De Realtime status van Gebruiker Agent wordt als Onbekend weergegeven

Inhoud

Inleiding Symptoom Oplossing

Inleiding

Na het implementeren van een Sourcefire gebruikersagent, kunt u de Realtime status onbekend zien na alle configuratiestappen. Dit document geeft instructies voor het wijzigen van de status van **Onbekend** naar **beschikbaar**.

Symptoom

De firewallinstellingen van de Domain Controller voorkomen dat de vereiste RPC-verbindingen worden gerealiseerd. De gebruikersagent gebruikt RPC Dynamische poortverbindingen om aan de controller van het Domein toe te voegen en controle in real-time op te zetten.

Oplossing

Maak een inkomende firewallregel op de beoogde controller van het domein met behulp van de **Windows Firewall met geavanceerde security** console, zodat de benodigde verbinding van de User Agent kan plaatsvinden. Hieronder vindt u een voorbeeld van de instellingen en stappen:

1. Voer in het tabblad Algemeen de regel in en selecteer Aansluitingen toestaan.

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 				
C verride block rules				
C Block the connections				
Learn more about these settings				
OK Cancel Apply				

- 2. Selecteer in het tabblad Protocollen en poorten de volgende items:
 - Protocoltype: TCP
 - Lokale poort: Dynamisch RPC
 - Remote-poort: Alle poorten

SF User Agent -	Realtime Prope	rties		×
General General Protocol:		Program cols and Ports	ns and Servi Scope	ces Advanced
Protocols ar Pr Pr Pr	nd ports rotocol type: rotocol number:	TCP 6		
Lo	ocal port:	Dynamic RP	°C	
B	emote port:	Example: 80 All Ports	, 445, 8080	<u> </u>
ln (10	ternet Control Mess CMP) settings:	Example: 80, age Protocol	, 445, 8080 Cus	tomize
Learn more at	bout protocol and p	orts		
		ОК	Cancel	Apply

3. Voeg in het tabblad **Toepassingsgebied** het **externe IP-adres toe**. Klik op **Add** om het IP adres van User Agent host in te voeren.

SF User Agent - Realtim	e Properties		×	
General Programs and Services				
Users and Computers	Protocols and Ports	Scope	Advanced	
Local IP address Any IP ad These IP	ldress addresses:	Add E dit		
Remote IP address Any IP ad These IP	ldress addresses:	Hemo	/e	
192.0.2.1	10	Add. Edit. Remov	 	
Learn more about setting	g the scope			
	ОК	Cancel	Apply	

4. Selecteer in het tabblad Geavanceerd de gewenste profielen.

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				

Sla de firewallregel op, schakelt u deze in en start de Sourcefire User Agent-service opnieuw. Uw real-time verbindingsstatus zou nu van **Onbekend** in **Beschikbaar** moeten veranderen.