

配置Windows Server以將DNS請求轉發到Umbrella

目錄

[簡介](#)

[概觀](#)

[設定步驟](#)

[最佳實踐說明](#)

簡介

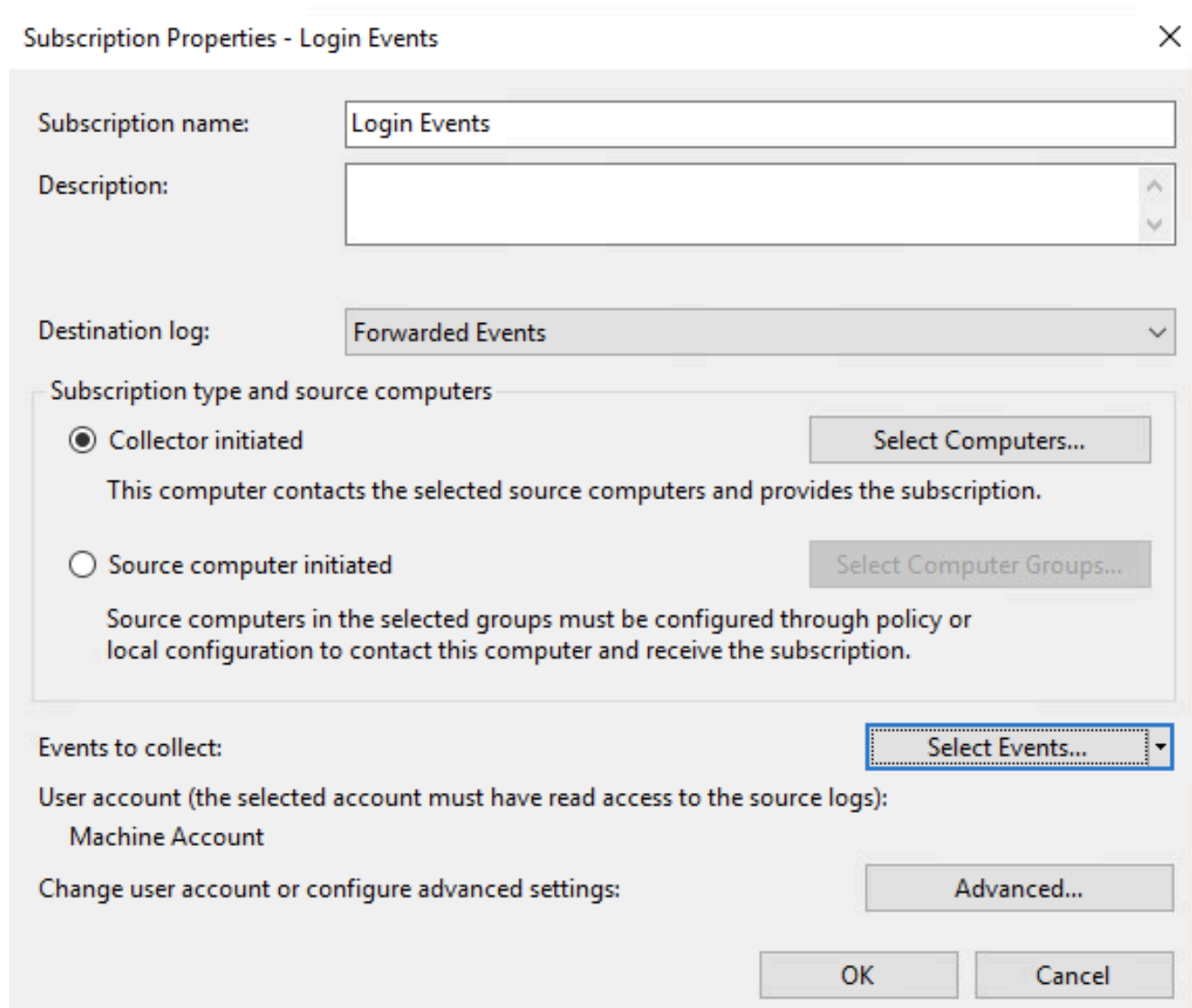
本文檔介紹如何配置Windows Server以將DNS請求轉發到Umbrella，以增強客戶端保護和日誌記錄。

概觀

Windows Server可以通過充當DNS轉發器[來保護](#)使用網路標識的客戶端。域控制器或具有DNS角色的任何其他伺服器可以從註冊網路將DNS傳送到Umbrella。

設定步驟

1. 開啟DNS Manager(dnsmgmt.msc)。
2. 在樹中按一下右鍵伺服器名稱，然後選擇屬性。
3. 選擇Forwarders頁籤。
4. 按一下Edit...並輸入[Umbrella DNS server IP地址](#)。
5. 在「編輯轉發器」(Edit Forwarders)視窗中按一下確定。條目顯示在轉發器清單中。
6. 如果沒有可用的轉發器，取消選中標籤為Use root hints的框。



Subscription Properties - Login Events

Subscription name: Login Events

Description:

Destination log: Forwarded Events

Subscription type and source computers

☒ Collector initiated Select Computers...

This computer contacts the selected source computers and provides the subscription.

☐ Source computer initiated Select Computer Groups...

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect: Select Events...

User account (the selected account must have read access to the source logs):

Machine Account

Change user account or configure advanced settings: Advanced...

OK Cancel

mceclip0.png

最佳實踐說明

- 確保Use root hints if no forwarders are available(如果沒有可用的轉發器，則使用根提示)未選中。如果選中，則Umbrella保護和日誌記錄變得不一致。例如，如果域未通過DNSSEC驗證或受到DDoS緩解事件的影響，則Windows DNS伺服器可以認為Umbrella無響應並嘗試使用根提示直接遞迴，從而繞過Umbrella。
- 僅使用Umbrella作為轉發器。請勿配置任何第三方解析程式。Umbrella只能記錄和保護其接收的DNS查詢。
- 為了獲得冗餘，請將所有四個Umbrella任播IP地址配置為轉發器，如前面的螢幕截圖所示。
- 如果使用Umbrella站點和虛擬裝置，請指向本地虛擬裝置作為轉發器，而不是Umbrella任播地址。

- 避免請求循環：如果虛擬裝置將您的伺服器列為本地DNS伺服器之一，請勿將該虛擬裝置新增為轉發器。
 - 虛擬裝置只能檢視DNS伺服器的IP地址，而不能檢視其服務的各個客戶端的地址。
 - 如果將Active Directory整合與虛擬裝置一起使用，請將Windows DNS伺服器IP新增為例外。導航到Umbrella Dashboard中的Deployments > Sites and Active Directory > Service Account Exceptions，然後新增DNS伺服器IP。這樣可以防止使用者標識與伺服器流量的不正確歸屬。
-
- 請勿將Umbrella伺服器新增到Root Hints選項卡。Umbrella DNS伺服器是遞迴解析器，不用作迭代查詢的根。將它們新增為根提示會導致不期望的行為，並繞過Umbrella保護和日誌記錄。

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）。