

Re: Frustrated with Trend CSM!

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-08/3089.html>

From: Merv Porter [SBS-MVP] (mwport_at_no_spam_hotmail.com)

Date: 08/09/04

Date: Mon, 9 Aug 2004 15:11:10 -0500

And let's give Chester you instructions for installing and configuring Trend CSM...

How to install Trend C/S/M for SMB

<http://msmvps.com/kwsupport/archive/2004/03/23/4153.aspx>

Configuring Exchange & Trend for spam/filtering

<http://msmvps.com/kwsupport/archive/2004/06/19/8543.aspx>

--

Merv Porter [SBS MVP]

=====

"Les Connor [SBS MVP]" <les.connor@DEL.cfive.ca> wrote in message
news:eoV5gvifEHA.236@tk2msftngpl3.phx.gbl...

> Chester,

>

> I suspect the Officescan (file space A/V) component may be scanning the
> Exchange folder(s) and/or database. You must exclude them from Officescan,
> on the server.

>

> <snip>

> 1. In the CSM console, click on the Clients view so you can see the
> Officescan 'domain'. Your SBS will be listed there.

> 2. Create a new Officescan 'domain', and move your SBS computer to the new
> domain. The original domain will be used for workstations.

> 3. Click on your SBS computer icon, and set the client privileges to your
> liking.

> 4. Click on Scan options | Real time Scan settings, and find the
Exclusions

> link.

> 5. Put <drive> pagefile.sys in the lower 'file' exclusion list.

> 6. Put <these are default locations> c:\Program files\exchsrvr, \trend,
> \trend micro in the directory exclusion area. Note that if you have moved
> your exchange data and or logs somewhere, be sure to exclude them. Note
also

> you can be more granular with your exclusions if you want - you don't have
> to exclude the entire directory. Another note - there is a tick box for
> excluding Trend product directories, but I do it manually anyway. Yet
> another note - On all screens make sure you APPLY the settings by
scrolling
> down to the bottom and clicking the button.

>

> What you've done with the two Officescan 'domains', is enabled different
> settings for the server versus the clients. Now when you add client

Re: Frustrated with Trend CSM!

microsoft.public.windows.server.sbs: Re: Frustrated with Trend CSM!

```
> machines, you can set the options on that domain (rather than each
> workstation) so they apply to all workstations, but not the server.
Sometime
> <endsnip>
>
> --
> Les Connor [SBS MVP]
> -----
> SBS Rocks !
>
>
>
> "Chester" <chester@NOSPAMprosoundusa.com> wrote in message
> news:ueffgnifEHA.2908@TK2MSFTNGP10.phx.gbl...
> > Thanks Phil, Lanwench, and Merv,
> >
> > I did check the log, and what bothers me is there are several messages
> > like
> > "Virus successfully detected, but infected file can neither be cleaned
nor
> > quarantined"
> > and the other one that bugs me is "See scan result in compressed file :
> > NTFS_5131bc4801c47be600000235.EML"
> >
> > The details show the virus name and things, but should I worry about
these?
> > The log shows the path as being to the ..\Queue, but of course, they are
> > gone from there now.
> >
> > Sorry if this all sounds elementary, I'm trying to get my head wrapped
> > around the security issues here.
> >
> > Thanks for the help!
> >
> > Chester
> > "Phil" <phil@phil.com> wrote in message
> > news:09IhSWifEHA.2812@tk2msftngp13.phx.gbl...
> > > Chester,
> > >
> > > See reply inline
> > >
> > > Thanks,
> > > Phil
> > >
> > > "Chester" <chester@NOSPAMprosoundusa.com> wrote in message
> > > news:%23697P0$eEHA.3988@tk2msftngp13.phx.gbl...
> > > > I have torn out my hair trying to understand how this program works.
I
> > > guess
> > > > I've just missed the boat on this one.
> > > >
> > > > 1. Installed the program several months ago, and got it set to check
> > > > for
> > > > updates hourly
> > > > 2. Installed the clients at the same time, and everything came up
> > > > clean.
> > > >
> > > > Now, when I look at the console on the server, it keeps telling me
> > > > that
> > > > the
> > > > server has 50 infected files, and that one of the clients has 1
> > > > infected
```

microsoft.public.windows.server.sbs: Re: Frustrated with Trend CSM!

> > > file. So I use the "Damage Cleanup Service" on the server and on the
> > > client,
> > > and NOTHING CHANGES!!! They DCS reports "no malware found" and when
I
> do
> > a
> > > manual scan, it reports "No viruses found!" What is UP!?!?! Why
can't
> I
> > > grasp this!?!
> > >
> > > DCS only cleans up a computer that is actually infected. You need to
> > check
> > > the virus log for the clients/server that is infected and see what
> action
> > > has been taken. If they have been quarantined or deleted, then you
have
> > > nothing to worry about. The status (the PC on fire icon) is
associated
> > with
> > > the number of viruses that the computer has encountered and does not
> > > necessarily mean that the computer is currently infected. (That's why
> you
> > > need to check the virus logs) If you'd like to be able to track the
> number
> > > of viruses and the source, etc. on the summary page, you need to leave
> > > everything as is. However if seeing the PC on fire icons are really
> > > bothering you, you must view the status of the client and click "Reset
> > Virus
> > > Count", or if there is more than one select the domain and click
"Reset
> > > Virus Count".
> > >
> > > >
> > > > Any help from someone with Trend CSM would be VERY much appreciated.
> > > >
> > > > The reason I'm sure we have a virus is because we keep getting virus
> > > > notifications in our email from the server saying it has removed an
> > > > attachment. The strange thing is, those emails (which are being
routed
> > to
> > > the users Junk Mail folder) are now showing as coming from people we
> > know
> > > and communicate with, but those people are not sending us email!
> > > >
> > >
> > > Someone is spoofing their addresses. I had someone internally here
get
> > > spoofed and the email got sent to another user here which caused a
> little
> > > confusion for them. As long as the viruses are getting cleaned or
> removed
> > I
> > > would not worry about it.
> > >
> > > > Thanks for your help!
> > > > 3.
> > > >
> > > >
> > > >
> > > >
> > > >
> > > >

microsoft.public.windows.server.sbs: Re: Frustrated with Trend CSM!

> >
>
>