Der Echtzeitstatus des Benutzer-Agenten wird als unbekannt angezeigt.

Inhalt

Einführung Symptom Lösung

Einführung

Nach der Bereitstellung eines Sourcefire-Benutzer-Agenten ist Ihnen möglicherweise bewusst, dass der Echtzeit-Status nach allen Konfigurationsschritten unbekannt bleibt. Dieses Dokument enthält Anweisungen zum Ändern des Status von **Unbekannt** in **Verfügbar**.

Symptom

Die Firewall-Einstellungen des Domänencontrollers verhindern, dass die erforderlichen RPC-Verbindungen hergestellt werden. Der Benutzer-Agent verwendet dynamische RPC-Port-Verbindungen, um eine Verbindung zum Domain Controller herzustellen und eine Echtzeitüberwachung einzurichten.

Lösung

Erstellen Sie eine Firewall-Regel für eingehenden Datenverkehr auf dem Ziel-Domänen-Controller mithilfe der **Windows-Firewall mit der Advanced Security-**Konsole, damit die erforderliche Verbindung vom Benutzer-Agent hergestellt werden kann. Im Folgenden finden Sie ein Beispiel für Einstellungen und Schritte:

1. Geben Sie auf der Registerkarte **Allgemein den** Namen der Regel, und wählen Sie **Verbindungen zulassen aus**.

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. Wählen Sie auf der Registerkarte Protokolle und Ports die folgenden Elemente aus:
 - Protokolltyp: TCP
 - Lokaler Port: Dynamisches RPC
 - Remote-Port: Alle Ports

General Programs and Services Users and Computers Protocols and Ports Scope Advanced Protocols and ports
Protocols and ports Protocols and Ports Scope Advanced
Protocols and ports
Protocol type: TCP
Protocol number: 6
Local port: Dynamic RPC
Example: 80, 445, 8080
Remote port: All Ports
Example: 80, 445, 8080
Internet Control Message Protocol Customize
Learn more about protocol and ports
OK Cancel Apply

3. Fügen Sie auf der Registerkarte **Scope** (Bereich) die **Remote-IP-Adresse hinzu**. Klicken Sie auf **Hinzufügen**, um die IP-Adresse des Benutzer-Agent-Hosts einzugeben.

SF User Agent - Realtime	e Properties		×
General Users and Computers	Program Protocols and Ports	ms and Servio Scope	ces Advanced
Local IP address Any IP ad These IP	ldress addresses:	Add Edit Remov	
Remote IP address Any IP ad These IP	ldress addresses:		
192.0.2.1	10	Add Edit Remov	 /e
Learn more about setting	g the scope		
	ОК	Cancel	Apply

4. Wählen Sie auf der Registerkarte Erweitert die entsprechenden Profile aus.

General Programs and Services Users and Computers Protocols and Ports Scope Advanced Profiles O All profiles			
Users and Computers Protocols and Ports Scope Advanced			
Profiles			
Profiles			
N All profiles			
These profiles:			
☑ Domain			
Specify the interface types to which this			
rule applies.			
Edge traversal			
Edge traversal allows traffic coming to and from the Internet			
(NAT) routers.			
Allow edge traversal			
Long serve shout these actions			
Learn more about these settings			
OK Cancel Apply			

Speichern Sie die Firewall-Regel, aktivieren Sie sie, und starten Sie den Sourcefire User Agent-Dienst neu. Der Status Ihrer Echtzeitverbindung sollte jetzt von **Unbekannt** auf **Verfügbar** geändert werden.