Lo stato in tempo reale dell'agente utente è indicato come Sconosciuto

Sommario

Introduzione Sintomo Soluzione

Introduzione

Dopo aver distribuito un agente utente Sourcefire, è possibile notare che lo stato in tempo reale rimane sconosciuto dopo aver eseguito tutti i passaggi di configurazione. In questo documento viene spiegato come modificare lo stato da **Sconosciuto** a **Disponibile**.

Sintomo

Le impostazioni del firewall del controller di dominio impediscono di stabilire le connessioni RPC necessarie. L'agente utente utilizza connessioni a porte dinamiche RPC per il collegamento al controller di dominio e per stabilire il monitoraggio in tempo reale.

Soluzione

Creare una regola firewall in entrata nel controller di dominio di destinazione utilizzando la console di **Windows Firewall con protezione avanzata**, consentendo la connessione necessaria dall'agente utente. Di seguito è riportato un esempio di impostazioni e passaggi:

1. Nella scheda Generale, assegnare un nome alla regola e selezionare Consenti connessioni.

SF User Agent - Realtime Properties	×
Users and Computers Protocols and Ports Scope Advanced General Programs and Services	
General Name: SF User Agent - Realtime Description:	
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. Nella scheda Protocolli e porte selezionare gli elementi seguenti:
 - Tipo di protocollo: TCP
 - Porta locale: RPC dinamico
 - Remote port: Tutte le porte

F User Agent - Realtime Properties 🛛 🛛 🔀					
) Users and	General Computers Protoco	Programs and Seconds s and Ports Di Second	Services		
Protoco	Is and ports Protocol type:				
	Protocol number:	6 🛫			
	Local port:	Dynamic RPC	<u> </u>		
	Remote port:	Example: 80, 445, 8 All Ports	3080		
	Example: 80, 445, 8080 Internet Control Message Protocol Customize				
Learn more about protocol and ports					
)K Cancel	Apply		

3. Nella scheda **Ambito** aggiungere l'**indirizzo IP remoto**. Fare clic su **Add** (Aggiungi) per immettere l'indirizzo IP dell'host dell'agente utente.

SF User Agent - Realtime	e Properties		×
General	ns and Services		
Users and Computers	Protocols and Ports	Scope	Advanced (
Local IP address	dress addresses:		
		Add	
		E dit	
		Remov	/e
Remote IP address — C Any IP ad	dress addresses:		
192.0.2.1	0	Add. Edit. Remov	 /e
Learn more about setting	the scope	1	
	OK	Cancel	Apply

4. Nella scheda Avanzate, selezionare i profili appropriati.

SF User Agent - Realtime Properties	×					
General Programs and Services						
Users and Computers Protocols and Ports Scope Advance/	зΪ					
Profiles	1					
📃 💭 🔿 All profiles						
These profiles:						
☑ Domain						
Private						
Interface types						
Specify the interface types to which this Customize						
rule applies.						
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						

Salvare la regola firewall, attivarla e riavviare il servizio Sourcefire User Agent. Lo stato della connessione in tempo reale dovrebbe passare da **Sconosciuto** a **Disponibile**.