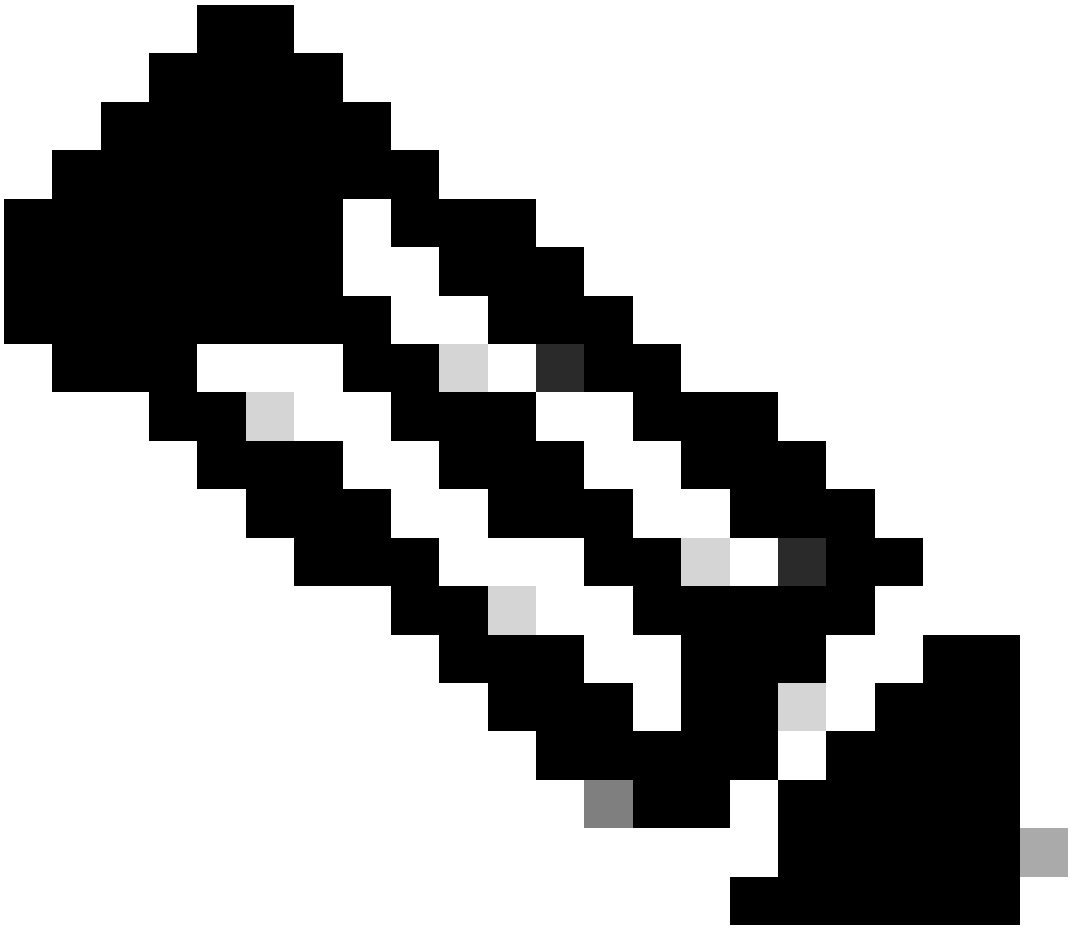
瞭解OpenDNS_Connector使用者所需的許可權

目錄

簡介

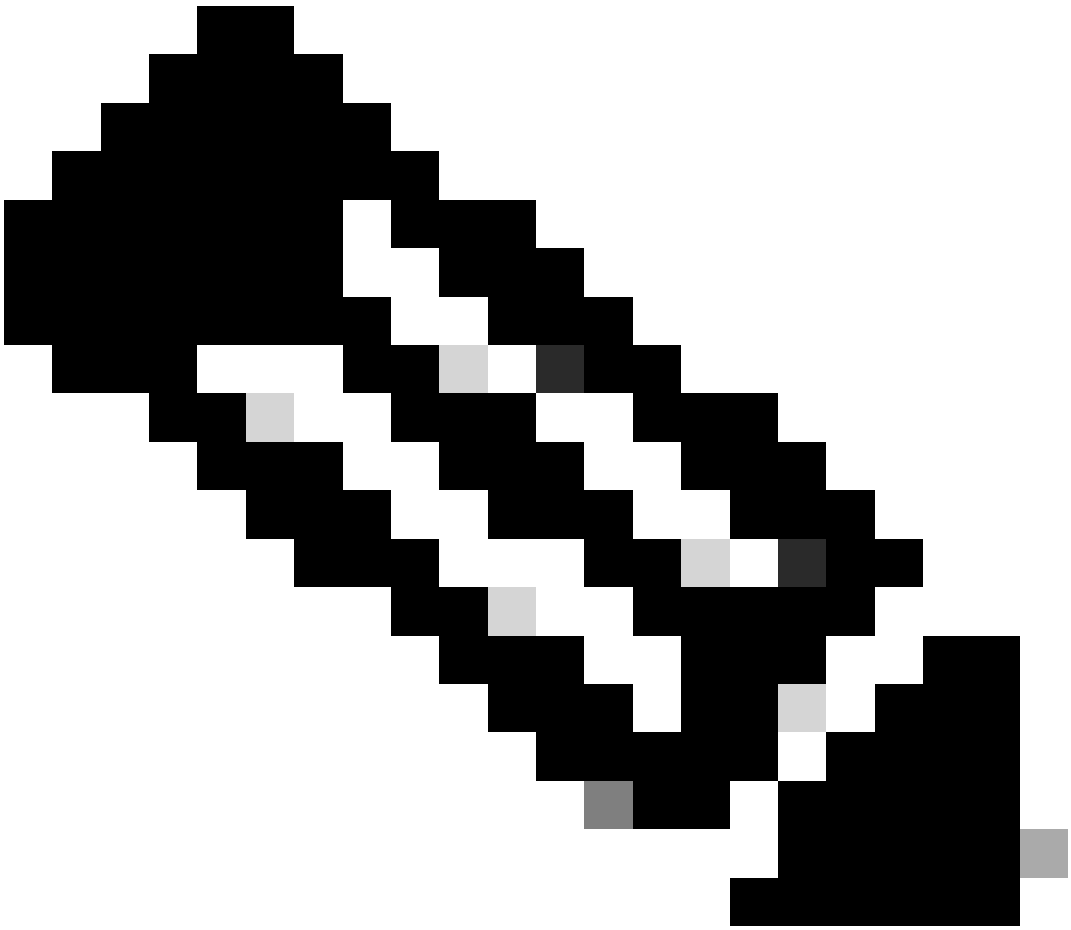
本文檔介紹OpenDNS_Connector使用者所需的許可權。



附註：為了配合品牌重塑工作，最近將假定AD使用者名稱「OpenDNS_Connector」更新為「Cisco_Connector」。

概觀

Windows Connector指令碼通常為Cisco_Connector使用者設定所需的許可權。但是，在嚴格的AD環境中，某些管理員可能不允許在其域控制器上運行VB指令碼，因此需要手動複製Windows配置指令碼的操作。本文詳細說明了在DC上需要設定哪些許可權。



附註：就本文而言，Cisco_Connector被假定為AD中您的聯結器帳戶的sAMAccountName。如果您使用的是自定義名稱，請使用聯結器帳戶的sAMAccountName而不是Cisco_Connector的相同說明。

如果Cisco_Connector使用者沒有足夠的操作許可權，則AD聯結器會在儀表板中顯示警報或錯誤狀態，當您將滑鼠懸停在警報上時，列出的消息是Access Denied，指向其中一個已註冊的域控制器。

確保Cisco_Connector使用者是AD組的成員：

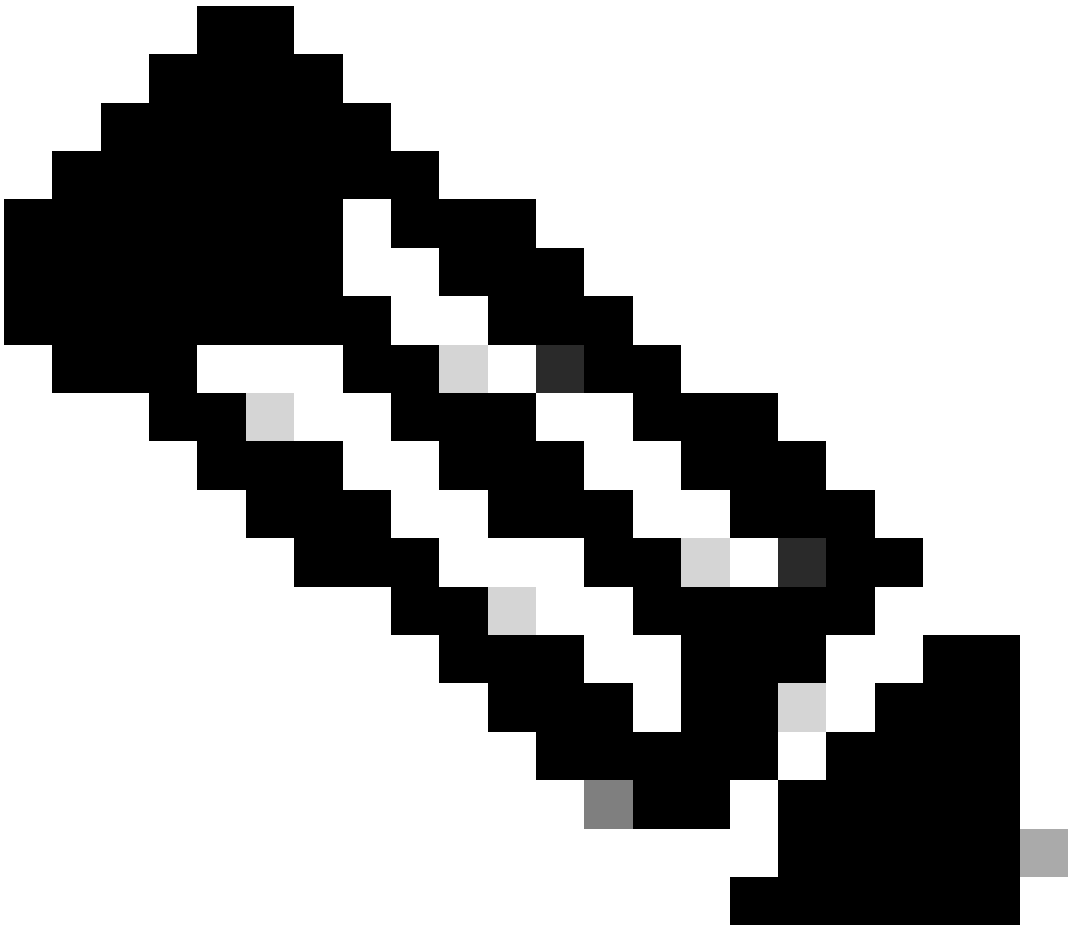
- 企業只讀域控制器
- 事件日誌讀取器（僅當部署包括虛擬裝置時）

此外，Cisco_Connector使用者必須屬於「域使用者」和「使用者」組。您可以使用以下命令驗證Cisco_Connector使用者的組成員身份：

dsquery user -samid Cisco_Connector | dsget user -memberof -expand

Umbrella AD聯結器執行需要這些許可權的兩個主要任務。首先，它從Active Directory提取LDAP資訊，以便根據AD組建立策略，並能夠在Umbrella儀表板中顯示AD使用者名稱和組名。`Replicate Directory Changes`許可權允許此操作。

其次，它從域控制器收集登入事件，並將它們傳遞到虛擬裝置。這允許虛擬裝置建立其IP到使用者的對映，從而識別使用者。除`複製目錄更改`許可權外，所有許可權都適用於此許可權。僅當部署包括與域控制器位於同一Umbrella站點中的虛擬裝置時，才需要這些許可權。



附註：除了設定Cisco_Connector使用者所需的許可權外，域控制器配置指令碼還通過向

Umbrella發出API呼叫來註冊域控制器。如果您手動修改許可權而不是使用配置指令碼，則還必須手動完成此註冊。有關如何在Umbrella控制面板上手動新增域控制器的資訊，請參閱Umbrella文檔。

需要許可權

- 複製目錄更改
- 事件日誌讀取器
- 遠端管理員
- 審計策略

複製目錄更改

此許可權允許Cisco_Connector使用者查詢LDAP。這是通常隨「企業只讀域控制器」組提供的必需許可權。這為Umbrella Dashboard提供了顯示AD對象名稱和確定組成員身份所需的資訊。聯結器請求以下屬性：

cn — 公用名。

dn — 可分辨名稱。

dNSHostName — 在DNS中註冊時的裝置名稱。

mail — 與使用者關聯的電子郵件地址。

memberOf — 包含使用者的組。

objectGUID — 對象的組ID。此屬性以雜湊形式傳送到Secure Access。

primaryGroupId — 可用於使用者和組的主組ID。

primaryGroupToken — 僅可用於組的主組令牌。不檢索密碼或密碼雜湊。安全訪問使用

訪問策略中的primaryGroupToken資料以及配置和報告。每個使用者或每台電腦過濾也需要此資料。

sAMAccountName — 用於登入Cisco AD聯結器的使用者名稱。

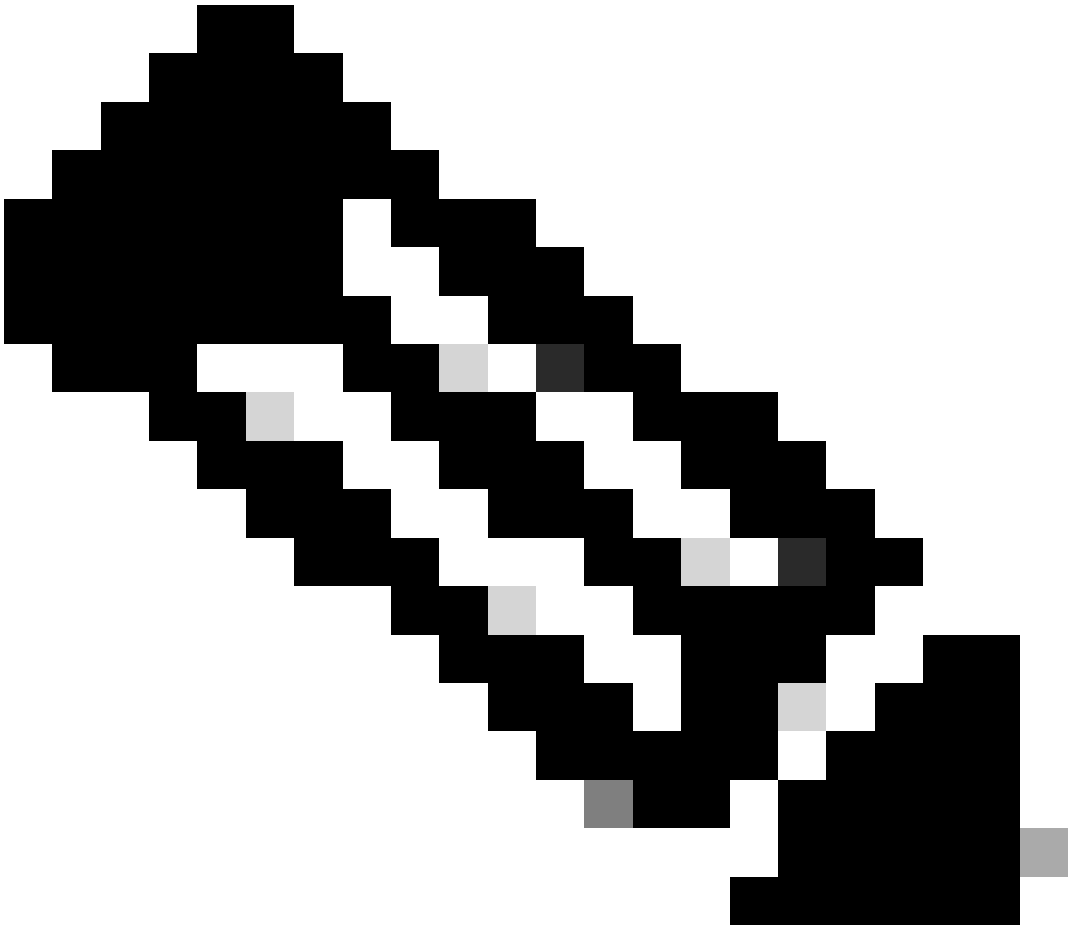
userPrincipalName — 使用者的主體名稱。

在這些對象類中：

```
(&(objectCategory=person)(objectClass=user))
(objectClass=organizationalunit)
(objectClass=computer)
(objectClass=group)
```

內建的「企業只讀域控制器」組必須提供此許可權，因此Cisco_Connector使用者必須是此組的成員。您可以驗證組的許可權或專門為Cisco_Connector使用者指定許可權（如果組不提供這些許可權）：

- 開啟Active Directory使用者和電腦管理單元
- 在「檢視」(View)選單中，按一下「高級功能」(Advanced Features)。
- 按一下右鍵域對象，如「company.com」，然後按一下「Properties（屬性）」。
- 在「安全」頁籤上，選擇「企業只讀域控制器」或「Cisco_Connector」使用者。
    - 如有必要，您可以通過按一下「新增」來新增「Cisco_Connector」使用者。
    - 在「選擇使用者、電腦或組」對話方塊中，選擇所需的使用者帳戶，然後按一下「新增」。
    - 按一下「確定」返回到「屬性」對話方塊。
- 按一下從清單中選擇Replicating Directory Changes和Read覈取方塊。
- 按一下「Apply（應用）」，然後按一下「OK（確定）」。
- 關閉管理單元。

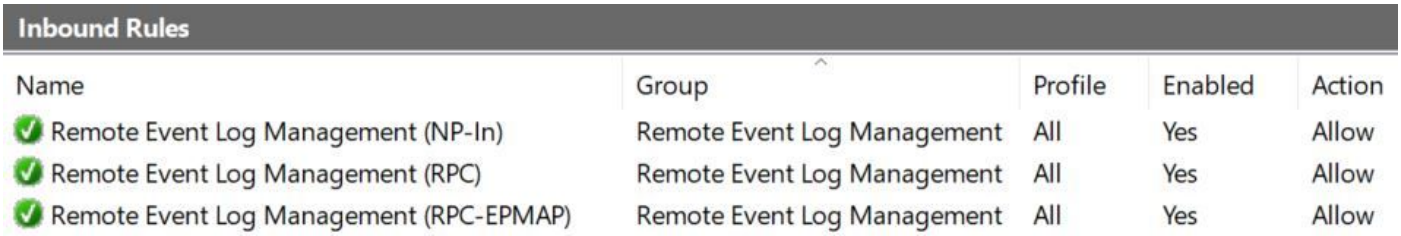


附註：在父/子域方案中，「企業只讀域控制器」僅存在於父域中。在這種情況下，必須手動為Cisco_Connector新增許可權，如下所示。

事件日誌讀取器

僅當部署包括與域控制器位於同一Umbrella站點中的虛擬裝置時，才需要此更改。此組中的成員身份允許Cisco_Connector使用者從事件日誌中讀取登入事件。

在域控制器電腦上，在Windows高級防火牆設定中，確保允許遠端事件日誌管理（NP-In、RPC和RPC-EPMAP）的入站規則。Umbrella AD聯結器可能會記錄一個錯誤資訊「RPC伺服器不可用」，並且如果不允許這些規則，則可能無法讀取登入事件。



360090909832

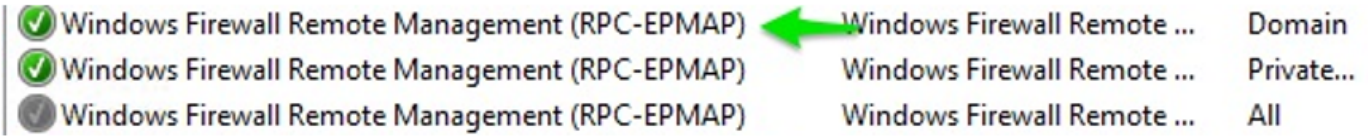
您也可以通過以下命令啟用這些規則：netsh advanced firewall set rule group="Remote Event Log Management" new enable=yes

遠端管理員

需要遠端管理來允許聯結器讀取域控制器上的登入事件。僅當部署包括與域控制器位於同一Umbrella站點中的虛擬裝置時，才需要此許可權。

請在命令提示符下運行以下命令：

```
netsh advfirewall firewall set rule group="remote administration" new enable=yes
netsh advfirewall set currentprofile settings remotemanagement enable
```



4413613529492

審計策略

僅當部署包括與域控制器位於同一Umbrella站點中的虛擬裝置時，才需要此更改。稽核策略定義在域控制器的事件日誌中記錄哪些事件。聯結器要求記錄成功的登入事件，以便使用者能夠對映到其IP地址。

在普通Windows Server 2008+環境中，必須配置舊的「稽核登入事件」設定。 具體來說，「稽核登入事件」策略必須設定為「成功」。 這可以通過在命令提示符下運行以下命令來驗證：

```
GPRESULT /z
```

此策略被定義為組策略對象。要修改它，請編輯適用於您的DC的組策略（通常為「預設域控制器策略」），並將此策略設定為包括「成功」事件：

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit lo
```

請確保在進行此更改後更新DC上的組策略。

但是，Windows Server 2008還引入了Advanced Audit Policy Configuration。雖然舊版Windows審計策略仍然可以使用，但如果定義了任何高級審計策略，則會忽略這些策略。請參閱Microsoft文檔以瞭解兩個稽核策略如何互動。

對於聯結器，如果定義了任何高級審計策略（包括與登入無關的高級審計策略），則必須使用高級審計策略。

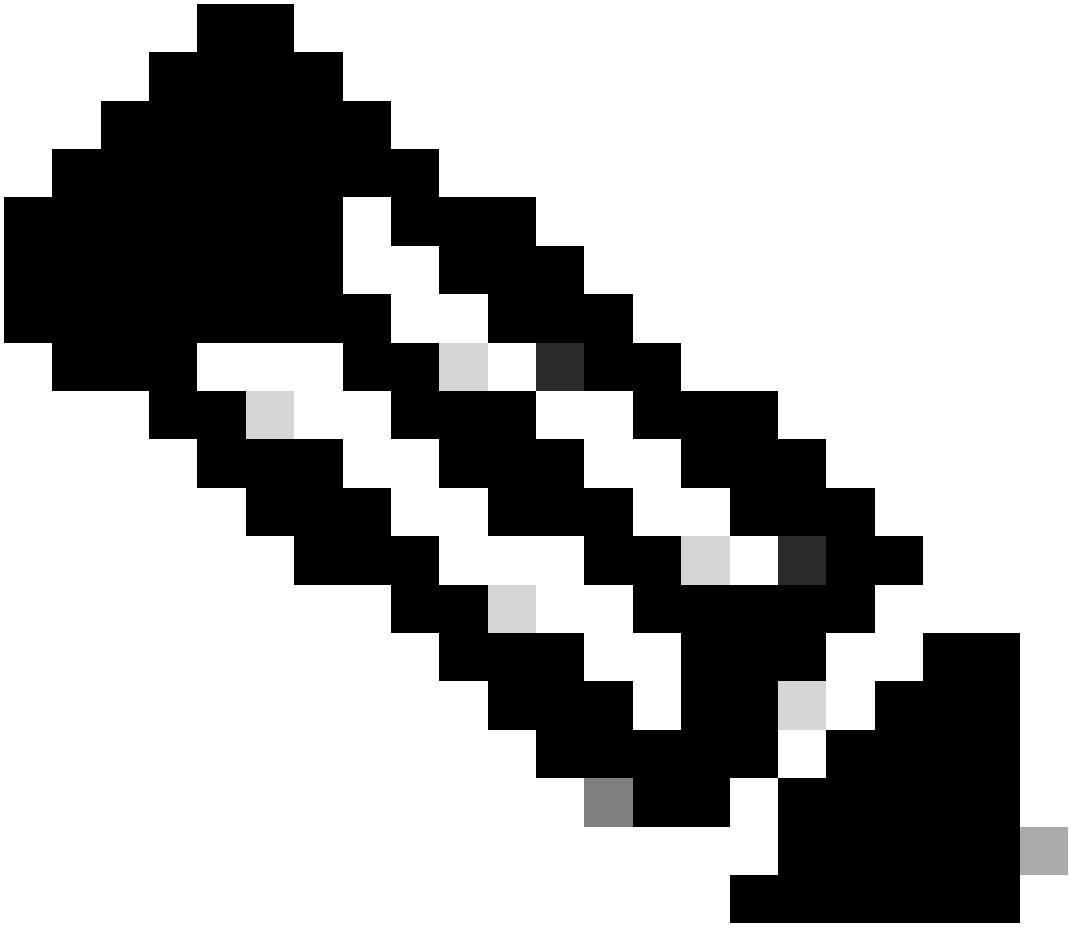
必須使用組策略為所有DC設定高級審計策略。 編輯適用於您的DC的組策略（通常為「預設域控制器策略」），然後轉到此部分：

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\
```

在該部分中，設定這些策略以同時包括「成功」和「失敗」事件：

```
Audit Logon
Audit Logoff
Audit Other Logon/Logoff Events
```

請確保在進行此更改後更新DC上的組策略。



附註：如果要通過虛擬裝置部署AD聯結器，必須在聯結器與之通訊的域中的所有域控制器上完成防火牆規則更改和稽核策略設定。

如果在確認/更改上述設定後，您仍然能在控制面板中看到「Access Denied」消息，請傳送Umbrella Support聯結器日誌，如本文所述：為AD聯結器日誌提供支援

當將此資訊提供給Support時，請包含這兩個命令的輸出：

```
auditpol.exe /get /category:* > DCNAME_auditpol.txt
GPRESULT /H DC_NAME.htm
```

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）。