使用事件日誌收集器和域配置ADC

目錄

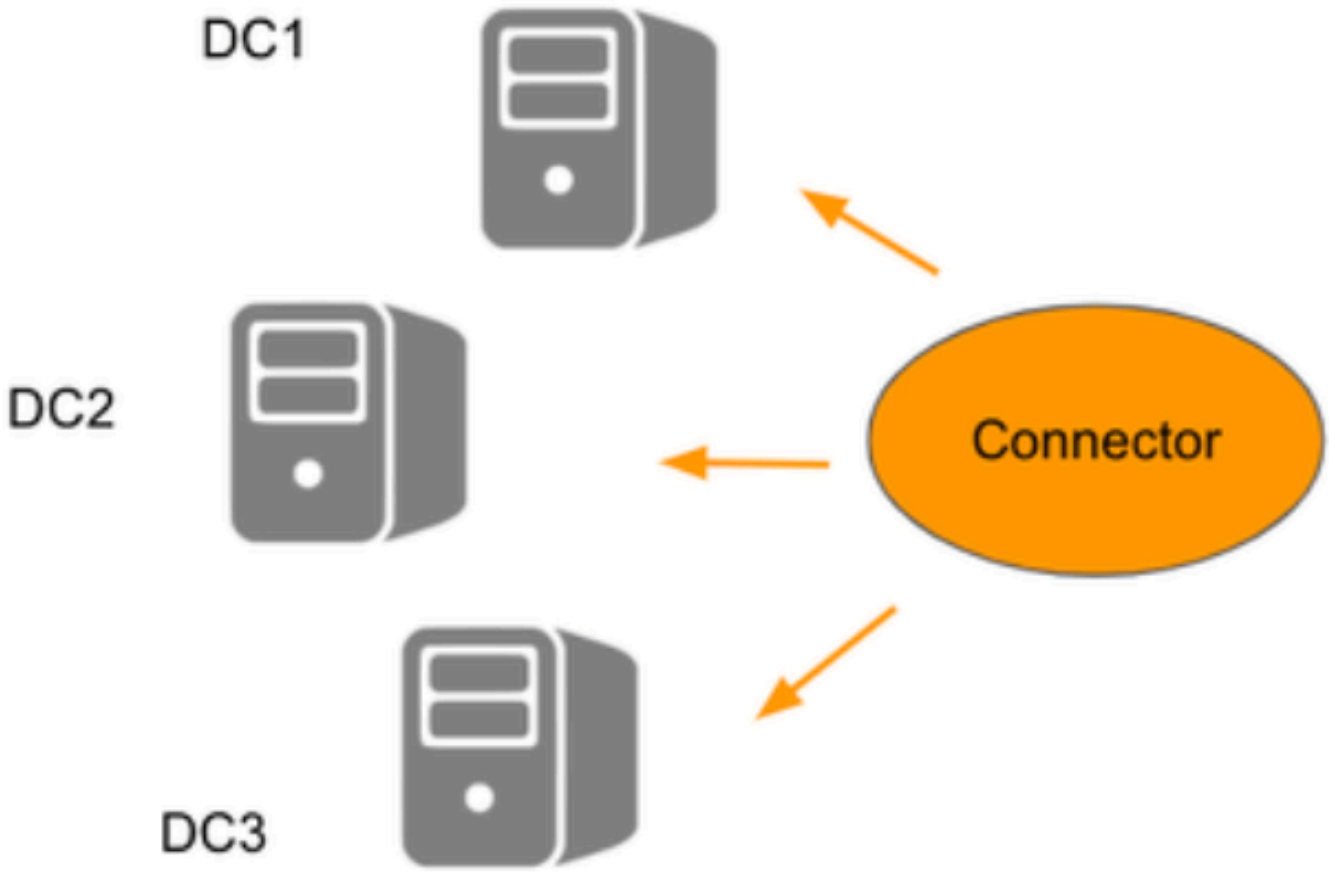
簡介

本文說明如何使用事件日誌收集器和域配置Active Directory聯結器(ADC)。

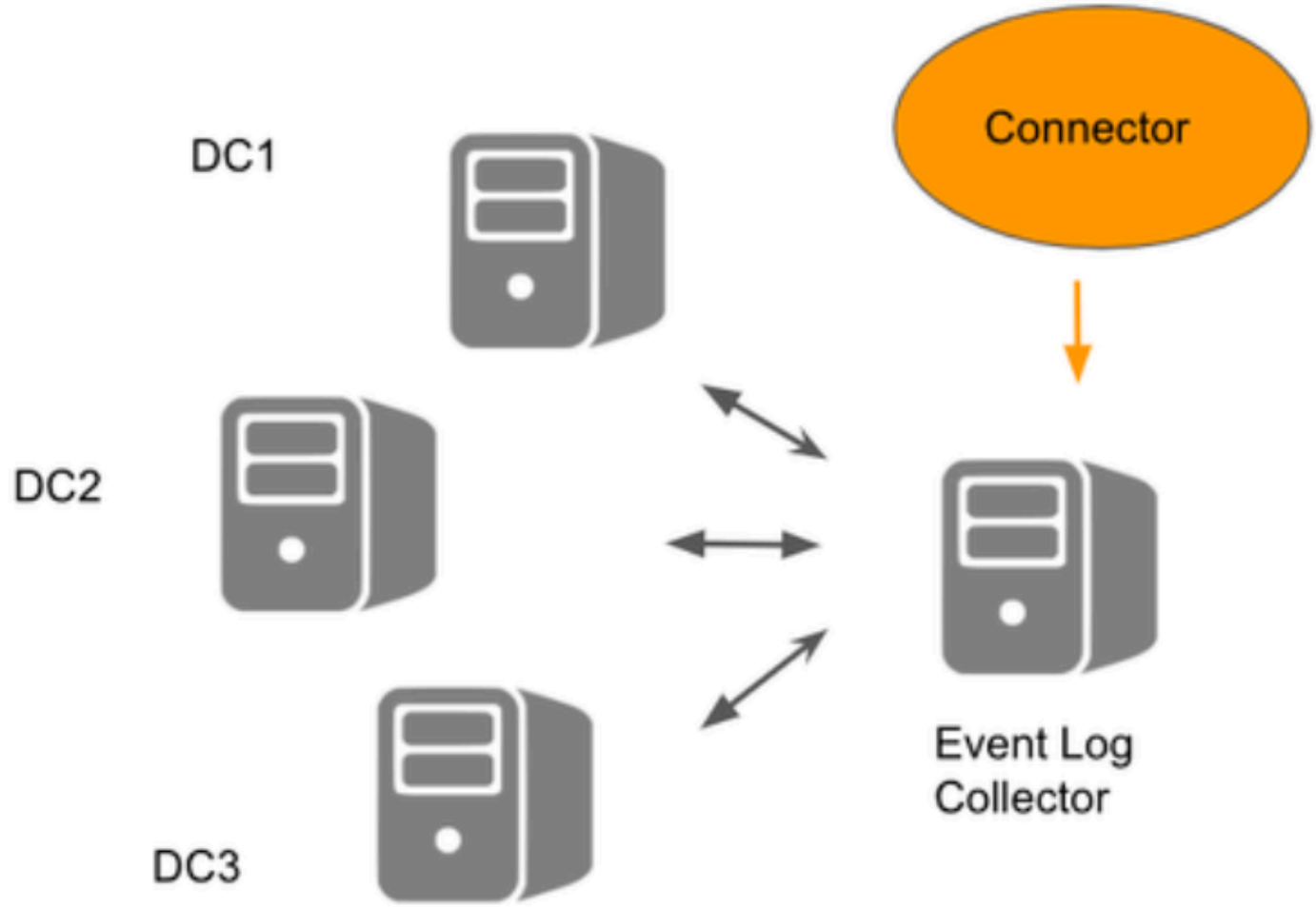
組態選項

有兩個設定選項可用於使用Active Directory:

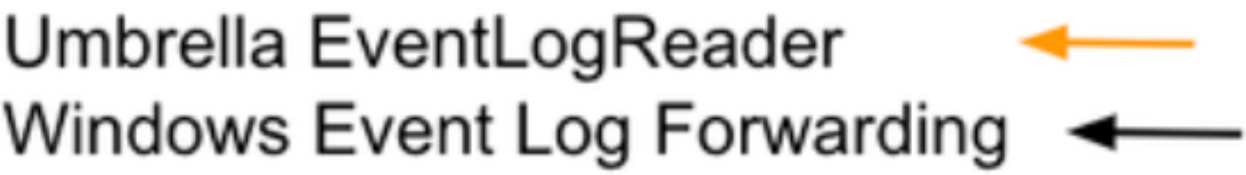
1. 正在註冊域控制器：這涉及使用虛擬裝置(VA)和AD聯結器，AD聯結器直接與所有已註冊的域控制器(DC)通訊。
2. **事件日誌收集器**：此設定包括域、VA和AD聯結器。在此場景中，Windows事件日誌轉發將資訊從DC傳送到中央事件日誌收集器伺服器。然後，AD聯結器僅與此中央伺服器通訊，而非DC



22062473499540

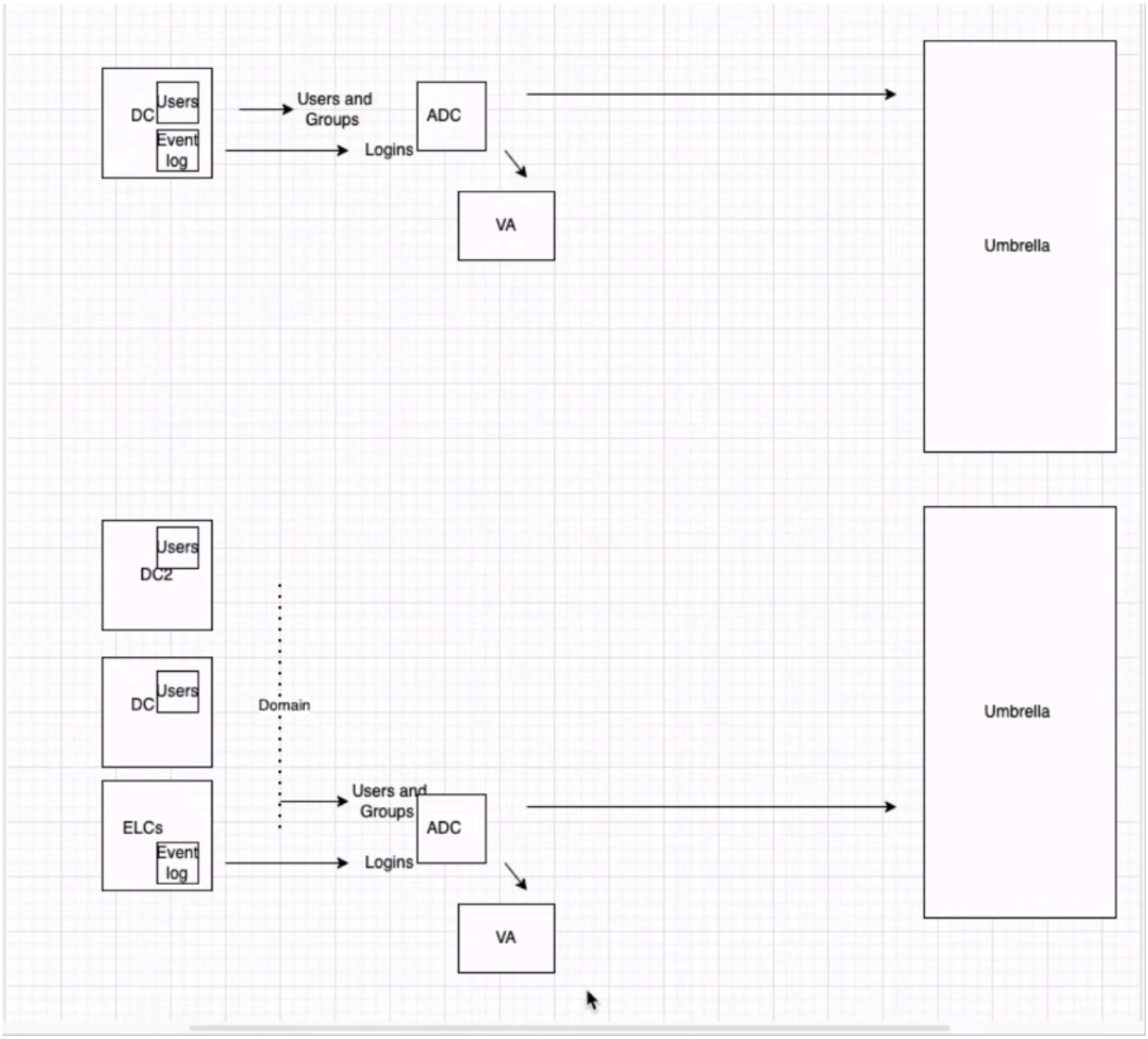


22062473502228



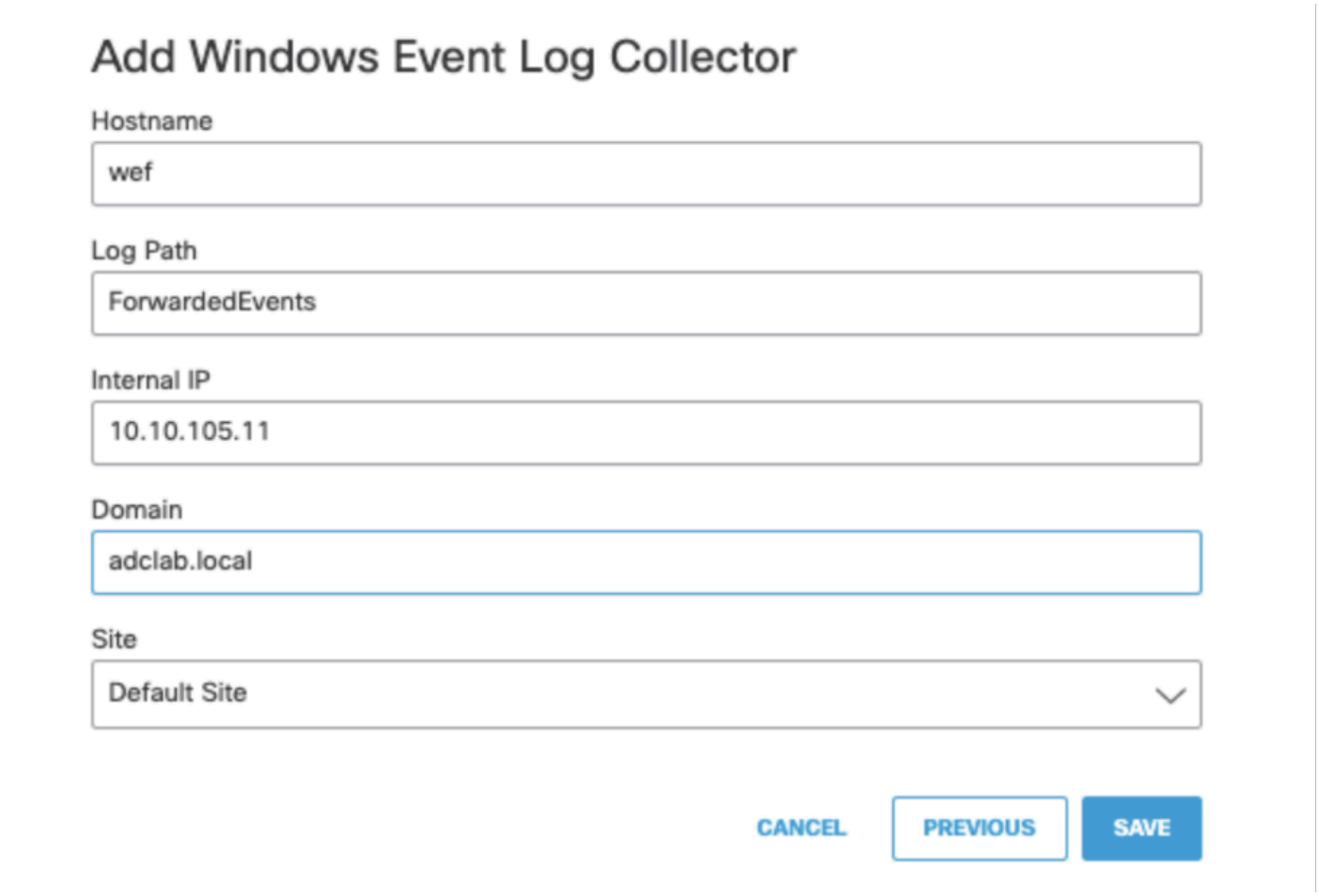
22062518240276

請注意：註冊域控制器和新增域是不同的過程。



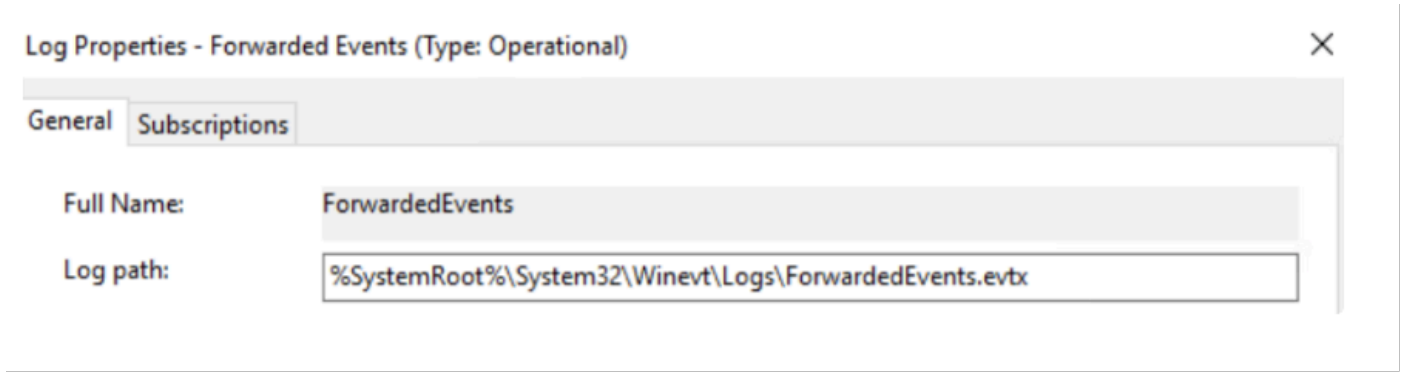
22062518241684

1. 要在Umbrella控制面板中啟動配置，請導航到Deployments > Configuration > Sites and Active Directory，然後點選Add。選擇Windows Event Log Collector，然後按一下「下一步」。



22062473507220

2.客戶可以檢查日誌檔案屬性（在Windows事件檢視器中）以查詢日誌的名稱。請注意，輸入的日誌檔名稱必須沒有.evtx副檔名或完整路徑詳細資訊。



22062518244756

重要注意事項：

為使聯結器正常工作，必須繼續執行正常部署步驟：

1. 在「站點和Active Directory」頁面上註冊「域」，以便進行使用者設定。這是必要的，因為沒有註冊的DC來同步使用者/組。
2. 部署「虛擬裝置」。

此部署模式存在一些已知限制：

- 即使工作正常，聯結器也可能出現錯誤狀態。

為了使AD聯結器高效工作，需要某些許可權。您可以在此處檢視這些許可權：OpenDNS_Connector使用者所需的許可權。

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）。