# 用户代理的实时状态显示为未知

#### 目录

<u>简介</u> <u>症状</u> <u>解决方案</u>

## 简介

部署Sourcefire用户代理后,您可能会注意到在执行所有配置步骤后,实时状态仍为未知。本文档提 供有关如何将状态从**未知**更改为**可用**的说明。

#### 症状

域控制器的防火墙设置阻止建立所需的RPC连接。 用户代理使用RPC动态端口连接连接到域控制器 并建立实时监控。

## 解决方案

使用Windows Firewall with Advanced Security控制台在目标域控制器上创建入站防火墙规则,从而 允许从用户代理进行必要的连接。设置和步骤示例如下所示:

1. 在General选项卡上,命名规则并选择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 <ul> <li>Allow the connections</li> <li>Allow only secure connections</li> <li>Allow only secure connections</li> <li>Require encyption</li> <li>Override block rules</li> <li>Block the connections</li> </ul>	
Learn more about these settings OK Cancel	Apply

- 2. 在Protocols and Ports选项卡上,选择以下项目:
  - 协议类型:TCP
  - 本地端口:动态RPC
  - 远程端口:所有端口

5F User Agent - Realtime Properties 🛛 🛛 🔀					
General Users and Compute	ers Protoco	Program Is and Ports	ns and Servi Scope	ces   Advanced	
Protocols and po Protoco Protoco	rts ol type: ol number:	TCP 6		•	
Local p	oort:	Dynamic RF	°C	<u> </u>	
Remote	e port:	Example: 80 All Ports	), 445, 8080	•	
Interne (ICMP)	t Control Messa settings:	Example: 80 ge Protocol	), 445, 8080 Cus	stomize	
Learn more about protocol and ports					
		ОК	Cancel	Apply	

3. 在**范围**选项卡上,添加**远程IP地址**。单击Add以输入用户代理主机的IP地址。

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

4. 在Advanced选项卡上,选择适当的Profiles。

5F User Agent - Realtime I	Properties		×	
General D Brearans and Convises				
Users and Computers	Protocols and Ports	Scope	Advanced	
		000000		
Profiles				
📃 📐 🔿 All profiles				
Image: These problems	files:			
🔽 Domai	n			
Private	9			
Interface types				
Specify the inte	arface types to which th	is Cur		
rule applies.				
Edge traversal		17 0		
to bypass devi	allows traffic coming to ces such as Network A	and from the ddress Trans	ation	
(NAT) routers.				
L Allow adar	trauaraal			
	; (raversai			
Learn more about these se	ettinas			
	<u>skundo</u>			
	OK	Cancel	Apply	

保存防火墙规则,将其启用并重新启动Sourcefire用户代理服务。 您的实时连接状态现在应从**未知** 更改为**可用**。