

<<<< SBS News of the week ended March 28th, 2004>>>>

Source:

<http://www.tech-archive.net/Archive/BackOffice/microsoft.public.backoffice.smallbiz/2004-03/0428.html>

From: Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP] (*sbradcpa_at_pacbell.net*)

Date: 03/29/04

Date: Sun, 28 Mar 2004 23:56:57 -0800

-----NEWS THIS WEEK ESPECIALLY FOR SBSERS-----

Services may stop abruptly when you shut down or restart a Windows Small Business Server 2003-based computer

<http://support.microsoft.com/?id=839262>

This reg key should be checked and corrected – no exceptions!

Here is a link to a VBS script provided by Jeff that automatically makes the appropriate registry change. I've tested it on my home server. Note: be sure you click on the link, and then save it to a network drive so you can access it and run it from the server. (That is, don't be like me and try to run it on your workstation ---- it will try to update your workstation's registry!).

http://www.csbsupport.com/KB839262_Fix_R1.vbs

The files are also located in the download files section of www.smallbizserver.net

A whole bunch of KB articles courtesy of Marie McFadden SBS Community Lead

<http://msmvps.com/bradley/posts/4282.aspx>

Stealing a post from Les Connor

Here's the procedure for Trend CSM for SMB.

1. Decide whether you want to use the Administrator account for CSM, or another account. If you don't want to use the Administrator account, create an account. (I use the Administrator account.)
2. Run setup – install on IIS is generally the only selection available.

3. Enter the FQDN server.domain.local OR the IP of the SBS. I prefer the IP, it seems to work better.
4. Install into IIS Virtual Web Site (NOT the default web site).
5. Use port 8085 for communication.
6. Deselect SSL.
7. Use Administrator account – If ISA enter proxy info, if no ISA enter nothing in proxy.
8. If you don't have the activation code – register now, the email with the code comes real quick. (note that you can go this far prior to the actual install if you like, and get the activation code so you don't have to do this while installing).
9. Accept the server/client port.
10. Accept the client installation for the SBS (installs the Officescan client on the server)
11. The install proceeds, then open the admin console.

– This completes Officescan installation, now on to Scanmail.

12. Go to the Scanmail link on the left, and install Scanmail to the IP of your SBS. Scanmail and eManager are installed.

– This completes the installation of CSM SMB. Now you need to make some settings.

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 machines, you can set the options on that domain (rather than each workstation) so they apply to all workstations, but not the server.

Sometime this is useful.

7. Click on Updates, Server updates, Automatic Update, check the options and set the frequency to hourly.

8. Click on Manual Update, select the options you want, and update now to get the latest files and make sure connectivity is there.

9. Log off Officescan console.

Scanmail

1. Use the non HTML console from start | all programs.
2. Log on, click on Scheduled Update.
3. Enable scheduled update, and set it to hourly, select pattern file and engine.
4. If you use ISA, click on the Proxy Settings button and enter the proxy info.
5. Click on Update Now, select the options, set proxy info if you use ISA, and click on Update now.

Those are the basics to get protection. You can learn the fine tuning and option stuff (including eManager) as you go.

--

Les Connor [SBS MVP]

Are you getting an error referring to #50070: Unable to connect to the database STS_Config?

<http://msmvps.com/bradley/posts/4292.aspx>

Looking for training on SBS2k3?

<http://msmvps.com/bradley/category/90.aspx>

In other news....

- - - - -
Bagle-U plays MS Hearts

A new variant in the Bagle worm series - Bagle-U is spreading quickly across the Internet this morning. As with its 20 previous siblings, Bagle-U spreads by email. This time, infected emails have an empty subject, no body text and a randomly-named attachment containing malicious code. If this attachment is run, the worm opens Microsoft Hearts card game (MSHEARTS.EXE file) before going through what have become standard virus routines, common to all the worms in the Bagle series.

<http://www.securityfocus.com/news/8340>

<http://www.eweek.com/article2/0,4149,1554954,00.asp>

<http://computerworld.com/securitytopics/security/virus/story/0,10801,91678,00.html>

- - - - -
Much Ado About Phatbot

Most computer security experts agree that the Phatbot Trojan horse program that burst onto the Internet earlier this month is a nasty bug, capable of giving hackers control over legions

of computers. What's not so clear is how much of a threat it poses.

<http://www.washingtonpost.com/wp-dyn/articles/A26463-2004Mar26.html>

Phatbot's Family Ties

<http://www.washingtonpost.com/wp-dyn/articles/A26442-2004Mar26.html>

Security product flaws attract attackers

The software vulnerability exploited by this week's Witty worm is only the latest in a growing list of flaws being discovered in the very products users invest in to safeguard their systems.

<http://computerworld.com/securitytopics/security/holes/story/0,10801,91688,00.html>

Witty worm frays patch-based security

http://news.com.com/2100-7355_3-5180482.html

Online virus war is slowing down

<http://news.bbc.co.uk/1/hi/technology/3571359.stm>

Virus Era Hits 5-Year Milestone

<http://www.wired.com/news/infostructure/0,1377,62809,00.html>

Making hotspots secure

Wireless access may improve productivity and customer service, but Wolfgang Held, 3Com systems architect, warns that wireless local area networks (WLANs) and public hotspot wireless connections are still risky from a security point of view.

<http://www.itweb.co.za/sections/computing/2004/0403261106.asp>

Man charged over keystroke logging

Larry Lee Ropp, a 46-year-old former insurance claims manager, is the first defendant charged in the US with a federal crime for using a 'keystroke logger' A California man who prosecutors say planted an electronic bugging device on a computer at an insurance company was indicted on Tuesday on federal wiretapping charges in what prosecutors said was the first case of its kind.

<http://news.zdnet.co.uk/internet/security/0,39020375,39149886,00.htm>

Security needs better education for programmers

Dealing with Internet computer worms and viruses requires a long-term education effort aimed at programmers while they are still in college, a Homeland Security Department executive said today.

<http://www.fcw.com/fcw/articles/2004/0322/web-secure-03-25-04.asp>

<http://www.securitypipeline.com/18402599>

The names, addresses, dates of birth, Social Security number and credit scores of some 200,000 GMAC customers are at risk because laptops containing the data were stolen.

--
<http://www.sbslinks.com/really.htm>