# L'état en temps réel de l'agent utilisateur est affiché comme Inconnu

#### Contenu

Introduction Symptôme Solution

### Introduction

Après le déploiement d'un agent utilisateur Sourcefire, vous remarquerez peut-être que l'état en temps réel reste inconnu après avoir suivi toutes les étapes de configuration. Ce document fournit des instructions sur la façon de changer l'état de **Inconnu** à **Disponible**.

## Symptôme

Les paramètres de pare-feu du contrôleur de domaine empêchent l'établissement des connexions RPC requises. L'agent utilisateur utilise les connexions de port dynamique RPC pour se connecter au contrôleur de domaine et établir une surveillance en temps réel.

#### Solution

Créez une règle de pare-feu entrante sur le contrôleur de domaine ciblé à l'aide de la console **Pare-feu Windows avec sécurité avancée**, permettant la connexion nécessaire à partir de l'agent utilisateur. Voici un exemple de paramètres et d'étapes :

1. Dans l'onglet General, nommez la règle et sélectionnez Allow the Connections.

SF User Agent - Realtime Properties 🛛 🛛 🗙				
Users and Computers   Protocols and Ports   Scope   Advanced				
General Programs and Services				
General				
Name:				
SF User Agent - Realtime				
Description:				
Enabled				
Action				
Allow the connections				
🔨 🏹 🔿 Allow only secure connections				
Require encyption				
C verride block rules				
C Block the connections				
Learn more about these settings				
OK Cancel Apply				

- 2. Dans l'onglet Protocoles et ports, sélectionnez les éléments suivants :
  - Type de protocole: TCP
  - Port local : RPC dynamique
  - Port distant : Tous les ports

F User Agent - Realtime Properties 🛛 🗙					
General Programs and Services			ces )		
Users and Computers Protocols		s and Ports	Scope	Advanced	
Protocols and ports					
-	Protocol type:	TCP		•	
~	Protocol number:	6	÷		
	Local port:	al port: Dynamic RPC 💌		•	
		Example: 80, 445, 8080			
	Remote port:	All Ports			
		Example: 80,	, 445, 8080		
Internet Control Message Protocol Customize			stomize		
Learn more about protocol and ports					
		IK I	Cancel	Apply	

3. Dans l'onglet **Scope**, ajoutez l'**adresse IP distante**. Cliquez sur **Add** pour entrer l'adresse IP de l'hôte User Agent.

SF User Agent - Realtime	Properties		×		
General Programs and Services					
Users and Computers Protocols and Ports		Scope	Advanced		
Local IP address Any IP add These IP a	tress addresses:	Add Edit Remov	/e		
Remote IP address C Any IP add C These IP a	dress				
192.0.2.10	כ	Add. Edit. Remov	 /e		
Learn more about setting	the scope				
	ОК	Cancel	Apply		

4. Dans l'onglet Avancé, sélectionnez les profils appropriés.

SF User Agent - Realtime Properties 🛛 🛛 🔀				
General Programs and Services				
Users and Computers   Protocols and Ports   Scope   Advanced				
Profiles				
N C All profiles				
• These profiles:				
✓ Domain				
Private				
Interface types				
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.				
Allow edge traversal				
Learn more about these settings				
OK Cancel Apply				

Enregistrez la règle de pare-feu, activez-la et redémarrez le service Sourcefire User Agent. L'état de votre connexion en temps réel doit maintenant passer de **Inconnu** à **Disponible**.