13 系統監控

13.1 本章目的

我想身為一個網管人員，維持企業資訊系統的運作順暢是一個最基本的職責，但隨著資訊系統的擴大，往往企業的資訊預算不見得會同步的提昇，也常使網管人員在資源不足的情況下疲於奔命，分身乏術。在這種情況下，一套能自動監控系統服務的運作狀態，並且可在系統服務發生問題時能即時的通知網管人員的自動化的監控軟體，將會成為減輕網管人員工作負荷的一大利器，在本文中，筆者將介紹一個開源碼社群中有名的監控軟體（monit），這是一套強大的監控軟體，不但可監控系統上的網路服務，甚至可監控系統相關的資源運用（例如磁碟用量，CPU 使用率等等），網管人員可利用此監控軟體，自動的監控主機的相關服務運作或其他的資源，一但發現問題即立刻以電子郵件方式通知網管人員，以減輕網管人員日常維運的工作負荷，而在本單元裏，將利用 monit 內檔案時間偵測機制來檢查網站伺服器所在目錄中的檔案時間是否有被更動，來檢查網站內的檔案是否有被不正常的存取。

13.2 實作設備

軟體名稱	官方網址	說明
Monit 5.5	http://mmonit.com/	本實作方案所使用的監控軟體

13.3 背景說明

monit 是一個功能非常強大的資源監控軟體，主要應用在監控服務主機上的相關資源，可監控的範圍包括檔案系統的變動（例如某個目錄或檔案變動），運作中的程序（Process）的監控以及網路服務（例如網站伺服器或郵件伺服器等網路服務）的監控，甚至可監控總體服務主機系統的資

源狀況（例如可設定監控系統 cpu（中央處理器）或記憶體的使用狀況），一旦，發現所監控的資源發生狀況（例如所監控的網站伺服器服務已中止），monit 監控軟體也會啟動管理者所設定相對應的應變措施（例如自動重啟網路服務或寄送警告信至管理者的信箱等功能）。簡而言之，monit 監控軟體是一個小而美的監控程式，除了可即時監控系統上的相關資源外，更可在所監控的資源發生問題時，啟動應變措施，自動重啟系統服務或以 email 通知管理者，為了方便管理者掌控系統狀況，monit 監控軟體也提供了網站伺服器的功能，以便管理者可利用網頁的方式來查看系統相關資源運作的狀況。

13.4 實作步驟

13.4.1 安裝 monit 監控軟體

安裝 monit 程式非常簡單，只需編譯三步驟：

```
./configure          #組態 monit 程式
make                 #編譯相關的 monit 程式
make install         #安裝 monit 相關程式
```

在安裝成功後即會產生名稱為 monit 的主程式，monit 程式提供了下列啟動程式時所使用的參數，如下表所示：

參數名稱	說明
-c [組態檔案名稱]	設定 monit 程式運作時所參考的組態檔名稱，Monit 預設組態檔的名稱為 monitrc
-d [秒數]	設定 monit 程式以常駐程式（daemon）方式執行並設定多久（單位為秒）會輪詢一次
-l [log 檔案名稱]	設定 monit 程式運作時，LOG 相關資訊存放的檔案名稱

參數名稱	說明
-p [pid 檔案名稱]	設定 monit 程式運作時，PID 資訊存放的檔案名稱
-s [狀態檔案名稱]	設定 monit 程式運作時所產生的狀態資訊所存放的狀態檔名稱
-t	檢查 monit 程式所使用組態檔中的設定的語法是否合法，即僅對 monit 的組態檔實施語法檢查
-v	可產生更多的輸出資訊以便追蹤
-vv	可產生最多的輸出資訊以便追蹤
-V	顯示 monit 程式的版本資訊

當 monit 以常駐程式（daemon）的形式執行時，您可使用下表的參數選項來控制 monit 程式的執行：

選項名稱	詳細說明
start all	啟動所有列在組態檔案中欲監控的服務
start name	啟動列在組態檔案中某個名稱的服務
stop all	停止所有列在組態檔案中欲監控的服務
stop name	停止列在組態檔案中某個名稱的服務
restart all	重新啟動所有列在組態檔案中欲監控的服務
restart name	重新啟動列在組態檔案中某個名稱的服務
monitor all	啟動監控所有列在組態檔案的服務
monitor name	啟動監控列在組態檔案中某個名稱的服務
unmonitor all	停止監控列在組態檔案的服務
unmonitor name	停止監控列在組態檔案中某個名稱的服務
Status	顯示所監控的服務目前狀態
Summary	顯示簡化所監控服務的目前狀態
reload	重新啟動 monit 程式並重新載入組態檔
quit	關閉 monit 程式的運作

在了解 monit 相關的程式與常用的啟動參數後，由於 monit 監控程式在運作時，需要參照相關的組態檔設定，所以接下來我們繼續來說明 monit 監控程式所提供的組態檔相關參數，如下表所示：

選項名稱	詳細說明
Set	設定指令，可利用 Set 指令來設定 monit 的相關組態
set daemon [n]	當 Monit 監控程式以常駐程式（daemon）的形式執行時，此選項即用來設定多久（單位為秒）需要輪詢檢查一次。如下例表示 60 秒輪詢檢查一次： Set daemon 60
set logfile [檔案名稱]	設定儲存 monit 監控程式所產生的 LOG 檔案名稱，如果沒有設定此選項，預設儲存的檔案 /var/log/messages。如下例即表示將 monit 程式所產生 LOG 資訊儲存在檔名為 /var/log/monit.log 的檔案中： set logfile /var/log/monit.log
set mailserver [郵件伺服器的位址]	設定要寄發警告電子郵件時，所使用的郵件伺服器的位址，如下例即表示所使用的郵件伺服器為 HINET 所提供的郵件伺服器： set mailserver msa.hinet.net
set alert [電子郵件位址]	設定當所監控的系統資源發生問題時，所要寄發的管理者的電子郵件信箱資訊，如下例即表示，當所監控的系統資源發生問題時，即將警告信寄發給 admin@XXX.XXX.XX set alert admin@XXX.XXX.XX

set mail-format{}	設定所寄發的電子郵件樣式，詳細格式如下例所示，其中 [] 內的文字為注釋：
	set mail-format
	{
	from: [來源信箱]
	subject:[主指] $SERVICE $EVENT at $DATE
	message: [信件內文]Monit $ACTION $SERVICE at $DATE
	on $HOST:
	$DESCRIPTION.
	Yours sincerely,
	monit
	}

選項名稱	詳細說明
set mail-format{}	Monit 程式提供了一些變數來儲存監控的狀態，如下簡述變數的相關意義： $EVENT：這個變數儲存異常事件的內容（例如系統服務逾時（Timeout）等等） $SERVICE：這個變數儲存發生異常事件的系統服務 $DATE：這個變數儲存的是發生異常事件時的時間 $ACTION：這個變數儲存的是 Monit 程式在發生異常事件時所執行的相關動作（例如：alert（發出警告信）或 restart（重新啟動系統服務）） $DESCRIPTION：這個變數儲存的是異常事件詳細的事件說明
set eventqueue basedir <目錄名稱> [slots] [事件數目]	有時所設定的郵件伺服器會因某種原因而無法正常的運作，monit 監控程式也很貼心的提供暫存（queue）的功能，當發現郵件伺服器出現問題時，可暫時將相關的事件暫存在本機上，等到郵件伺服器恢復正常時再將相關的事件發送出去，其中 <目錄名稱> 即是設定相關異常事件資訊暫時儲存的位置，而 slots 即是限定儲存相關異常事件最大的數量（如果沒有設定 slots 即表示不限制儲存異常事件最大的數量），如下例即表示要將相關的事件暫時儲存在 /var/log/qmonit 的目錄下： set eventqueue basedir /var/log/qmonit
If [條件式] then [動作]	條件式判斷，假如符合所設定的條件式即執行相關的動作，其中 monit 提供下列的動作選項： ALERT：當符合條件時即發出警告信通知管理者 RESTART：當符合條件時即重新啟動系統服務並發出警告信通知管理者 START：當符合條件時即啟動系統服務並發出警告信通知管理者 STOP：當符合條件時即重新啟動系統服務並發出警告信通知管理者 EXEC：當符合條件時即執行相關程式並發出警告信通知管理者 UNMONITOR：當符合條件時即停止監控相關服務並發出警告信通知管理者

選項名稱	詳細說明

check filesystem [自定義名稱] with path [路徑名稱]	檢查系統檔案系統，其中 [路徑名稱] 表示欲監控的系統目錄或檔案，如下例即表示，假如所監控的硬碟所使用的空間已超過 60% 時，即送出警告信通知管理者：
	`check filesystem root-filesystem with path /dev/sda1`
	`if space usage > 60% then alert`

check file [自定義名稱] with path [檔案實際路徑]	檢查系統檔案，其中 [檔案實際路徑] 表示欲監控的系統檔案，如下例即表示，假如所監控的 httpd.conf（為 apache 網站伺服器的設定檔）的時間屬性被更動，即重新啟動 apache：
	`check file httpd.conf with path /usr/local/apache/conf/httpd.conf`
	`if changed timestamp`
	`then exec "/usr/local/apache/bin/apachectl restart"`
	從了基本的檔案屬性（如大小、時間屬性等等）的監控外，monit 監控程式更提供了如檔案內容變動的進階監控，此部份即留待讀者自行研究了

check directory [自定義名稱] path [目錄路徑位置]	檢查系統目錄。其中 [目錄路徑位置] 表示欲監控的系統目錄實際的位置，如下例即表示，如果 /etc/ 目錄下有發生變動（例如：新增該目錄下的檔案或刪除該目錄下的檔案）的情形即會發出警告信通知管理者：
	`check directory mydir /etc/`
	`if changed hour then alert`

check host [主機名稱] with address [主機 IP 位置]	檢查主機相關的資源，其中 [主機名稱] 表示欲監控的主機名稱，[主機 IP 位置] 即為該監控主機的 IP 位置，如下例即表示監控主機 IP 為 xxx.xxx.xxx.xxx 的網站伺服器，一旦該網站伺服器在 20 秒內沒有回應即寄發警告信給管理者：
	`check host http-host with address xxx.xxx.xxx.xxx`
	`if failed port 80 protocol http with timeout 20 seconds then alert`

check system [自定義名稱]	監控系統相關的資源，例如可監控 CPU 或記憶體等使用率，如下例即為只要記憶體使用率超過 80% 即寄出警告信給管理者：
	`check system Memory`
	`if memory usage > 80% then alert`

選項名稱	詳細說明
set httpd port [通訊埠號]	Monit 監控程式有提供網站功能,以便管理者可利用網頁的方式查看系統狀態，此選項即設定啟動網站服務，其中 [通訊埠號] 指的是此網站要運作在那一個通訊埠（一般預設皆為 80 埠）如下例即為運作在 8080 埠： set httpd port 8080 另外，此選項也有提供來源控制的功能（ACL），可限制來源端連接，如下例即為僅允許 IP 位址為 xxx.xxx.xxx.xxx 的主機可連接 monit： set httpd port 8080 allow xxx.xxx.xxx.xxx 另外基於安全的考量，Monit 監控程式更提供的支援 SSL 的網站伺服器。

一般而言，monit 通常都是用來監控系統程式的運作（例如 httpd 程式是否仍在運作中），但另一方面，它也提供了系統檔案變動的監控，所以我們可利用此類監控功能來監控網站檔案的變動情形，籍此來監控網站的內容是否有被不當的更改。在此假設網站伺服器的網站根目錄為 /usr/local/apache2/htdocs，我們將利用 monit 監控程式來監控網站根目錄內的相關網頁檔案，一但相關網頁（即位於該目錄的檔案）發現變動，即寄發警告信至管理者的信箱。另外一方面，也同時監控網站伺服器的運作，如果發現網站伺服器停止服務，即寄發相關警告信至管理的信箱。接下來，我們繼續來設定相關的組態檔（檔案名稱為 /etc/monit.cf）。

monit 監控程式組態檔設定如下圖所示：

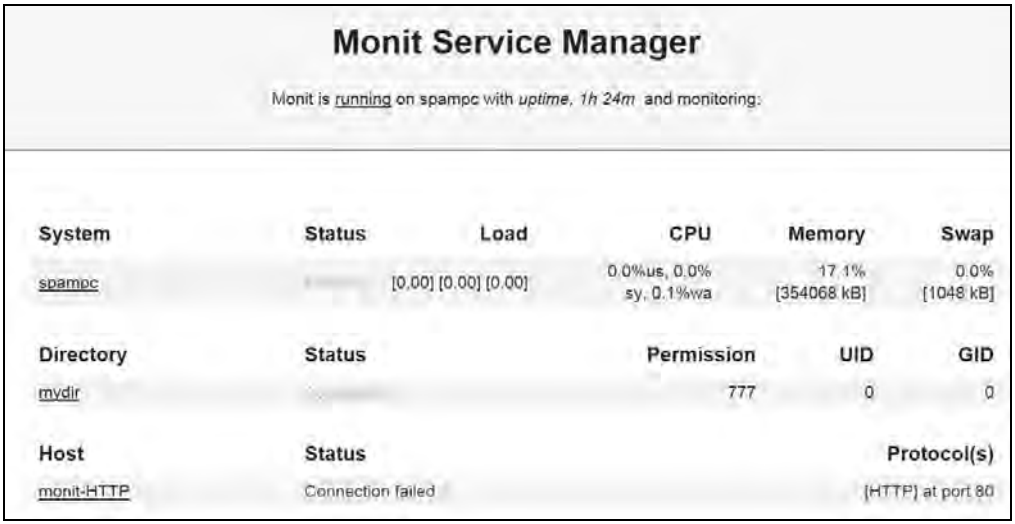
```
set daemon  60
set logfile /var/log/monit.log
set mailserver [redacted]
set mail-format {
 From: monit@[redacted]
 Subject: [monit] - $EVENT $SERVICE
 message:$EVENT item $SERVICE
        date:$DATE
        action:$ACTION
        host:$HOST
        descr:$DESCRIPTION
}
set alert [redacted]
set httpd port 2812 and  allow admin:admin
check directory mydir with path /usr/local/apache2/htdocs
 if changed  timestamp  then alert
check host monit-HTTP with address [redacted]
 if failed port 80 protocol http with timeout 10 seconds then alert
```

如下表說明相關參數設定的意義：

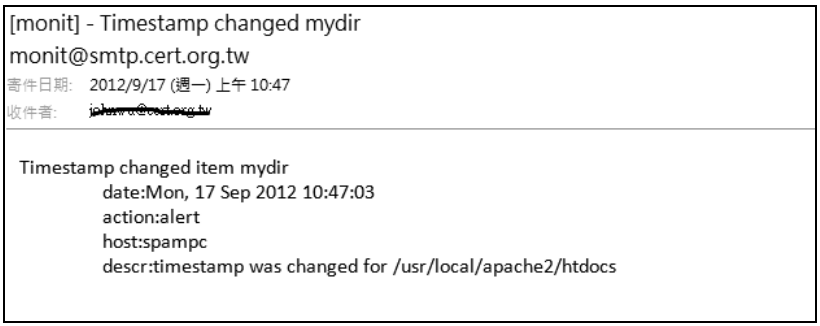
參數欄位	說明
set daemon 60	將 monit 監控程式設定為常駐程式（daemon）形式執行，並每 60 秒輪詢檢查一次。
set mailserver [郵件伺服器位址]	設定郵件伺服器的位置，此郵件伺服器即為用來寄發警告信之用。
set mail-format	設定所寄發警告信之內文與標題等相關資訊。
set alert [管理者信箱]	設定當觸發監控的異常情況發生後，所要寄發的管理者信箱。
set httpd port 2812 and allow admin:admin	啟動 monit 監控程式的網站伺服器功能（運作於 2812 埠），並設定登入的帳號／密碼為 admin/admin，在此為測試方便，僅使用帳號／密碼來控管，但在實務上，還是建議除了帳號／密碼的控管外，還要再加上來源 IP 主機的控管。
check directory mydir with path /usr/local/apache2/htdocs if changed timestamp then alert	設定當所監控的目錄發生變動時（當目錄內的檔案發生新增、修改、刪除的情況時，即會改變目錄的時間欄位（timestamp））時即發送警告信通知管理者。

參數欄位	說明
check host monit-HTTP with address [網站伺服器的位址] if failed port 80 protocol http with timeout 10 seconds then alert	設定當所監控的網站伺服器，如果在 10 秒沒有回覆，即判定為停止服務並寄送警告信通知管理者。

在設定完成後，可利用 monit -c /etc/monit.cf 來啟動 monit 程式。在啟動成功後，可先利用瀏覽器瀏覽 http://[IP]:2812/測試 monit 監控程式是否已啟動網頁管理的服務，如果一切正常，monit 監控程式會要求輸入帳號與密碼，讀者在輸入正確的帳號密碼後，即可看到如下之畫面即表示已成功啟動 monit 監控程式。



接下來，可測試更改所監控的目錄內的檔案（如在該目錄下新增或刪除檔案等），monit 監控程式將會發出如下圖示（告知所監控的目錄已發生變動）的警告信，即表示 monit 監控程式已正常的運作。



至此，一個可自動監控系統相關資源的監控軟體已告完成。