臺灣集中保管結算所股份有限公司

票券保管結算交割系統

系統備援／回復計畫書

V2.1

目　錄

壹、前言……貳~一~4
貳、範圍……貳~一~5
　一、系統架構……貳~一~5
　二、系統備援/回復規劃原則……貳~一~5
　三、磁帶命名原則……貳~一~5
參、系統備援/回復……貳~一~6
　一、系統備援……貳~一~6
　　(一)內容……貳~一~6
　　(二)時機……貳~一~6
　　(三)備援方式……貳~一~6
　　(四)備份前注意事項……貳~一~6
　　(五)備援人員……貳~一~6
　二、系統回復……貳~一~6
肆、資料庫備份/回復……貳~一~7
　一、資料庫備份……貳~一~7
　　(一)內容……貳~一~7
　　(二)資料庫備份時機……貳~一~7
　　(三)資料庫備份方式……貳~一~8
　　(四)資料庫備份步驟……貳~一~8
　　(五)資料庫備份人員……貳~一~8
　二、資料庫回復……貳~一~9
　　(一)資料庫回復方式……貳~一~9
　　(二)資料庫回復時機……貳~一~9
　　(三)資料庫回復步驟……貳~一~11
伍、備援機制……貳~一~13
　一、同地備援及異地備援……貳~一~13
　　(一)同地備援……貳~一~13
　　(二)異地系統備援……貳~一~13
　二、符合異地備援 Tier6 之規格……貳~一~13
　三、異地備援演練……貳~一~13

圖　目　錄

圖 4-1 資料庫備份作業示意圖……貳~一~7
圖 4-2 資料庫回復作業……貳~一~9

壹、前言

為滿足票券保管結算交割系統(以下簡稱 BCSS)每日大量資料庫備份之需求，本公司購置 2 台開放式磁帶館作為 BCSS 系統備援及備份之用，並依據此系統架構進行系統及資料庫備援／回復之規劃。

貳、範圍

一、系統架構

BCSS RS/6000 系統與備份設備架構，為透過本公司 DWDM 網路，串連南港主中心與異地備援中心，除可供資料同步（PPRC）外，尚可將磁帶備份即時傳至異地備援中心，同時製作磁帶備份。

二、系統備援/回復規劃原則

(一) BCSS 系統 Volume Group 之規劃如下：

1. Root VG(系統內部硬碟)：安裝 AIX 系統及各軟體產品、程式等，基本上 Root VG 之內容不常變動。
2. 非 Root VG(系統外部硬碟)：主要用於存放異動資料，如 MQ 之 Queue、與 Websphere 之 Repository object、Log 或資料庫之 Table space 及 Log 等，當 HACMP 啟動時，此 Volume Group 必須隨之切換到另一台主機，以使得 BCSS 繼續運作。

(二) BCSS 系統備援可分為

1. Root VG 之定期備援
2. 非 Root VG 之每日備份

三、磁帶命名原則

磁帶命名長度為 6 位，採二階六位，標示於媒體上，其原則如下：

（一）第一階為前一碼，用以區分儲存地點，3代表南港主中心；6代表異地備援中心。

（二）第二階為後五碼，為流水號。

參、系統備援/回復

一、系統備援

(一)內容

系統備援係包括BCSS系統CHANNEL、AP、DB主機正式及備援等共六部RS/6000主機之AIX system image的備援。

(二)時機

1. 每週乙次為原則，如貳範圍之二系統備援/回復規劃原則所述 system image 備援乃指 rootvg 備援，BCSS rootvg 具有 mirroring 功能因此備援時間將會較長一點。
2. 若系統有更動，則於更動之後立即備援，rootvg 通常儲存著應用程式之原始程式檔或執行檔，因此可能會被更動，一旦系統資料更改就必須立即備份以確保備援之及時性。

(三)備援方式

先將 rootvg 備份到 NIM（Network Installation Manager）主機後，再使用本公司之備份軟體備份至磁帶。AIX 系統備份，請以 AIX 之 “smit mksysb”指令依照其選單方式或 mksysb 系統指令為之。

(四)備份前注意事項

1. 察看 AIX errlog 有無任何有關 filesystem 之錯誤訊息，若有請先解決。
2. 確定/tmp，/var 空間使用率小於 90%。
3. 確定/etc/filesystem 檔案裡的/，/tmp，/var 之記錄 ”boot = true”， 若非請更正。
4. 儘可能利用系統離峰時間行使系統備援。

(五)備援人員

本公司系統工程師及系統操作人員。

二、系統回復

系統因任何原因，必須靠著 system image 磁帶回復時，工作人員可以用最近備份之磁帶為之，回復的方式請參考 AIX 系統回復手冊。

肆、資料庫備份/回復

資料庫的備份原則是希望在最短的時間內對資料庫作適當的備份，若資料庫毀損時能在最短的時間內回復其原狀態。

一、資料庫備份

BCSS 完成該營業日交易作業後，BCSS 系統將停止服務，並進行資料庫備份作業(整個資料庫作離線備份)，資料庫備份之 Image 檔案儲存於磁碟目錄中，VERITAS 於特定時間執行磁帶備份作業，一份置於本公司電腦主機房媒體儲存室內，另一份置放於備援機房，以作為資料庫毀損時復原之用。

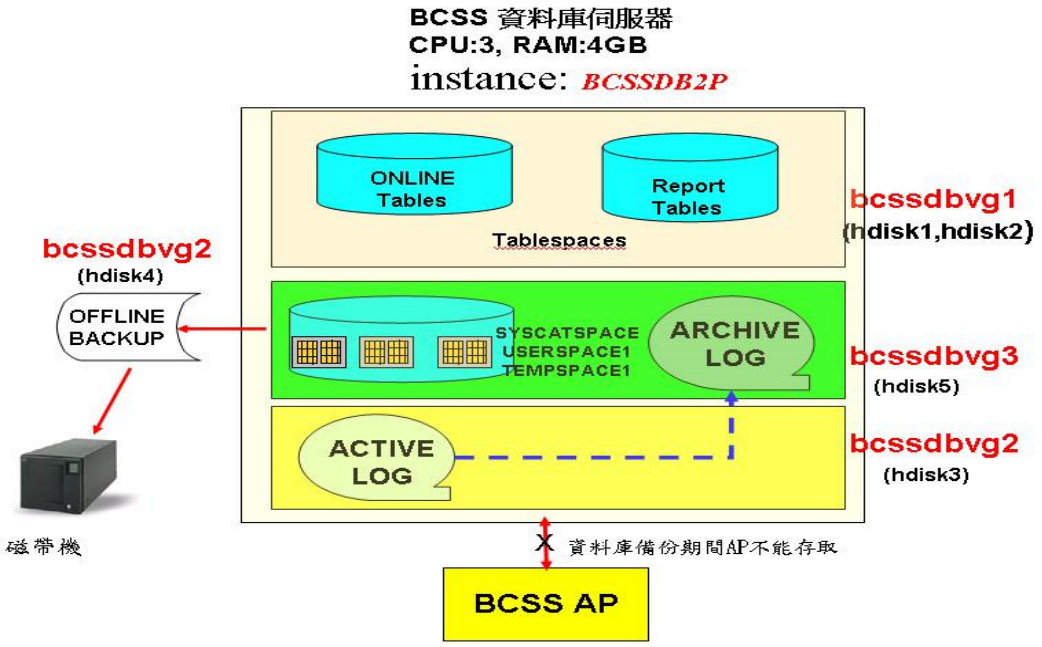

圖 4-1 資料庫備份作業示意圖

資料庫備份使用備份軟體 VERITAS 自動執行磁帶備份作業，以每天為一代，共三十一代（一個月），每一個月循環一次。

(一)內容

資料庫(IBMSF)作備份外，另將資料庫系統使用之 Log 同時作備份(db2parclog、db2pactlog 目錄)。

(二)資料庫備份時機

BCSS 完成當日 EOD 批次作業後，BCSS 系統將停止服務，於 EodCondense（UNIX JOB）前、後各執行一次整個資料庫(IBMSF)

備份到磁碟作業。

(三)資料庫備份方式

資料庫備份採取 Offline 備份方式，當備份進行中所有應用系統均暫停 Access 資料庫。

(四)資料庫備份步驟

系統操作員透過 MENU 方式執行「DB Server 備份作業」，即可對整個資料庫作備份。備份完成後，將會出現以下訊息「Backup successful. The timestampfor this backup image is : yymmddhhmmss」(yymmddhhmmss 為 BACKUP 成功之 Timestamp - yymmddhhmmss. 若未來資料庫需要回復時，必需敘述此正確的 Timestamp)。

(五)資料庫備份人員

資料庫備份由系統操作員負責操作，VERITAS 於特定時間執行磁帶備份作業。

二、資料庫回復

資料庫回復處理原則能於最短時間內回復其原狀態。資料庫回復係利用 DB2 SYSTEM RESTORE 功能以自動回復資料庫之原狀態,其示意圖如下:

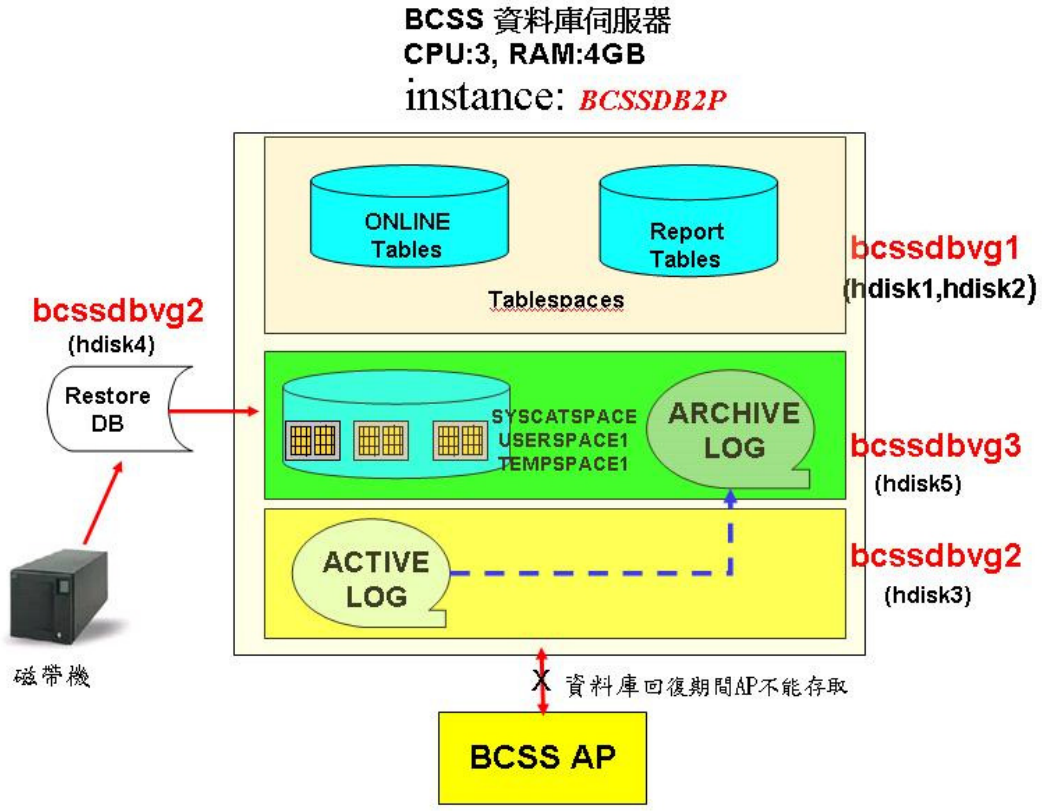

圖 4-2 資料庫回復作業

(一)資料庫回復方式

資料庫回復時應先找出備份磁帶之 Timestamp-yyyymmddhhmmss.

(二)資料庫回復時機

任何因素導致資料庫無法正常存取資料(如磁碟損毀等)狀況發生時,必須進行資料庫回復。

資料庫回復作業時尚無法得知備份之 Timestamp, 可由下列兩種方式查明:

1. 自資料庫主機之/db2pbackup 目錄中,以 ls -l 指令查詢。
2. 在 db2 command window 下輸入 db2 list history backup all for db ibmsf 指令 : 下列畫面將顯示詳細 Timestamp:

```
**********************************************************************
                  List History File for ibmsf

 Op Obj 時間戳記+順序       類型 Dev 最舊日誌      現行日誌      備份
ID
-- --- ------------------ ---- --- ------------ ------------ ---------
 B  D  20071002150607001   F    D  S0000000.LOG S0000000.LOG
----------------------------------------------------------------------
----
 含有 17 個表格空間：

 00001 SYSCATSPACE
 00002 USERSPACE1
 00003 BCSSTS001
 00004 BCSSTS002
 00005 BCSSTS003
 00006 BCSSTS004
 00007 BCSSTS005
 00008 BCSSTS006
 00009 BCSSTS007
 00010 BCSSTS008
 00011 BCSSTS009
 00012 BCSSTS010
 00013 BCSSTS011
 00014 BCSSTS016
 00015 BCSSTS017
 00016 BCSSTS020
 00017 SYSTOOLSPACE
----------------------------------------------------------------------
----
   註解：DB2 BACKUP IBMSF OFFLINE
```

```
開始時間： 20071002150607
  結束時間： 20071002150621
    狀態：I
--------------------------------------------------------------
----
 EID：140 位置：/db2pbackup
```

(三)資料庫回復步驟

資料庫回復方式依不同發生狀況其處理步驟詳述如下:

1.DB 損毀，DB2 active log 正常

(1)Restore database from backup disk:

DB2 RESTORE DB ibmsf from /db2pbackup TAKEN AT yyyymmddhhmmss;

(2)Roll forward database:

DB2 ROLLFORWARD DB ibmsf TO END OF LOG AND STOP;

(3)繼續執行正常交易

2.DB 正常， DB2 active log 損毀

(1)DB2 cold start:

DB2 UPDATE DB CFG FOR ibmsf USING NEWLOGPATH /new device;

(2)Restart DB2 system:

DB2STOP

DB2START

(3)即刻作資料庫備份（執行/bcssdb2p/DBA/backupdb.sh）

(4)繼續執行正常交易

3.DB 損毀， DB2 active log 損毀

(1)DB2 cold start:

DB2 UPDATE DB CFG FOR ibmsf USING NEWLOGPATH /new device

(2)Restart DB2 system by enter Command:

DB2STOP

DB2START

(3)Restore database from backup disk:

DB2 RESTORE DB ibmsf from /db2pbackup TAKEN AT yyyymmddhhmmss;

(4)Roll forward database:

DB2 ROLLFORWARD DB ibmsf AND STOP

(5)即刻作資料庫備份（執行/bcssdb2p/DBA/backupdb.sh）

(6)繼續執行正常交易（損毀前之交易須重做）

伍、備援機制

一、同地備援及異地備援

(一)同地備援

本公司主中心 BCSS 系統採雙主機備援，並建置有高可靠叢集系統建置服務(HACMP High Availability Cluster Multi-processing)，可自動偵測系統主機異常，並於主系統無法運作時，自動切換至同地備援系統，維持系統正常運作。

(二)異地系統備援

本公司於異地備援中心，另建有一套與主中心 BCSS 系統相同備援主機與磁碟陣列之異地備援中心，當主中心遭受颱風、地震、火災或疫情威脅等重大災害無法正常運作時，將由備援中心接管主中心功能，並維持系統正常運作。

二、符合異地備援 Tier6 之規格

本公司主中心之 BCSS 系統或資料庫備份，除採用磁帶備份兩份，一份置於本公司媒體儲存室保管，一份置於異地備援中心保管外，主中心與異地備援中心間之磁碟陣列資料，透過高速網路連接並即時同步備份(PPRC)，如遇緊急狀況需啟動異地備援系統時，將可保持資料一致性避免資料遺失，符合異地備援 Tier6 之規格。

三、異地備援演練

鑒於 BCSS 系統係全國性結算交割平台，每日交割金額龐大，如遇重大災害致主中心機房受損時，須於最短時間內繼續提供各參加單位結算交割作業服務，俾維持票券保管結算交割機制營運不中斷；本公司除定期維護異地備援系統及強化控管外，每年至少定期與中央銀行及全體參加單位執行二次異地備援演練，並依演練測試計劃及備援切換操作程序，確實執行備援接管作業。

異地備援演練測試目的，在確保主中心系統遭受突發狀況無法運作時，系統能於 4 小時內，由主中心切換至異地備援中心，並可繼續正常提供票券保管結算交割作業服務，維持營運不中斷。