Exchange 與 Windows Server AD 的關係

Exchange Server 可以退出網域再加入嗎？

Exchange Server 雖然技術上能退出網域再重新加入，但這樣做風險高、不安全，還很容易讓 Exchange 完全掛掉。因為 Exchange 與 AD 之間依賴網域信任關係、電腦物件（Machine Account）、Exchange 服務帳戶、AD Schema 設定、Autodiscover / Service Connection Point (SCP) 以及 RBAC 權限，一旦退出網域，這些連結都會中斷。

Exchange Server 退出網域後可能遇到的問題包括：

1. 所有服務可能無法啟動，因為無法用機器帳戶驗證、讀取 AD 組態 Partition，且 Kerberos/NTLM 會失效。
2. EAC 和 PowerShell 管理介面將無法登入，會出現 Unable to connect to remote PowerShell server、401 或 503 等錯誤。
3. Transport Service 也無法投遞郵件，因為查不到 AD 用戶和連線器等資訊。
4. Outlook 和 Autodiscover 功能則會全面失效，因為 SCP 無法正確讀取。

什麼情況下可以安全地退出再加入？其實只有一種情況值得考慮：當 DC 與 Exchange 之間的機器帳戶信任關係損壞（常見問題），也就是 AD 機器帳戶密碼不同步、secure channel 中斷，並且 **nltest /sc_verify:domain.local** 測試失敗。如果是這種情況，應該直接修復信任關係，而不是退出網域。

正確做法：修復機器帳戶信任（不退出網域）

1. 用本機 Administrator 登入 Exchange Server
2. 執行

   nltest /sc_reset:domain.loca

   nltest /sc_verify:domain.local

   或用 PowerShell

   Reset-ComputerMachinePassword -Server DC_ServerName -Credential (Get-Credential)

   如果 /sc_reset 成功，/sc_verify 就會變成：

   Status = 0x0 NERR_Success

   修復成功後，Exchange 會恢復正常。

   如出現 reset-computerMachinePassword 找不到符合參數名稱'Credential'的參數，改用 **netdom**

   請用本機 Administrator 權限開 CMD 後執行

   netdom resetpwd /server:<DC 名稱> /userD:<domain\administrator> /passwordD:*

   會跳出密碼詢問 → 輸入網域 Administrator 密碼即可。

   執行後再測試：

   Test-ComputerSecureChannel

   如果成功會回 True。

   如果出現

   Flags: ...

   Trusted DC Name ...

   Trusted DC Connection Status ...

The secure channel from SERVER to DOMAIN has been reset.
Status = 0x5 ERROR_ACCESS_DENIED
或
I_NetLogonControl failed: Status = 0x5
這表示機器帳戶安全通道完全損毀無法驗證 DC 的狀況。
重點：這還是可以修復，不需要退出網域、不需要重灌 Exchange。
請依「逐步修復流程」照做即可。
第一步：確認使用『本機 Administrator』登入
第二步：檢查與 DC 的基礎連線
ping <DC 名稱>
第三步：強制重設機器帳戶密碼
請用「本機 Administrator」執行 PowerShell：
$cred = Get-Credential
Reset-ComputerMachinePassword -Server < DC 名稱> -Credential $cred
輸入憑證時請用：DOMAIN\Administrator

成功後請執行：
nltest /sc_verify:domain.local
如果看到：
Status = 0x0 NERR_Success
表示安全通道已修復完成。
如果 netdom 說 “Access denied”
這代表 DC 不接受你的機器帳戶重建要求 → 可能是 AD 重設機器帳戶或信任出問題。
此時請你做下一步：

從 DC 重設 Exchange 的機器帳戶
在 DC：

1. 打開「Active Directory 使用者與電腦」
2. 找到電腦帳戶：
   EXCHANGESERVERNAME$
3. 右鍵 → Reset Account（重設帳戶）

不要刪除物件，只要 Reset。
完成後回 Exchange Server 再執行：
netdom resetpwd /server:DC01 /userD:domain\Administrator /passwordD:*
然後：
nltest /sc_verify:domain.local

如果已經退出 Domain，能否重新加入？

可以，但重新加入後 Exchange 很可能還是無法運作，並且需要進行修復。
可能需要：

- 重新註冊 Exchange 服務主體
- 修復 SCP
- 修復 IIS virtual directories
- 重新抓取 AD Configuration

甚至最糟：

- 需重新安裝 Exchange（使用 /RecoverServer 模式）

指令如下：

Setup.exe /Mode:RecoverServer /IAcceptExchangeServerLicenseTerms

RecoverServer 會依照 AD 設定重建 Exchange 配置。