嘉因資訊
TQUARK INFORMATION

使用 gMSA 服務帳號執行工作排程

適用門將版本:4.XX.XXXX.XX
修訂日期:2023/05/12

1 適用情境

1.1 作業目的

gMSA 有較小的權限，且密碼管理會移至 Windows OS，每 30 天自動變更高強度密碼，使系統安全性大大提升。

1.2 適用環境

需有 AD 網域架構，且 Member Server 的這些電腦也必須要 Windows Server 2012 以上或 Windows 8 的環境才可以使用。

本文主機 OS 以 Windows 10 為例。

2 前置作業

AD Server 啟用 gMSA，並加入相關 Member Server，請參考微軟說明

https://learn.microsoft.com/zh-tw/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts

3 Client Server 設定

3.1 Client 設定 gMSA

各 OS 的 gMSA 帳號設定方式。

Windows 8～11
● 安裝 RSAT:Active Directory Domain Services 和輕量型目錄服務工具 ● 使用系統管理員，開啟 PowerShell 執行指令 ■ Install-adserviceaccount -identity “gMSA 帳號” ● 測試使用下面指令 ■ Test-adserviceaccount -identity “gMSA 帳號”
Windows Server
● 安裝 Windows PowerShell 的 Active Directory 模組 ■ 位於遠端伺服器管理工具=>角色管理工具=>AD DS 及 AD LDS 工具 ● 使用系統管理員，開啟 PowerShell 執行指令 ■ Install-adserviceaccount -identity “gMSA 帳號” ● 測試使用下面指令 ■ Test-adserviceaccount -identity “gMSA 帳號”

```
PS C:\Users\KUANGLIANG> install-adserviceaccount -identity "gMSAService"
PS C:\Users\KUANGLIANG> Test-adserviceaccount -identity "gMSAService"
True
```

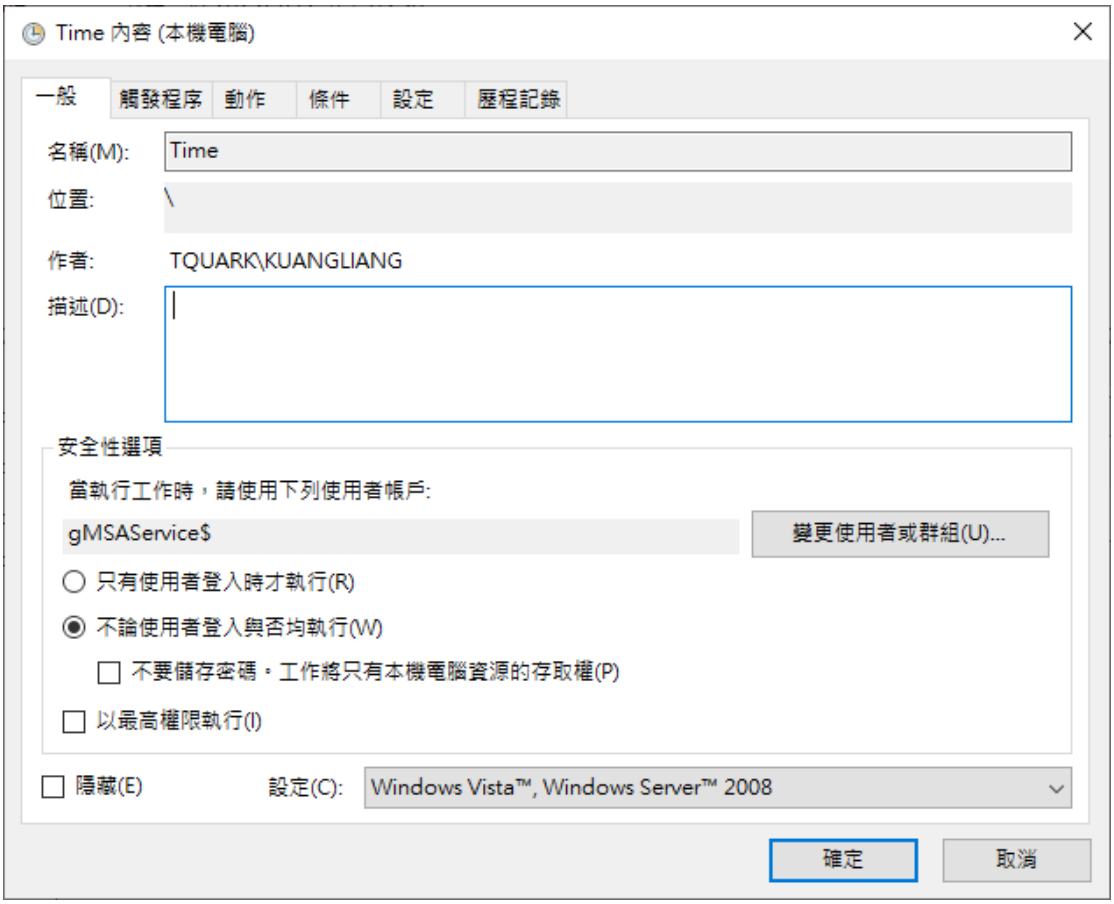
3.2 套用排程

先將排程建立好後，使用系統管理員，開啟 PowerShell 執行下列指令。

schtasks /change /TN "排程名稱" /RU "網域\gMSA 帳號$" /RP ""

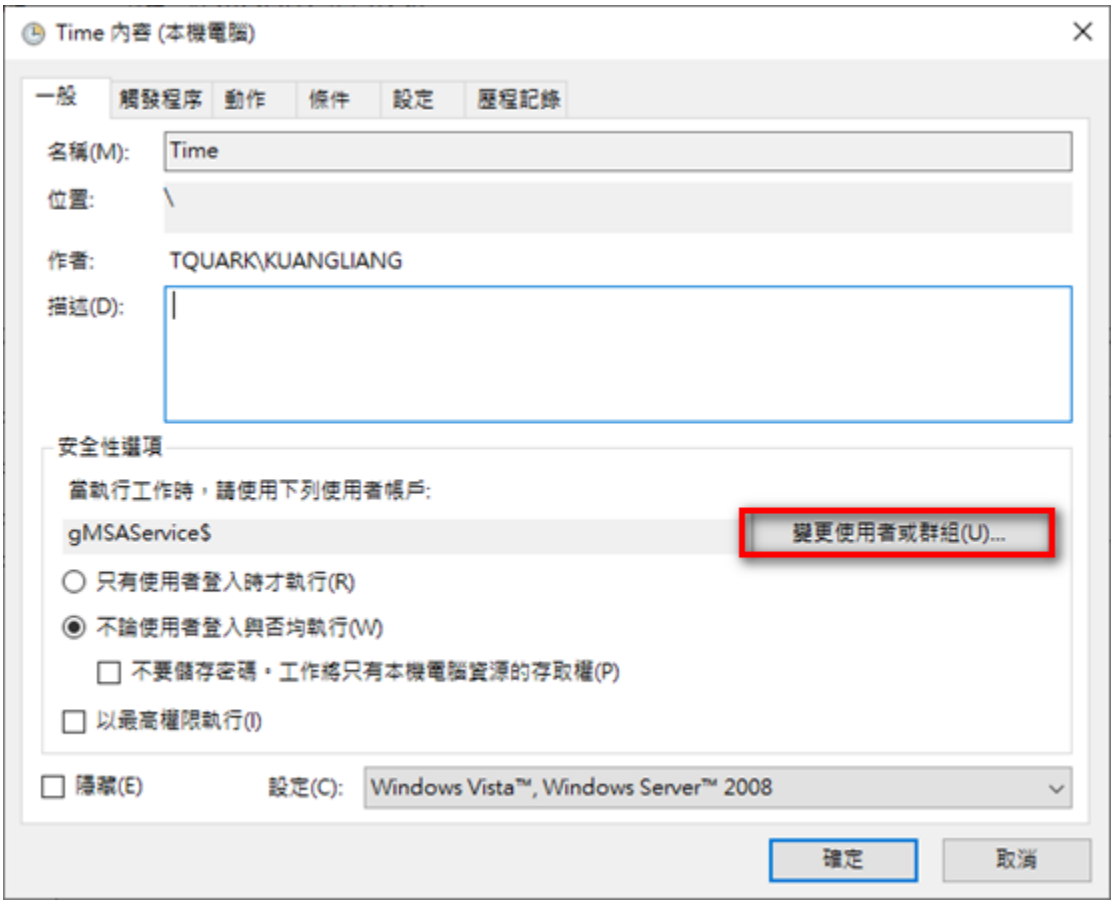
成功後，該排程的使用帳號就會改為 gMSA。

```
PS C:\Users\KUANGLIANG> schtasks /change /TN "Time" /RU "TQUARK\gMSAService$" /RP ""
警告: 當執行身分密碼是空白時，排程工作可能因為安全性原則而無法執行。
成功: 排程工作 "Time" 的參數已經變更。
```



3.3 修改排程

若事後排程需要修改，須先更換帳號，待修改完成後，重新執行 3.2 套用排程步驟。


Time 內容 (本機電腦)
一般
觸發程序
動作
條件
設定
歷程記錄
名稱(M):
Time
位置:
\
作者:
TQUARK\KUANGLIANG
描述(D):
安全性選項
當執行工作時，請使用下列使用者帳戶:
gMSAService$
變更使用者或群組(U)...
只有使用者登入時才執行(R)
不論使用者登入與否均執行(W)
不要儲存密碼。工作將只有本機電腦資源的存取權(P)
以最高權限執行(I)
隱藏(E)
設定(C):
Windows Vista™, Windows Server™ 2008
確定
取消