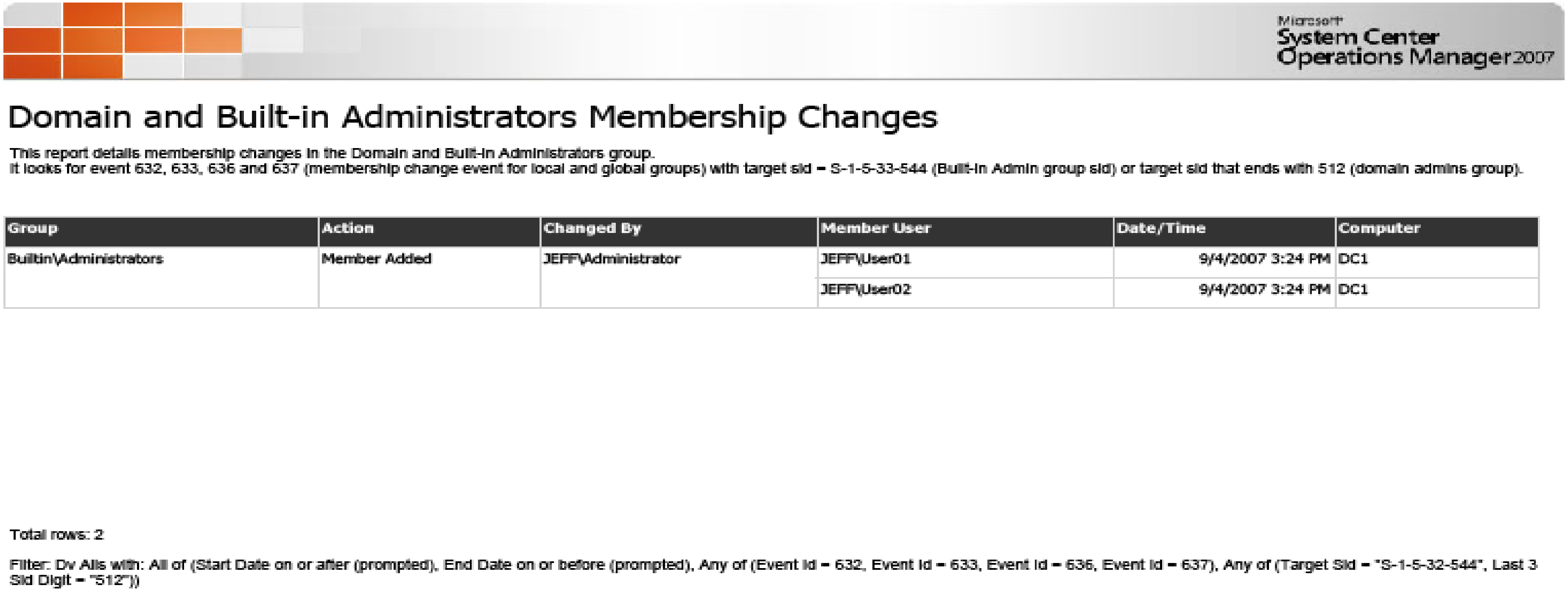
Event 529-537 and 539 indicates that somebody has tried to logon unsucessfully. This report details who and where.
Large number of unsuccessful logon attempt for the same user or computer may indicate a potential intrusion.

| User | IP Address | Computer | Logon Process | Auth Package | Logon Type | Count |
|---|---|---|---|---|---|---|
| JEFF\Administrator | - | W2KSRV | Negotiate | n/a | Interactive | 2 |
| | | | Total | | | 2 |
| | | Total | | | | 2 |
| | Total | | | | | 2 |
| JEFF\fjj'ds | - | W2KSRV | Negotiate | n/a | Interactive | 1 |
| | | | Total | | | 1 |
| | | Total | | | | 1 |
| | Total | | | | | 1 |
| Total | | | | | | 3 |

Total rows: 2

Filter: Dv Alls with: All of (Start Date on or after (prompted), End Date on or before (prompted), Any of (Event Id from 529 to 537, Event Id = 539))

# 帳戶管理: 網域管理者關係異動



## Domain and Built-in Administrators Membership Changes

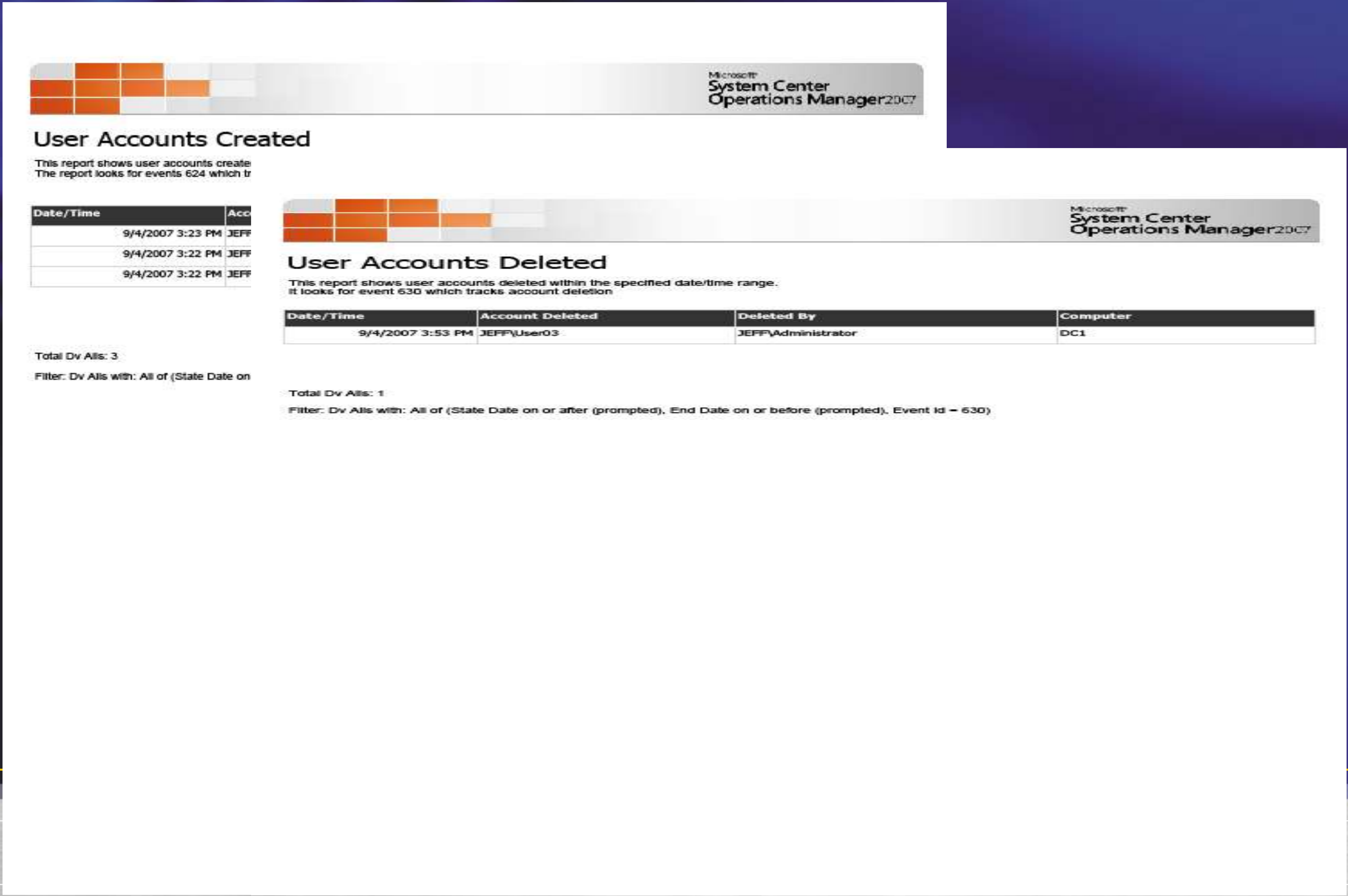
This report details membership changes in the Domain and Built-in Administrators group.
It looks for event 632, 633, 636 and 637 (membership change event for local and global groups) with target sid = S-1-5-33-544 (Built-in Admin group sid) or target sid that ends with 512 (domain admins group).

| Group | Action | Changed By | Member User | Date/Time | Computer |
|---|---|---|---|---|---|
| Builtin\Administrators | Member Added | JEFF\Administrator | JEFF\User01 | 9/4/2007 3:24 PM | DC1 |
| | | | JEFF\User02 | 9/4/2007 3:24 PM | DC1 |

Total rows: 2

Filter: Dv Alis with: All of (Start Date on or after (prompted), End Date on or before (prompted), Any of (Event Id = 632, Event Id = 633, Event Id = 636, Event Id = 637), Any of (Target Sid = "S-1-5-32-544", Last 3 Sid Digit = "512"))

# 帳戶管理: 帳號新增與刪除



## User Accounts Created

This report shows user accounts create
The report looks for events 624 which tr

| Date/Time | Acc |
|---|---|
| 9/4/2007 3:23 PM | JEFF |
| 9/4/2007 3:22 PM | JEFF |
| 9/4/2007 3:22 PM | JEFF |

Total Dv Alls: 3

Filter: Dv Alls with: All of (State Date on

## User Accounts Deleted

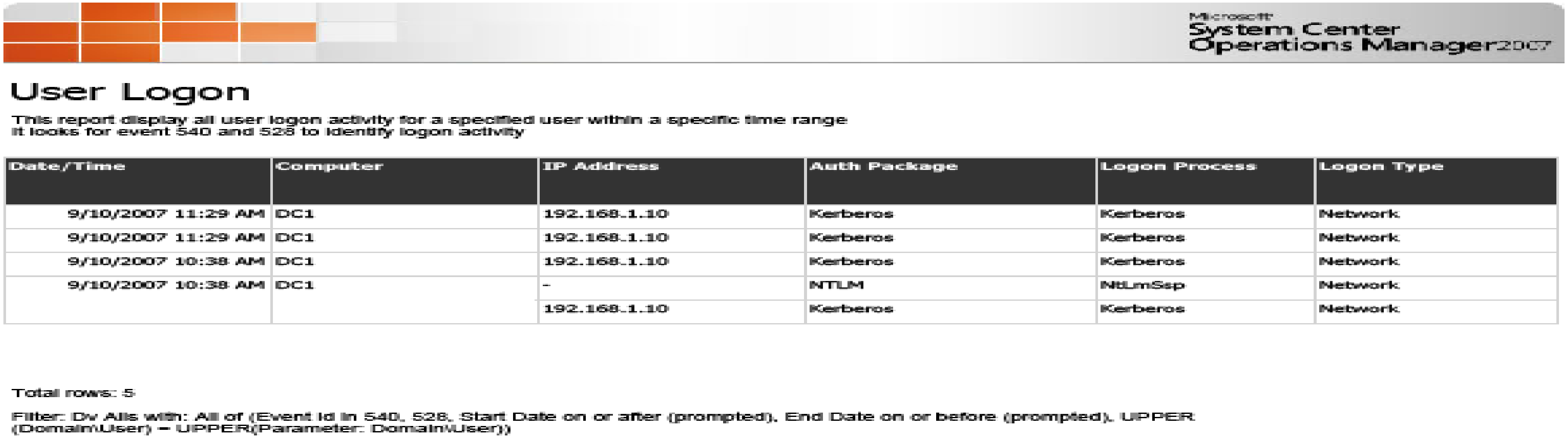
This report shows user accounts deleted within the specified date/time range.
It looks for event 630 which tracks account deletion

| Date/Time | Account Deleted | Deleted By | Computer |
|---|---|---|---|
| 9/4/2007 3:53 PM | JEFF\User03 | JEFF\Administrator | DC1 |

Total Dv Alls: 1

Filter: Dv Alls with: All of (State Date on or after (prompted), End Date on or before (prompted), Event Id = 630)

# 使用者登入狀態



## User Logon

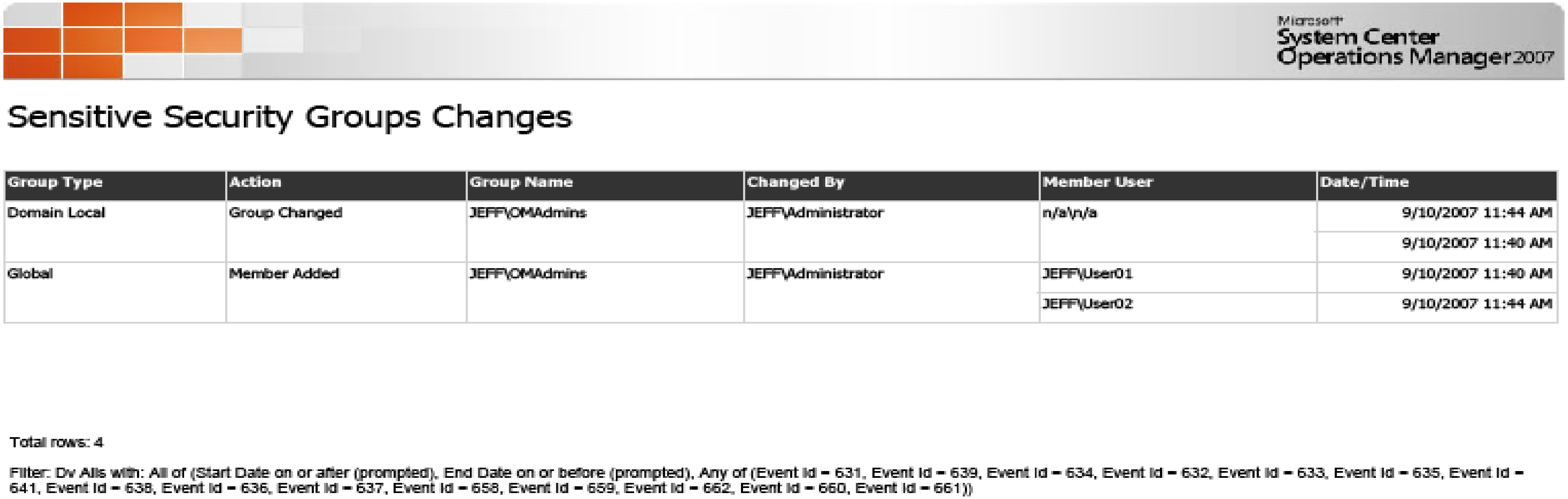
This report display all user logon activity for a specified user within a specific time range
It looks for event 540 and 528 to identify logon activity

| Date/Time | Computer | IP Address | Auth Package | Logon Process | Logon Type |
|---|---|---|---|---|---|
| 9/10/2007 11:29 AM | DC1 | 192.168.1.10 | Kerberos | Kerberos | Network |
| 9/10/2007 11:29 AM | DC1 | 192.168.1.10 | Kerberos | Kerberos | Network |
| 9/10/2007 10:38 AM | DC1 | 192.168.1.10 | Kerberos | Kerberos | Network |
| 9/10/2007 10:38 AM | DC1 | - | NTLM | NtLmSsp | Network |
| | | 192.168.1.10 | Kerberos | Kerberos | Network |

Total rows: 5

Filter: Dv Alls with: All of (Event Id in 540, 528, Start Date on or after (prompted), End Date on or before (prompted), UPPER (Domain\User) = UPPER(Parameter: Domain\User))

# 特殊群組關係異動



Microsoft System Center Operations Manager 2007

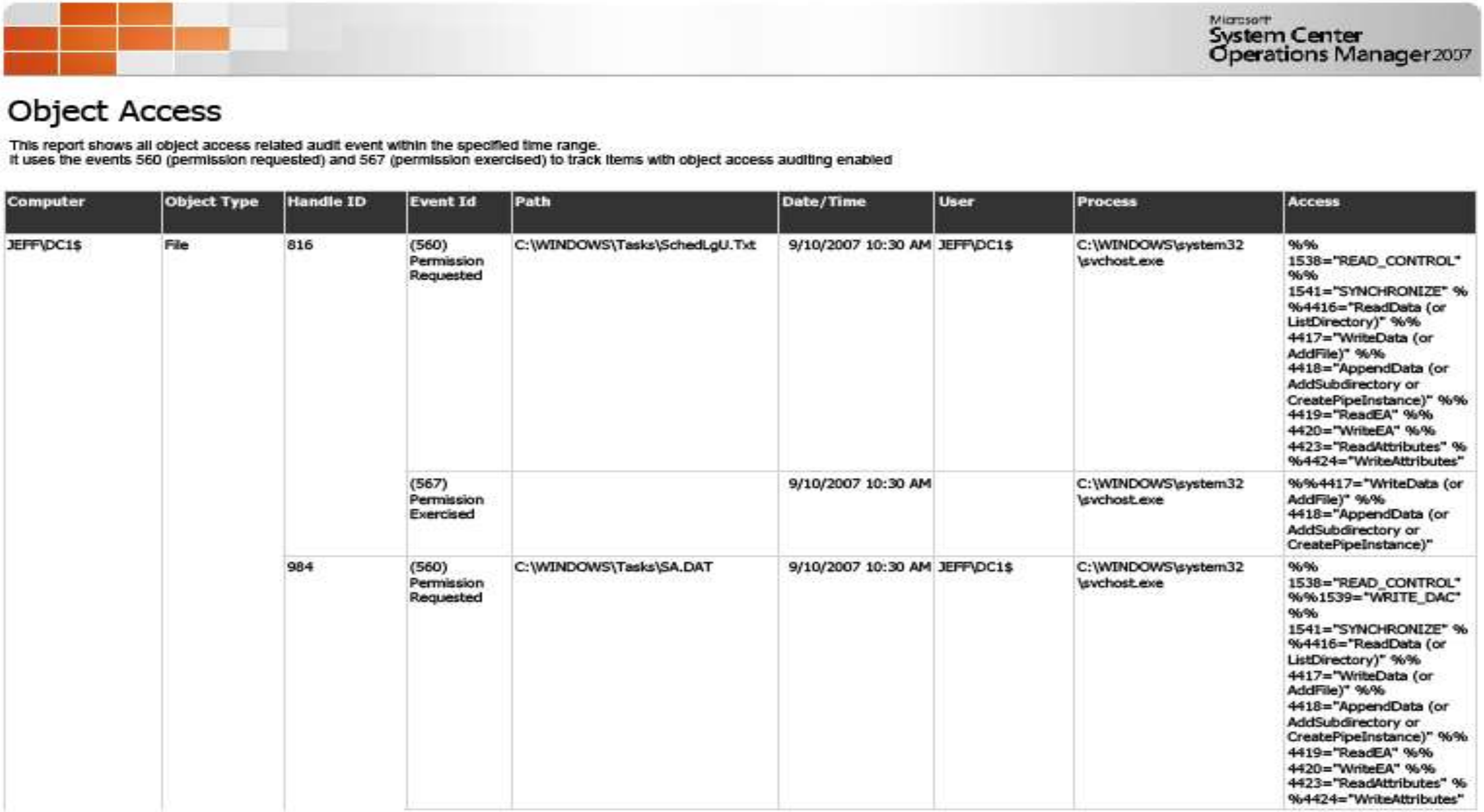
## Sensitive Security Groups Changes

| Group Type | Action | Group Name | Changed By | Member User | Date/Time |
|---|---|---|---|---|---|
| Domain Local | Group Changed | JEFF\OMAdmins | JEFF\Administrator | n/a\n/a | 9/10/2007 11:44 AM |
| | | | | | 9/10/2007 11:40 AM |
| Global | Member Added | JEFF\OMAdmins | JEFF\Administrator | JEFF\User01 | 9/10/2007 11:40 AM |
| | | | | JEFF\User02 | 9/10/2007 11:44 AM |

Total rows: 4

Filter: Dv Alls with: All of (Start Date on or after (prompted), End Date on or before (prompted), Any of (Event Id = 631, Event Id = 639, Event Id = 634, Event Id = 632, Event Id = 633, Event Id = 635, Event Id = 641, Event Id = 638, Event Id = 636, Event Id = 637, Event Id = 658, Event Id = 659, Event Id = 662, Event Id = 660, Event Id = 661))

# 物件存取稽核記錄



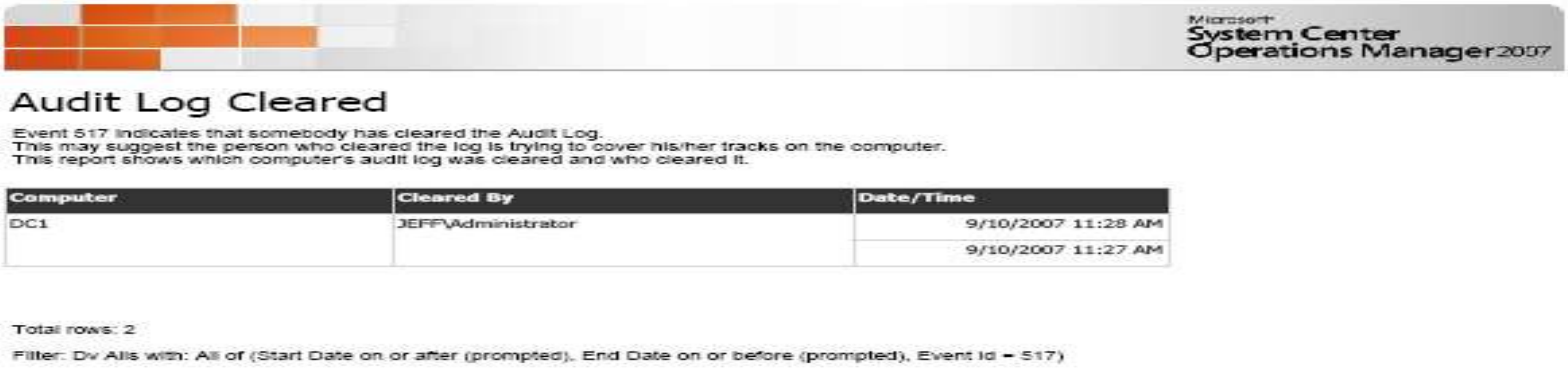
Microsoft System Center Operations Manager 2007

## Object Access

This report shows all object access related audit event within the specified time range.
It uses the events 560 (permission requested) and 567 (permission exercised) to track items with object access auditing enabled

| Computer | Object Type | Handle ID | Event Id | Path | Date/Time | User | Process | Access |
|---|---|---|---|---|---|---|---|---|
| JEFF\DC1$ | File | 816 | (560) Permission Requested | C:\WINDOWS\Tasks\SchedLgU.Txt | 9/10/2007 10:30 AM | JEFF\DC1$ | C:\WINDOWS\system32 \svchost.exe | %%1538="READ_CONTROL" %%1541="SYNCHRONIZE" %%4416="ReadData (or ListDirectory)" %%4417="WriteData (or AddFile)" %%4418="AppendData (or AddSubdirectory or CreatePipeInstance)" %%4419="ReadEA" %%4420="WriteEA" %%4423="ReadAttributes" %%4424="WriteAttributes" |
| | | | (567) Permission Exercised | | 9/10/2007 10:30 AM | | C:\WINDOWS\system32 \svchost.exe | %%4417="WriteData (or AddFile)" %%4418="AppendData (or AddSubdirectory or CreatePipeInstance)" |
| | | 984 | (560) Permission Requested | C:\WINDOWS\Tasks\SA.DAT | 9/10/2007 10:30 AM | JEFF\DC1$ | C:\WINDOWS\system32 \svchost.exe | %%1538="READ_CONTROL" %%1539="WRITE_DAC" %%1541="SYNCHRONIZE" %%4416="ReadData (or ListDirectory)" %%4417="WriteData (or AddFile)" %%4418="AppendData (or AddSubdirectory or CreatePipeInstance)" %%4419="ReadEA" %%4420="WriteEA" %%4423="ReadAttributes" %%4424="WriteAttributes" |

# 安全稽核清除記錄



Microsoft System Center Operations Manager 2007

## Audit Log Cleared

Event 517 indicates that somebody has cleared the Audit Log.
This may suggest the person who cleared the log is trying to cover his/her tracks on the computer.
This report shows which computer's audit log was cleared and who cleared it.

| Computer | Cleared By | Date/Time |
|---|---|---|
| DC1 | JEFF\Administrator | 9/10/2007 11:28 AM |
| | | 9/10/2007 11:27 AM |

Total rows: 2

Filter: Dv Alls with: All of (Start Date on or after (prompted), End Date on or before (prompted), Event Id = 517)

# 在何處取得 TechNet 相關資訊？

- 訂閱 **TechNet** 資訊技術人快訊 http://www.microsoft.com/taiwan/technet/flash/
- 訂閱 **TechNet Plus**

http://www.microsoft.com/taiwan/technet/

- 參加 **TechNet** 的活動 http://www.microsoft.com/taiwan/technet/
- 下載 **TechNet** 研討會簡報與錄影檔 http://www.microsoft.com/taiwan/technet/webcast/

Your potential. Our passion.™