

### 使用 gMSA 服務帳號執行門將

適用門將版本:4.XX.XXXXXXXXX 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-servi ce-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。



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

# 3.2 套用 IIS

True

開啟 IIS 應用程式集區,選擇 OGSystem4 後,點擊進階設定



🖣 應用程式	集區			
此網頁可讓您檢視及管 工作者處理序相關聯、 式隔離。	理伺服器. 包含一個:	上的應用程式集 或多個應用程式	區清單。應用程式身 ,,而且會將不同的應	長區與 展用程
飾選器:	-	💚 移至(G) 👻	🕁 全部顯示(A) 🗎	÷
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	し取到	没角 Man	整合式	Appli



將識別改成 gMSA 帳號(不用輸入密碼)



序用設定變更時的回收 身用記憶體限制 (KB) 產生回收事件記錄項目 壓擬記憶體限制 (KB)	False 0
厚用記憶體限制 (KB) 產生回收事件記錄項目 國擬記憶體限制 (KB)	0
崔生回收事件記錄項目 ᄛ擬記憶體限制 (KB)	
o擬記憶體限制 (KB)	
	0
快速失敗保護	
「服務無法使用」回應類型	HttpLevel
已啟用	True
もない (分輪)	5
曼 應用程式集區識別	? ×
6)	
圓 ○ 內建帳戶(B):	
3	
№ 自訂帳戶(C):	
tquark\gMSAService\$	設定(S)
ir	
ir.	
-]	
-	確定 取消
×∟	
罟渝時(分)	300
	<b>T</b>
1] <u>二</u> 逾時動作	Terminate
3.当应11(5) 13置逾時動作 13.入使用者設定檔	True
調査通時動作 載入使用者設定檔 問	Terminate True tquark\gMSAService\$
	啟用 正規區(公會) 應用程式集區識別 ○ 內建帳戶(B): ● 自訂帳戶(C): tquark\gMSAService\$ 生處理序模型事件記錄項目

# 3.3 建立 SQL 登入帳號

新增登入帳號



-	6	. (S	QL	Serv	er	13.	0.425	i9.0 -	TQU	ARK\K	lua	ngLiang)
	+		資料	庫								
	-		安全	≧lŧ								
		-				新	増登,	λ(N).				ogin##
					ľ	篩	選(T)					gin##
						啟	動 Po	owerS	hell(H	H)		
						報	表(P)			I	•	
						重	新整理	璽(F)				

#### 選取 Windows 驗證後,執行搜尋

▋ 登入 - 新増		_		×
選取頁面	🖵 指令碼 👻 😯 說明			
<ul> <li>              一般             ・</li></ul>	登入名稱(N):	 	搜尋(E	3)
	○ Willdows 級證(W) ○ SQL Server 驗證(S) 密碼(P):			
	確認密碼(C):			

#### 點擊位置,選取網域

選取使用者或群組	×	
選取這個物件類型(S):		-
使用者或內建安全性主體	物件類型(O)	
從這個位置(F):		
KLWIN102	位置(L)	
结翰入物件之稱來選取 (新像\\/F\·		
		×
選取您想尋找的位置。		
位置(L):		
  整個目錄 <u> 中</u> … <mark> 融</mark> ·· 聞 tquark.com.tw		

點擊物件類型,勾選服務帳號



選取使用者、服務帳戶或群組	×	
選取這個物件類型(S): 使用者或內建安全性主體	物件類型(O)	
物件類型		Х
選取您想尋找的物件類型。		
物件類型(O): ☑ 總 內建安全性主體 ☑ 總 服務帳戶 □ 總 群組 ☑		

輸入 gMSA 的帳號

選取使用者、服務帳戶或群組	×
選取這個物件類型( <u>S</u> ):	
使用者、服務帳戶或內建安全性主體	物件類型( <u>O</u> )
從這個位置(E):	
tquark.com.tw	位置(L)
請輸入物件名稱來選取 ( <u>範例</u> )( <u>E</u> ):	
gMSAService	檢查名稱(C)
·	取当
x2PB()	HX//R

賦予 OGSystem,db\_owner 角色



1 登入 - 新增		- 0	×
<b>選取頁面</b> メー般 メ 伺服器角色 を 使田 去對 m	丘指令碼 ▼ ? 說明       已對應到此登入的使用者(D):		
▶ 使用者到應 ▶ 安全性審體 ▶ 狀態	對應 資料庫 使用者	預設結構描述	~
連線	<	>	
伺服器: KLWIN102	_ 已啟用 OGS ystem_4 的 Guest 帳戶 資料庫角色成員資格對象:OGS ystem 4(R)		
連接: TOHARK\KuangLiang	db_accessadmin		^
	db_backupoperator db_datareader db_datawriter db_ddladmin		
進度	☐ db_denydatareader ☐ db_denydatawriter		
就緒	db_securityadmin		~
		確定 取消	

# 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 "<mark>排程名稱</mark>" /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> <mark>schtasks</mark> /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" 的參數已經戀罪。

透過 gMSA 執行 OGSchedule 排程

🕒 Time 內容	(本機	電腦)					$\times$
一般觸	發程序	動作	條件	設定	歷程記錄		
名稱(M):	Time	9					
位置:	X.						
作者:	TQU	ARK\KU	ANGLIA	NG			
描述(D):							
安全性選	頁——						
當執行工	作時,	請使用下	列使用者	首帳戶:			
gMSASe	ervice\$					變更使用者或群組(U)	
	使用者會	登入時才朝	丸行(R)				
● 不論(	使用者會	登入與否均	匀執行(W	0			
□ <b>7</b>	要儲存	密碼・エ	作將只有	有本機電腦	◎資源的存取權(P)		
	高權限執	丸行(1)					
□ 隱藏(E)		設》	萣(C):	Windows	s Vista™, Windows Server™ 20	008	~
						確定 取消	

透過 gMSA 執行 OGServer



OGSe	rver 內容 (	(本機電腦)	)			
般	觸發程序	動作	條件	設定	歷程記錄	
名稱(M	I): OGS	Server				
立置:	X					
乍者:	TQU	JARK\Kua	ngLiang	9		
苗述(D)	):					
安全的	E選塤 行工作時,	建使用下	利使用者	≚dE ES.		
gMS	AService\$		20182/101#	a mx/~~-		變更使用者或群組(U)
ОЯ	有使用者	登入時才朝	九行(R)			
● 不	論使用者	登入與否均	自執行(W	)		
	] 不要儲存	字密碼・エ	作將只有	有本機電腦	資源的存取權(P)	
	最高權限報	訙行(I)				
]隱藏	t(E)	設為	ጀ(C): \	Windows	Vista™, Windows Serve	r™ 2008 ∨

### 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。



Time	內容	(本機會	電腦)						×
一般	觸發	程序	動作	條件	設定	歷程記錄			
名稱(M	1):	Time	•						
位置:		١							1
作者:		TQU	ARK\KU	ANGLIA	NG				
描述(D	):	I							1
									1
一安全的	主選項								
畜執	17 I 1	作時,	請使用♪	列使用1	首帳户:			·····································	
gMS	ASer	vice\$						變更使用者或群組(U)	
OR	有使	用者量	2入時才報	丸行(R)					
● 7	論使	用者曾	と うちょう しんしょう しんしょ しんしょ	匀執行(M	0				
	] 不	要儲存	密碼・エ	作將只不	有本機電腦	資源的存取權(P)			
	最高	權限動	1行(1)						
	(E)		設)	E(C):	Windows	Vista™, Windows S	erver™ 20	08 ~	
								確定 取消	

## 3.6 修改目錄權限

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



OGServer 的權限		2
₹全性		
物件名稱: C:\OGServer		
群組或使用者名稱(G):		
Authenticated Users		
SYSTEM		
& gMSAService\$		
Administrators (KLWIN102)	Administrators)	
🕵 Users (KI WIN102\Users)		
	新増(D)	移除(R)
	新増(D)	移除(R)
gMSAService\$ 的權限(P)	新増(D) 允許	移除(R) 拒絕
gMSAService\$ 的權限(P) 完全控制	新増(D) 允許 ☑	移除(R) 拒絕
gMSAService\$ 的權限(P) 完全控制 修改	新増(D) 允許 ☑	移除(R) 拒絕
gMSAService\$ 的權限(P) 完全控制 修改 請取和執行	新増(D) 允許 ☑ ☑	移除(R) 拒絕
gMSAService\$ 的權限(P) 完全控制 修改 請取和執行 列出答料本內容	新増(D) 允許 ☑ ☑ ☑	移除(R) 拒絕
gMSAService\$ 的權限(P) 完全控制 修改 請取和執行 列出資料夾內容 請取	新増(D) 允許 ☑ ☑ ☑ ☑	移除(R) 拒絕
gMSAService\$ 的權限(P) 完全控制 修改 讀取和執行 列出資料夾內容 讀取	新増(D) 允許 ☑ ☑ ☑ ☑ ☑ ☑	移除(R) 拒絕
gMSAService\$ 的權限(P) 完全控制 修改 請取和執行 列出資料夾內容 請取	新増(D) 允許 ビ ビ ビ ビ ビ	移除(R) 拒絕
gMSAService\$ 的權限(P) 完全控制 修改 請取和執行 列出資料夾內容 請取	新増(D) 允許 ダ ダ ダ ジ	移除(R) 拒絕