使用者代理的即時狀態顯示為未知

目錄

<u>簡介</u> <u>症狀</u> <u>解決方案</u>

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。

| SF User Agent - Realtime Properties | × |
|--|-------------------|
| Users and Computers Protocols and Ports Scope General Programs and Service | Advanced ces |
| General Name: SF User Agent - Realtime Description: Enabled | |
| Action Allow the connections Allow only secure connections Allow only secure connections Require encyption Override block rules Block the connections | |
| Learn more about these settings OK Cancel | Apply |

- 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

| 5F User Agent - R | tealtime Prope | rties | | × |
|-------------------------------|---|---------------------------|-----------------------|-------------------|
| Gener Users and Comp | al puters Protoc | Program: | s and Servio Scope | ces Advanced |
| Protocols and Prot Prot | l ports tocol type: tocol number: | TCP 6 | | • |
| Loc | al port: | Dynamic RP0 | C | |
| Rer | note port: | Example: 80, All Ports | 445, 8080 | |
| Inte (ICN | rnet Control Mess IP) settings: | age Protocol | 443, 8888 Cus | tomize |
| Learn more abo | out protocol and p | orts | | |
| | | ок с | Cancel | Apply |

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。

| SF User Agent - Realtime | Properties | | × | | |
|---|-------------------------------|----------------------|--------|--|--|
| General | General Programs and Services | | | | |
| Users and Computers Protocols and Ports Scope Advance | | | | | |
| Local IP address | ress ddresses: | | | | |
| | | Add | | | |
| | | Edit | | | |
| | | Remov | /e | | |
| Remote IP address | ress ddresses: | | | | |
| 192.0.2.10 |) | Add Edit Remov | /e | | |
| Learn more about setting t | the scope | | | | |
| | OK | Cancel | Apply | | |

4. 在Advanced索引標籤上,選擇適當的Profiles。

| F User Agent - Realtime Properties 🛛 🛛 🗙 | | | | |
|--|--|--|--|--|
| General Programs and Services | | | | |
| Users and Computers Protocols and Ports Scope Advanced | | | | |
| Profiles All profiles These profiles: Domain Private Public | | | | |
| Specify the interface types to which this Customize | | | | |
| Edge traversal | | | | |
| Edge traversal allows traffic coming to and from the Internet to bypass devices such as Network Address Translation (NAT) routers. | | | | |
| | | | | |
| Learn more about these settings | | | | |
| OK Cancel Apply | | | | |

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**。