

# 瞭解Windows DC配置指令碼

## 目錄

---

[簡介](#)

[DC配置指令碼概述](#)

[階段1 — 測試](#)

[階段1b — 測試結果](#)

[階段2 — 自動配置更改](#)

[階段2b — 自動配置警告](#)

[第3階段 — 註冊](#)

---

## 簡介

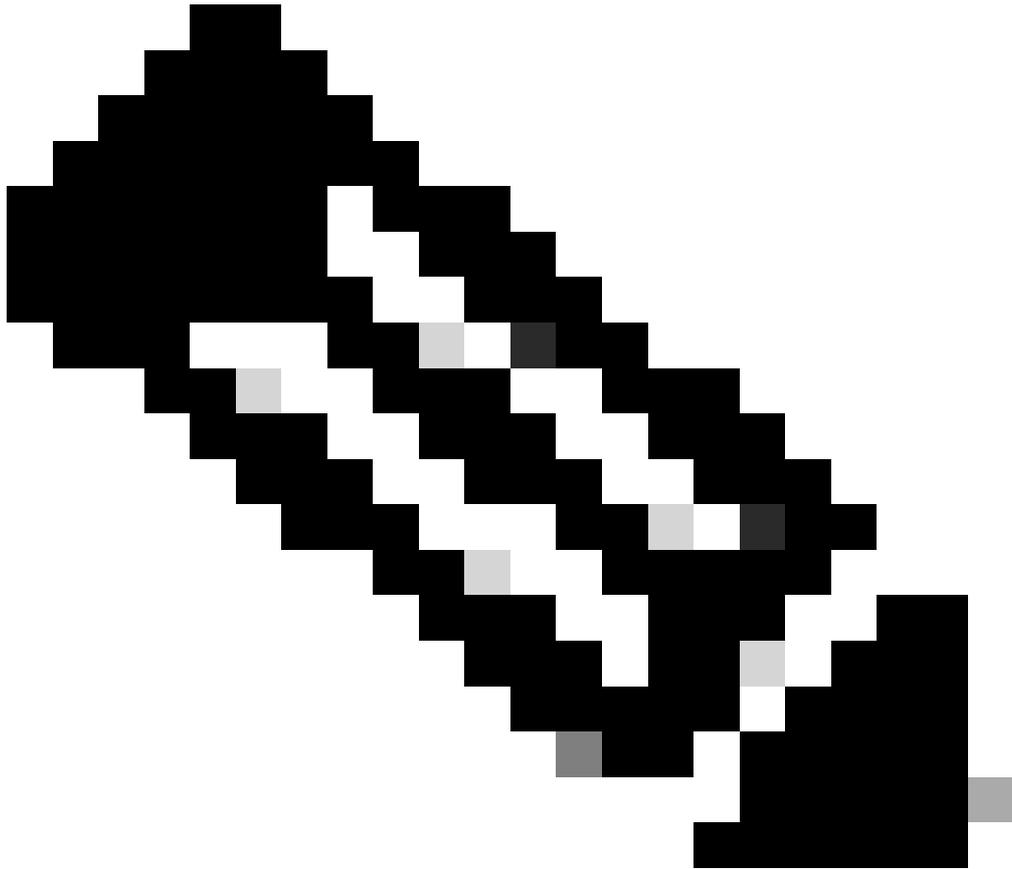
本文檔介紹由我們的域控制器配置指令碼對您的Windows環境所做的更改。

- 有關基本前提條件，請參閱見解文檔：  
<https://docs.umbrella.com/deployment-umbrella/docs/2-prerequisites>
- 有關如何手動設定這些許可權的詳細資訊，請參閱以下文章：  
[OpenDNS Connector使用者所需的許可權](#)。

## DC配置指令碼概述

每個域控制器都需要向Umbrella API/儀表板進行一次性註冊。我們的[DC配置指令碼](#)會啟動此指令碼以及以下功能：

1. 檢查必需的許可權和防火牆規則是否已配置
2. ( 可選 ) 自動配置這些許可權
3. ( 可選 ) 僅當這些檢查成功時，才向Umbrella API/儀表板註冊域控制器。



附註：域控制器清單也可由Umbrella支援手動註冊。這通常在域控制器無法進行API/Internet訪問的情況下有用。但是，仍然必須配置所述的許可權更改，因此我們仍然強烈建議運行配置指令碼。

---

最初運行指令碼時，不會對環境進行任何更改。該指令碼將檢查是否所有必要的許可權都已就位。如果出現問題，系統會提示您(Y/N)，但要求您進行更改。

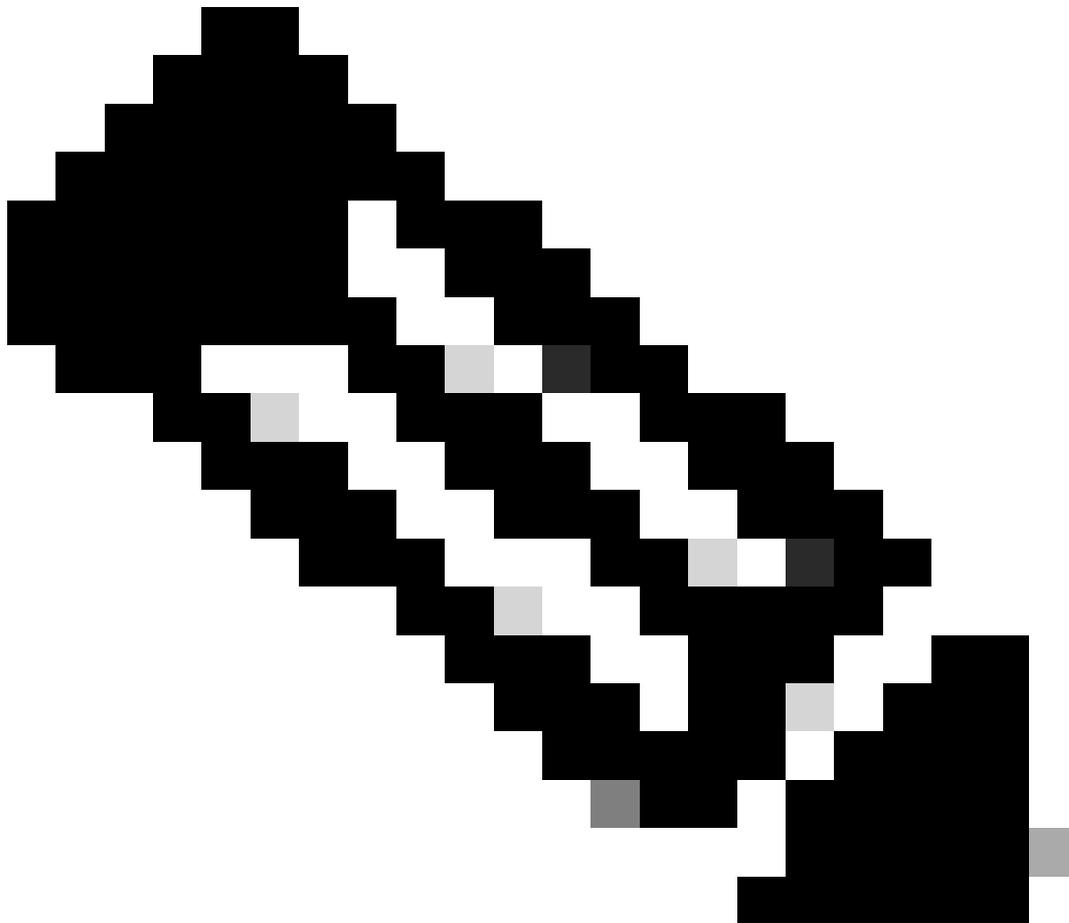
註冊指令碼完成後，無需在域控制器上運行任何軟體。但是，[OpenDNS Connector服務](#)必須安裝在至少一台電腦上(例如，域控制器或成員伺服器)。

## 階段1 — 測試

指令碼最初收集以下資訊：

- 檢查OS版本和系統功能級別
- 檢查指令碼是否以管理員身份運行。
- 獲取伺服器的IP地址、主機名和域名信息

- 檢查是否已啟用Windows防火牆，以及是否允許內置「遠端管理」規則
  - 檢查所需的域使用者帳戶「OpenDNS\_Connector」
- 



附註：如果OpenDNS\_Connector使用者不存在，指令碼將列印結果並中止。在運行指令碼之前，必須手動建立此域使用者。如果OpenDNS\_Connector帳戶存在，指令碼將繼續進行這些檢查。

- 
- 檢查OpenDNS\_Connector使用者是否具有根\cimv2 WMI名稱空間中的「遠端啟用」和「讀取安全」許可權。
  - 檢查OpenDNS\_Connector帳戶是否具有Active Directory「Replicating Directory Changes」許可權，該許可權通常由企業只讀域控制器組的成員授予。
  - 檢查OpenDNS\_Connector帳戶是否是「事件日誌讀取器」組的成員。
  - 檢查OpenDNS\_Connector帳戶是否是「分散式COM使用者」組的成員。
  - 檢查策略的結果集(RSOP)，以檢視「審計登入事件」是否通過組策略啟用
  - 檢查策略的結果集(RSOP)，以檢視OpenDNS\_Connector帳戶是否分配了「管理稽核和安全日誌」許可權

## 階段1b — 測試結果

配置指令碼列印的結果因作業系統版本而異。

在server 2003和更新版本中，您可以看到以下結果：

```
AD User Exists:           true/false
WMI Permissions Set:      true/false
DCOM Permissions Set:    true/false
RDC Permissions Set:     true/false
Audit Policy Set:        true/false
Manage Event Log Policy Set: true/false
Distributed COM MemberOf: true/false
```

在Server 2008和更新版本中（僅當林功能級別為2008+時），也會顯示此資訊。（此組在早期版本中不存在）：

```
Event Log Readers MemberOf: true/false
```

## 階段2 — 自動配置更改

如果此檢查失敗，系統將提示「是否要讓我們自動配置此域控制器（y或n）？」然後進行任何更改。

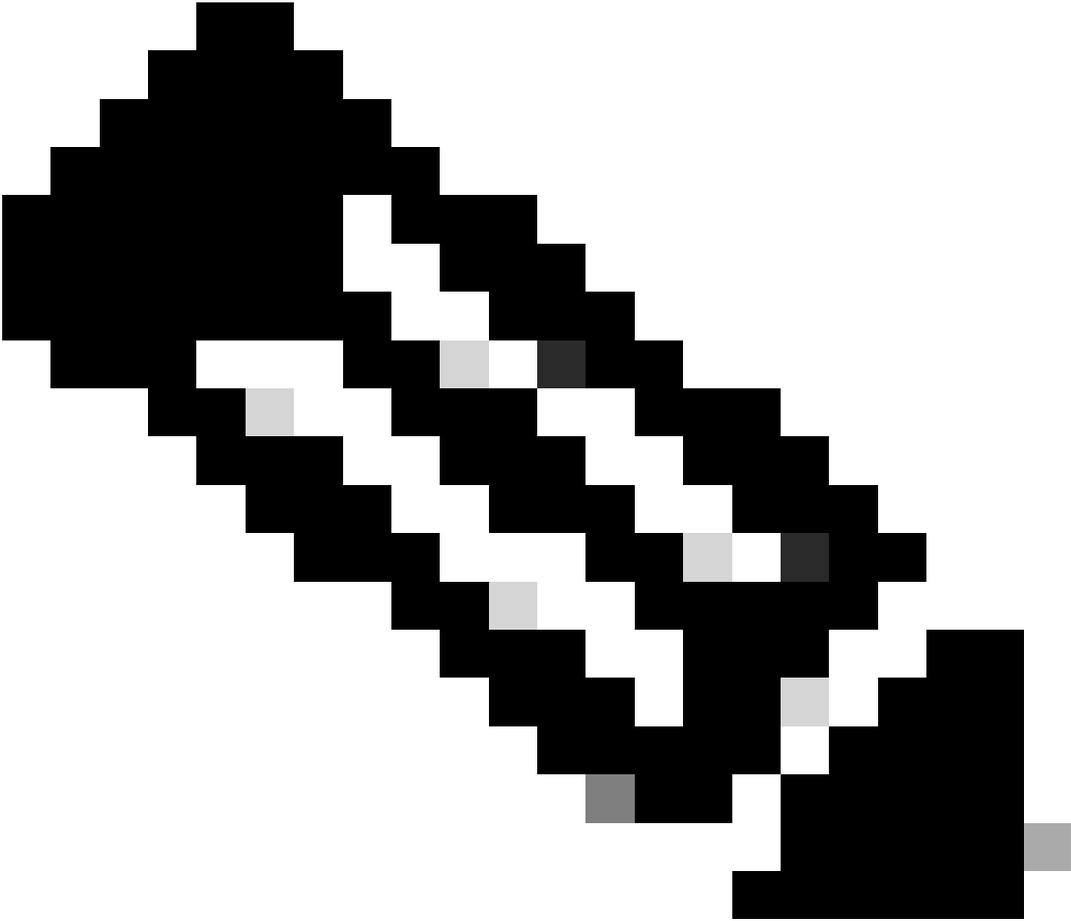
進行以下變更：

- 如有必要，啟用內置「遠端管理」Windows防火牆規則
- 在root\cimv2 WMI名稱空間中顯式授予「OpenDNS\_Connector」帳戶「Remote Enable」和「Read Security」權限。
- 明確授予「OpenDNS\_Connector」帳戶「複製目錄更改」權限
- 將「OpenDNS\_Connector」帳戶新增到「分散式COM使用者」組

在2008+年也進行了以下更改：

- 將「OpenDNS\_Connector」帳戶新增到「事件日誌讀取器」組

---



附註：如果自動配置被拒絕，或者這些更改失敗，指令碼將不會繼續註冊。

---

## 階段2b — 自動配置警告

如果未正確配置組策略設定，指令碼將生成警告。 指令碼無法更正這些問題。

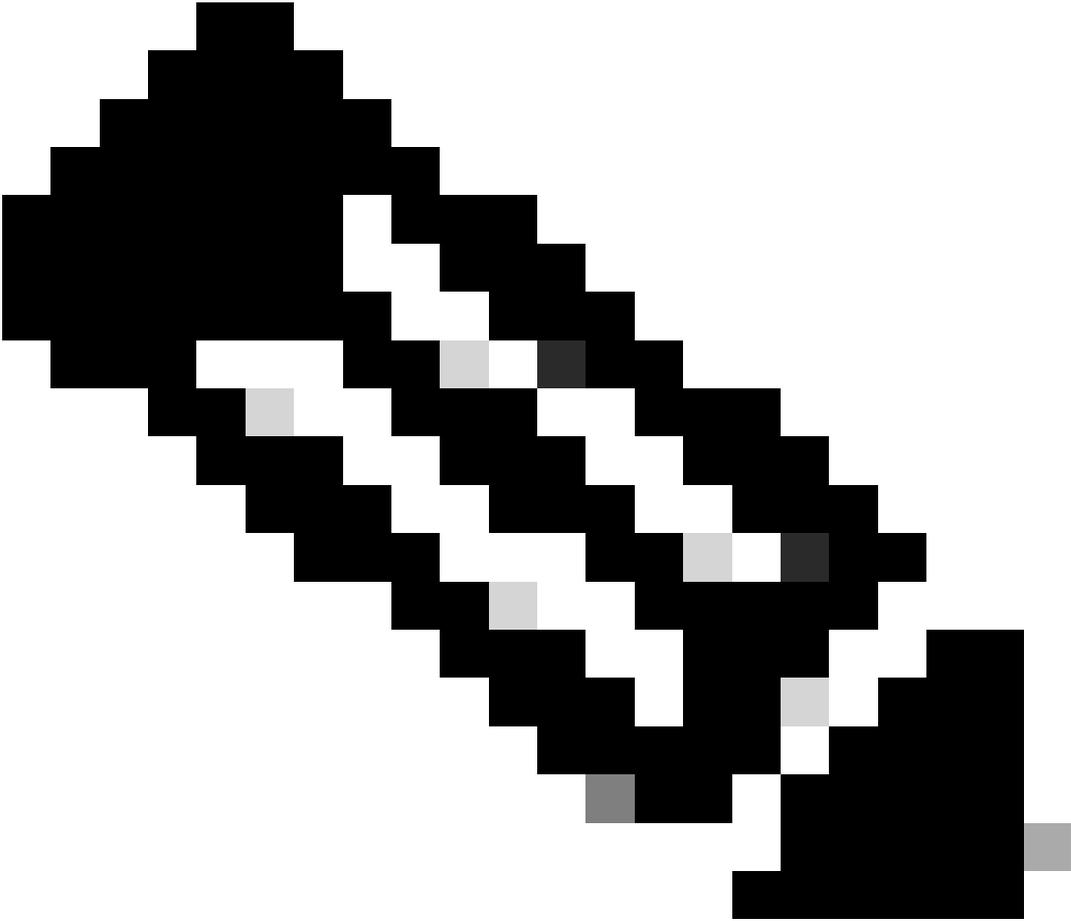
所有作業系統：

- 如果在組策略中未正確配置「審核登入事件」設定，但無法修改組策略，指令碼將發出警告。

在2003 ( 和2003功能級別 ) 上：

- 如果組策略中的「管理稽核和安全日誌」許可權配置不正確，指令碼會發出警告，但不會修改組策略。

---



附註：請手動更正這些問題，然後重新運行配置指令碼。在更正這些錯誤之前，指令碼不會繼續註冊。

---

## 第3階段 — 註冊

在向Umbrella註冊域控制器之前，指令碼會提示「是否要註冊此域控制器（y或n）？」。此資訊將發送到Umbrella：

- 域控制器主機名/標籤
- 域名
- IP 位址
- 您的唯一組織ID和令牌（包含在指令碼中），以便使用Umbrella組織唯一標識DC。

通過<https://api.opendns.com>安全進行註冊

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。