使用者代理的即時狀態顯示為未知

目錄

簡介

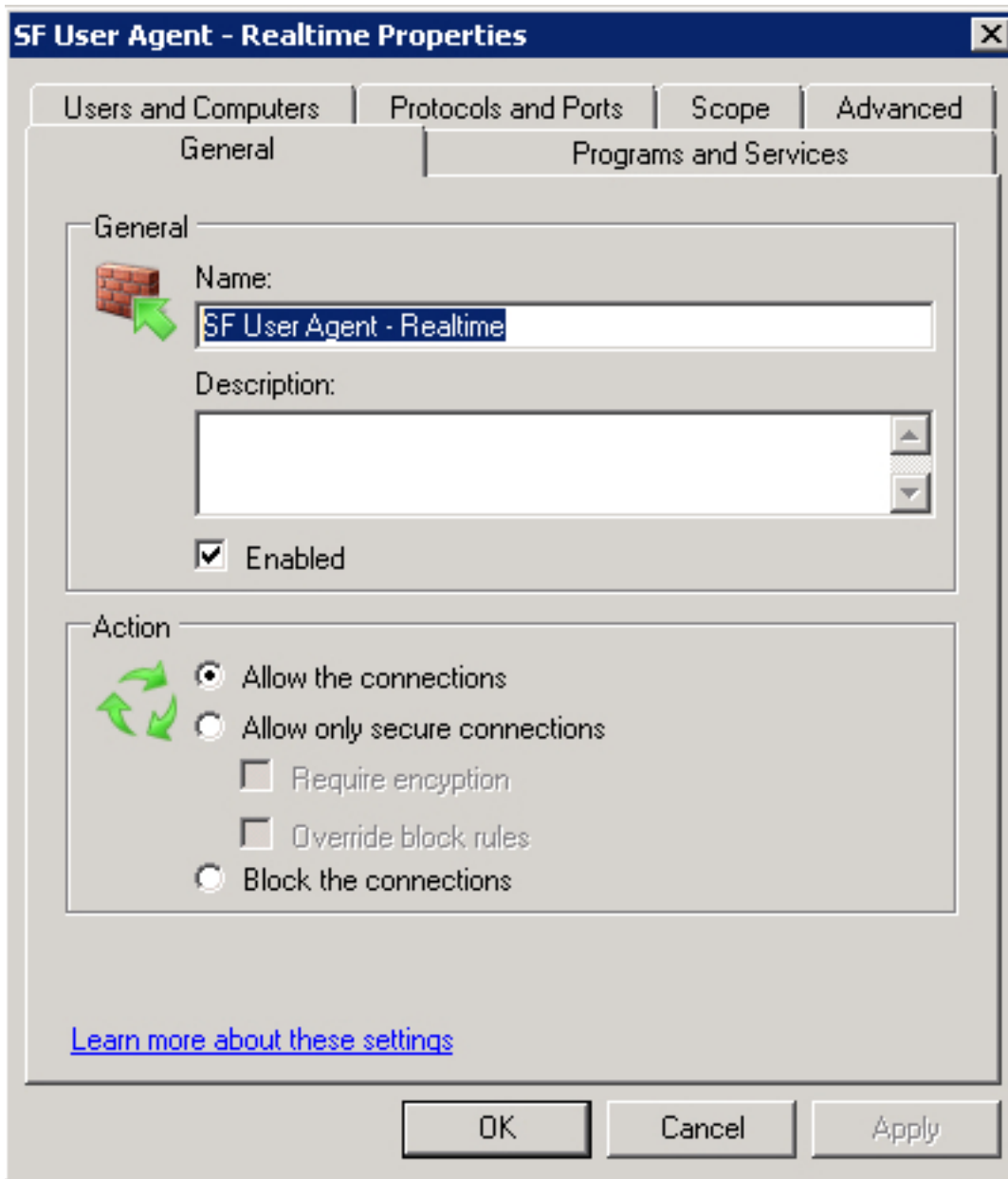部署Sourcefire使用者代理後，您可能會注意到完成所有配置步驟後的即時狀態仍為未知。本文說明如何將狀態從Unknown更改為Available。

症狀

域控制器的防火牆設定阻止建立所需的RPC連線。 使用者代理使用RPC動態埠連線連線到域控制器並建立即時監視。
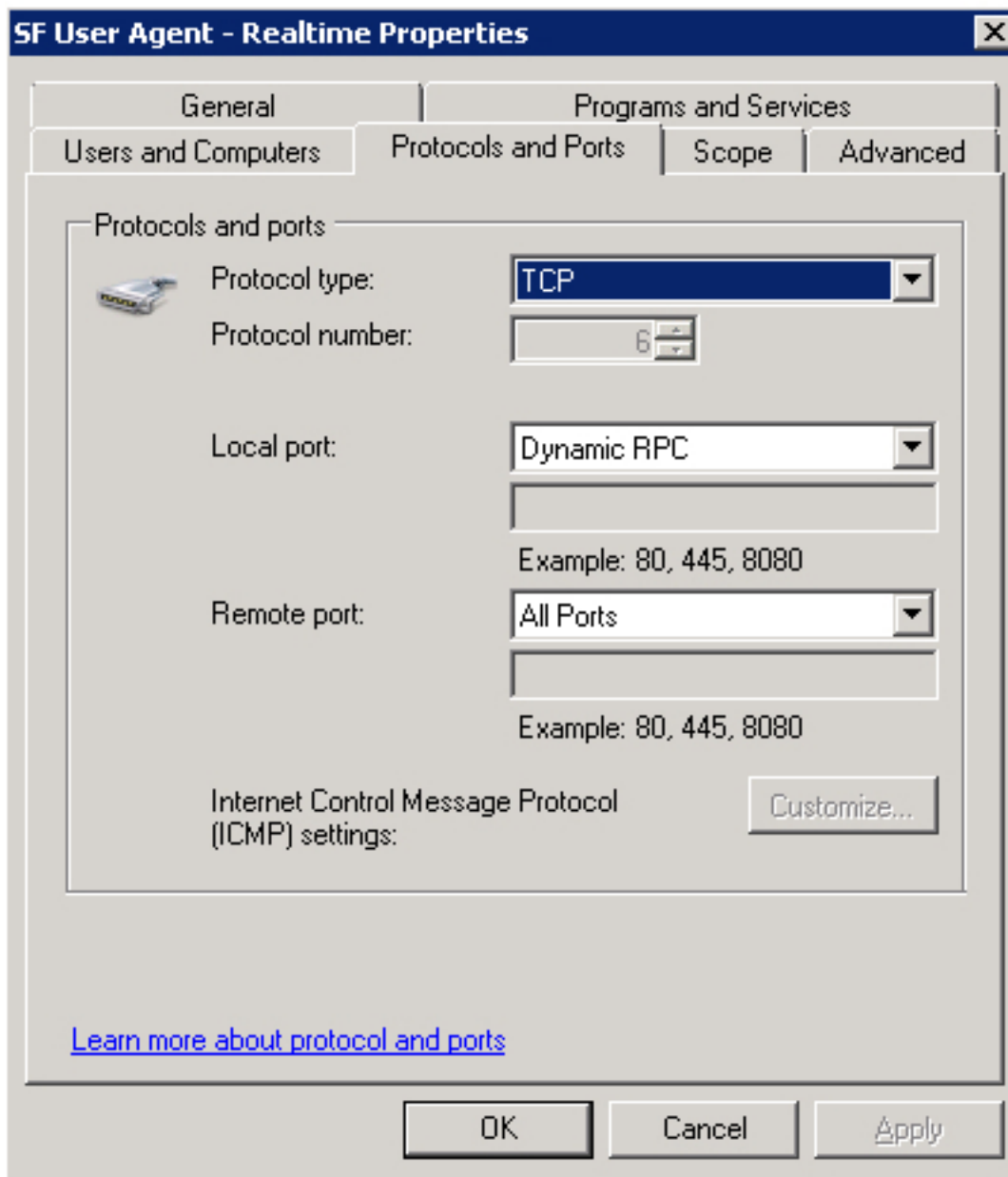
解決方案

使用Windows Firewall with Advanced Security控制檯，在目標域控制器上建立入站防火牆規則，允許從使用者代理進行必要的連線。設定和步驟的示例如下所示：
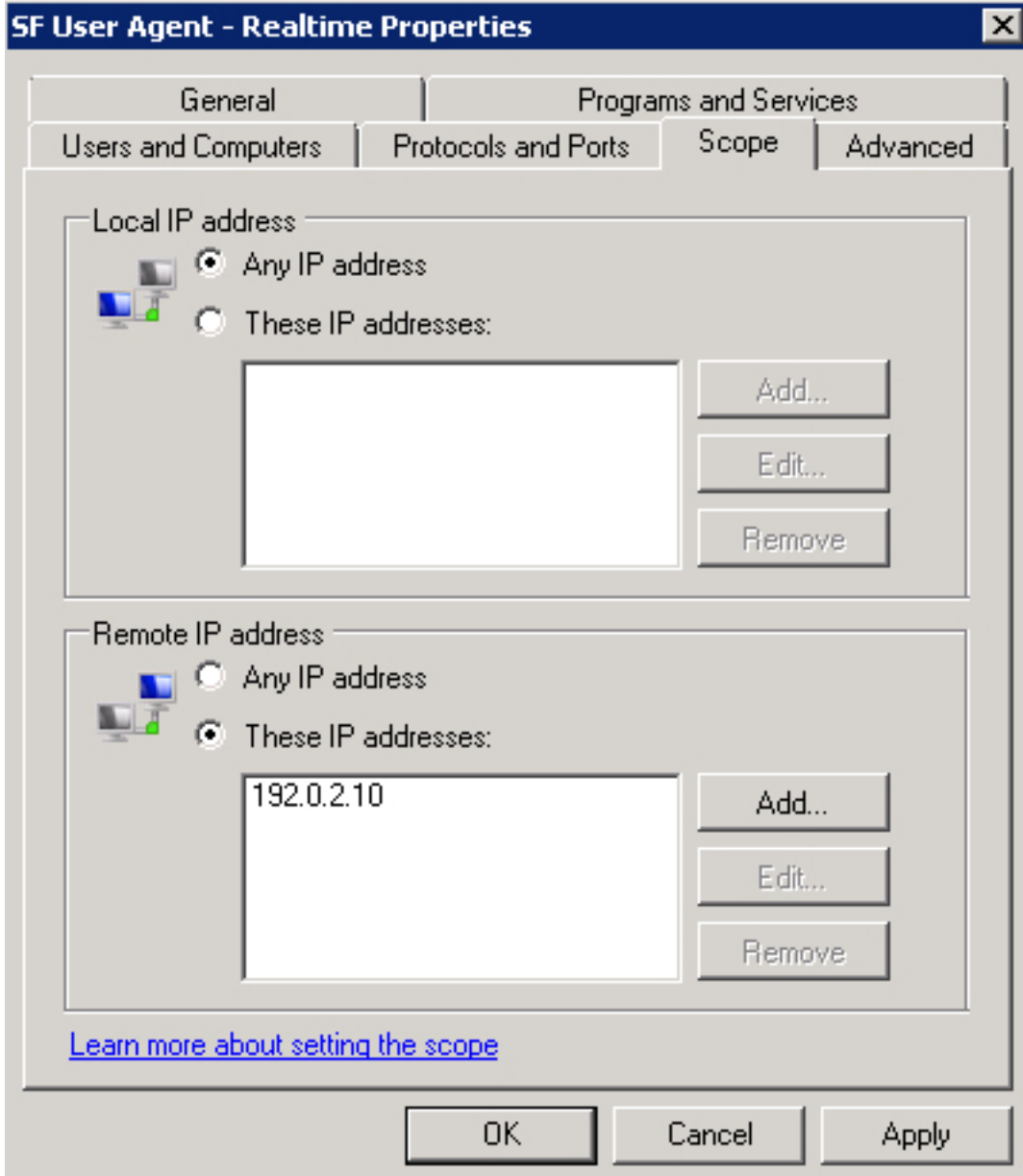
1. 在General頁籤上，命名規則並選擇Allow the Connections。
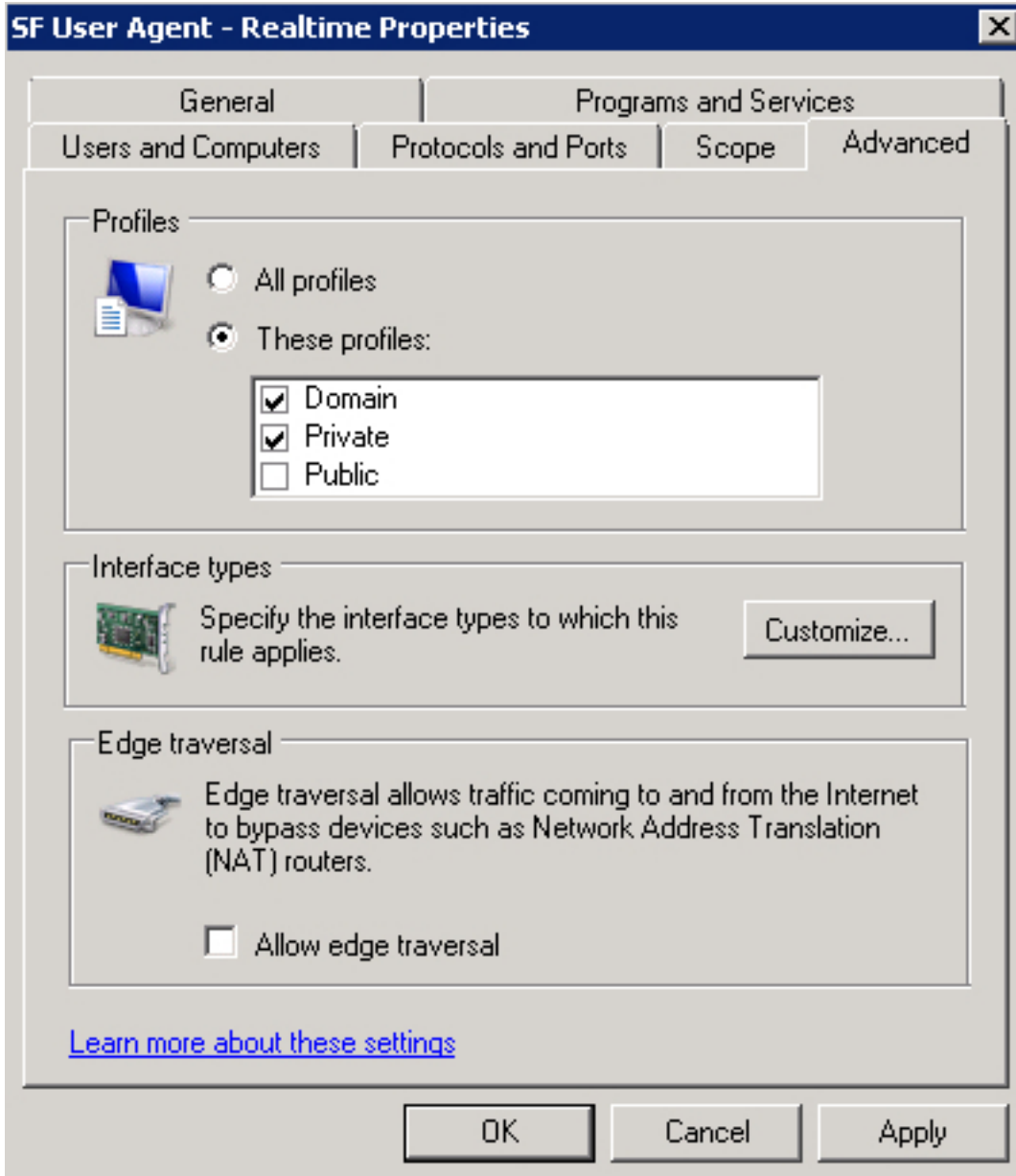
2. 在**Protocols and Ports**頁籤上，選擇以下專案：

- **通訊協定類型:**TCP
- **本地埠:**動態RPC
- **遠端連線埠:**所有埠

3. 在Scope頁籤上，新增Remote IP address。按一下Add以輸入使用者代理主機的IP地址。

4. 在Advanced索引標籤上，選擇適當的Profiles。

儲存防火牆規則，啟用該規則並重新啟動Sourcefire使用者代理服務。 即時連線狀態現在應從**未知**更改為**可用**。