O status em tempo real do agente de usuário é mostrado como desconhecido

Contents

Introduction Sintoma Solução

Introduction

Depois de implantar um Sourcefire User Agent, você poderá observar que o Real-Time Status permanece desconhecido depois de seguir todas as etapas de configuração. Este documento fornece instruções sobre como alterar o status de **Desconhecido** para **Disponível**.

Sintoma

As configurações de firewall do Controlador de Domínio impedem o estabelecimento das conexões RPC necessárias. O Agente de Usuário usa conexões de Porta Dinâmica RPC para se conectar ao Controlador de Domínio e estabelecer monitoramento em tempo real.

Solução

Crie uma regra de firewall de entrada no Controlador de Domínio de destino usando o console do **Firewall do Windows com Segurança Avançada**, permitindo a conexão necessária do Agente de Usuário. Um exemplo de configurações e etapas é mostrado abaixo:

1. Na guia Geral, nomeie a regra e selecione Permitir as Conexões.

SF User Agent - Realtime Properties			
Users and Computers Protocols and Ports Scope Advan General Programs and Services			
General Image: SF User Agent - Realtime Description: Image: Securit - Realtime Image: Securit - Realtime			
Action Action Allow the connections Allow only secure connections Require encyption Override block rules Block the connections			
Learn more about these settings OK Cancel Apply			

- 2. Na guia Protocolos e Portas, selecione os seguintes itens:
 - Tipo de protocolo: TCP
 - Porta local: RPC dinâmico
 - Porta remota: Todas as portas

F User Agent - Realtime Properties 🛛 🛛 🔀					
General Consultant		Programs and Services			
Users and Computers Protocol			s and r ons	scope	Advanced
Protocols and ports					
	Protocol type	B:	TCP		
	Protocol nur	nber:	6		
	Local port:		Dynamic RI	PC	<u> </u>
			Example: 80	0, 445, 8080	
	Remote port:		All Ports		
	Example: 80, 445, 8080				
Internet Control Message Protocol Customize				stomize	
Learn mor	re about protoc	col and port	<u>s</u>		
			к	Cancel	Apply

3. Na guia **Scope**, adicione o **endereço IP remoto**. Clique em **Add** para inserir o endereço IP do host do agente de usuário.

SF User Agent - Realtime	Properties		×			
General Programs and Services						
Users and Computers	Protocols and Ports	Scope	Advanced			
Local IP address	dress addresses:					
		Add.,				
		E dit				
		Remov	ve l			
Remote IP address C Any IP address C These IP addresses:						
192.0.2.1	0	Add Edit Remov	 			
Learn more about setting	the scope					
	OK	Cancel	Apply			

4. Na guia Advanced, selecione Profiles apropriados.

SF User Agent - Realtime Properties 🛛 🛛 🔀						
Constal Programs and Sourison						
Users and Consistent Distants and Distants and Services						
Users and Computers Protocols and Ports Scope Advanced						
Profiles						
🔊 🔿 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						

Salve a regra de firewall, ative-a e reinicie o serviço Sourcefire User Agent. O status da conexão em tempo real deve mudar de **Desconhecido** para **Disponível**.