Windows Defender - Performance and Functional Problems on Telephony Server

Sometimes Windows Defender will run with extremely high CPU usage, and lock files required by the telephony server.

In particular, when it locks call recording files, the effect can be that voice / recording resources eventually run out.

Notes

Scanning Programs

The telephony server is a real-time communications system.

Running incorrectly configured scanning programs for malware or viruses or other "deep scan" programs on the telephony server can seriously impact the real-time behaviour and / or functionality of the system.

jtel provides absolutely no support whatsover for problems related to this.

jtel also does not recommend any particular scanner or program used for this purpose.

Symptoms

High CPU Usage

This effect can be seen in the task manager. Look for the process:



and check if it is constantly using a lot of CPU.

Loss of Resources

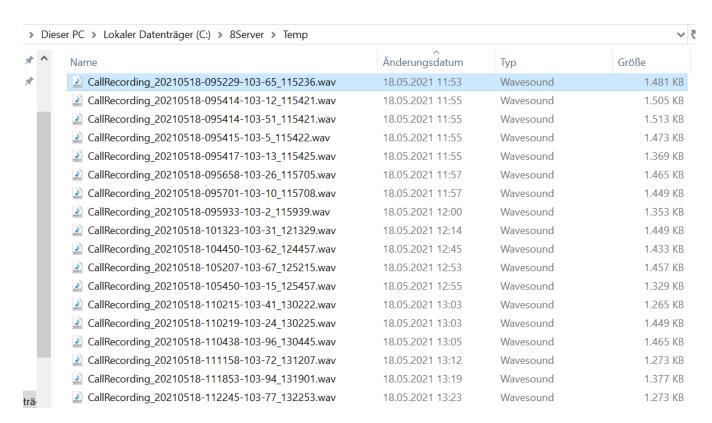
Check the resources in the telephony server using the command giResView.exe in a cmd shell when the server is idle.

This sample output is for a 284 line system with 142 lines and 142 P2 resources:

C:\Users\Administrator>giresview							
type	provider	name	max	in use	free		
RES_TRUNK	100000:SIP	port:0 in	284	142	142		
RES_TRUNK	100000:SIP	port:0 dx	284	0	142		
RES_TRUNK	100000:SIP	port:0 out	284	0	284		
RES_VOICE	100000:m0	Voice	-1	0	-1		
RES_CONFERENCE	100000:m0	Conference	-1	0	-1		
RES_CONFERENCE_PARTY	100000:m0	Conf-Party	-1	0	-1		
RES_CONFERENCE_MONITOR	100000:m0	Conf-Monitor	-1	0	-1		
RES_FAX	100000:m0	Fax/tx	-1	0	-1		
RES_FAX	100000:m0	Fax/rx	-1	0	-1		
RES_TELBUS		H100/H110	4.096	0	4.096		
RES_MIXER_MONITOR	100000:m0	Audio Monitor	-1	0	-1		
RES_VMP	100000:m0	VMP/G729ab	568	0	568		
RES_VMP	100000:m0	VMP/iLBC	568	0	568		
RES_VMP	100000:m0	VMP/G711	568	0	568		
RES_STREAM		STREAM	-1	0	-1		

If the system is idle, only inbound trunks should be "in use". This number should exactly equal the number of configured inbound lines. All other counters should be 0.

If you notice RES_MIXER_MONITOR instances, then you will probably also find call recording files in **c:\8Server\Temp**



If you cannot delete these, and there are no calls on the system, then the anti-malware program is blocking writes to these files.

You can verify this by stopping the anti-malware service, and re-running the checks above. If the counters return to 0, then you have found the culprit.

Fix

To fix this problem, add exceptions to the anti-malware service for the following:

What	Where
Directory	c:\8Server
Directory	c:\aculab
Process	robot5.exe
Process	giHal.exe
Process	giAcu.exe

Process	sipserv.exe
Process	ProsodySServ.exe

For windows defender, you can do this with the following commands:

```
powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath "C:\8Server"

powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath "C:\aculab"

powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionProcess robot5.exe"

powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionProcess giHal.exe"

powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionProcess giAcu.exe"

powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionProcess giAcu.exe"

powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionProcess sipserv.exe"

powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionProcess ProsodySServ.exe"
```