| **表1-AD本機之安全性設定(Default Domain Controller Policy)**  **AD主機：** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **項次** | **類別** | **項目** | **GCB及綜合建議值** | **機關設定** | **結果** |
| 1 | 密碼原則 | 密碼最短使用期限 | 1天 |  |  |
| 2 | 密碼最長使用期限 | 90天以下 |  |  |
| 3 | 最小密碼長度 | 12字元 |  |  |
| 4 | 密碼必須符合複雜性需求 | 啟用 |  |  |
| 5 | 強制執行密碼歷程記錄 | 3代以上 |  |  |
| 6 | 使用可還原的加密來存放密碼 | 停用 |  |  |
| 7 | 帳戶鎖定原則 | 帳戶鎖定閾值 | 5次 |  |  |
| 8 | 重設帳戶鎖定計數器的時間間隔 | 15分鐘 |  |  |
| 9 | 帳戶鎖定期間 | 15分鐘 |  |  |
| 10 | 安全性選項 | Microsoft網路用戶端：傳送未加密的密碼到其他廠商的SMB伺服器 | 停用 |  |  |
| 11 | Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意) | 已啟用 |  |  |
| 12 | Microsoft網路用戶端：數位簽章用戶端的通訊(自動) | 已啟用 |  |  |
| 13 | Microsoft網路伺服器：伺服器SPN目標名稱驗證層級 | 關閉 |  |  |
| 14 | Microsoft網路伺服器：數位簽章伺服器的通訊(自動) | 已啟用 |  |  |
| 15 | Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意) | 已啟用 |  |  |
| 16 | Microsoft網路伺服器：暫停工作階段前，要求的閒置時間 | 15分鐘 |  |  |
| 17 | Microsoft網路伺服器：當登入時數到期時，中斷用戶端連線 | 已啟用 |  |  |
| 18 | MSS：(NoDefaultExempt) Configure IPSec exemptions for various types of network traffic. | Multicast, broadcast, and ISAKMP are exempt (Best for Windows XP) |  |  |
| 19 | MSS：(KeepAliveTime) How often keep-alive packets are sent in milliseconds | 300000 or 5 minutes (recommended) |  |  |
| 20 | MSS：(TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | 3 |  |  |
| 21 | MSS：(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | 已啟用 |  |  |
| 22 | MSS：(Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments) | 已啟用 |  |  |
| 23 | MSS：(DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) | Highest protection, source routing is completely disabled |  |  |
| 24 | MSS：(DisableIPSourceRouting IPv6)IP source routing protection level(protects against packet spoofing) | Highest protection, source routing is completely disabled |  |  |
| 25 | MSS：(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers | 已啟用 |  |  |
| 26 | MSS：(TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) | 3 |  |  |
| 27 | MSS：(PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | 已啟用 |  |  |
| 28 | MSS：(AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments) | 已啟用 |  |  |
| 29 | MSS：(WarningLevel) Percentage threshold for the security event log at which the system will generate a warning | 0.9 |  |  |
| 30 | MSS：(SafeDllSearchMode) Enable Safe DLL search mode (recommended) | 已啟用 |  |  |
| 31 | MSS：(AutoAdminLogon) Enable Automatic Logon (not recommended) | 已停用 |  |  |
| 32 | MSS：(AutoShareServer) Enable Administrative Shares (recommended except for highly secure environments) | 已啟用 |  |  |
| 33 | MSS：(ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) | 0 |  |  |
| 34 | 互動式登入：在密碼到期前提示使用者變更密碼 | 14天 |  |  |
| 35 | 互動式登入：要求網域控制站驗證以解除鎖定工作站 | 已啟用 |  |  |
| 36 | 互動式登入：網域控制站無法使用時，要快取的先前登入次數 | 0次 |  |  |
| 37 | 互動式登入：智慧卡移除操作 | 鎖定工作站 |  |  |
| 38 | 互動式登入：須有智慧卡 | 已停用 |  |  |
| 39 | 互動式登入：不要求按CTRL+ALT+DEL鍵 | 已停用 |  |  |
| 40 | 互動式登入：不要顯示上次登入的使用者名稱 | 已啟用 |  |  |
| 41 | 系統加密編譯：對使用者儲存在電腦上的金鑰強制使用增強式金鑰保護 | 當新金鑰被儲存及使用時，不要求使用者的輸入 |  |  |
| 42 | 系統加密編譯：使用FIPS 140相容加密演算法，包括加密、雜湊以及簽署演算法 | 已啟用 |  |  |
| 43 | 系統物件：加強內部系統物件的預設權限(例如：符號連結) | 已啟用 |  |  |
| 44 | 系統物件：要求不區分大小寫用於非Windows子系統 | 已啟用 |  |  |
| 45 | 系統設定：選擇性的子系統 | Posix |  |  |
| 46 | 系統設定：於軟體限制原則對Windows可執行檔使用憑證規則 | 已啟用 |  |  |
| 47 | 使用者帳戶控制：提示提升權限時切換到安全桌面 | 已啟用 |  |  |
| 48 | 使用者帳戶控制：允許UIAccess應用程式不使用安全桌面來提升權限 | 已停用 |  |  |
| 49 | 使用者帳戶控制：在管理員核准模式，系統管理員之提升權限提示的行為 | 提示要求同意非 Windows 二進位檔案 |  |  |
| 50 | 使用者帳戶控制：僅針對已簽署與驗證過的可執行檔，提高其權限 | 已停用 |  |  |
| 51 | 使用者帳戶控制：所有系統管理員均以管理員核准模式執行 | 已啟用 |  |  |
| 52 | 使用者帳戶控制：偵測應用程式安裝，並提示提升權限 | 已啟用 |  |  |
| 53 | 使用者帳戶控制：使用內建的Administrator帳戶的管理員核准模式 | 已啟用 |  |  |
| 54 | 使用者帳戶控制：標準使用者之提升權限提示的行為 | 提示輸入認證 |  |  |
| 55 | 使用者帳戶控制：僅針對在安全位置安裝的UIAccess應用程式，提高其權限 | 已啟用 |  |  |
| 56 | 使用者帳戶控制：將檔案及登錄寫入失敗虛擬化並儲存至每一使用者位置 | 已啟用 |  |  |
| 57 | 修復主控台：允許軟碟複製以及存取所有磁碟和所有資料夾 | 已停用 |  |  |
| 58 | 修復主控台：允許自動系統管理登入 | 已停用 |  |  |
| 59 | 帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台 | 已啟用 |  |  |
| 60 | 帳戶：重新命名來賓帳戶名稱 | Renamed\_Guest |  |  |
| 61 | 帳戶：重新命名系統管理員帳戶 | Renamed\_Admin |  |  |
| 62 | 裝置：防止使用者安裝印表機驅動程式 | 已啟用 |  |  |
| 63 | 裝置：允許卸除而不須登入 | 已停用 |  |  |
| 64 | 裝置：允許格式化以及退出卸除式媒體 | Administrators |  |  |
| 65 | 裝置：CD-ROM存取只限於登入本機的使用者 | 已停用 |  |  |
| 66 | 裝置：軟碟機存取只限於登入本機的使用者 | 已停用 |  |  |
| 67 | 網域成員：停用電腦帳戶密碼變更 | 已停用 |  |  |
| 68 | 網域成員：最長電腦帳戶密碼有效期 | 30天 |  |  |
| 69 | 網域成員：安全通道資料加以數位加密或簽章(自動) | 已啟用 |  |  |
| 70 | 網域成員：安全通道資料加以數位簽章(可能的話) | 已啟用 |  |  |
| 71 | 網域成員：要求增強式(Windows 2000或更新)工作階段金鑰 | 已啟用 |  |  |
| 72 | 網域成員：安全通道資料加以數位加密(可能的話) | 已啟用 |  |  |
| 73 | 網域控制站：拒絕電腦帳戶密碼變更 | (無此項目) |  |  |
| 74 | 網域控制站：允許伺服器操作者排程工作 | (無此項目) |  |  |
| 75 | 網域控制站：LDAP伺服器簽章要求 | (無此項目) |  |  |
| 76 | 網路存取：讓Everyone權限套用到匿名使用者 | 已停用 |  |  |
| 77 | 網路存取：共用和安全性模式用於本機帳戶 | 傳統 - 本機使用者以自身身份驗證 |  |  |
| 78 | 網路存取：不允許SAM帳戶的匿名列舉 | 已啟用 |  |  |
| 79 | 網路存取：限制匿名存取具名管道和共用 | 已啟用 |  |  |
| 80 | 網路存取：可遠端存取的登錄路徑及子路徑 | System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog |  |  |
| 81 | 網路存取：允許匿名SID/名稱轉譯 | 已停用 |  |  |
| 82 | 網路存取：可以匿名存取的共用 | 無 |  |  |
| 83 | 網路存取：可以匿名存取的具名管道 | 無 |  |  |
| 84 | 網路存取：可遠端存取的登錄路徑 | System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion |  |  |
| 85 | 網路存取：不允許存放網路驗證的密碼與認證 | 已停用 |  |  |
| 86 | 網路存取：不允許SAM帳戶和共用的匿名列舉 | 已啟用 |  |  |
| 87 | 網路安全性：下次密碼變更時不儲存LAN Manager雜湊數值 | 已啟用 |  |  |
| 88 | 網路安全性：允許Local System對NTLM使用電腦身分識別 | 已啟用 |  |  |
| 89 | 網路安全性：LAN Manager驗證等級 | 只傳送 NTLMv2 回應\拒絕 LM 和 NTLM |  |  |
| 90 | 網路安全性：允許對此電腦的PKU2U驗證要求使用線上身分識別 | 已停用 |  |  |
| 91 | 網路安全性：NTLM SSP為主的(包含安全RPC)伺服器的最小工作階段安全性 | 要求NTLMv2工作階段安全性 要求128位元加密 |  |  |
| 92 | 網路安全性：允許LocalSystem NULL工作階段回復 | 已停用 |  |  |
| 93 | 網路安全性：NTLM SSP為主的(包含安全RPC)用戶端的最小工作階段安全性 | 要求NTLMv2工作階段安全性 要求128位元加密 |  |  |
| 94 | 網路安全性：設定Kerberos允許的加密類型 | RC4\_HMAC\_MD5, AES128\_HMAC\_SHA1, AES256\_HMAC\_SHA1, 未來的加密類型 |  |  |
| 95 | 網路安全性：LDAP用戶端簽章要求 | 交涉簽章 |  |  |
| 96 | 網路安全性：強制限制登入時數 | 已停用 |  |  |
| 97 | 稽核：當無法記錄安全性稽核時，系統立即關機 | 已停用 |  |  |
| 98 | 稽核：稽核通用系統物件的存取 | 已停用 |  |  |
| 99 | 稽核：稽核備份與還原權限的使用 | 已停用 |  |  |
| 100 | 稽核：強制執行稽核原則子類別設定(WindowsVista或更新版本)以覆寫稽核原則類別設定 | 已啟用 |  |  |
| 101 | 關機：允許不登入就將系統關機 | 已停用 |  |  |
| 102 | 關機：清除虛擬記憶體分頁檔 | 已停用 |  |  |
| 103 | 使用者權限指派 | 鎖定記憶體中的分頁 | No One |  |  |
| 104 | 增加處理程序工作組 | Administrators, Local Service |  |  |
| 105 | 關閉系統 | Administrators |  |  |
| 106 | 調整處理程序的記憶體配額 | Administrators, Local Service, Network Service |  |  |
| 107 | 取代處理程序等級權杖 | Local Service, Network Service |  |  |
| 108 | 取得檔案或其他物件的擁有權 | Administrators |  |  |
| 109 | 拒絕透過遠端桌面服務登入 | Guests,本機帳戶 |  |  |
| 110 | 拒絕從網路存取這台電腦 | Guests,本機帳戶與Administrators群組的成員 |  |  |
| 111 | 載入及解除載入裝置驅動程式 | Administrators |  |  |
| 112 | 拒絕以服務方式登入 | Guests |  |  |
| 113 | 讓電腦及使用者帳戶受信賴，以進行委派 | No One |  |  |
| 114 | 備份檔案及目錄 | Administrators |  |  |
| 115 | 修改物件標籤 | No One |  |  |
| 116 | 當成作業系統的一部分 | No One |  |  |
| 117 | 變更系統時間 | LOCAL SERVICE, Administrators |  |  |
| 118 | 允許透過遠端桌面服務登入 | Administrators |  |  |
| 119 | 修改韌體環境值 | Administrators |  |  |
| 120 | 建立通用物件 | Administrators, SERVICE, LOCAL SERVICE, NETWORK SERVICE |  |  |
| 121 | 設定檔系統效能 | Administrators,NT SERVICE\WdiServiceHost |  |  |
| 122 | 產生安全性稽核 | Local Service, Network Service |  |  |
| 123 | 以服務方式登入 | No One |  |  |
| 124 | 存取認證管理員做為信任的呼叫者 | No One |  |  |
| 125 | 變更時區 | LOCAL SERVICE, Administrators |  |  |
| 126 | 執行磁碟區維護工作 | Administrators |  |  |
| 127 | 建立權杖物件 | No One |  |  |
| 128 | 強制從遠端系統進行關閉 | Administrators |  |  |
| 129 | 建立符號連結 | Administrators |  |  |
| 130 | 從銜接站移除電腦 | Administrators |  |  |
| 131 | 略過周遊檢查 | Administrators, Authenticated Users, Local Service, Network Service |  |  |
| 132 | 建立分頁檔 | Administrators |  |  |
| 133 | 增加排程優先順序 | Administrators |  |  |
| 134 | 將工作站新增至網域 | (無此項目) |  |  |
| 135 | 管理稽核及安全性記錄檔 | Administrators |  |  |
| 136 | 拒絕以批次工作登入 | Guests |  |  |
| 137 | 同步處理目錄服務資料 | (無此項目) |  |  |
| 138 | 拒絕本機登入 | Guests |  |  |
| 139 | 偵錯程式 | Administrators |  |  |
| 140 | 建立永久共用物件 | No One |  |  |
| 141 | 還原檔案及目錄 | Administrators |  |  |
| 142 | 設定檔單一處理程序 | Administrators |  |  |
| 143 | 以批次工作登入 | Administrators |  |  |
| 144 | 在驗證後模擬用戶端 | Administrators, SERVICE, Local Service, Network Service |  |  |
| 145 | 從網路存取這台電腦 | Administrators, Authenticated Users |  |  |
| 146 | 允許本機登入 | Administrators |  |  |
| 147 | 系統管理範本 | 永遠以較高的特殊權限安裝 | 已停用 |  |  |
| 148 | 關閉自動播放 | 已啟用：所有磁碟機 |  |  |
| 149 | 設定用戶端連線加密層級 | 已啟用：高等級 |  |  |
| 150 | 事件日誌服務 | 安全性\保留舊事件 | 已停用 |  |  |
| 151 | 安全性\記錄檔大小上限(KB) | 已啟用：196608KB |  |  |
| 152 | 系統\保留舊事件 | 已停用 |  |  |
| 153 | 系統\記錄檔大小上限(KB) | 已啟用：32768KB |  |  |
| 154 | 應用程式\記錄檔大小上限(KB) | 已啟用：32768KB |  |  |
| 155 | 應用程式\保留舊事件 | 已停用 |  |  |
| 156 |  | Wired AutoConfig | (無此項目) |  |  |
| 157 |  | TPM Base Services | (無此項目) |  |  |
| 158 |  | Diagnostic Policy Service | (無此項目) |  |  |
| 159 |  | Secondary Logon | (無此項目) |  |  |
| 160 |  | Computer Browser | (無此項目) |  |  |
| 161 |  | SSDP Discovery | (無此項目) |  |  |
| 162 |  | PnP-X IP Bus Enumerator | (無此項目) |  |  |
| 163 |  | Thread Ordering Server | (無此項目) |  |  |
| 164 |  | Interactive Services Detection | (無此項目) |  |  |
| 165 |  | Desktop Window Manager Session Manager | (無此項目) |  |  |
| 166 |  | Network Location Awareness | (無此項目) |  |  |
| 167 |  | Diagnostic Service Host | (無此項目) |  |  |
| 168 |  | Windows Event Collector | (無此項目) |  |  |
| 169 |  | Extensible Authentication Protocol | (無此項目) |  |  |
| 170 |  | Print Spooler | (無此項目) |  |  |
| 171 |  | Distributed Transaction Coordinator | (無此項目) |  |  |
| 172 |  | Microsoft Fibre Channel Platform Registration Service | (無此項目) |  |  |
| 173 |  | User Profile Service | (無此項目) |  |  |
| 174 |  | DNS Client | 自動 |  |  |
| 175 |  | Portable Device Enumerator Service | (無此項目) |  |  |
| 176 |  | Smart Card | (無此項目) |  |  |
| 177 |  | Windows Color System | (無此項目) |  |  |
| 178 |  | Special Administration Console Helper | (無此項目) |  |  |
| 179 |  | Remote Access Connection Manager | (無此項目) |  |  |
| 180 |  | Remote Access Auto Connection Manager | (無此項目) |  |  |
| 181 |  | Windows Modules Installer | (無此項目) |  |  |
| 182 |  | Resultant Set of Policy Provider | (無此項目) |  |  |
| 183 |  | Telephony | (無此項目) |  |  |
| 184 |  | Windows Audio | (無此項目) |  |  |
| 185 |  | IP Helper | (無此項目) |  |  |
| 186 |  | Remote Procedure Call (RPC) Locator | (無此項目) |  |  |
| 187 |  | Windows Event Log | (無此項目) |  |  |
| 188 |  | Problem Reports and Solutions Control Panel Support | (無此項目) |  |  |
| 189 |  | Application Management | (無此項目) |  |  |
| 190 |  | System Event Notification Service | (無此項目) |  |  |
| 191 |  | KtmRm for Distributed Transaction Coordinator | (無此項目) |  |  |
| 192 |  | Secure Socket Tunneling Protocol Service | (無此項目) |  |  |
| 193 |  | CNG Key Isolation | (無此項目) |  |  |
| 194 |  | Remote Procedure Call (RPC) | (無此項目) |  |  |
| 195 |  | Power | (無此項目) |  |  |
| 196 |  | Function Discovery Resource Publication | (無此項目) |  |  |
| 197 |  | Microsoft .NET Framework NGEN v2.0.50727\_X86 | (無此項目) |  |  |
| 198 |  | Remote Desktop Configuration | (無此項目) |  |  |
| 199 |  | Plug and Play | (無此項目) |  |  |
| 200 |  | Smart Card Removal Policy | (無此項目) |  |  |
| 201 |  | Routing and Remote Access | (無此項目) |  |  |
| 202 |  | Network Access Protection Agent | (無此項目) |  |  |
| 203 |  | Windows Update | (無此項目) |  |  |
| 204 |  | Volume Shadow Copy | (無此項目) |  |  |
| 205 |  | Network List Service | (無此項目) |  |  |
| 206 |  | Windows Firewall | (無此項目) |  |  |
| 207 |  | Microsoft iSCSI Initiator Service | (無此項目) |  |  |
| 208 |  | Application Experience | (無此項目) |  |  |
| 209 |  | Application Layer Gateway Service | (無此項目) |  |  |
| 210 |  | Windows Audio Endpoint Builder | (無此項目) |  |  |
| 211 |  | ASP .NET State Service | (無此項目) |  |  |
| 212 |  | Task Scheduler | (無此項目) |  |  |
| 213 |  | Group Policy Client | 自動 |  |  |
| 214 |  | Health Key and Certificate Management | (無此項目) |  |  |
| 215 |  | UPnP Device Host | (無此項目) |  |  |
| 216 |  | Certificate Propagation | (無此項目) |  |  |
| 217 |  | Distributed Link Tracking Client | 手動 |  |  |
| 218 |  | Protected Storage | (無此項目) |  |  |
| 219 |  | COM+ Event System | (無此項目) |  |  |
| 220 |  | Multimedia Class Scheduler | (無此項目) |  |  |
| 221 |  | Internet Connection Sharing (ICS) | (無此項目) |  |  |
| 222 |  | Windows Driver Foundation - User-mode Driver Framework | (無此項目) |  |  |
| 223 |  | Workstation | 自動 |  |  |
| 224 |  | Security Accounts Manager | (無此項目) |  |  |
| 225 |  | Windows Remote Management (WS-Management) | (無此項目) |  |  |
| 226 |  | Windows Time | 自動 |  |  |
| 227 |  | Windows Error Reporting Service | (無此項目) |  |  |
| 228 |  | COM+ System Application | (無此項目) |  |  |
| 229 |  | Virtual Disk | (無此項目) |  |  |
| 230 |  | Shell Hardware Detection | (無此項目) |  |  |
| 231 |  | Function Discovery Provider Host | (無此項目) |  |  |
| 232 |  | Windows Management Instrumentation | (無此項目) |  |  |
| 233 |  | Performance Logs & Alerts | (無此項目) |  |  |
| 234 |  | IKE and AuthIP IPsec Keying Modules | (無此項目) |  |  |
| 235 |  | Background Intelligent Transfer Service | (無此項目) |  |  |
| 236 |  | Network Connections | (無此項目) |  |  |
| 237 |  | Link-Layer Topology Discovery Mapper | (無此項目) |  |  |
| 238 |  | Application Information | (無此項目) |  |  |
| 239 |  | WinHTTP Web Proxy Auto-Discovery Service | (無此項目) |  |  |
| 240 |  | WMI Performance Adapter | (無此項目) |  |  |
| 241 |  | DHCP Client | (無此項目) |  |  |
| 242 |  | Microsoft Software Shadow Copy Provider | (無此項目) |  |  |
| 243 |  | Remote Registry | (無此項目) |  |  |
| 244 |  | Server | 自動 |  |  |
| 245 |  | DFS Replication | 自動 |  |  |
| 246 |  | Windows Installer | (無此項目) |  |  |
| 247 |  | Base Filtering Engine | (無此項目) |  |  |
| 248 |  | Diagnostic System Host | (無此項目) |  |  |
| 249 |  | Remote Desktop UserMode Port Redirector | (無此項目) |  |  |
| 250 |  | DCOM Server Process Launcher | (無此項目) |  |  |
| 251 |  | Human Interface Device Access | (無此項目) |  |  |
| 252 |  | Software Protection | (無此項目) |  |  |
| 253 |  | TCP/IP NetBIOS Helper | (無此項目) |  |  |
| 254 |  | Remote Desktop Services | (無此項目) |  |  |
| 255 |  | Cryptographic Services | (無此項目) |  |  |
| 256 |  | Network Store Interface Service | (無此項目) |  |  |
| 257 | 進階稽核原則設定 | 稽核目錄服務變更 | 成功及失敗 |  |  |
| 258 | 稽核詳細目錄服務複寫 | 沒有稽核 |  |  |
| 259 | 稽核目錄服務複寫 | 沒有稽核 |  |  |
| 260 | 稽核目錄服務存取 | 成功及失敗 |  |  |
| 261 | 稽核系統完整性 | 成功與失敗 |  |  |
| 262 | 稽核IPsec驅動程式 | 成功與失敗 |  |  |
| 263 | 稽核安全性系統延伸 | 成功與失敗 |  |  |
| 264 | 稽核其他系統事件 | 沒有稽核 |  |  |
| 265 | 稽核安全性狀態變更 | 成功與失敗 |  |  |
| 266 | 稽核其他物件存取事件 | 沒有稽核 |  |  |
| 267 | 稽核控制代碼操作 | 沒有稽核 |  |  |
| 268 | 稽核檔案共用 | 沒有稽核 |  |  |
| 269 | 稽核篩選平台連線 | 沒有稽核 |  |  |
| 270 | 稽核憑證服務 | 沒有稽核 |  |  |
| 271 | 稽核檔案系統 | 沒有稽核 |  |  |
| 272 | 稽核SAM | 沒有稽核 |  |  |
| 273 | 稽核篩選平台封包丟棄 | 沒有稽核 |  |  |
| 274 | 稽核產生的應用程式 | 沒有稽核 |  |  |
| 275 | 稽核登錄 | 沒有稽核 |  |  |
| 276 | 稽核詳細的檔案共用 | 沒有稽核 |  |  |
| 277 | 稽核核心物件 | 沒有稽核 |  |  |
| 278 | 稽核篩選平台原則變更 | 沒有稽核 |  |  |
| 279 | 稽核驗證原則變更 | 成功 |  |  |
| 280 | 稽核授權原則變更 | 沒有稽核 |  |  |
| 281 | 稽核「稽核原則變更」 | 成功與失敗 |  |  |
| 282 | 稽核MPSSVC規則層級原則變更 | 沒有稽核 |  |  |
| 283 | 稽核其他原則變更事件 | 沒有稽核 |  |  |
| 284 | 稽核機密特殊權限使用 | 成功與失敗 |  |  |
| 285 | 稽核非機密特殊權限使用 | 沒有稽核 |  |  |
| 286 | 稽核其他特殊權限使用事件 | 沒有稽核 |  |  |
| 287 | 稽核Kerberos驗證服務 | 沒有稽核 |  |  |
| 288 | 稽核認證驗證 | 成功與失敗 |  |  |
| 289 | 稽核Kerberos服務票證操作 | 沒有稽核 |  |  |
| 290 | 稽核其他帳戶登入事件 | 沒有稽核 |  |  |
| 291 | 稽核應用程式群組管理 | 沒有稽核 |  |  |
| 292 | 稽核電腦帳戶管理 | 成功及失敗 |  |  |
| 293 | 稽核其他帳戶管理事件 | 成功與失敗 |  |  |
| 294 | 稽核安全性群組管理 | 成功與失敗 |  |  |
| 295 | 稽核發佈群組管理 | 沒有稽核 |  |  |
| 296 | 稽核使用者帳戶管理 | 成功與失敗 |  |  |
| 297 | 稽核帳戶鎖定 | 沒有稽核 |  |  |
| 298 | 稽核IPsec延伸模式 | 沒有稽核 |  |  |
| 299 | 稽核網路原則伺服器 | 成功 |  |  |
| 300 | 稽核IPsec主要模式 | 沒有稽核 |  |  |
| 301 | 稽核其他登入/登出事件 | 沒有稽核 |  |  |
| 302 | 稽核登出 | 成功 |  |  |
| 303 | 稽核登入 | 成功與失敗 |  |  |
| 304 | 稽核IPsec快速模式 | 沒有稽核 |  |  |
| 305 | 稽核特殊登入 | 成功 |  |  |
| 306 | 稽核RPC事件 | 沒有稽核 |  |  |
| 307 | 稽核DPAPI活動 | 沒有稽核 |  |  |
| 308 | 稽核建立處理程序 | 成功 |  |  |
| 309 | 稽核終止處理程序 | 沒有稽核 |  |  |
| 310 |  | 帳戶：Administrator帳戶狀態 | (無此項目) |  |  |
| 311 | 帳戶：Guest帳戶狀態 | (無此項目) |  |  |
| 312 | 具有進階安全性的Windows防火牆 | Windows 防火牆: 網域設定檔: 輸出連線 | 允許(預設) |  |  |
| 313 | Windows 防火牆: 網域設定檔: 防火牆狀態 | 開啟(建議選項) |  |  |
| 314 | Windows 防火牆: 網域設定檔: 輸入連線 | 封鎖(預設) |  |  |
| 315 | Windows 防火牆: 網域設定檔: 允許套用本機防火牆規則 | 是(預設) |  |  |
| 316 | Windows 防火牆: 網域設定檔: 顯示通知 | 是 |  |  |
| 317 | Windows 防火牆: 網域設定檔: 允許套用本機連線安全性規則 | 是(預設) |  |  |
| 318 | Windows 防火牆: 網域設定檔: 允許單點傳播回應 | 否 |  |  |
| 319 | Windows 防火牆: 私人設定檔: 防火牆狀態 | 開啟(建議選項) |  |  |
| 320 | Windows 防火牆: 私人設定檔: 輸入連線 | 封鎖(預設) |  |  |
| 321 | Windows 防火牆: 私人設定檔: 允許套用本機防火牆規則 | 是(預設) |  |  |
| 322 | Windows 防火牆: 私人設定檔: 顯示通知 | 是 |  |  |
| 323 | Windows 防火牆: 私人設定檔: 允許單點傳播回應 | 否 |  |  |
| 324 | Windows 防火牆: 私人設定檔: 允許套用本機連線安全性規則 | 是(預設) |  |  |
| 325 | Windows 防火牆: 私人設定檔: 輸出連線 | 允許(預設) |  |  |
| 326 | Windows 防火牆: 公用設定檔: 允許單點傳播回應 | 否 |  |  |
| 327 | Windows 防火牆: 公用設定檔: 顯示通知 | 是 |  |  |
| 328 | Windows 防火牆: 公用設定檔: 允許套用本機連線安全性規則 | 是(預設) |  |  |
| 329 | Windows 防火牆: 公用設定檔: 輸入連線 | 封鎖(預設) |  |  |
| 330 | Windows 防火牆: 公用設定檔: 允許套用本機防火牆規則 | 是(預設) |  |  |
| 331 | Windows 防火牆: 公用設定檔: 輸出連線 | 允許(預設) |  |  |
| 332 | Windows 防火牆: 公用設定檔: 防火牆狀態 | 開啟(建議選項) |  |  |
| 333 | 安全性選項 | 互動式登入：電腦未使用時間限制 | 900秒 |  |  |
| 334 | 系統管理範本 | 防止使用 OneDrive 儲存檔案 | 已啟用 |  |  |
| 335 | 允許遠端殼層存取 | 已停用 |  |  |
| 336 | 系統起始的重新啟動之後自動登入最後一個互動式使用者 | 已停用 |  |  |
| 337 | 關閉市集應用程式 | 已啟用 |  |  |
| 338 | 關閉自動下載和安裝更新 | 已啟用 |  |  |
| 339 | 關閉更新至最新版 Windows 的服務 | 已啟用 |  |  |
| 340 | 不要顯示網路選取UI | 已啟用 |  |  |
| 341 | 在建立處理程序事件中包含命令列 | 已停用 |  |  |
| 342 | 允許加密檔案索引 | 已停用 |  |  |
| 343 | 設定 [搜尋] 中可以分享的資訊 | 已啟用：匿名資訊 |  |  |
| 344 | 允許選用Microsoft帳戶 | 已啟用 |  |  |
| 345 | 關閉Windows Messenger客戶經驗改進計畫 | 已啟用 |  |  |
| 346 | 關閉搜尋小幫手內容檔更新 | 已啟用 |  |  |
| 347 | 關閉檔案和資料夾的 [發佈到網站] 工作 | 已啟用 |  |  |
| 348 | 防止啟用鎖定畫面投影片放映 | 已啟用 |  |  |
| 349 | 防止啟用鎖定畫面相機 | 已啟用 |  |  |
| 350 | 系統服務 | Active Directory Domain Services | 自動 |  |  |
| 351 | Active Directory Web Services | 自動 |  |  |
| 352 | Application Identity | 自動 |  |  |
| 353 | DFS Namespace | 自動 |  |  |
| 354 | DNS Server | 自動 |  |  |
| 355 | File Replication | 已停用 |  |  |
| 356 | Intersite Messaging | 自動 |  |  |
| 357 | Kerberos Key Distribution Center | 自動 |  |  |
| 358 | Netlogon | 自動 |  |  |
| 359 | 系統管理範本 | 防止下載隨函附件 | 已啟用 |  |  |
| 360 | 加入 Microsoft MAPS | 已停用 |  |  |
| 361 | 允許使用者控制安裝 | 已停用 |  |  |
| 362 | 防止出現 Windows Installer 指令碼的 Internet Explorer 安全性提示 | 已停用 |  |  |
| 363 | 不允許摘要式驗證 | 已啟用 |  |  |
| 364 | 允許未加密的流量 | 已停用 |  |  |
| 365 | 允許基本驗證 | 已停用 |  |  |
| 366 | 不允許 WinRM 儲存 RunAs 認證 | 已啟用 |  |  |
| 367 | 允許未加密的流量 | 已停用 |  |  |
| 368 | 允許基本驗證 | 已停用 |  |  |
| 369 | 不允許非磁碟區裝置的自動播放 | 已啟用 |  |  |
| 370 | 設定 AutoRun 的預設行為 | 已啟用：不執行任何 Autorun 命令 |  |  |
| 371 | 關閉定位 | 已啟用 |  |  |
| 372 | 不要顯示密碼顯示按鈕 | 已啟用 |  |  |
| 373 | 提升權限時列舉系統管理員帳戶 | 已停用 |  |  |
| 374 | 連線時永遠提示密碼 | 已啟用 |  |  |
| 375 | 需要安全的 RPC 通訊 | 已啟用 |  |  |
| 376 | 不允許磁碟重新導向 | 已啟用 |  |  |
| 377 | 不要使用每一工作階段的暫存資料夾 | 已停用 |  |  |
| 378 | 結束後不刪除暫存資料夾 | 已停用 |  |  |
| 379 | 不允許儲存密碼 | 已啟用 |  |  |
| 380 | 設定 Windows SmartScreen 篩選工具 | 已啟用：在執行不明軟體下載之前需要系統管理員核準 |  |  |
| 381 | 損毀時關閉終止堆集 | 已停用 |  |  |
| 382 | 關閉殼層通訊協定受保護模式 | 已停用 |  |  |
| 383 | 關閉檔案總管的資料執行防止 | 已停用 |  |  |
| 384 | 列舉加入網域電腦上的本機使用者 | 已停用 |  |  |
| 385 | 關閉鎖定畫面上的應用程式通知 | 已啟用 |  |  |
| 386 | 開機啟動驅動程式初始化原則 | 已啟用：良好和不明 |  |  |
| 387 | 喚醒電腦時必須使用密碼 (一般電源) | 已啟用 |  |  |
| 388 | 喚醒電腦時必須使用密碼 (使用電池) | 已啟用 |  |  |
| 389 | Microsoft 支援服務診斷工具: 開啟 MSDT 與支援提供者的互動式通訊 | 已停用 |  |  |
| 390 | 啟用/停用 PerfTrack | 已停用 |  |  |
| 391 | 關閉 HTTP 上的列印 | 已啟用 |  |  |
| 392 | 關閉 Windows客戶經驗改進計畫 | 已啟用 |  |  |
| 393 | 關閉手寫辨識錯誤報告 | 已啟用 |  |  |
| 394 | 關閉市集的存取權 | 已啟用 |  |  |
| 395 | 關閉透過 HTTP 下載印表機驅動程式 | 已啟用 |  |  |
| 396 | 設定提供遠端協助 | 已停用 |  |  |
| 397 | 設定請求遠端協助 | 已停用 |  |  |
| 398 | 關閉 Microsoft 對等網路服務 | 已啟用 |  |  |
| 399 | 使用 Windows Connect Now 進行無線設定 | 已停用 |  |  |
| 400 | 禁止存取 Windows Connect Now 精靈 | 已啟用 |  |  |
| 401 | 開啟 Mapper I/O (LLTDIO) 驅動程式 | 已停用 |  |  |
| 402 | 開啟 Responder (RSPNDR) 驅動程式 | 已停用 |  |  |
| 403 | 要求網域使用者在設定網路的位置時必須提升權限 | 已啟用 |  |  |
| 404 | 禁止在您的 DNS 網域網路上安裝、設定及使用網路橋接 | 已啟用 |  |  |
| 405 | 在鎖定畫面上關閉快顯通知 | 已啟用 |  |  |
| 406 | 防止轉碼器下載 | 已啟用 |  |  |
| 407 | 不要保留檔案附件的區域資訊 | 已停用 |  |  |
| 408 | 開啟附件時通知防毒程式 | 已啟用 |  |  |
| 409 | 防止使用者共用其設定檔內的檔案 | 已啟用 |  |  |
| 410 | 以密碼保護螢幕保護裝置 | 已啟用 |  |  |
| 411 | 啟用螢幕保護裝置 | 已啟用 |  |  |
| 412 | 強制特定螢幕保護裝置 | 已啟用：scrnsave.scr |  |  |
| 413 | 系統服務 | Background Tasks Infrastructure Service | (無此項目) |  |  |
| 414 | Credential Manager | (無此項目) |  |  |
| 415 | Device Association Service | (無此項目) |  |  |
| 416 | Device Install Service | (無此項目) |  |  |
| 417 | Device Setup Manager | (無此項目) |  |  |
| 418 | Encrypting File System (EFS) | (無此項目) |  |  |
| 419 | Hyper-V Data Exchange Service | (無此項目) |  |  |
| 420 | Hyper-V Guest Shutdown Service | (無此項目) |  |  |
| 421 | Hyper-V Heartbeat Service | (無此項目) |  |  |
| 422 | Hyper-V Remote Desktop Virtualization Service | (無此項目) |  |  |
| 423 | Hyper-V Time Synchronization Service | (無此項目) |  |  |
| 424 | Hyper-V Volume Shadow Copy Requestor | (無此項目) |  |  |
| 425 | IPsec Policy Agent | (無此項目) |  |  |
| 426 | KDC Proxy Server service (KPS) | (無此項目) |  |  |
| 427 | Local Session Manager | (無此項目) |  |  |
| 428 | Net.Tcp Port Sharing Service | (無此項目) |  |  |
| 429 | Network Connectivity Assistant | (無此項目) |  |  |
| 430 | Optimize drives | (無此項目) |  |  |
| 431 | Performance Counter DLL Host | (無此項目) |  |  |
| 432 | Printer Extensions and Notifications | (無此項目) |  |  |
| 433 | RPC Endpoint Mapper | (無此項目) |  |  |
| 434 | SNMP Trap | (無此項目) |  |  |
| 435 | Spot Verifier | (無此項目) |  |  |
| 436 | Superfetch | (無此項目) |  |  |
| 437 | Themes | (無此項目) |  |  |
| 438 | User Access Logging Service | (無此項目) |  |  |
| 439 | Windows All-User Install Agent | (無此項目) |  |  |
| 440 | Windows Font Cache Service | (無此項目) |  |  |
| 441 | Windows Store Service (WSService) | (無此項目) |  |  |
| 442 | Data Deduplication Service | (無此項目) |  |  |
| 443 | Data Deduplication Volume Shadow Copy Service | (無此項目) |  |  |
| 444 | File Server Resource Manager | (無此項目) |  |  |
| 445 | File Server Storage Reports Manager | (無此項目) |  |  |
| 446 | Microsoft File Server Shadow Copy Agent Service | (無此項目) |  |  |
| 447 | Microsoft iSCSI Software Target | (無此項目) |  |  |
| 448 | Application Host Helper Service | (無此項目) |  |  |
| 449 | Web Management Service | (無此項目) |  |  |
| 450 | Windows Process Activation Service | (無此項目) |  |  |
| 451 | World Wide Web Publishing Service | (無此項目) |  |  |
| 452 | 系統管理範本 | Configure SMB v1 client driver | (無此項目) |  |  |
| 453 | Configure SMB v1 server | (無此項目) |  |  |
| 454 | 封鎖未受信任的字型 | (無此項目) |  |  |
| 455 | 啟用不安全的來賓登入 | (無此項目) |  |  |
| 456 | 資料防止執行 | 啟用資料執行保護 | 為所有的Windows程式和服務開啟DEP |  |  |
| 457 | 校時 | 設定時間自動校正 | 設定NTP Server校正 |  |  |
| 458 | AD本機 | 限制存取來源IP | 設定存取來源IP |  |  |
| 459 | 禁止將主機資料輸出至未經授權之儲存媒體(如USB、燒錄光碟、外接式硬碟等) | 禁止使用未經授權之儲存媒體 |  |  |
| 460 | 禁止主機主動連出Internet，若有例外則需要提出足夠說明，並依公司資安政策進行申請作業 | 禁止連出Internet |  |  |
| 461 | 主機使用者皆有個人專用的唯一識別碼 | 不應共用帳號 |  |  |
| 462 | 定期執行Microsoft Windows update | 應定期執行Microsoft Windows update |  |  |