

Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.networking/2005-04/msg00354.html>

- *From:* "mrklaxon" <mrklaxon@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 13 Apr 2005 06:49:05 -0700
-

Sorry I haven't been able to monitor this thread. I understand not running an AV product on certain server types but it is certainly recommended and supported. At the very least it should be installed and disabled except for manual scans. – More below:

"Bill-MT" wrote:

> "Phillip Windell" wrote:

>

>>> I've done a simple procedure that appears to have eliminated the issue.

>>> Please bare with me for 24hours and I'll get back to you on what has

>>> happened between now and then with this issue.

>>

>> Sounds good. We'll see what happens.

>>

>

> Last night I 'dis-connected' the specific DC from the network for 5 mins. I

> didn't reboot (i.e. didn't clear memory of any executing programs). For the

> next 15 hours the server's behavior was normal (usual per previous

> experience).

>

> When I checked on the 16th hour LSASS.EXE was again running at 98% for 10

> sec, then there was an interval of 60 secs when cpu was normal (pretty much

> idle on this DC), then the cycle repeats, just like the event looked before.

>

> Tonight after hours I intend to reboot this DC to see if it forces this

> 'event' to move to another DC just like the previous reboot did last weekend

> when I caused the event to move to this DC...

>

> I still don't see any evidence of worm activity in the sniffer capture logs

> (in either direction). I also don't see a lot of difference in the sniffer

> logs between when the event was not occurring and when it is occurring (that is

> there is no spike in either network traffic or communication patterns (hosts

> contacted) when CPU spikes as I would expect with a network worm).

>

> As a standard practice I don't load any 3rd party software on my DCs. But

> I'm considering putting up a temporary DC (think of it as a honey-pot) with

Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent

> an AV as you suggest. If I do can you answer the following.

>

> 1) If I then log a pay call to MS on this after I install an AV on the DC,

> will microsoft still support it.

Yes, they have for me.

>

> 2) We have a site license for McAfee AV (currently at version 8.0i) is that

> a supported AV on a DC.

Yes, we are using it. There have been some problems though. We had one server that crashed until we applied a hotfix. That example follows your reasoning of why you shouldn't install it. 8.0i also has port blocking that can affect some apps like Exchange. Read up on it.

>

> 3) Are there any known requirements (features to turn on/off) to installing

> an AV on a DC to be considered still running a 'supported' installation.

Yes, again read the DOCs also check the online KB, the DOCs leave a lot out.

You should exclude the SYSVOL, NTDS and more depending on the system's use.

>

> I intend on moving my W2K AD domain to W2K3 this summer and if installing an

> AV on DCs is a recommended option, I'd like to know that before I start

> building new servers. I prefer new builds to upgrades.

>

> Finally, even though you don't want to entertain this option. What TCP/UDP

> port does in-bound LSASS.EXE communicate (listen) on – I'd like to filter my

> sniffer captures by this port to see who is kicking off that process by

> remotely sending packets to this server.

>

>

>

.

• **Follow-Ups:**

◆ **Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent**

◇ From: Bill-MT

• **References:**

◆ **100% cpu usage for LSASS.EXE on DC intermittently, consistent inte**

◇ From: Bill-MT

◆ **Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent**

◇ From: Bill-MT

◆ **Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent**

◇ From: mrklaxon

◆ **Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent**

◇ From: Bill-MT

◆ **Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent**

◇ From: Bill-MT

◆ **Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent**

◇ From: Bill-MT

◆ **Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent**

Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent

◇ *From:* Bill-MT

- Prev by Date: ***Redirector errors***
- Next by Date: ***Server Cannot See Clients***
- Previous by thread: ***Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent***
- Next by thread: ***Re: 100% cpu usage for LSASS.EXE on DC intermittently, consistent***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***