

Re: DHCP Logging (can't find a solution!)

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2008-02/msg00121.html>

- *From:* "Gaspar" <noreply@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 11 Feb 2008 08:50:27 -0200
-

ISA doesn't have "Client Host name" in Web logs (as it does in Firewall logs)

So, I don't know how to log this, how to do this correctly.

Thanks

"Phillip Windell" <philwindell@xxxxxxxxxxxx> wrote in message <news:%23hP0q2naIHA.5164@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

"Gaspar" <noreply@xxxxxxxxxxxxxxxxxxxx> wrote in message <news:e7dZ1KkaIHA.3696@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

I know this question has been asked before but I can't find a solution for my problem: I need to find which host had a certain IP assigned to it in a specific date.

Windows 2003's DHCP server maintains only logs for a week (no longer than that).

The normal DHCP behavior is that Clients will always ask for the same config they had the last time. So barring unforeseen circumstances it will still be using the same IP config today.

This will be use to analyze ISA logs (which only logs client ip address, not host names). For example, given the following data:

ISA will log the host name if done correctly.

ISA Logging

http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/tb_logging.mspx

<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/logging-best-practices.mspx>

<http://www.microsoft.com/technet/isa/2004/plan/faq-monitoring.mspx>

ISA Server 2004 FAQ: Monitoring and Logging

<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/faq-monitoring.mspx>

Re: DHCP Logging (can't find a solution!)

"2008-01-01,192.168.0.22,www.someadultsite.com"

Which hostname/computer was assigned to "192.168.0.22" in "01/01/2008"?

The ISA log will include the Username, which is more important than the host name.

Don't use SecureNAT Clients (which can't authenticate) and you will always get the Username

Don't use generic "shared" user account and you will always know who the person was.

Without considering all the above, your findings will never be solid enough to legally enact discipline upon the user(s) if the user chooses to sue the company over your disciplinary actions.

—
Phillip Windell
www.wandtv.com

The views expressed, are my own and not those of my employer, or Microsoft,
or anyone else associated with me, including my cats.
