Identifying and resolving Websense Web Security v7.6 logging issues when reports are blank

Webinar Question/Answer
Webinar Date: January 18, 2012

1. **How do you get to the Log Server Configuration?**

   A. Log Server Configuration is under Start > Programs > Websense > Log Server Configuration. It can also be accessed as an executable (logserver.exe) from the Websense bin directory.

2. **Why is the SQL ‘sa’ account being used? As a security focused company, I would expect Websense to discourage the use of sa. We do not use sa here, rather we use a dedicated websense SQL account. I am just curious.**

   A. You care correct, disabling the SQL sa account and then creating another account is more secure. The 'sa' account is for demonstration purpose. It lets folks unfamiliar with SQL know that we are using a local SQL account. For even greater security, you should consider using a directory service account and routinely change the password. Additionally, the 2008 SQL version is substantially more secure than earlier versions. We have several Knowledge Base articles detailing the required read/write permissions for our Websense database. Here are a few articles that I like:

   - Which permission sets does Websense require?
   - How do I create a limited SQL account for Websense?
   - How do I use a Windows trusted account for Websense Reporting?

3. **Can I query the SQL database for hits within a particular date "and time"**

   A. Yes, you can query SQL for a specific date. This query is actually already available in the SQL query article that I referenced in the presentation. Please examine the following article for your answer.

   - Can I query the SQL database for hits on a particular day?

4. **We are getting this message when I go to create an investigative report. What can the DBA do to prevent this from happening again?**

'[Microsoft][ODBC SQL Server Driver][SQL Server]The transaction log for database 'wslogdb70' is full. To find out why space in the log cannot be reused, see the log_reuse_wait_desc column in sys.databases (SQL-42000)

   A. From the error, it looks like the catalog database (wslogdb70) log file (.ldf) is full. The catalog database may be set to full recovery mode. Switch to simple recovery mode and then shrink the database. See this article for details: Reducing the size of the Log Database

5. **Where do I find the script to create the new database?**

A. You can search our support site with 'createdbu' term. Several articles will display. I like the following article:

- v7: Can I manually create a new catalog database?

6. **How does hybrid filtering integrate into this?**

A. Hybrid filtering downloads logging data at 15-minute intervals. A warning will appear in TRITON - Web Security if a hybrid logging download has not occurred for 24 hours. As the file only appears once every 15 minutes, you best bet is to run a Source Server report in Investigative Reports. This will allow you to see the latest log data for a hybrid filtered user.

7. **Which is the best log insertion method?**

A. Technically, the BCP insertion method is best. It sends logging data to SQL Server in batches rather than individually like the ODBC insertion method. BCP requires installing SQL Server Client Tools on the same server as the Log Server service. This decision comes into play, if you are seeing files backing up in the **bin\Cache** directory during the busy time of the day and then clearing out after business hours. This is an example of Log Server not being able to keep up with the incoming Web activity traffic. Your alternatives are either increasing resources to Log Server, such as CPU or RAM, or enabling the BCP feature. The bottom line is if you are a smaller company, then the ODBC is most likely working sufficiently for you. If you are a medium size company, then the amount of Web activity data generated by your users typically necessitates enabling the BCP feature.

8. **Can I force logs to push to logserver from the Hybrid Cloud?**

There is no way to force logs to the log server, logs are automatically sent every 15 minutes.

9. **Can cache file directories be placed somewhere else?**

Yes, the cache file directories can be moved to alternate locations. If you need to move the cache file directories including the BCP file directory, then you need to change the path in the Log Server configuration utility and simply restart the Log Server service.

10. **Can a non-standard port be used for the ODBC connection?**

Yes, a non-standard port can be used for an ODBC connection. You will need to perform additional steps when configuring the ODBC configuration. A Knowledge Base article is available if you search for the term, “non-standard port”.

11. **What are some of the errors are seen in the error log activity in Websense Manager?**

You would see errors such as “no active partitions”, if a partition may be have become suspect. It may also say that a partition is offline.

12. **Can you use multiple logservers for one Policy Server?**

    No, it is one logserver per Policy Server

13. **Is there a way to run testlogserver without stopping logserver?**

    Yes, there is a way and requires a little bit of configuration. We have a KB with the exact steps.

14. **Why is BCP grayed out on my new installation?**

    Remember, that you have to install SQL tools in order to enable BCP.

15. **Would it be safe to say that if you enable Full URL logging or disable visits, you get more logging information?**

    Yes, you will have more logging information resulting in a larger database growth.

16. **Is there any limit to the number of partitions you can have?**

    The number of partitions depends on the resources your SQL server can have. The number of active partitions for logging is around 61 to 69 depending on whether you are integrated with Content Gateway. So, you can have 100 partitions but only actively log and report on 61 to 69 of them.

17. **Can WISP trace be ran continuously?**

    There is a limited a buffer for WISP trace. As a result, if left running it will timeout.

18. **Can the partition path be changed?**

    Yes in the TRITON Web Security > Settings under Reporting > Log Database you can specify a different path.

19. **Can you report off older databases using Presentation Reports?**

    No, remember presentation reports will run reports for the ODBC connection that logserver is connected to. Investigative reports will can run reports of older databases.

20. **Can I move my databases to a new server or directory?**

    Yes, you must disable SQL jobs and rop all connections before detaching databases. We have a searchable KB that has the detailed steps.