

使用 gMSA 服務帳號執行門將

適用門將版本:4.XX.XXXX.XX

修訂日期: 2024/01/04

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。

1.3 應用限制

OGWin、OGBioScan 與 OGProxyWin 不適用此設定。

若 OGWeb 啟用 Windows 認證方式登入，不適用此設定。

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 <ul style="list-style-type: none">● 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<ul style="list-style-type: none">■ Install-adserviceaccount -identity "gMSA 帳號"● 測試使用下面指令<ul style="list-style-type: none">■ Test-adserviceaccount -identity "gMSA 帳號"
Windows Server <ul style="list-style-type: none">● 安裝 Windows PowerShell 的 Active Directory 模組<ul style="list-style-type: none">■ 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<ul style="list-style-type: none">■ Install-adserviceaccount -identity "gMSA 帳號"● 測試使用下面指令<ul style="list-style-type: none">■ 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 IIS

開啟 IIS 應用程式集區，選擇 OGSysm4 後，點擊進階設定

應用程式集區

此網頁可讓您檢視及管理伺服器上的應用程式集區清單。應用程式集區與工作者處理序相關聯，包含一個或多個應用程式，而且會將不同的應用程式隔離。

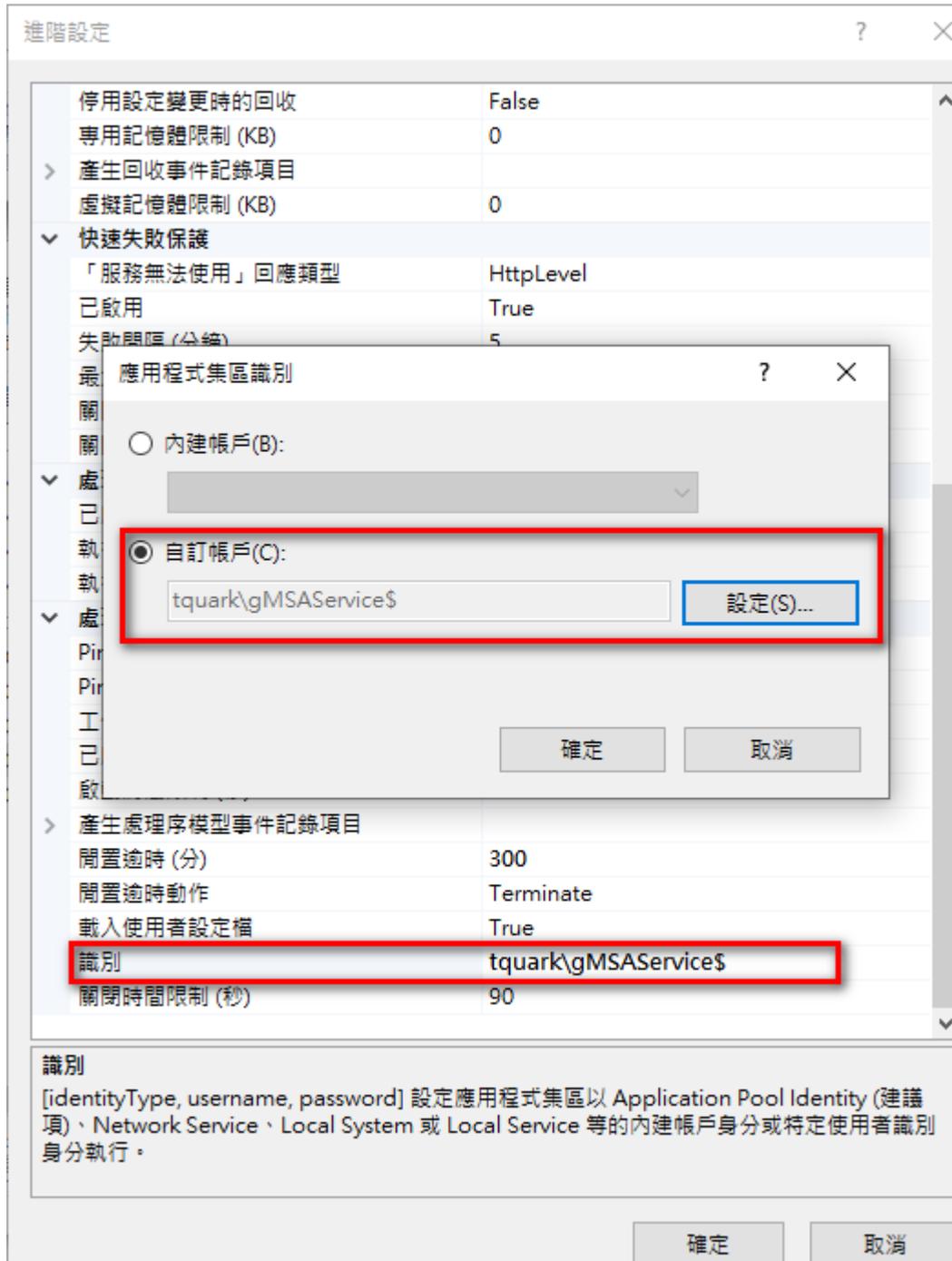
名稱	狀態	.NET CLR ...	Managed 管...	識別
.NET v2.0	已啟動	v2.0	整合式	Appli
.NET v2.0 Classic	已啟動	v2.0	傳統	Appli
.NET v4.5	已啟動	v4.0	整合式	Appli
.NET v4.5 Classic	已啟動	v4.0	傳統	Appli
Classic .NET Ap...	已啟動	v2.0	傳統	Appli
DefaultAppPool	已啟動	v4.0	整合式	Appli
OGSystem4	已啟動	v4.0	整合式	Netw
OGWebCore	已啟動	沒有 Man...	整合式	Appli

篩選器: 移至(G) 全部顯示(A)

動作

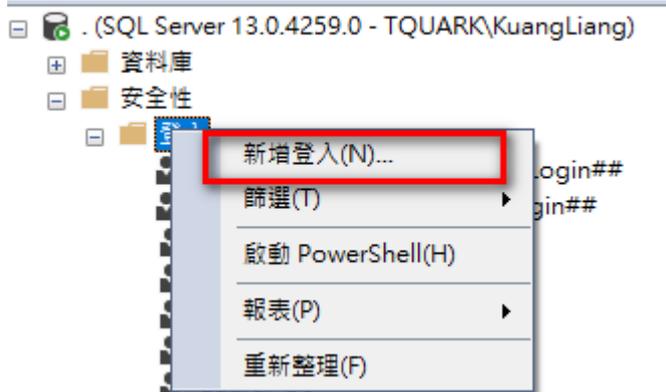
- 新增應用程式集區...
- 設定應用程式集區預設值...
- 應用程式集區工作
 - 啟動
 - 停止
 - 回收...
- 編輯應用程式集區
 - 基本設定...
 - 回收...
 - 進階設定...**
 - 重新命名
- 刪除
- 檢視應用程式
- 說明

將識別改成 gMSA 帳號(不用輸入密碼)



3.3 建立 SQL 登入帳號

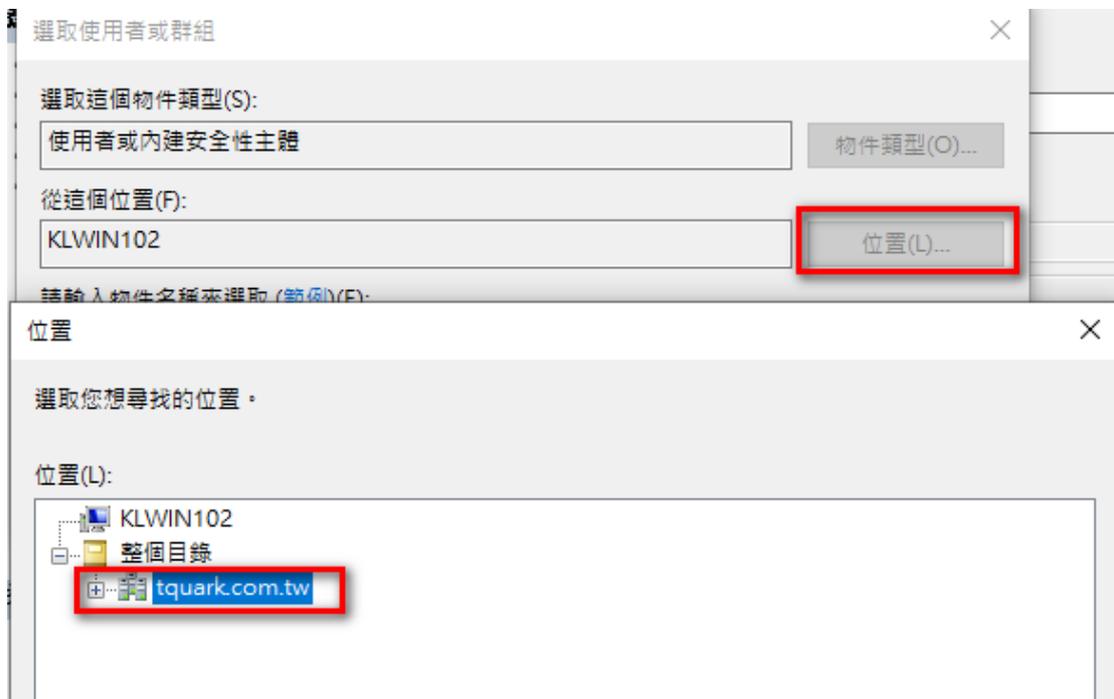
新增登入帳號



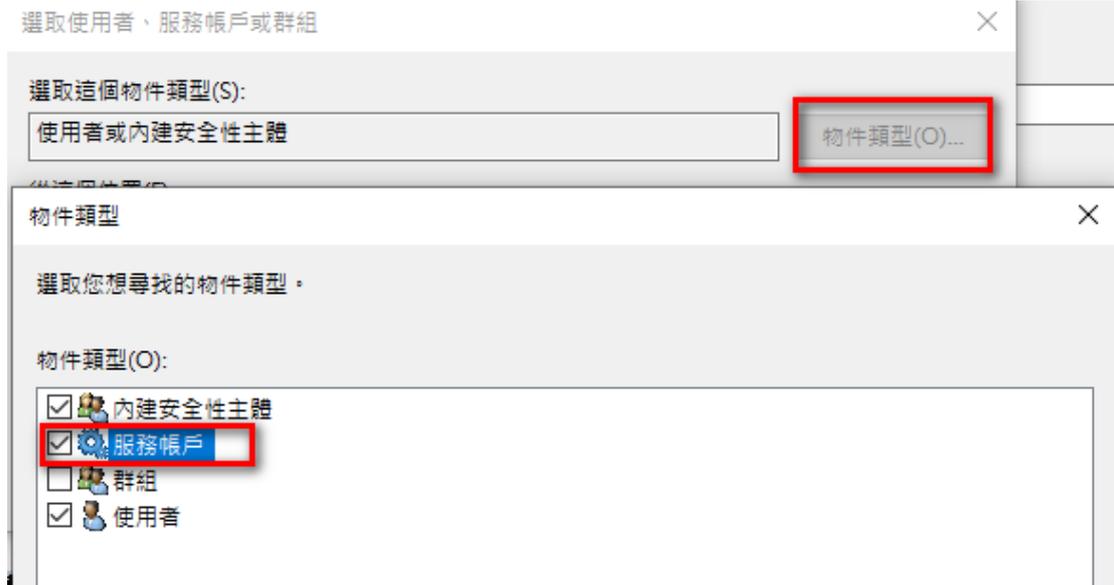
選取 Windows 驗證後，執行搜尋



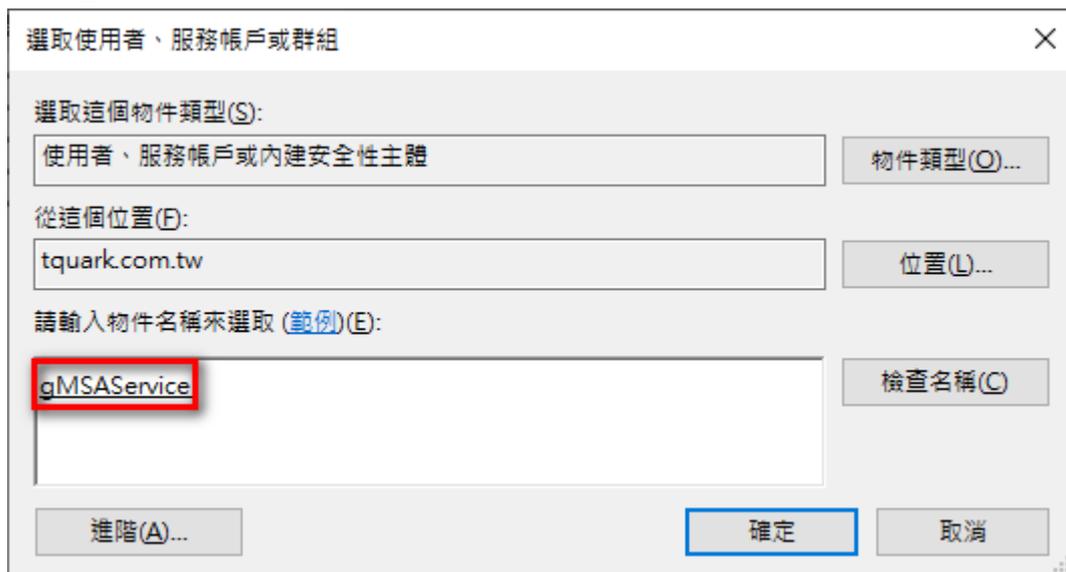
點擊位置，選取網域



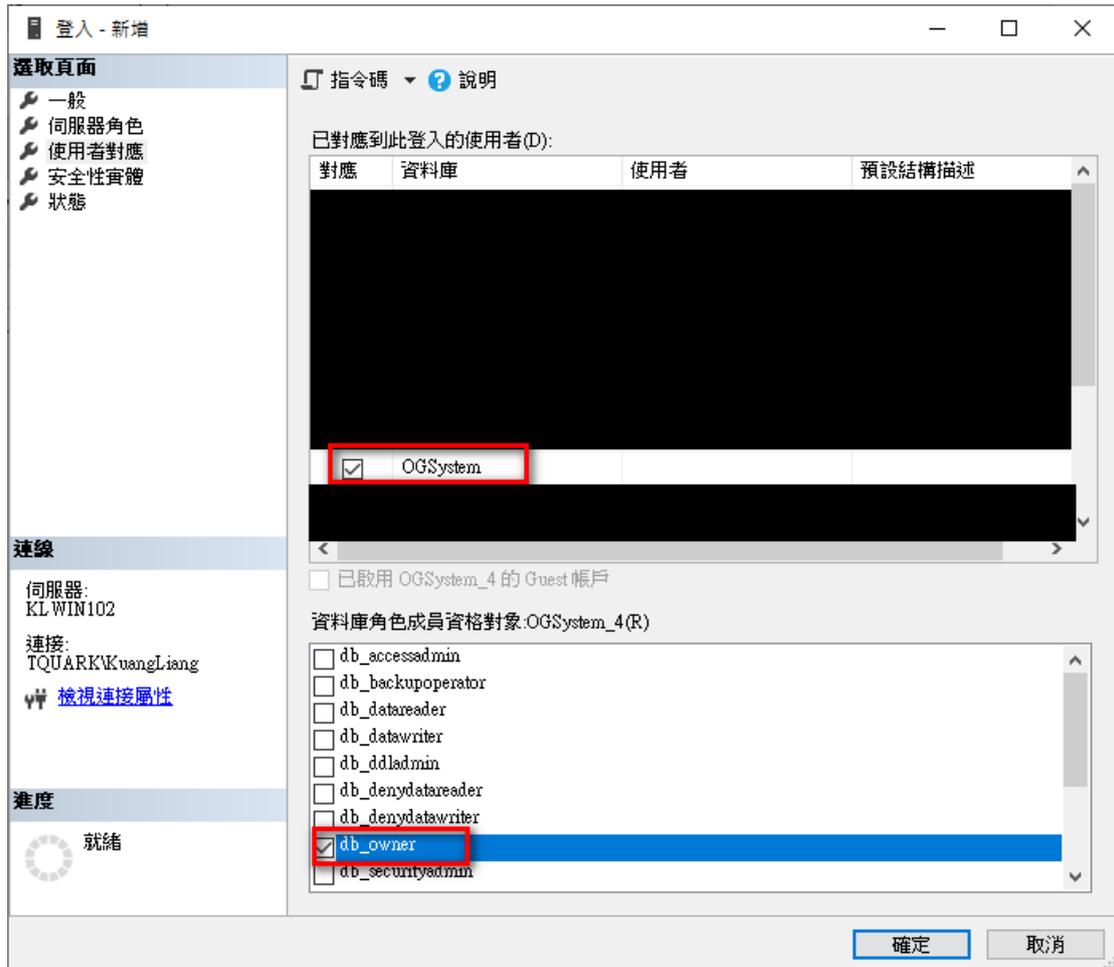
點擊物件類型，勾選服務帳號



輸入 gMSA 的帳號



賦予 OGSystem，db_owner 角色



3.4 Config 修改

開啟 OGWeb、OGServer、OGScheduleAgent 內的相關 Config，將 connectionStrings 改用 Windows 認證

搜尋 connectionStrings，將 User 與 Password 改為 Integrated Security=True
修改前

```
<add name="OGSystem" providerName="System.Data.SqlClient"
connectionString="data source=KLWIN102;initial
catalog=OGSystem_4;User=sa;Password=TQUARK123!;Application
Name=OGServer" />
```

修改後

```
<add name="OGSystem" providerName="System.Data.SqlClient"
connectionString="data source=KLWIN102;initial catalog=OGSystem_4; Integrated
Security=True;Application Name=OGServer" />
```

3.5 套用排程

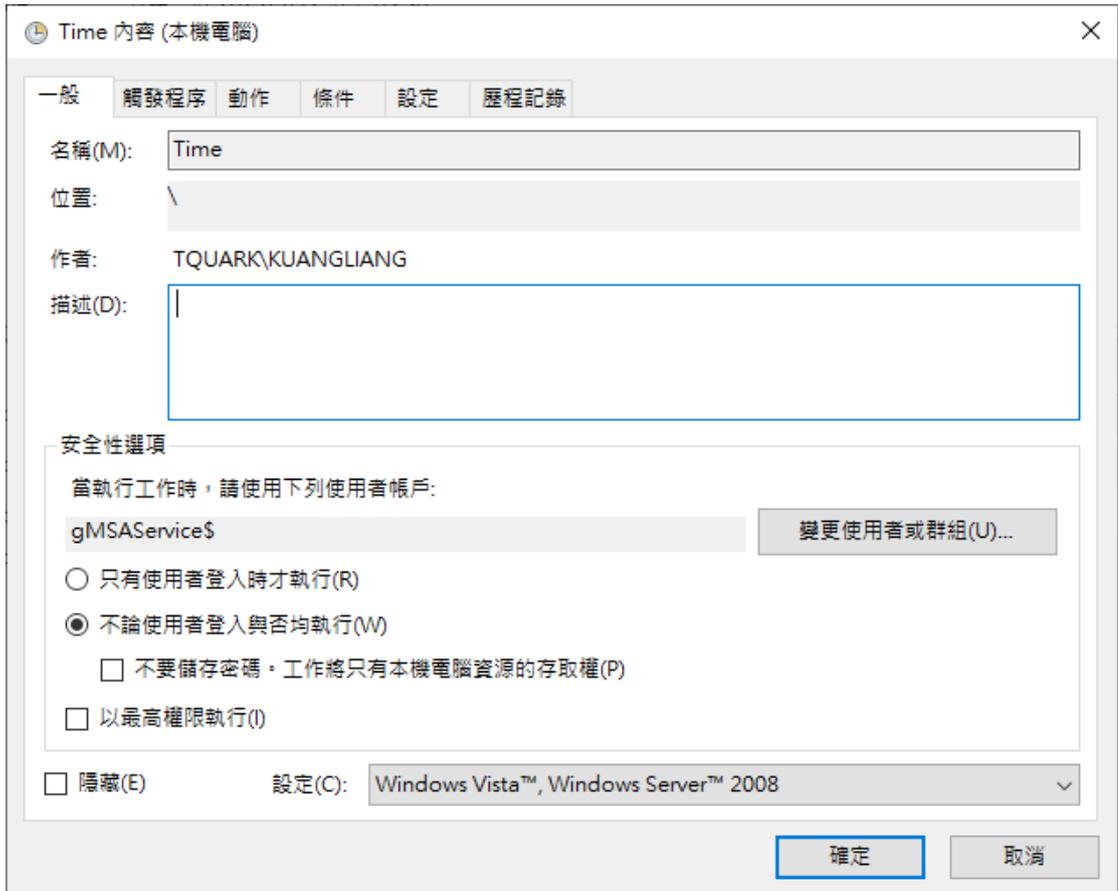
先將排程建立好後，使用系統管理員，開啟 PowerShell 執行下列指令。

```
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。
```

透過 gMSA 執行 OGSchedule 排程



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)

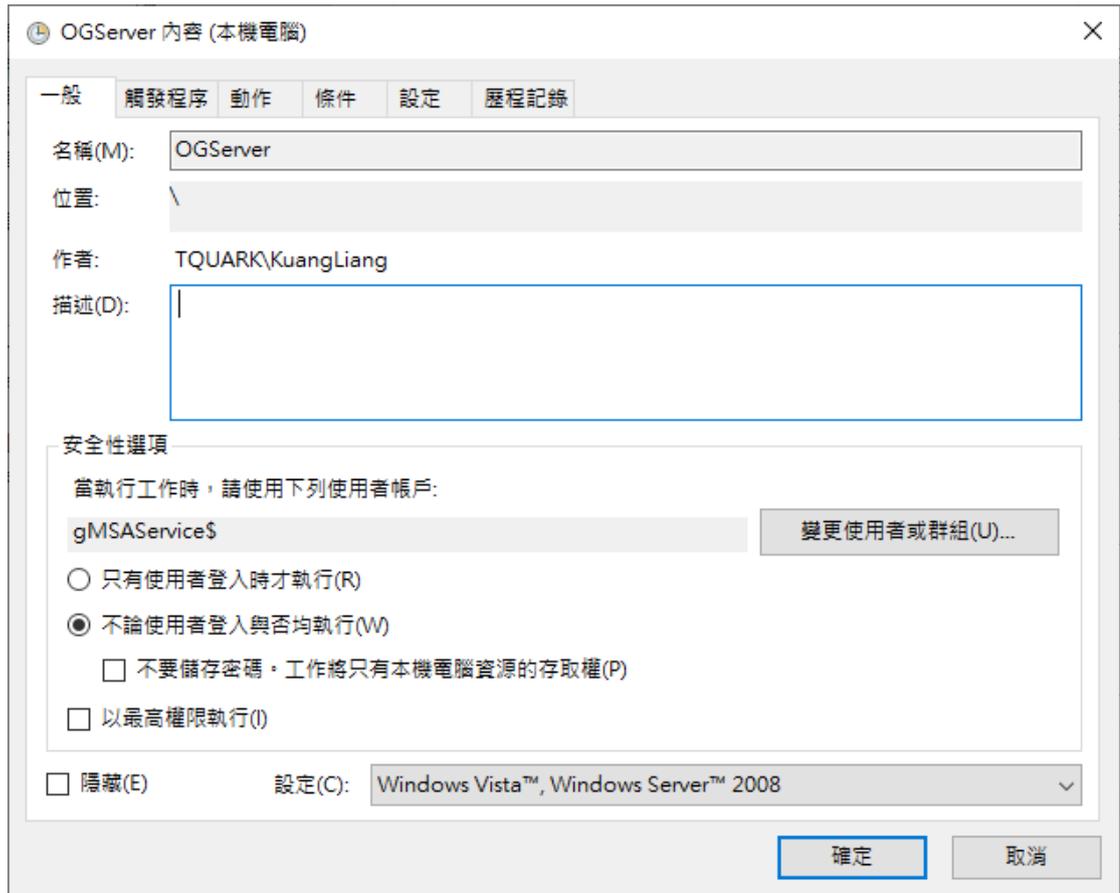
不要儲存密碼，工作將只有本機電腦資源的存取權(P)

以最高權限執行(I)

隱藏(E) 設定(C): Windows Vista™, Windows Server™ 2008

確定 取消

透過 gMSA 執行 OGServer



OGServer 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): OGSerVer

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)

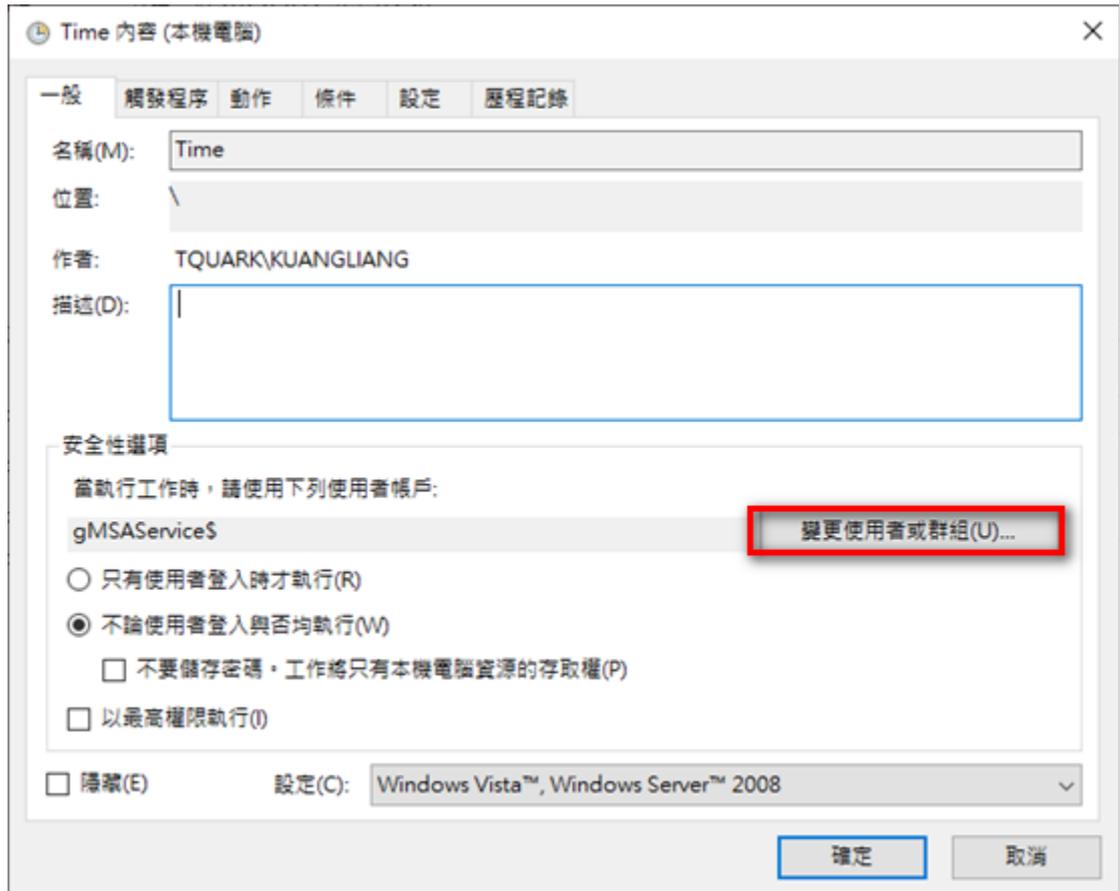
以最高權限執行(I)

隱藏(E) 設定(C): Windows Vista™, Windows Server™ 2008

確定 取消

3.5.1 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。



3.6 修改目錄權限

賦予 OGWeb、OGServer、OGScheduleAgent 目錄，gMSA 完全控制權限

