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

Webinar January 2012
Webinar Presenter

Title: Support Specialist

Accomplishments:
– 9 years supporting Websense products

Qualifications:
– Technical Support Mentor
– Product Trainer

Greg Didier
Goals And Objectives

- Logging components
  - Chain of communication
  - Data flow process

- Reporting (SQL Server) database
  - Connection
  - Account permissions

- Diagnostics

- Troubleshooting

- After this webinar
  - Increased confidence in troubleshooting Websense reporting tools.
Major Components

Microsoft SQL Server
- Hosts the reporting database (Websense Log Database).

Log Server
- Accepts Web activity data and forwards to SQL Server.

Reporting
  - Investigative Reports
  - Presentation Reports
  - Status > Today and History pages
Stepping through the flow process from the beginning.

- First, we need SQL Server available in our network...
Logging and Database Files

Physical files

- Websense Log Database files.
  - One catalog database: **wslogdb70**
  - One or more partition databases: **wslogdb70_x**
- Log Server “\bin\Cache” files
- Log Server “\bin\Cache\BCP” files
Logging and Database Files

File paths:

- TRITON - Web Security management interface
- Microsoft SQL Server Management Studio
- Web Security Log Server Configuration utility
Logging and Database Files

File paths:

- TRITON - Web Security management interface
- Microsoft SQL Server Management Studio
- Web Security Log Server Configuration utility
Recap

Structured environment:

1. **Integration** sends filtering requests to Filtering Service.
2. **Filtering Service** sends Web activity data to Log Server.
   - Log Server is identified in TRITON - Web Security.
3. **Log Server** processes data and forwards it to SQL Server.
   - Cache files (ODBC or BCP)
   - ODBC connection
4. **SQL Server** places data in the catalog database (wslogdb70).
   - **SQL Server Agent** moves data to a partition.
     - Websense_ETL_Job_wslogdb70
   - **Service Broker** (SQL Server 2008 R2 Express) moves data to a partition.
6. **Reports** display user Web activity.
The first symptom may be that reports contain no Web activity data.

**TIP:** Schedule a daily report.

– A blank report indicates that a problem exists.

Where to start troubleshooting?

Start by diagnosing the issue.

– Identify the *point-of-failure*.
  * Components communicate in a logical chain of events.
  * A verification can be performed at each step.

When the *point-of-failure* is identified.

– Start troubleshooting.
We only need to examine the handful of services that interact with Websense Log Server.
Log Server
- Receives Web activity data from Filtering Service and forwards it to SQL Server.

Begin diagnostics with Log Server

Diagnostics
- New .tmp files appearing in either Cache or BCP directories? (no)
- Log Server running? (yes)

Demonstration
Diagnostic Demonstration

- Filtering Service
  - Receives filtering requests from integration and forwards Web activity data to Log Server.

- Diagnostics
  - Filtering Service running? (yes)
  - Log Server location identified? (yes)
  - Log Server port 55805 open? (yes)
  - URL Categories enabled? (yes)
  - Integration sending filtering requests? (no)

- Demonstration
Diagnostic Demonstration

- **Integration**
  - Sends filtering requests to Filtering Service

- **Diagnostics**
  - Integration sending filtering request? (yes)
    - Check WISP integration statistics.
    - Re-configure the integration.
  - Validation, users receiving block page? (yes)

- **Demonstration**
Diagnostic Demonstration

- **Log Server**
  - Receives Web activity data from Filtering Service and forwards it to SQL Server.

- **Diagnostics**
  - Log Server running? (yes)
  - Filtering Service sending data? (yes)
  - New `.tmp` files backing up in either Cache or BCP directories? (no)
  - Connect to SQL Server port 1433? (yes)
  - Reset ODBC and Log Server connections credentials? (yes)

- **Demonstration**
Diagnostic Demonstration

SQL Server
- Accepts logging data and then moves it to a partition.

Diagnostics
- SQL Server running? (yes)
- SQL Agent running? (yes)
- Websense SQL Jobs exist? (yes)
- ETL_Job runs without error? (yes)
- Data moving in and out of the INCOMINGBUFFER table? (yes)
- Daily top 10 hits changing? (yes)
- Examine databases? (yes)

Demonstration
Diagnostic Demonstration

- **TRITON - Web Security**
  - Offers database options and settings.

- **Diagnostics**
  - Error Log Activity? (no)
  - Databases available and enabled? (yes)
  - Create new database partition? (yes)

- **Demonstration**
Diagnostic Demonstration

- **Reporting**
  - Displays Web activity.

- **Diagnostics**
  - Investigative Reports displaying correct database? (yes)
  - Presentation Reports displaying Web activity? (yes)
  - Today page displaying Web activity? (yes)
  - History page displaying Web activity? (yes)
  - Validation? (yes)

- **Demonstration**
Diagnostics Recap

Multiple components:

1. Integration
2. Filtering Service
3. Log Server
4. SQL Server
5. TRITON - Web Security settings
6. Reporting

Start diagnostics with Log Server.

Troubleshooting starts when you identify the point of failure.
First, ensure Web filtering is working.

Log Server running?
- If not starting, then run Log Server debug.
  - Log Server is not running
  - Stopping and starting Websense services
  - Web Log Server does not start
No log files entering the `\bin\cache` folder

- Run TestLogServer to check for incoming logs.
  - Using TestLogServer with Websense Web Filter
  - How do I run TestLogServer without stopping the Log Server service?
- If no traffic appears, verify that Filtering Service is running and seeing traffic. Run a WISP debug.
  - Websense isn't filtering integration traffic
  - Component statistics and diagnostics
- If no traffic appears, check TRITON - Web Security logging settings.
  - No Log Server is installed for a Policy Server
  - Can I keep internal traffic from being logged in reports?
Log files amassing in the `\bin\cache` folder.

- Is SQL Server service is running?
  - Log Database is not available
- Reset the ODBC connection.
  - How to update the ODBC and the Log Server connections
- Is SQL Server Agent service running?
  - Diagnostic steps for when logging is not working
  - Error message: "Summary tables used by Investigative Reports are empty"
- Useful Database queries.
  - Can I query the SQL database for hits on a particular day?
Log files amassing in the `\bin\cache` folder (cont.).

– Run Log Server debug.
  • [Debugging Websense Log Server](#)

– Verify SQL has available free disk space.
  • [Log Server is not recording data in the Log Database](#)
  • [Reducing the size of the Log Database](#)

– Verify partition: online status and quantity.
  • [Diagnostic steps for when logging is not working](#)

– Verify Websense components are same version.
  • Right click executable, check the Version or Details tab.
Troubleshooting Resources

- Reports
  - Pointed to correct database?
    - Database connection and report defaults

- Check for errors
  - Application Event Log and websense.log file.

- Check for available hotfixes

- Quick remedies:
  - Run the CreateDbU process.
    - Can I manually create a new catalog database?
  - Remove and reinstall Log Server.
    - Web Security Log Server
    - Log Server installation

- Demonstration
Additional Resources

Knowledge Base articles:
- Why is data not being logged to the database?
- Reports have no data or no recent data and Log Server is not logging data (my favorite article)
- Log Server FAQs
- Log Server and Log Database issues
- Ensure Proper Data Logging in Websense Enterprise and Websense Web Security Suite
- Which permission sets does Websense require?

Documents:
- Deployment and Installation Center
- Detailed Websense component diagram
- Simplified Web filtering logging diagram
- Web Security default ports
**Support Online Resources**

🔍 **Knowledge Base**
- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.

🗣 **Support Forums**
- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.

🔥 **Tech Alerts**
- Subscribe to receive product-specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

💬 **ask.websense.com**
- Create and manage support service requests using our online portal.
Webinar Announcement

Title: Making best use of Websense Web Security delegated administration and reporting

Date: February 22\textsuperscript{nd}, 2012

Time: 8:30 AM PDT (GMT -8)

How to register: http://www.websense.com/content/SupportWebinars.aspx
Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit: http://www.websense.com/findaclass

- Websense Training Partners also offer classes online and onsite at your location.

- For more information, please send email to: readiness@websense.com