高穩定、高效能、高安全資料庫系統

SQL Server 2008資料庫管理體驗營(1)

陳俊宇 http://sharedderrick.blogspot.com/

精誠公司 恆逸資訊

Microsoft® SQL Server™ 2008

討論主題

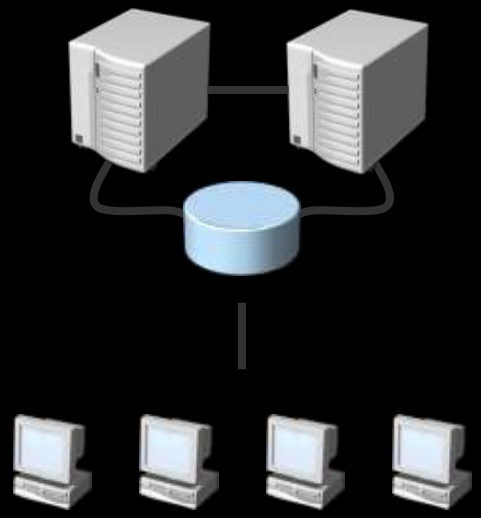
- 營運持續管理
- 提昇資料安全性，降低支出成本
- 降低儲存成本

營運持續管理

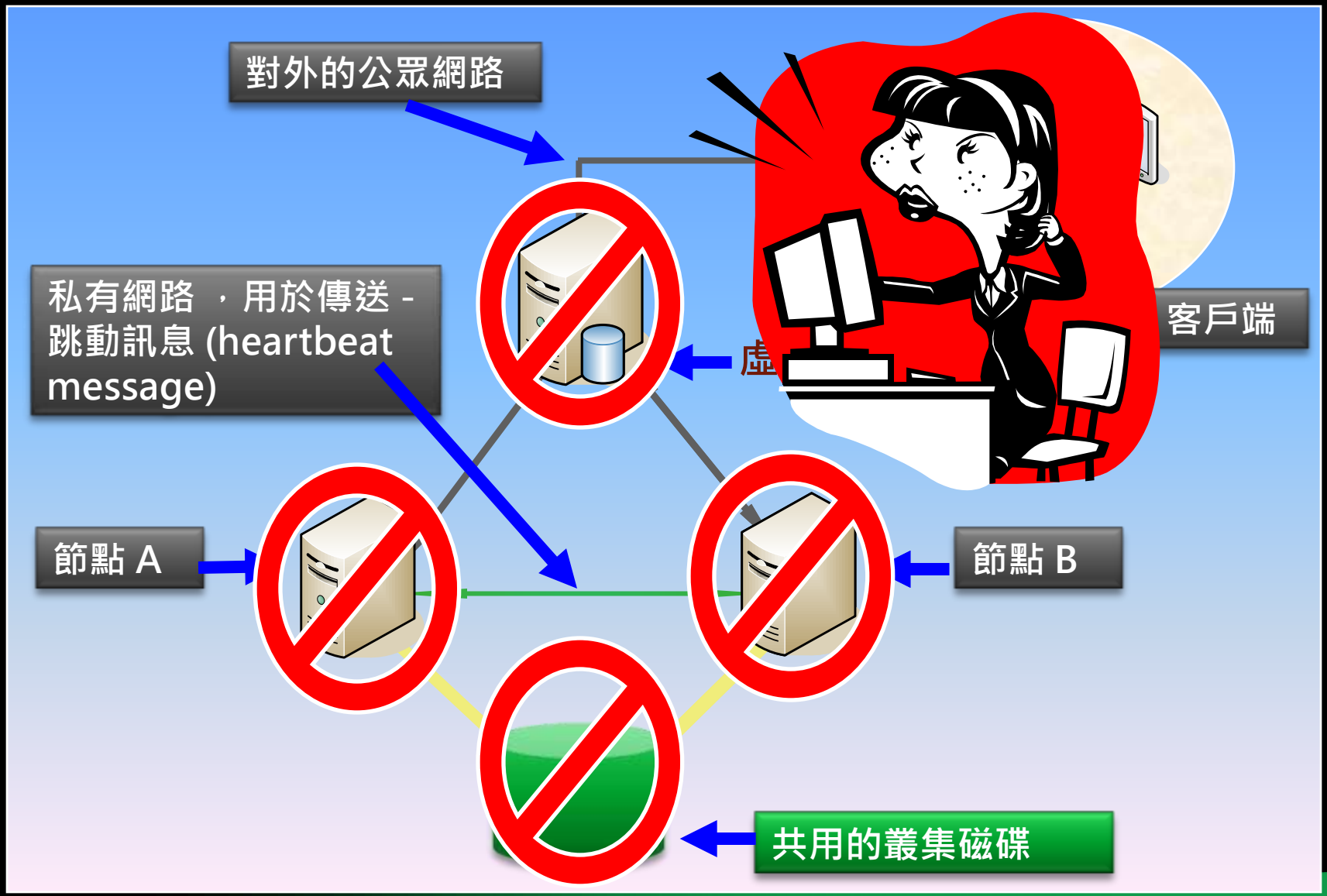
容錯移轉叢集
資料庫鏡像
點對點複寫
記錄傳送
線上索引作業與線上還原
熱新增 CPU與熱新增記憶體

容錯移轉叢集(1)

- 容錯移轉叢集(Failover Clustering)
  - 提供熱備援(Hot Standby)機制
  - 防護各個節點伺服器
  - 不會有已完成認可(Commit)資料的損失
  - 支援版本：SQL Server 2008 Standard、Enterprise Edition
- 整合Windows Server 2008叢集伺服器功能
  - 更簡易的叢集伺服器設定工具
  - 支援 16 個節點
  - 支援SAS、iSCSI、FC
  - 支援 GUID 磁碟分割表(GPT)的磁碟
  - 叢集仲裁(Cluster Quorum)的改善
    - 包含整個叢集組態設定
    - 利用多數節點集合或複合多數節點集合與仲裁資源模式設定叢集
    - 不會成為單一點故障

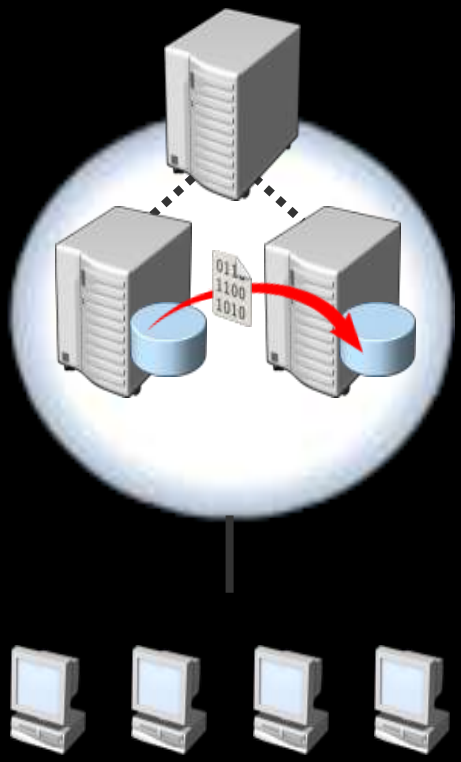


容錯移轉叢集(2)

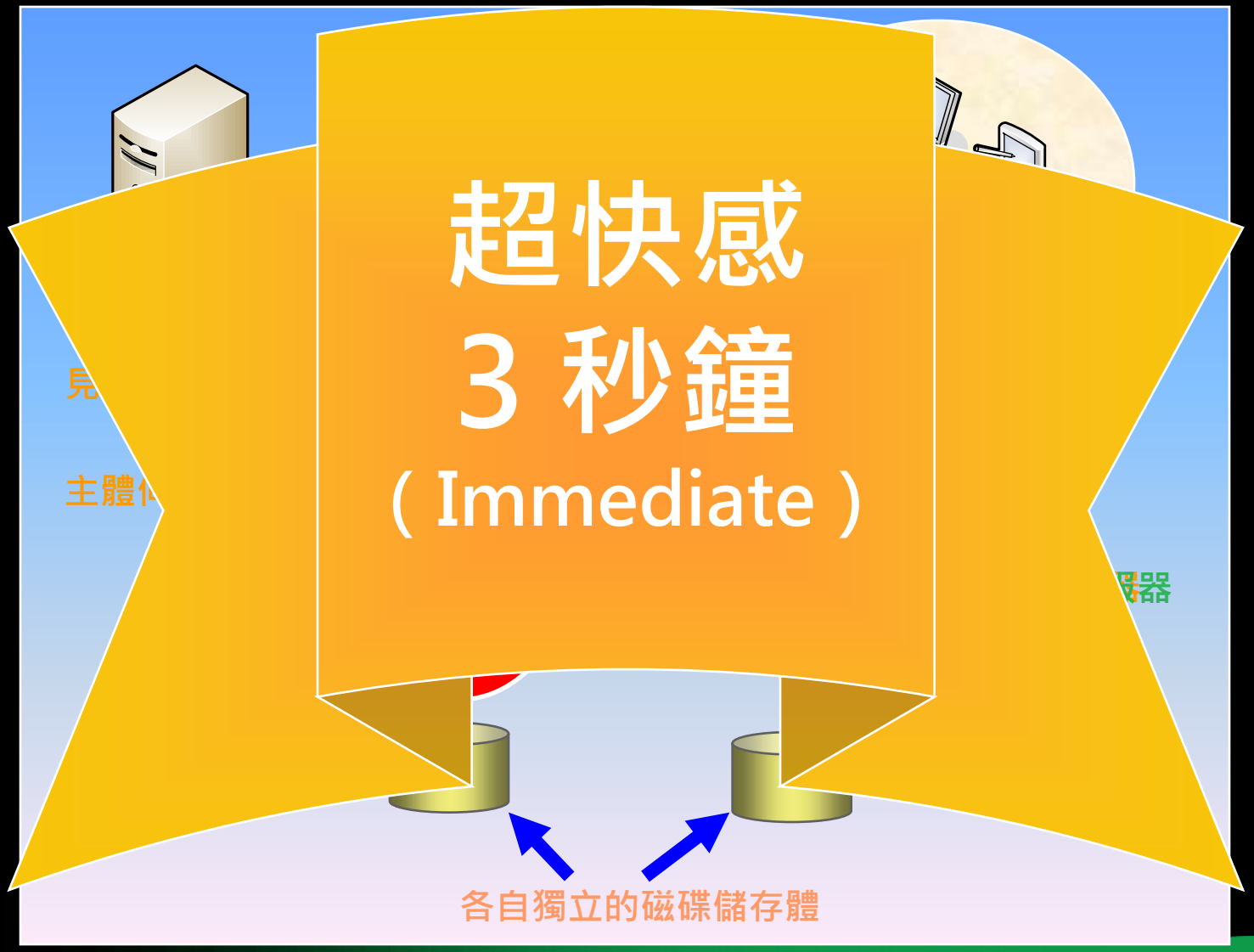

對外的公眾網路
私有網路 ，用於傳送 - 跳動訊息 (heartbeat message)
虛
客戶端
節點 A
節點 B
共用的叢集磁碟

資料庫鏡像(1)

- 資料庫鏡像(Database Mirroring)
  - 叢集替代方案
  - 熱備援
  - 無硬體限制
  - 支援個別使用者資料庫執行容錯移轉
  - 資料庫鏡像的成員模型
    - 主體伺服器(Principal Server)
    - 鏡像伺服器(Mirror Server)
    - 見證伺服器(Witness Server)
  - 支援版本
    - Standard、Enterprise Edition



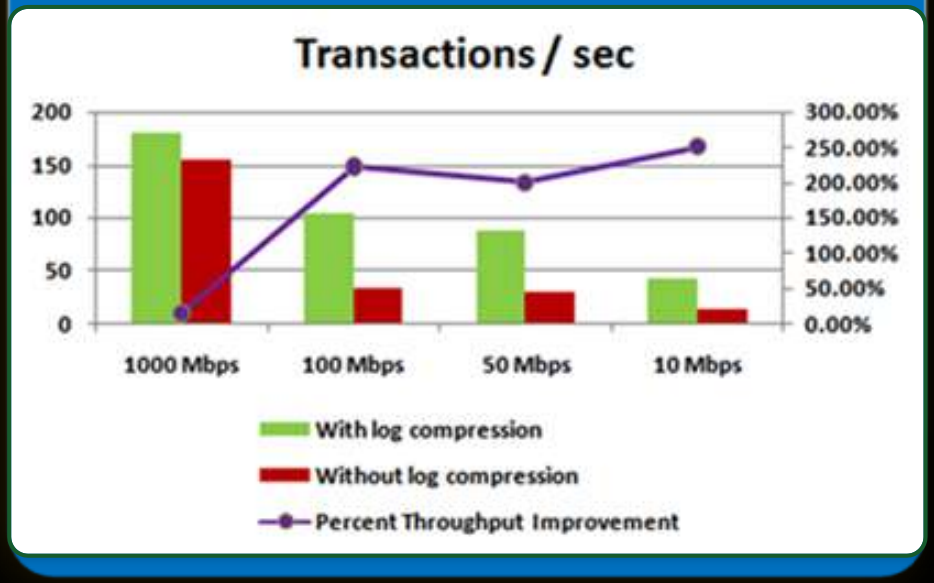
資料庫鏡像(2)

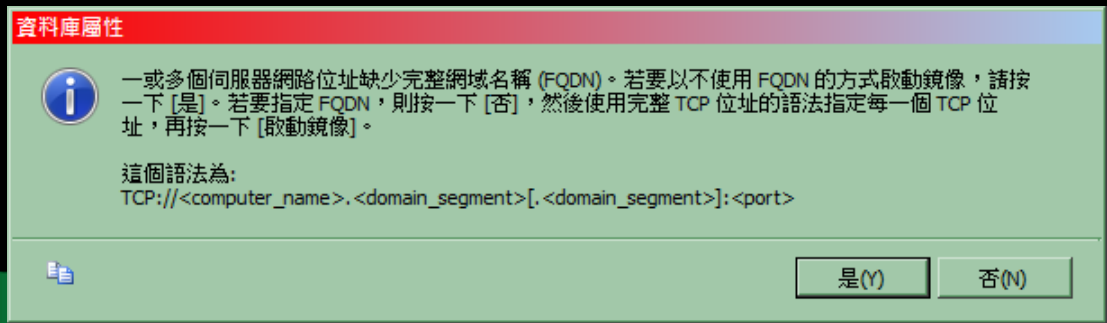


資料庫鏡像新增強的功能

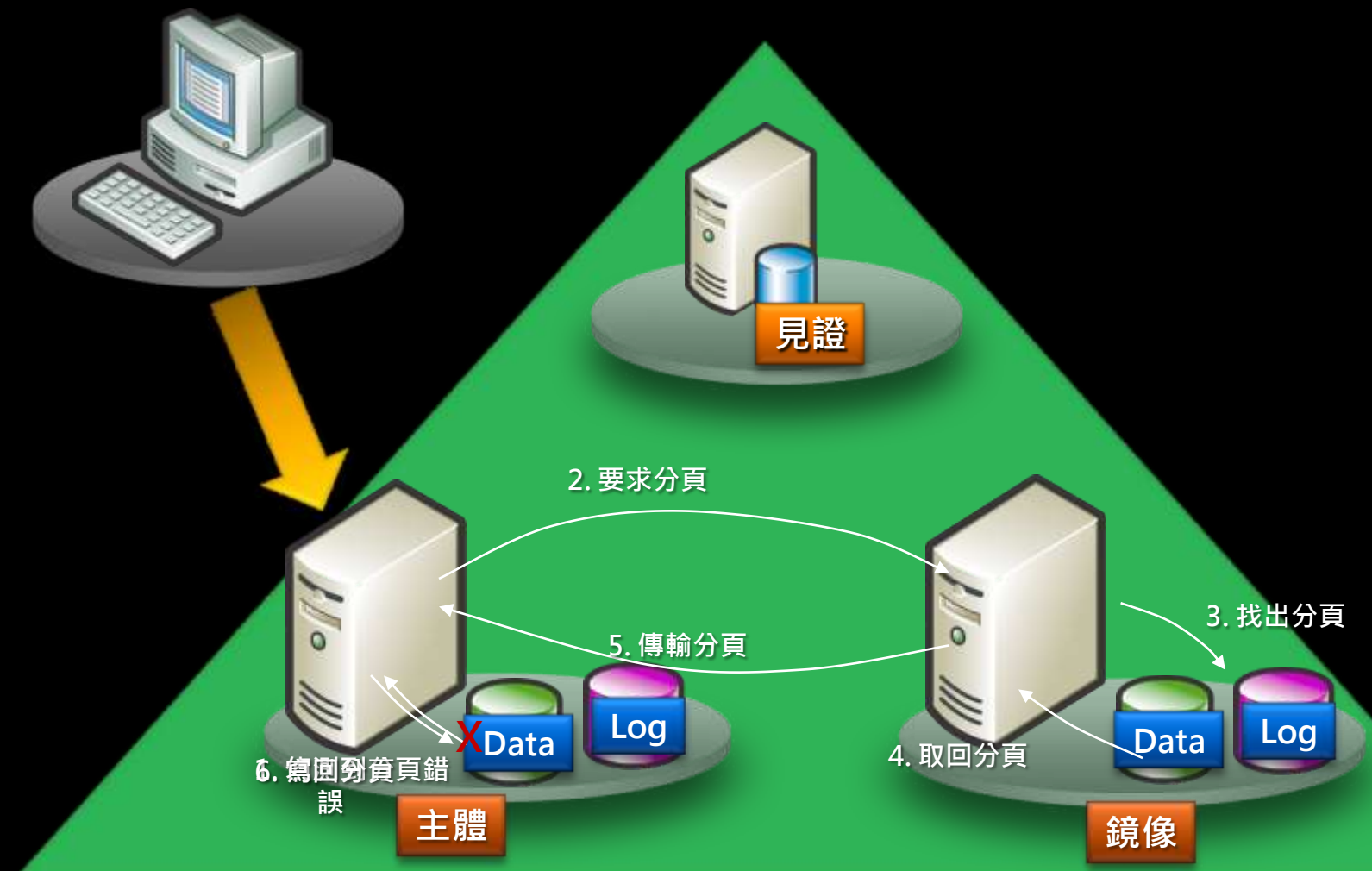
- 效能再提昇
  - 備份壓縮
- 自動修復頁面
  - 可處理的錯誤類型：823、824、829
  - 在背景中執行的非同步程序
  - 避免錯誤的資料分頁造成資料庫無法提供服務
    - 主體伺服器偵測到錯誤的資料庫分頁
    - 從鏡像伺服器要求正確的分頁
  - 支援不使用完整網域名稱(FQDN)

壓縮傳輸的交易記錄





自動修復損毀的資料頁



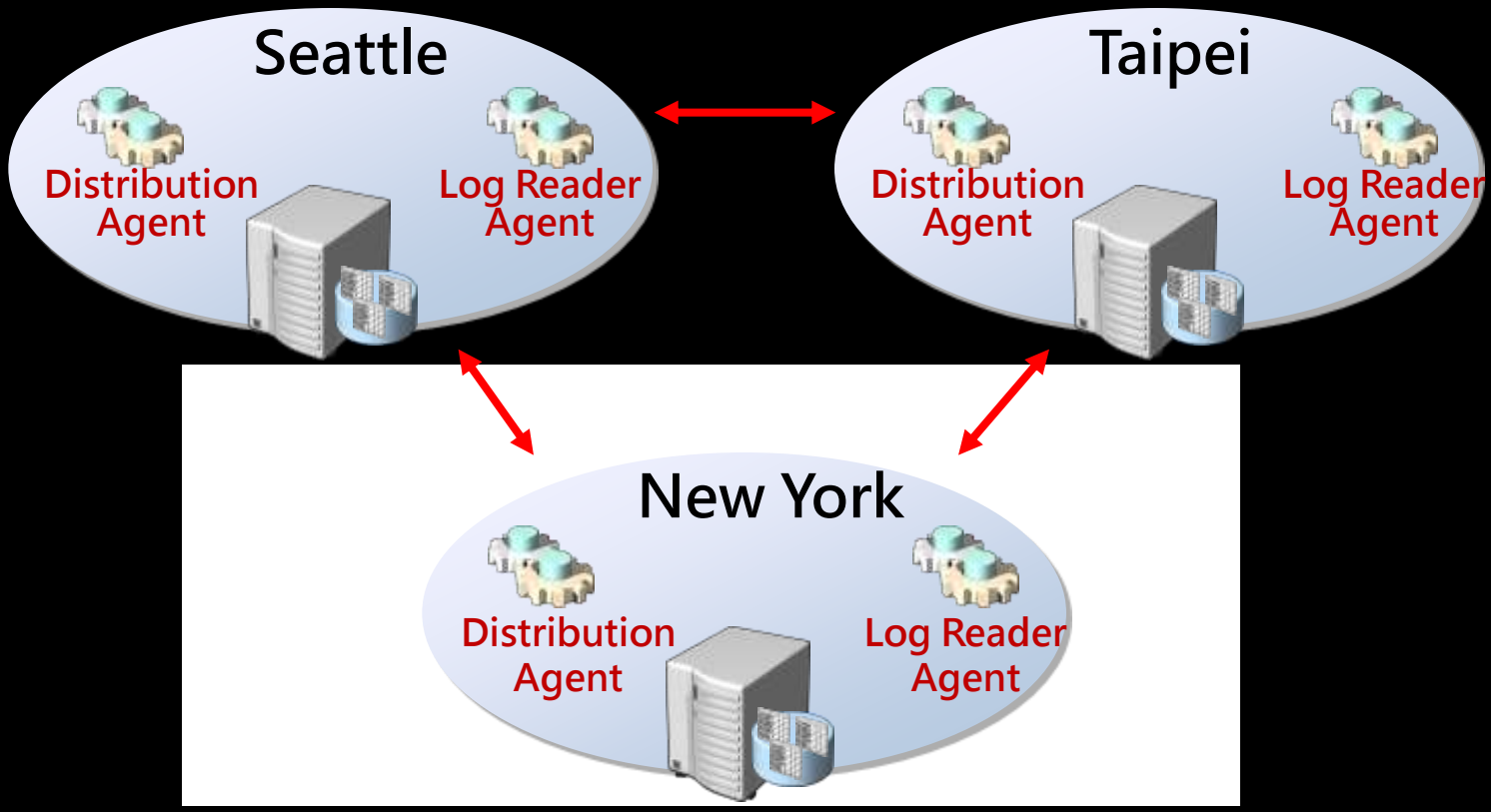
資料庫鏡像

demo

點對點複寫(1)

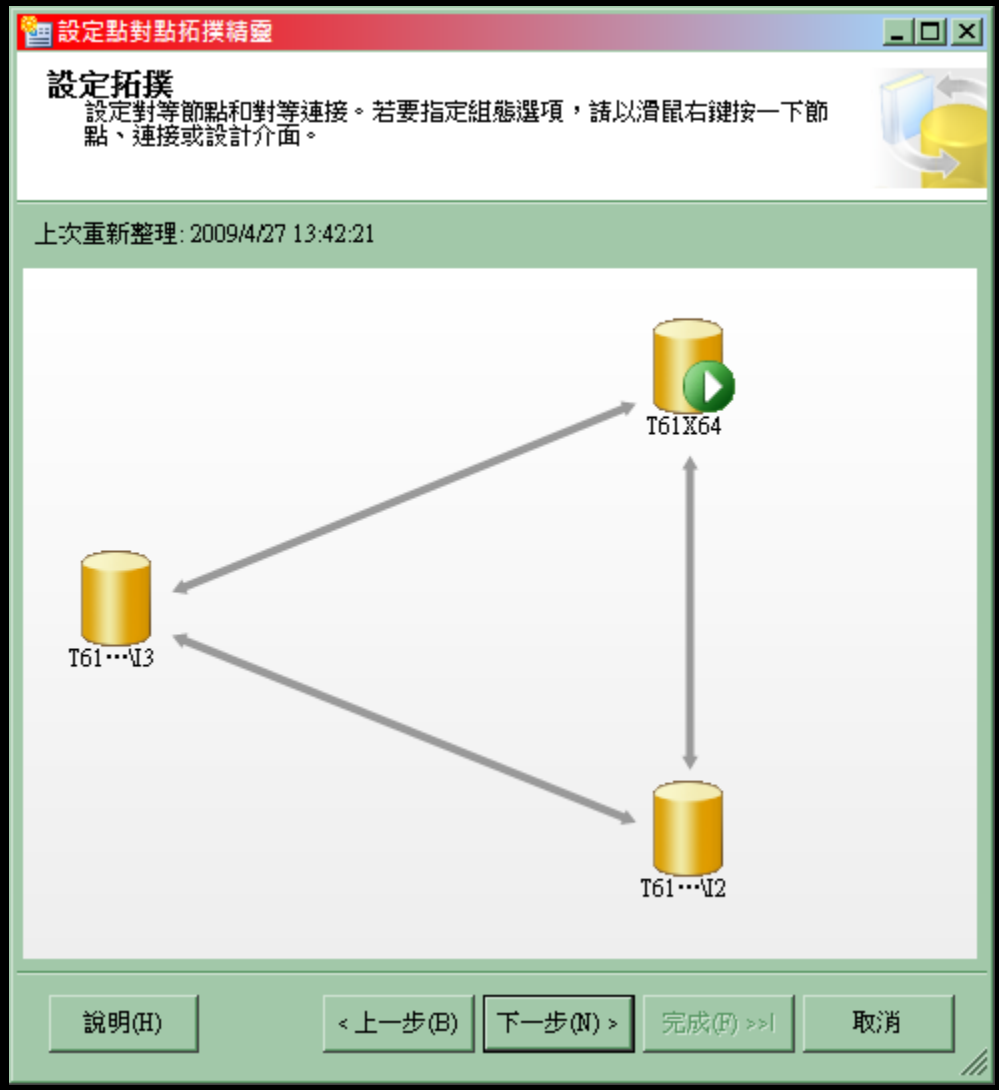
- 點對點複寫(Peer-to-Peer Replication)
  - 提供熱備援
  - 每個節點(Node)的位階均相同
    - 兼任發行者(Publisher)、散發者(Distributor)、訂閱者(Subscriber)
  - 複寫整個資料庫
  - 大幅提升效能
  - 沒有硬體限制
  - 已完成認可(Commit)資料，有可能來不及執行複寫
  - 利用備份檔案即可啟始複寫機制
  - 支援版本
    - Enterprise Edition

點對點複寫(2)


Seattle
Distribution Agent
Log Reader Agent
Taipei
Distribution Agent
Log Reader Agent
New York
Distribution Agent
Log Reader Agent

點對點複寫新增強的功能

- 使用「設定點對點拓撲精靈」
  - 輕鬆設定
- 線上新增節點
- 衝突偵測
  - 使用「衝突檢視器」來
    確認偵測到的衝突
  - 設定衝突警示(Alert)

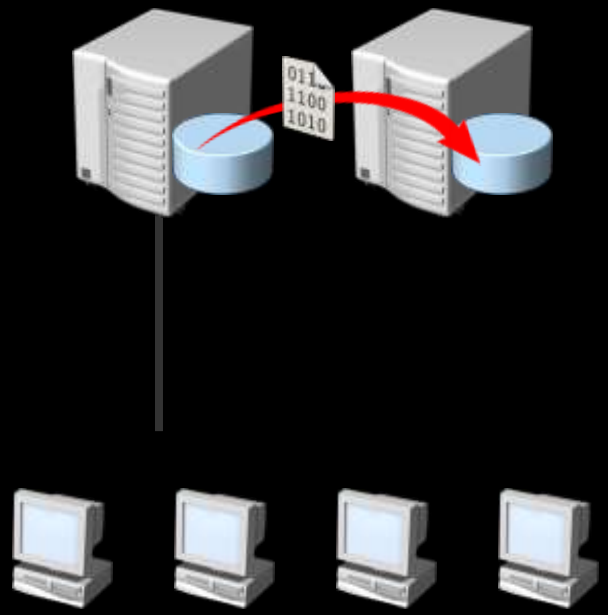


點對點複寫

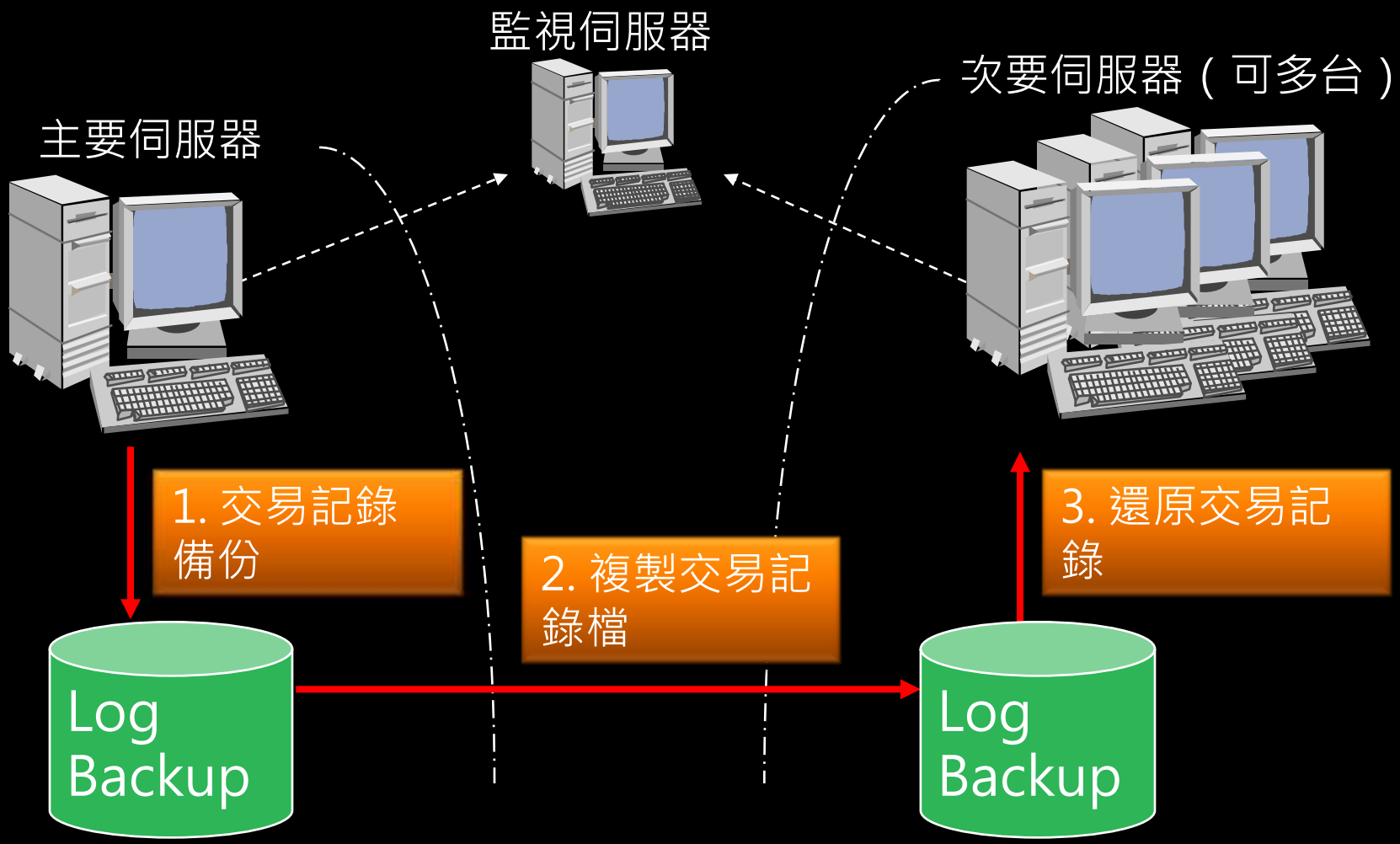
demo

記錄傳送(1)

- 記錄傳送(Log Shipping)
  - 對交易記錄檔，定期自動執行「備份(Backup)」、「複製(Copy)」「還原(Restore)」
  - 適用於使用者資料庫
  - 支援一對多的記錄傳送
  - 支援版本
    - Web、Workgroup、Standard、Enterprise Edition

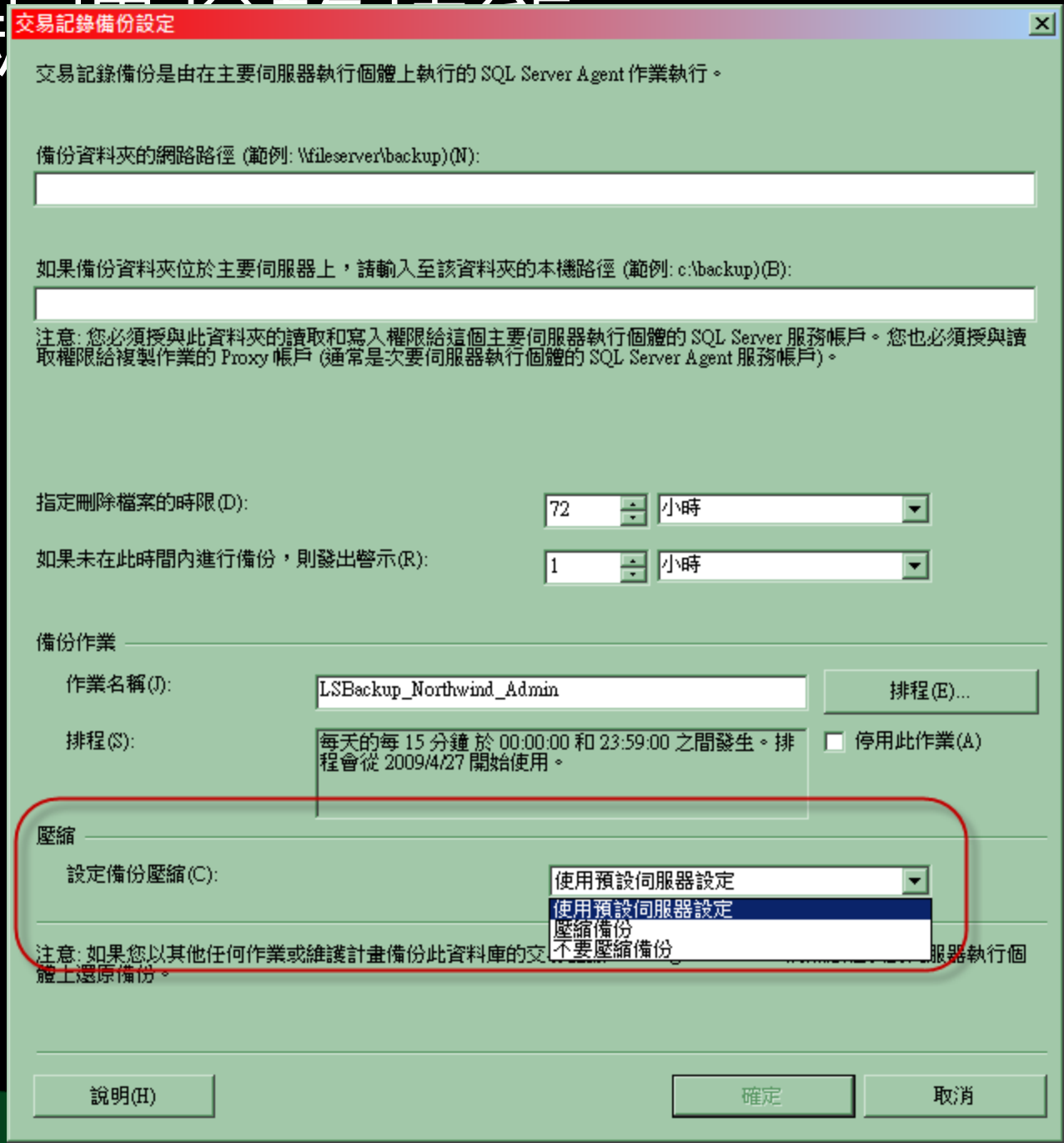


記錄傳送(2)


監視伺服器
次要伺服器（可多台）
主要伺服器
1. 交易記錄備份
2. 複製交易記錄檔
3. 還原交易記錄
Log Backup
Log Backup

記錄傳送新增設定

- 備份壓縮



主要的高可用性技術之分析

功能	資料庫鏡像	容錯移轉叢集	點對點複寫	記錄傳送
資料遺失	依據模式	無	可能	可能
容錯移轉	可自動執行	自動執行	手動	手動
移轉時間	數秒	~ 20+ 秒	手動決定	手動決定
使用特殊硬體	不需要	Shared Storage	不需要	不需要
支援多點備援	無	無	有支援	有支援
是否可查詢備援伺服器	搭配資料庫快照	不支援	支援	搭配 WITH STANDBY 選項
保護單位	使用者資料庫	節點伺服器	使用者資料庫	使用者資料庫
傳輸距離	TCP/IP	磁碟連線線材	TCP/IP	TCP/IP
資料異動的效能衝擊	較高	無(A/P mode)	低	低

線上索引作業與線上還原

- 減少計畫性停機的時間
- 支援Enterprise Edition
- 線上索引作業(Online Index)
  - ONLINE 選項
    - 可讓並行使用者存取基礎資料表
  - 線上建立(CREATE)、線上重建(REBUILD)、線上刪除(DROP)
- 線上還原(Online Restore)
  - 在資料庫還在線上時，還原資料

熱新增 CPU與熱新增記憶體

- 減少計畫性停機的時間
- 熱新增 CPU
  - 將 CPU 動態新增到執行中系統的功能
  - 可發生於實體上新增硬體、邏輯上進行線上硬體分割或是虛擬上透過虛擬化層時
  - 作業系統
    - 64 位元版本的 Windows Server 2008 Datacenter、Enterprise Edition
  - 支援SQL Server 2008 Enterprise Edition
- 熱新增記憶體
  - 不需要重新啟動伺服器即可增加實體記憶體
    - 硬體廠商支援特殊的硬體
  - 作業系統
    - Windows Server 2003/2008 Enterprise、Datacenter Edition
  - 支援SQL Server 2008 Enterprise Edition

提昇資料安全性，降低支出成本

可延伸金鑰管理
透明資料加密

全方位的防禦機制

- 更安全的資料存取
  - 更安全的配置
  - 多樣的驗證機制
  - 更微細的授權權限
- 協助保全資料
  - 金鑰加密資料
  - 透明資料加密 (TDE)
  - 可延伸金鑰管理 (EKM)
- 防禦術
  - 安全性稽核
  - 企業層級的安全原則

安全機制：SQL Server 2005

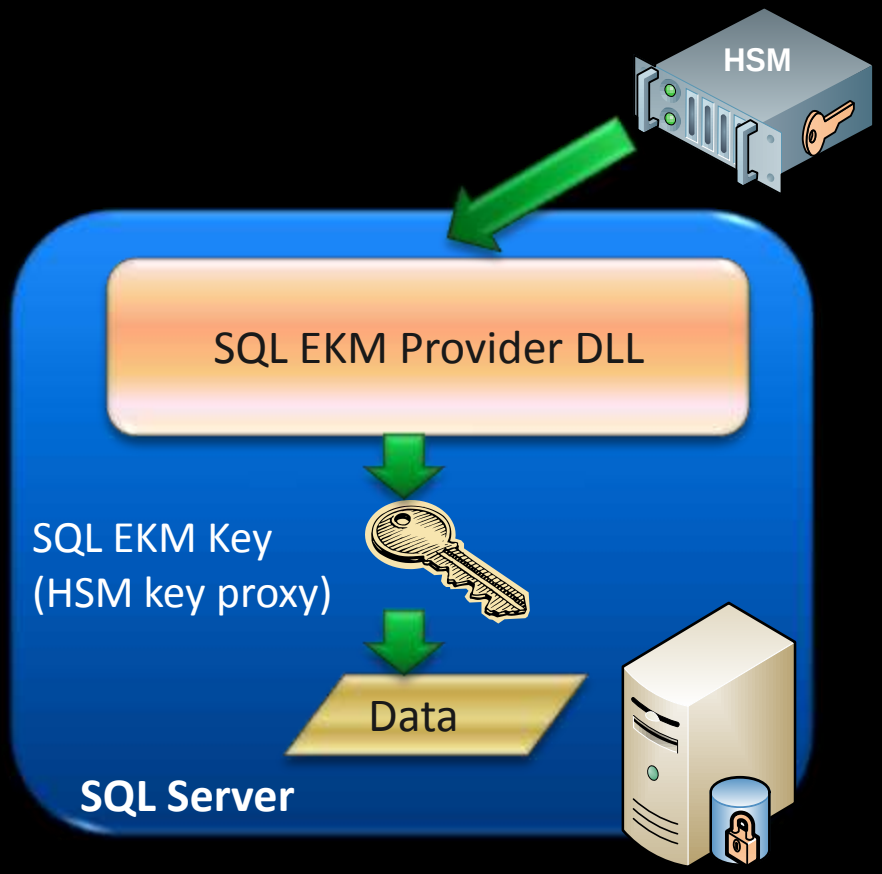
威脅與挑戰	增強的功能
弱式密碼	密碼原則機制：增強式密碼
缺少稽核的資料	利用DDL 觸發程序、登入觸發程序
機密資料的保護	內建：密碼片語(PassPhrase) 、對稱金鑰(Symmetric)、非對稱(Asymmetric)、憑證(Certificate)的加密功能
保護Metadata	安全性目錄檢視
需要各層級的權限配置	精確的顆粒權限：伺服器層級、資料庫層級、結構描述層級、物件、資料行...等
更安全的開發：最小權限原則	模組簽署、內容切換：EXECUTE AS
保護連接的安全性	登入帳號密碼已經加密、使用憑證、端點(Endpoint)

創新的防禦術
SQL SERVER 2008

資料加密

- 資料加密
  - 透過密碼、加密金鑰等方式讓資料變成模糊無法識別
  - 讓具備管理權限的人員或是入侵的駭客，也無從得知資料的原貌
  - 早期的資料加密作業
    - 多半是由前端應用程式自行控制
    - 需要使用大量的 CPU資源
    - 加密金鑰與加密資料一起存放
- SQL Server 2005
  - 內建：密碼片語、對稱金鑰、非對稱、憑證的加密功能
  - 使用 SQL Server 作為金鑰管理
  - 加密檔案系統 (Encrypted File System，EFS)
  - BitLocker 磁碟加密功能
- SQL Server 2008
  - 可延伸金鑰管理(Extensible Key Management，EKM)
  - 透明資料加密(Transparent Data Encryption，TDE)

可延伸金鑰管理 (EKM)



- 使用「硬體安全性模組」(Hardware Security Modules，HSM)
- 廠商可以對 HSM、金鑰組態和金鑰存取提供管理軟體 -- MSCAPI提供者
- SQL EKM金鑰提供代理功能來存取HSM金鑰
- 讓 SQL Server 可以使用由協力廠商所開發的模組元件，支援進階加密功能和金鑰管理函數

EKM的特性

- 優點
  - 安全性
    - 外部加密金鑰儲存 (實體分隔資料和金鑰)
    - 企業能中央管理與儲存金鑰機制
    - 額外的授權檢查 (啟用責任分隔)
    - 分隔資料庫擁有者(db_owner)與資料擁有者(data owner)
  - 效能
    - 硬體架構加密/解密的效能高
- 限制
  - 適用 Enterprise版本

EKM密碼編譯提供者與金鑰

- EKM提供伺服器層級物件

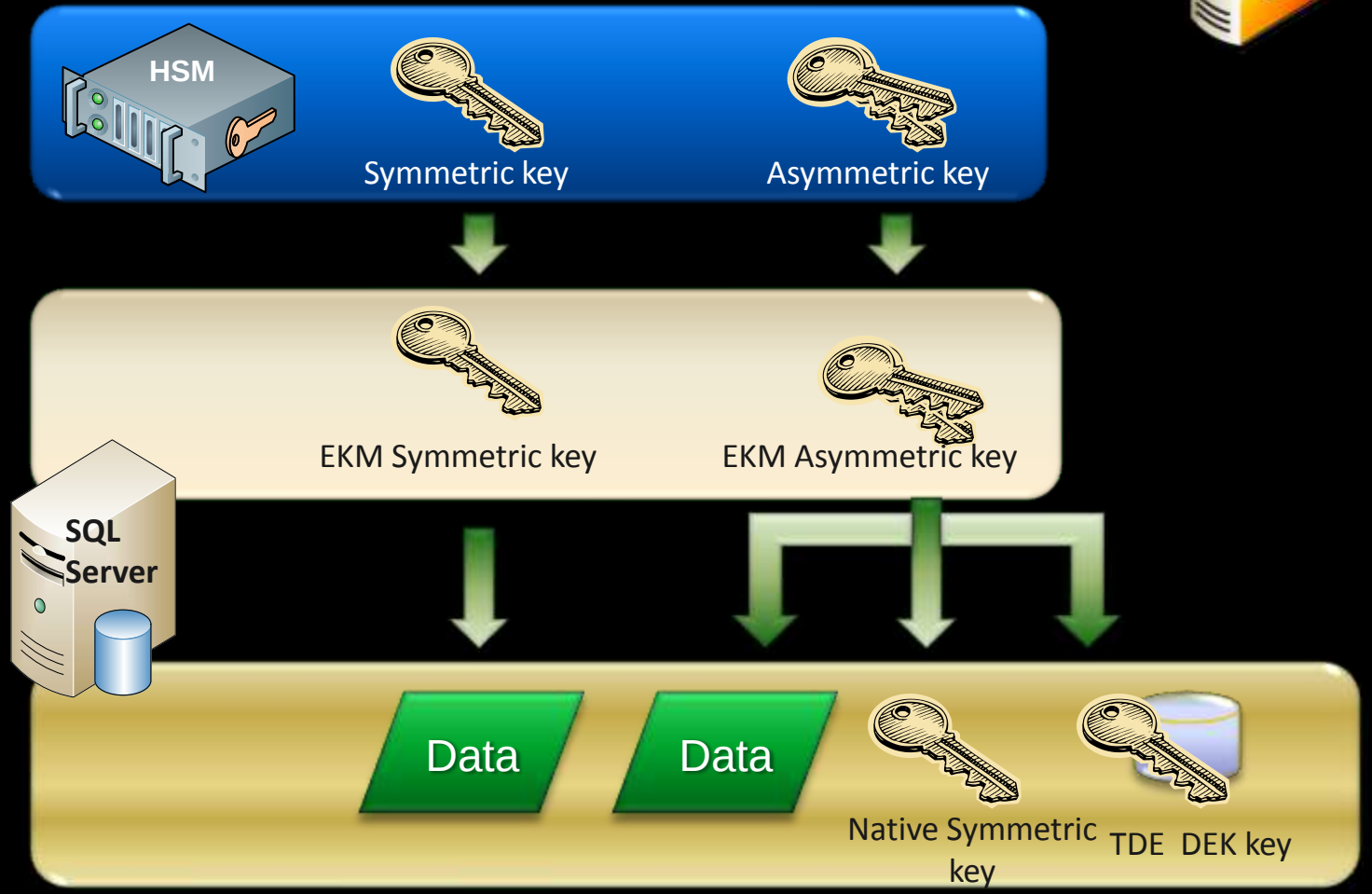
```
CREATE CRYPTOGRAPHIC PROVIDER DataSafeProvider
FROM FILE = 'DataSafeProvider.dll'
```

- 使用EKM的金鑰
  - 管理-相同的T-SQL

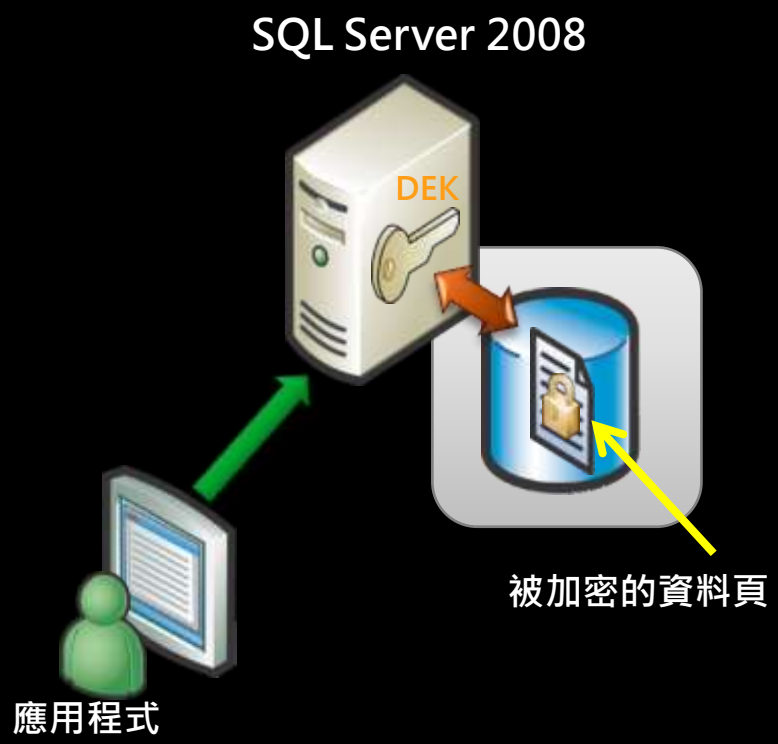
```
CREATE SYMMETRIC KEY SymmKeyEkm
FROM Provider DataSafeProvider
WITH ALGORITHM AES_256 …
```

  - 使用-相同的T-SQL
    - 檢視金鑰資訊、資料的加解密等
    - EncryptByKey、DecryptByKey、EncryptByAsmKey、DecryptByAsmKey 等

EKM 金鑰的階層結構


HSM
Symmetric key
Asymmetric key
EKM Symmetric key
EKM Asymmetric key
SQL Server
Data
Data
Native Symmetric key
TDE DEK key

透明資料加密(TDE)



- 無需修改應用程式
- 在資料庫層級：加密與解密
  - 使用資料庫加密金鑰 (DEK)
- DEK 使用以下的方法來保護
  - 憑證
  - 硬體安全性模組(HSM)
- 必須有DEK
  - 還原資料庫
  - 附加資料庫檔案

TDE-加密金鑰階層

- 加密資料
  - 選用 AES 或是 3DES加密演
  - 雖然會增加 CPU使用量，
    不會增加資料庫的使用空
  - 執行資料庫備份作業時，
- 運作原理
  - 先對存放在記憶體的資料
    寫入到磁碟上。
  - 完成加密後，使用總和檢
    護機制。
  - 需要解密的分頁載入記憶
    查碼，事先即可偵測分頁
  - 資料分頁進行解密，再載

使用 TDE 的理由

- 保護機密資料(data at rest)
- 整個資料庫受到防護
- 應用程式無需修改
  - 索引或資料類型也沒限制(但不支援 FileStream)
- 對於效能衝擊很小
- 備份時無需使用金鑰

TDE 使用情境

阻斷使用者直接存取資料庫的檔案系統

防禦未經授權的使用者取得資料庫備份檔案

符合規範：保護機密的靜態資料(data at rest)

沒有使用憑證或HSM解開金鑰，將無法開啟資料庫

使用 TDE 的考量

- 可與資料壓縮一併使用
- 不建議與備份壓縮一併使用
- 資料庫鏡像
  - 複製憑證到主體與鏡像伺服器上
- 將虛擬記錄檔案 (virtual log file) 內的其餘部分設為零，以強制使用下一個虛擬記錄檔案
  - 無法使用立即檔案初始化(instant file initialization)，對於復原資料庫、取得磁碟空間，有負面影響
- 一旦某一資料庫使用 TDE
  - tempdb 系統資料庫也將加密，這對於未啟用 TDE 的資料庫將會有效能的影響
- 適用 Enterprise版本

透明資料加密(TDE)

demo

降低儲存成本

備份壓縮
資料壓縮

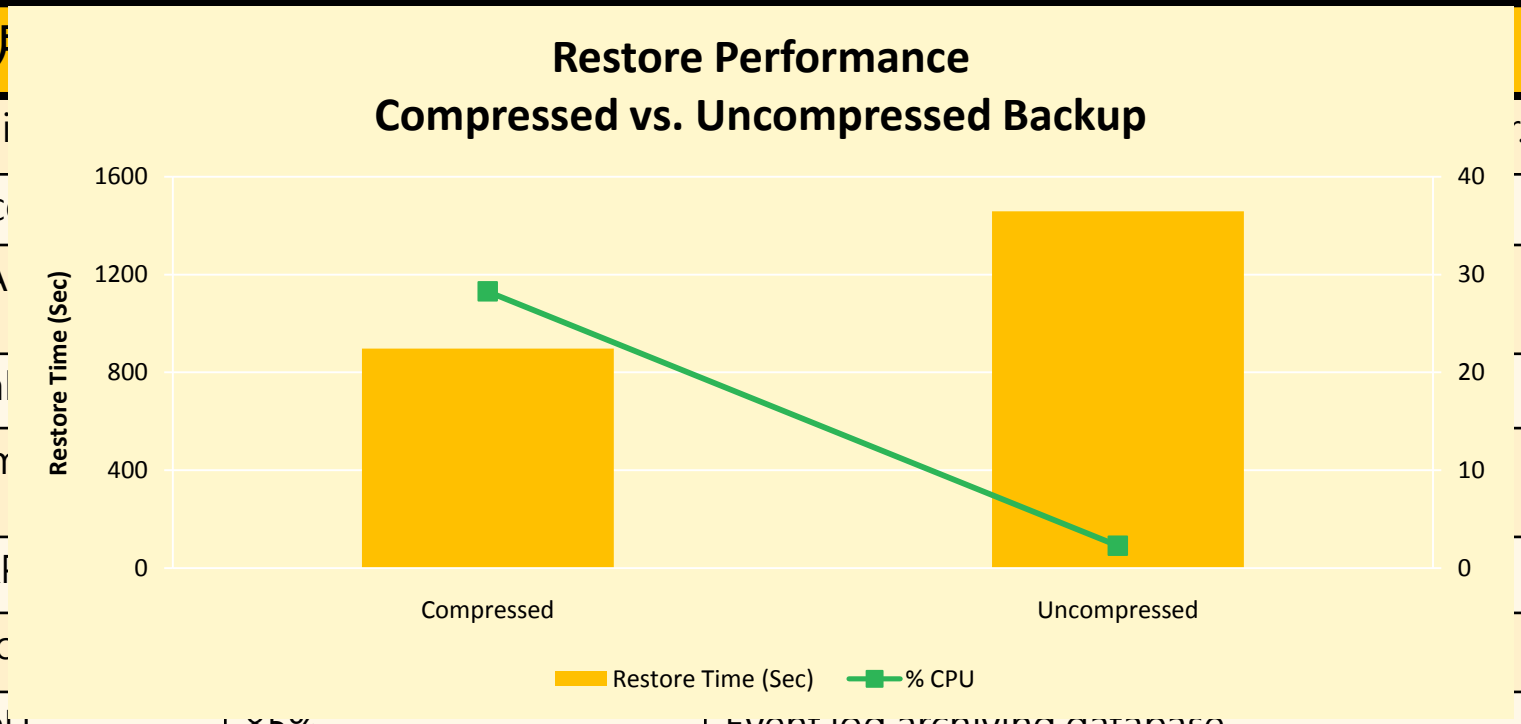
縮減磁碟IO，進而提升執行效能

- 磁碟系統
  - 提供的倍數成長的使用空間(由GB邁向TB)
  - 執行效能卻未能有倍數的提升
- 面臨的挑戰，舉例來說
  - 備份與還原資料庫的時間大幅拉長
  - 資料量愈大，造成系統在存取大型資料表時，過多的時間耗費在磁碟 I/O上
- SQL Server 2008 新增加
  - 備份壓縮(Backup Compression)
  - 資料壓縮(Data Compression)

備份壓縮的效能分析

- 增加 CPU 的使用量
- 以 AdventureWorks 資料庫為例
  - 使用備份壓縮的環境，整體的 CPU 使用量增加了 10%，但是備份的時間，大幅縮減了 45%，而且備份壓縮下來的檔案約是原來大小的 25% 左右
  - 在進行還原資料庫時，使用備份壓縮的環境，整體的 CPU 使用量增加了 6.5%，但是還原的時間，大幅縮減了 50%。
- 建議
  - 搭配 資源管理員 來限制備份壓縮的 CPU 使用量
  - 雖然會讓備份的速度受到衝擊，但是仍然擁有還原備份檔案時的優勢
- 適用 Enterprise版本
  - 但是備份壓縮的備份集檔案，是可以還原到 SQL Server 2008 其他的版本上

備份壓縮所節省的時間與空間



客戶		
RedPrai		
BWIN.c		
NASDA		
GE Heal		
First Am Title		
SAP ERI		
Caregrc		
ServiceU	85%	Event log archiving database.

Backup Size (GB)

Backup Time (sec)

備份壓縮(Backup Compression)

demo

資料壓縮

- 分成
  - 資料列壓縮、頁面壓縮
- 資料壓縮
  - 依據其資料行的資料類型，資料值的重複性等等
  - 適用物件
    - 叢集索引、非叢集索引、堆積結構的資料表、索引檢視、資料分割資料表與其索引
  - 增加 CPU 的使用量
    - 減少存取磁碟 I/O所造成的負載
  - 增加記憶體的重複使用率
    - 資料在記憶體內也是持續保持被壓縮狀態
  - 磁碟系統的挑戰
    - 額外多使用一點 CPU資源，進而提升系統的整體執行效能
- 適用情境
  - 資料倉儲、報表系統等等
- 適用於 SQL Server 2008 Enterprise

資料列壓縮(Row Compression)

- 無需修改前端應用程式

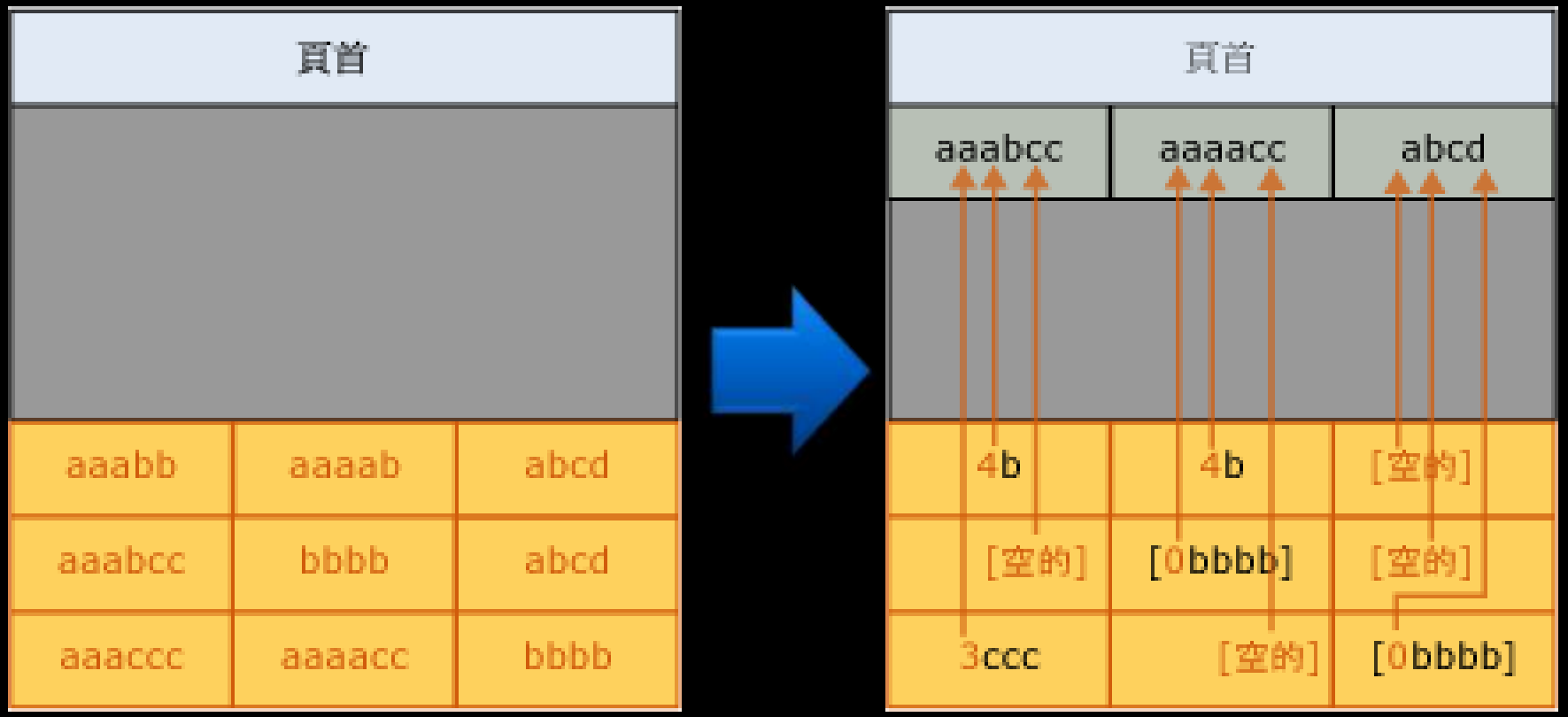
下表描述資料列壓縮如何影響 SQL Server 中的現有類型。此表格不包含可藉由使用頁面壓縮而達成的節省量。

資料類型	儲存是否受到影響？	描述
tinyint	否	所需的最小儲存區是 1 個位元組。
smallint	是	如果 1 個位元組能容納此值，只會使用 1 個位元組。
int	是	僅使用所需的位元組。例如，如果值可以儲存在 1 個位元組內，則儲存只會使用 1 個位元組。
bigint	是	僅使用所需的位元組。例如，如果值可以儲存在 1 個位元組內，則儲存只會使用 1 個位元組。
decimal	是	此儲存與 Vardecimal 儲存格式完全相同。如需詳細資訊，請參閱 <將十進位資料儲存成可變長度>。
numeric	是	此儲存與 Vardecimal 儲存格式完全相同。如需詳細資訊，請參閱 <將十進位資料儲存成可變長度>。
bit	是	中繼資料負荷將此設為 4 個位元。
smallmoney	是	藉由使用 4 位元組整數來使用整數資料表示。貨幣值會乘以 10000，再移除小數點之後的任何數字以儲存產生的整數值。此類型的儲存最佳化與整數類型類似。
money	是	藉由使用 8 位元組整數來使用整數資料表示。貨幣值會乘以 10000，再移除小數點之後的任何數字以儲存產生的整數值。此類型的範圍比 smallmoney 大。此類型的儲存最佳化與整數類型類似。
float	是	不會儲存具有零的最低有效位元。float 壓縮大多適用於尾數中的非小數值。
real	是	不會儲存具有零的最低有效位元。real 壓縮大多適用於尾數中的非小數值。
smalldatetime	否	藉由使用兩個 2 位元組整數來使用整數資料表示。日期會使用 2 個位元組，是 1901 年 1 月 1 日之後的日數。這需要 2 個位元組，從 1902 開始；因此在該時間點後就無法進行節省。 時間是午夜之後的分鐘數。稍微超過 4AM 的時間值會開始使用第二個位元組。 如果 smalldatetime 只會用來表示日期 (常見的情況)，則時間是 0.0。壓縮會針對資料列壓縮以最大顯著性位元組格式儲存時間而節省 2 個位元組。
datetime	是	藉由使用兩個 4 位元組整數來使用整數資料表示。整數值代表日數，基底日期則是 1900 年 1 月 1 日。第一個 2 位元組最多可代表到 2079 年。在該時間點之前，此處的壓縮一定可以節省 2 個位元組。每個整數值都代表 3.33 毫秒。壓縮在第一個五分鐘內就會用盡第一個 2 個位元組，而需要在 4PM 之後使用第四個位元組。因此，在 4PM 之後僅能節省 1 個位元組。當 datetime 像任何其他整數一樣進行壓縮時，壓縮可以在日期中節省 2 個位元組。

頁面壓縮(Page Compression)

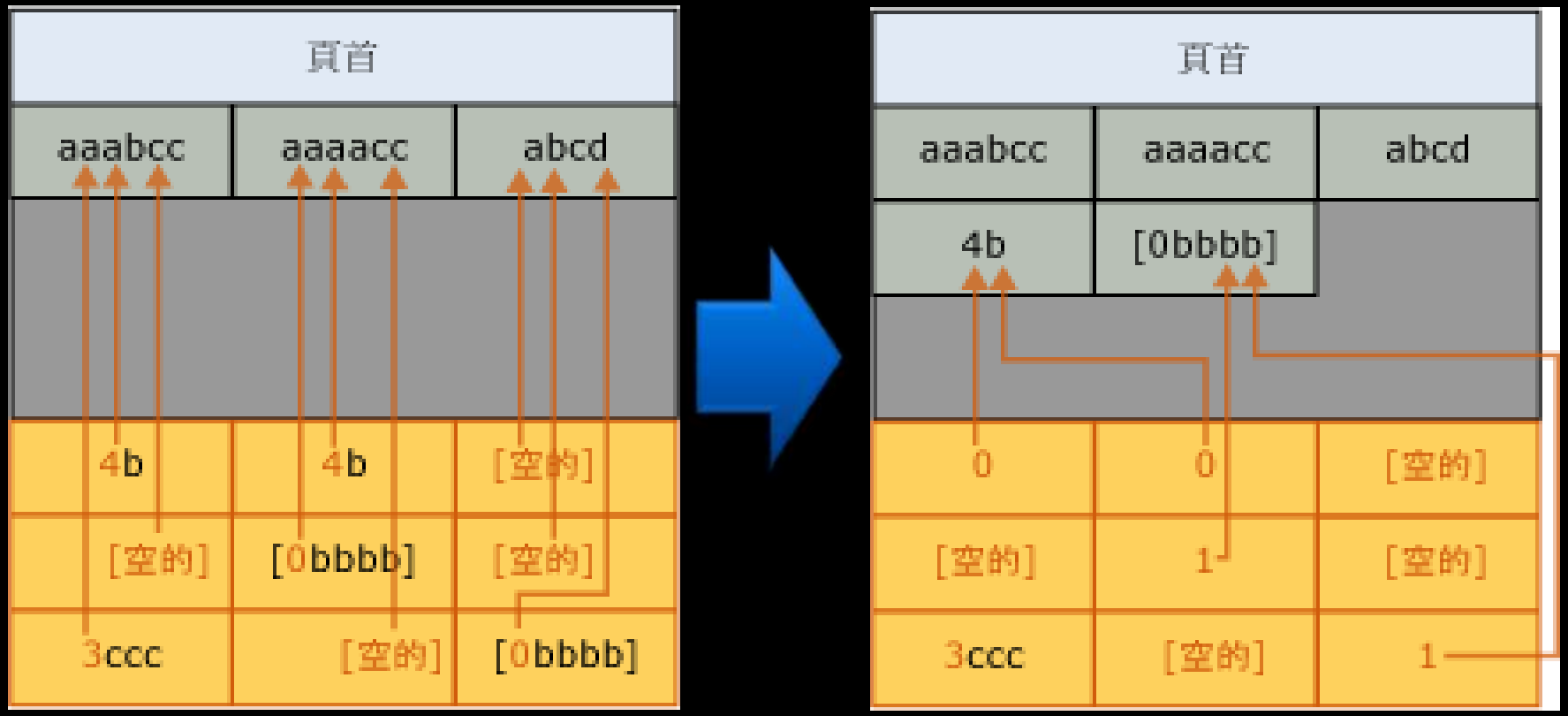
- 執行以下三種壓縮作業
  - 資料列壓縮(Row Compression)
  - 前置詞壓縮(Prefix Compression)
  - 字典壓縮(Dictionary Compression)

前置詞壓縮(Prefix Compression)



- 壓縮後
  - 在第一個資料列的第一個資料行中，值 4b 指出該資料列有前置詞 (aaab) 的前四個字元以及字元 b。這會產生值 aaabb，也就是原始的值。
  - 壓縮資訊 (CI) 結構

字典壓縮(Dictionary Compression)



- 在完成前置詞壓縮後，就會套用字典壓縮。字典壓縮會搜尋頁面上的任何位置是否有重複的值，然後將它們儲存在 CI 區域中
- 與前置詞壓縮不同的是，字典壓縮並不是限定於單一資料行。字典壓縮可以取代頁面上任何位置的重複值
- 請注意，值 4b 已由頁面的不同資料行參考

資料壓縮(Data Compression)

demo

結論

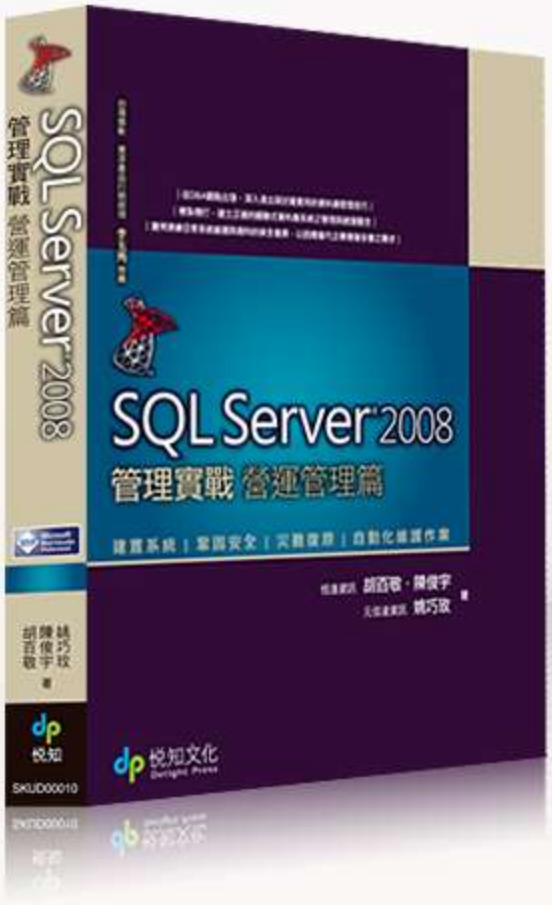
- 使用SQL Server 2008
  - 營運持續管理
  - 提昇資料安全性，降低支出成本
  - 降低儲存成本

參考書

- SQL Server 2008 管理實戰 **進階維護篇**
- SQL Server 2008 管理實戰 **營運管理篇**

SQL Server 2008
管理實戰 營運管理篇

作者 | MVP Microsoft Most Valuable Professional 微軟最有價值專家
恆逸資訊【胡百敬・陳俊宇】
元信達資訊【姚巧玫】



國內第一本SQL Server 2008大作

帶您搶先體驗全新版本強大的技術與服務

- 從DBA觀點出發，深入淺出探討最實用的資料庫管理技巧
- 穩紮穩打，建立正確關聯式資料庫系統管理與維護觀念。
- 實例演練日常系統維運與資料的保全復原，以因應當代企業複雜多變之需求。

建議售價 | $590，現場優惠75折，$443
出版日期 | 2008年9月19日

悅知文化 | http://www.delightpress.com.t