Installing, upgrading, and managing reporting databases for Websense Web Security v7.6

Webinar September 2011

web security | data security | email security

Webinar Presenter

Greg Didier

- Title: Support Specialist
- Accomplishments:
  - 10 years supporting Websense products
- Qualifications:
  - Technical Support Mentor
  - Product Trainer

Goals And Objectives

websense
ESSENTIAL INFORMATION PROTECTION™

- Reporting requirements
- Database upgrades
- Database management
- Troubleshooting: log records not in the SQL database?
  - Component communication
  - Logging data flow
- After this webinar
  - Understand the process of moving and storing logging data for ease of maintenance, increased performance, and increased confidence in troubleshooting reporting databases

Components

- Microsoft SQL Server
  - Hosts the reporting database
- Log Server
  - Accepts Web activity data and forwards to SQL Server
- Reporting
  - Available from TRITON - Web Security, which is a module of the TRITON Unified Security Center
  - The machine hosting the TRITON Unified Security Center is called the TRITON Management Server

Microsoft SQL Server

- Reporting data warehouse
- Before installing Websense components, SQL Server must be installed and running in your network.
  - Full version not included with your Websense subscription
- A free, limited-performance SQL Server version is available.
  - SQL Server 2008 R2 Express
    - Replaces MSDE
    - For small enterprises only
    - Only database platform supported on the TRITON Management Server
- As a best practice, run TRITON Unified Security Center and a full SQL Server on separate physical machines.

System Requirements

- Operating system
  - TRITON management, reporting, and logging components (Web Security only)
    - Windows Server 2003 R2 32-bit
    - Windows Server 2008 32-bit
    - Windows Server 2008 R2 64-bit
  - Log Server: Windows-only component (not support on Linux)
- Hardware
  - Depends if the Log Database is local or remote
    - See the Deployment and Installation Center.

System Requirements

- Log Database
  - On the TRITON Management Server
    - Only SQL Server 2008 R2 Express (32-bit version)
  - On a separate machine
    - SQL Server 2008 R2 Express
    - SQL Server 2005*
    - SQL Server 2008*
    - SQL Server 2008 R2**

* Except Web, Express, and Compact; all SPs; 32- and 64-bit; not IA64

**Except Web and Compact; all SPs, 32- and 64-bit; not IA64

Recap

- Microsoft SQL Server
- System requirements
  - Operating system
  - Hardware
- Log Database
  - Compatible SQL version

- Next…
  - Local and remote SQL installations
  - Database upgrade and creation

Local SQL Server Installation

- Install only SQL Server 2008 R2 Express locally.
  - Log in as a domain user to install SQL Express.
  - Use the Websense installer.
  - The Websense installer automatically installs:
    - .NET 3.5 SP1
    - PowerShell 1.0
    - Windows Installer 4.5
  - **mssqlserver** is the default database instance name.
  - **TRITONSQL2K8R2X** is the instance name if *mssqlserver* already exists.
  - Verify that the SQL Server Browser service is running and that TCP/IP is enabled in SQL Server Configuration Manager.
  - Use the SQL Server **sa** account

Remote SQL Server Installation

websense
ESSENTIAL INFORMATION PROTECTION™

- Full SQL Server
  - Verify that SQL Server (MSSQLSERVER) is running
  - Verify SQL Server Agent (SQLSERVERAGENT) is running
  - If using a Windows trusted account for SQL Server, must have:
    - *db_creator server* role, *SQLAgent* role, *db_datareader* in msdb
    - Use this logon ID when installing Websense components
  - Install SQL Server client tools before installing Log Server
    - Allows using Bulk Copy Program option
  - Restart the SQL Server machine after installation

Database Upgrade

- Reporting database is hosted on Microsoft SQL Server.
  - The database remains unaffected when uninstalling any or all Websense components.
  - An upgrade only occurs when installing Log Server.
- Starting in v7.6, database connection information is retained in the TRITON Unified Security Center
  - You are not prompted for the database connection during Log Server installation
  - To change the SQL connection, select Modify

Database Upgrade

- Preparing SQL Server
  - Back up Websense databases
  - Stop Websense Log Server
  - Disable Websense SQL Server Agent jobs
  - Perform the upgrade of Web Security or Web Filter
  - After upgrade, enable the disabled jobs
- Migrating from MSDE to SQL Server 2008 R2 Express
  - If you currently use MSDE, and want to use that data after upgrade, additional steps are required.
    - The databases must be moved to SQL Express before you install Websense Log Server.
    - See chapter 58 of the Deployment and Installation Center.

Database Creation

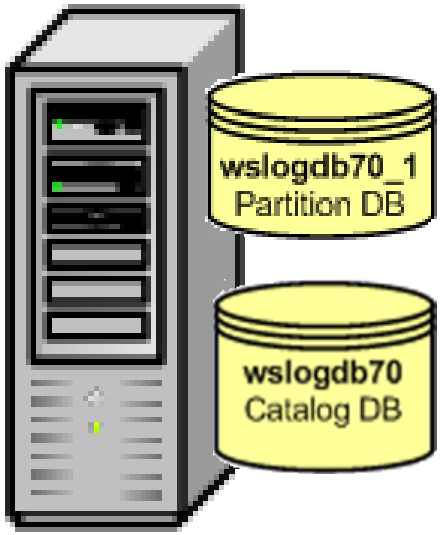
- Server Name
  - **Hostname** or **IP address** of the SQL Server machine
- Authentication method
  - **SQL Server Authentication** - connects using a SQL Server account
  - **Windows Authentication** - connects using a Windows trusted connection. This account must have certain roles assigned, see Configuring Microsoft SQL Server user roles. Use this account to run the Websense installer.
- Database location
  - The path refers to the machine on which the database engine is located. The directory for the Log Database files **must already exist**. The installer cannot create a new directory.

Recap

- Guidelines and tips...
  - Remote SQL installation
  - Local SQL installation
  - Database upgrade
  - Database creation
- Next...
  - Demonstrate where configuration settings relating to the Log Database are found

Database Management

- Reporting and settings:
  - TRITON - Web Security management interface
  - Web Security Log Server Configuration utility
  - Microsoft SQL Server Management Studio
  - Physical server where the database files are located



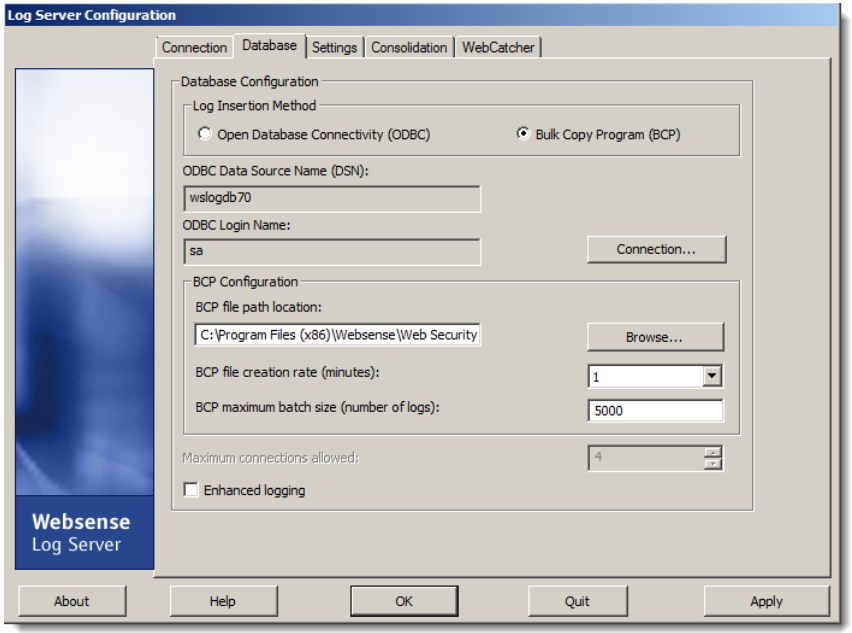
Database Management

websense
ESSENTIAL INFORMATION PROTECTION™

- TRITON - Web Security
  - Main tab
    - Reporting > Presentation Reports *and* Investigative Reports
      - Database connection
    - Policy Management > Policies > Default > Protocol Filter
      - Protocol > Advanced > Log protocol data
  - Settings tab
    - General > Logging
      - Reporting log records, selective category logging
    - General > Risk Class
    - Network Agent > Global > IP_address > NIC Configuration
      - Stand-Alone, Integrations, Protocol Management
    - Reporting > Log Database
      - Database Rollover, Maintenance, Full URL Logging, Internet Browse Time
- Demonstration

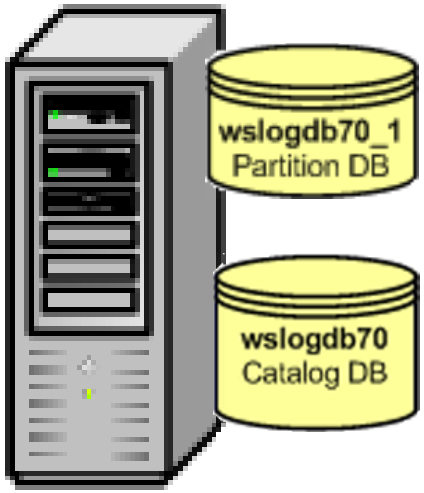
Database Management

- Log Server Configuration
  - Connection tab
  - Database tab
  - Settings tab
  - Consolidation tab
  - WebCatcher tab
- Demonstration
  - The service must be restarted for changes to take effect.
  - No Internet activity is logged when Log Server is stopped.



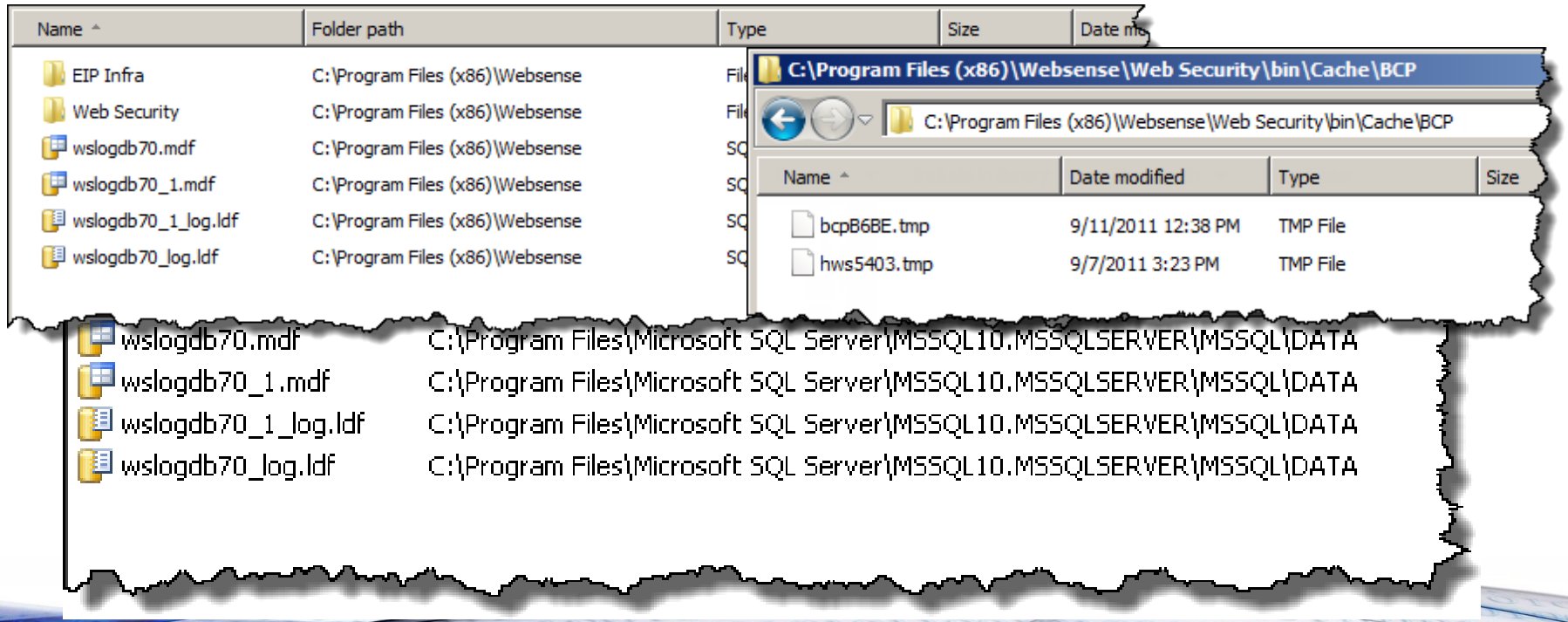
Database Management

- SQL Server Management Studio
  - Websense databases
    - Recovery model
    - Owner
    - File location
  - Websense SQL Server Agent jobs
    - Owner
    - Job history
    - Running state
- Demonstration



Database Management

- Physical files
  - Location of database files
    - Remote full SQL Server
    - Local SQL Server 2008 R2 Express
      - If upgraded from MSDE, database may be named **wslogdb76**
  - Log Server cached log files

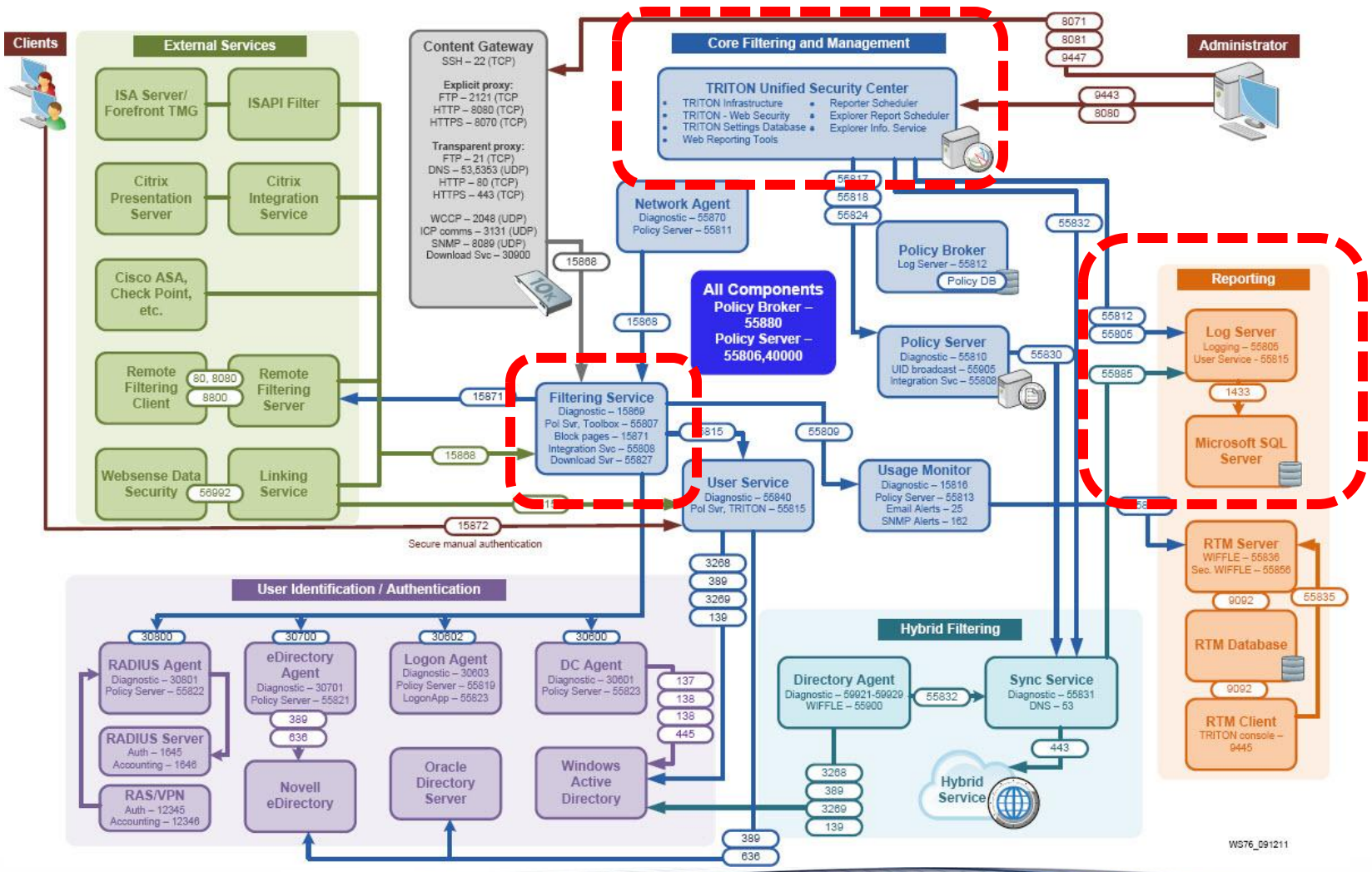


Recap

- Reporting and log databases settings
  - TRITON interface
  - Log Server Configuration utility
  - SQL Server interface
  - File locations
- Next...
  - Logging data flow

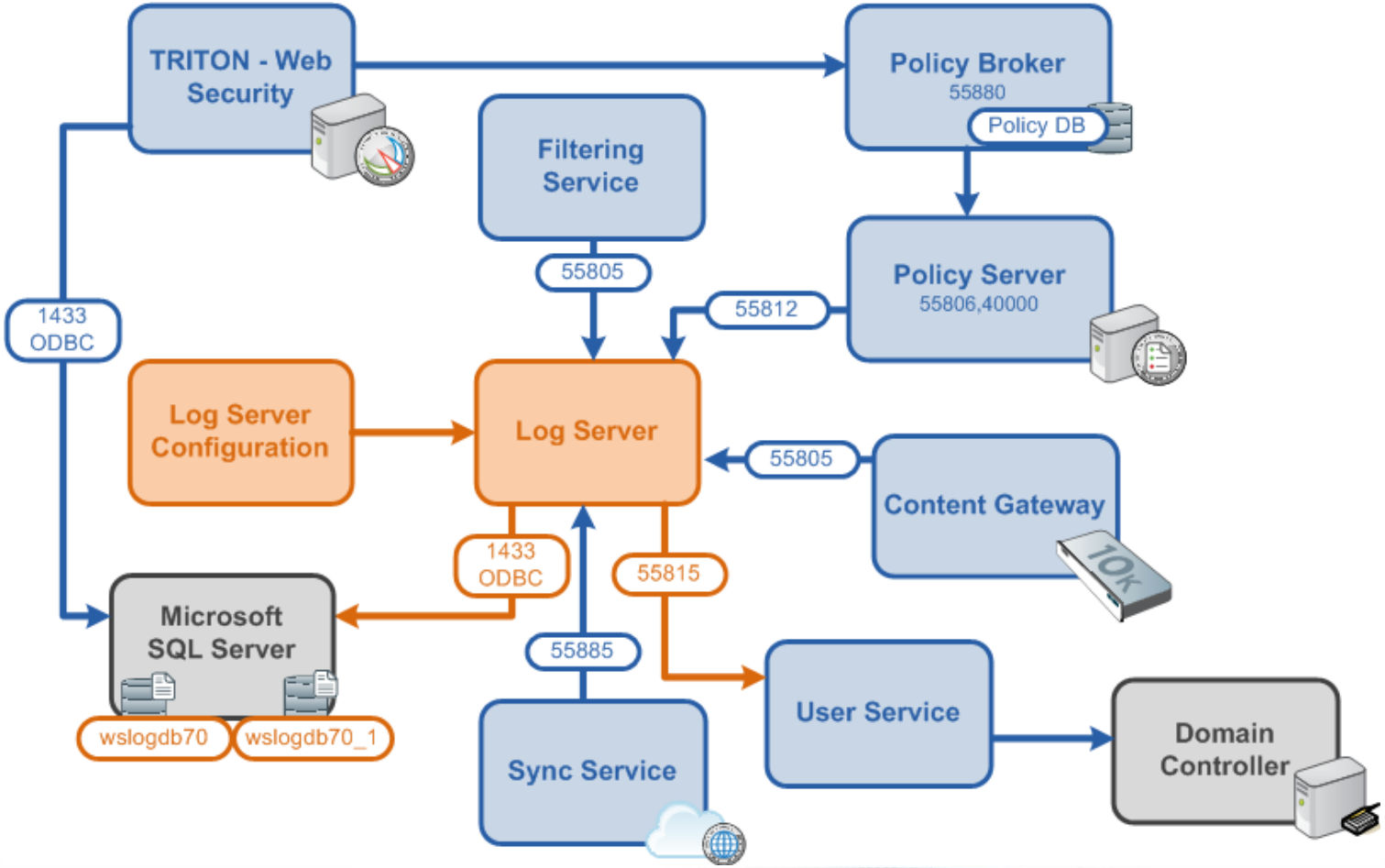
Websense Component Diagram

- Logging is only a small part of the component diagram



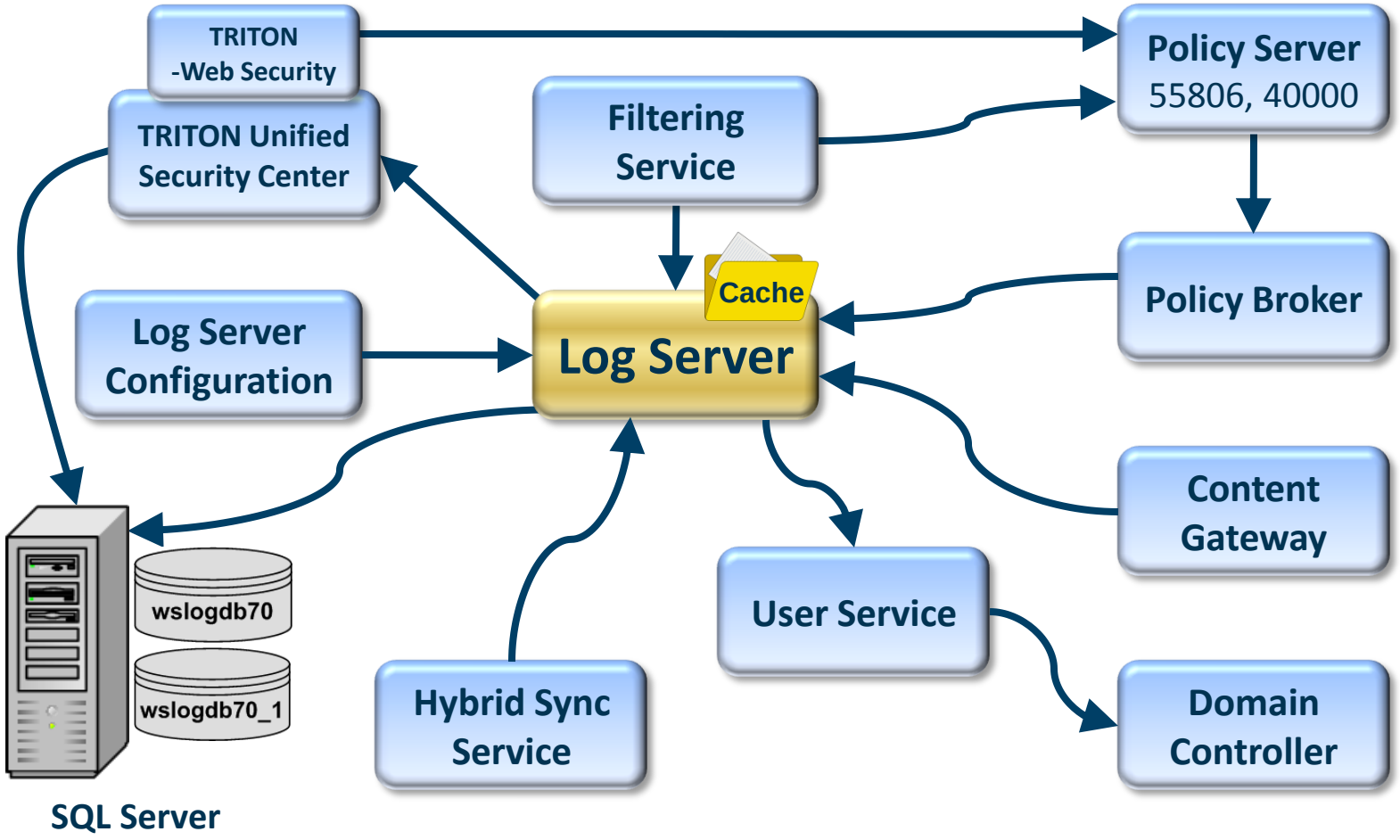
Simplified Logging Diagram

- We only need to examine the handful of services that interact with Websense Log Server.



Logging

- Stepping through the flow process from the beginning
  - First, we need SQL Server available in our network…



Recap

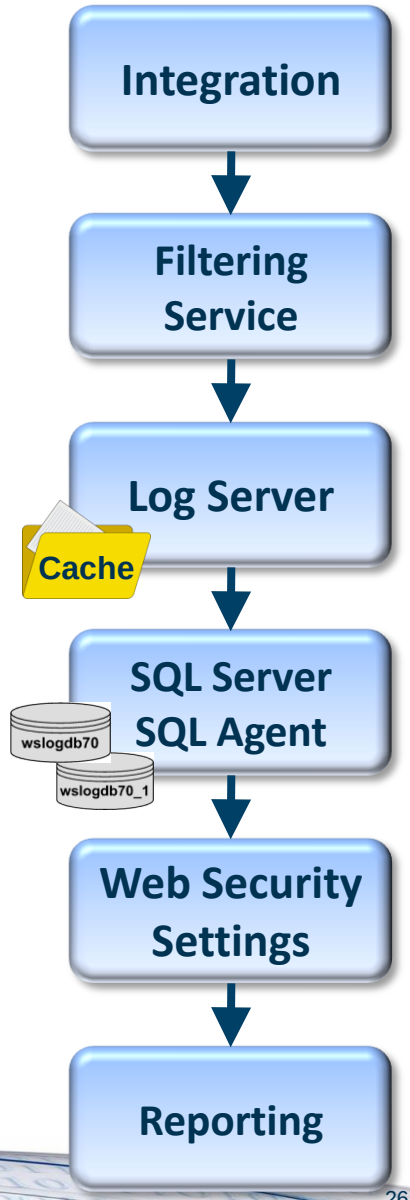
- We learned about:
  - SQL Server
  - Log Server
  - Configuration interfaces
  - Component diagram
- Next...
  - Troubleshooting

Troubleshooting

- Logging issues are discovered when reports contain no data
- Identify the point of failure using a systematic approach.
  - Understand Websense component communication
  - Understand the flow of logging data
- Know where to start troubleshooting.

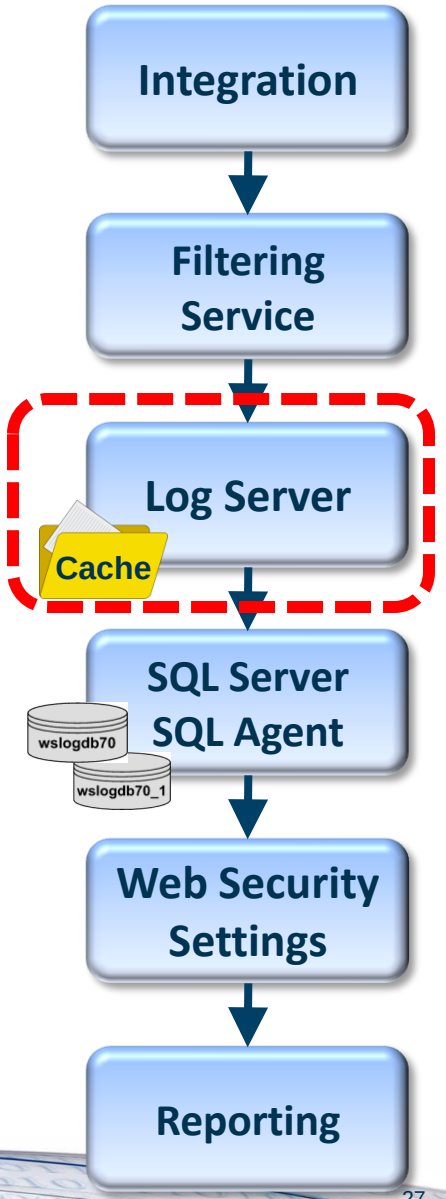
Troubleshooting Logging

- Identify the point of failure:
  1. Integration
  2. Filtering Service
  3. Log Server
  4. SQL Server
  5. TRITON - Web Security
- Resolution
  - Reports show data



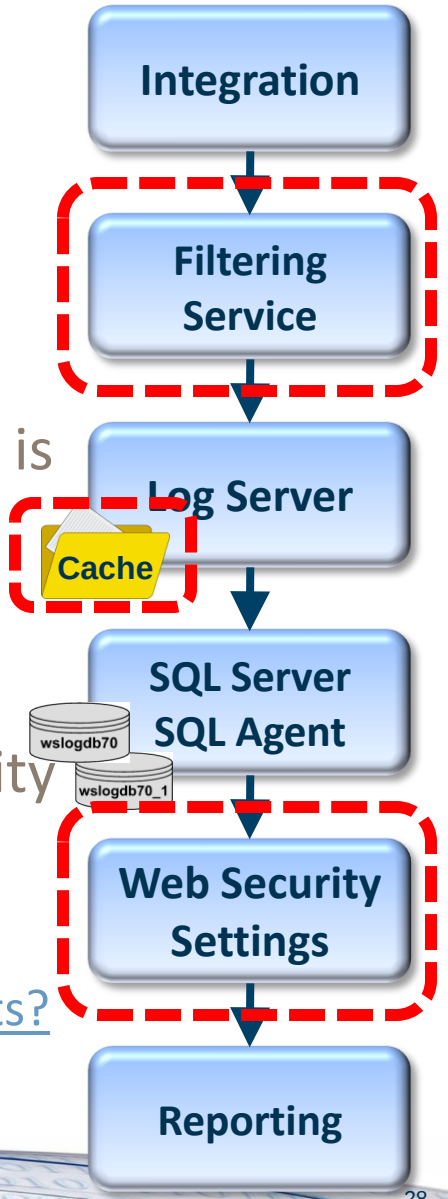
Troubleshooting Logging

- 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



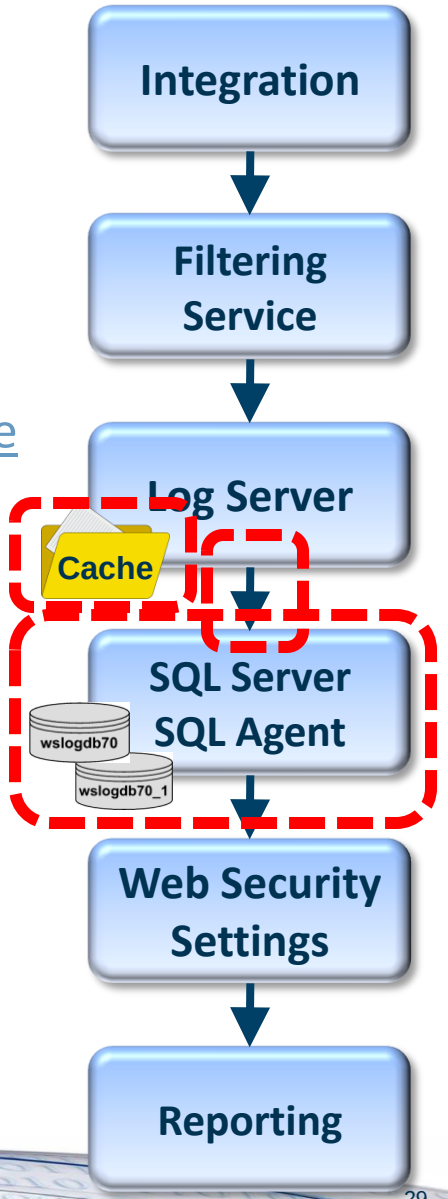
Troubleshooting Logging

- **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 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?



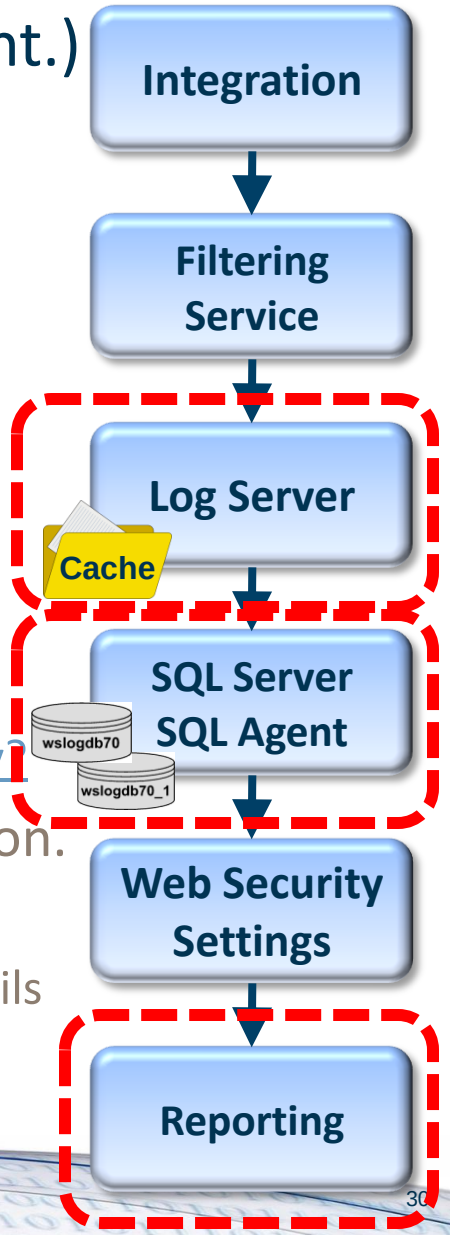
Troubleshooting Logging

- Log files amassing in the **\bin\cache** folder
  - Is SQL Server service is running?
    - Log Database is not available
  - Is SQL Server Agent service running?
    - Diagnostic steps for when logging is not working
    - Error message: "Summary tables used by Investigative Reports are empty"
  - Reset the Log Server connection
    - Setting up the database connection
    - Updating the Log Server connection account or password
    - Configure Log Server to use a database account
  - Reset the ODBC connection
    - How to update the ODBC and the Log Server connections



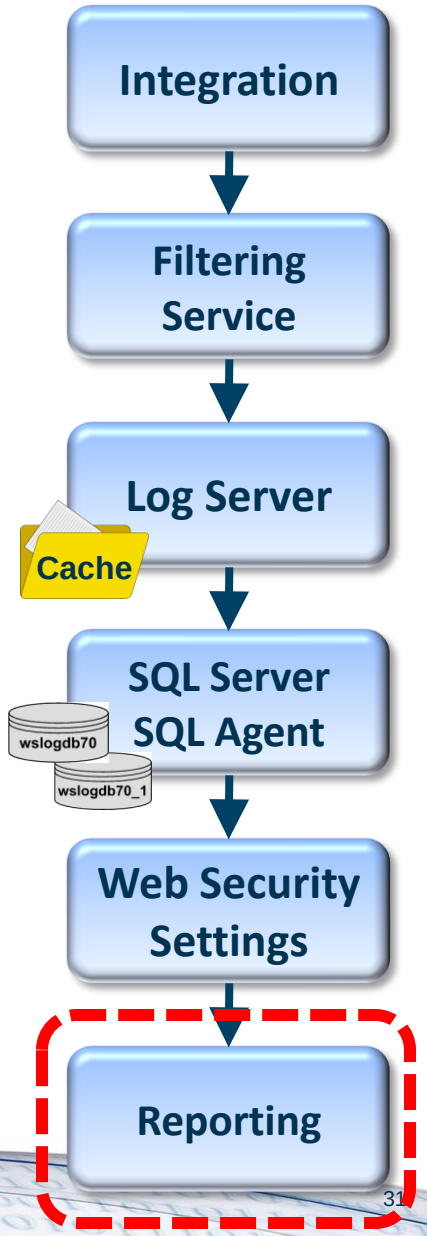
Troubleshooting Logging

- 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
  - View latest database activity--generate a report
    - Can I query the SQL database for hits on a particular day?
  - Verify all Websense components are the same version.
    - Check remote components.
    - Right click the executable and check the Version or Details tab.



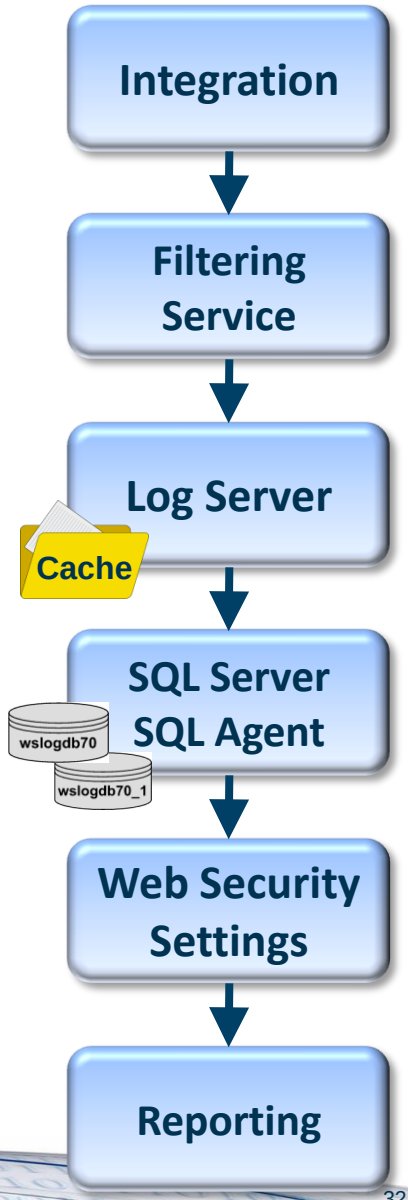
Troubleshooting Logging

- Reports
  - Pointed to correct database?
    - Database connection and report defaults
- Check for errors
  - Application event log, websense.log
- Quick remedy
  - Run the CreateDbU process
    - Can I manually create a new catalog database?
  - Remove and reinstall Log Server
    - Web Security Log Server
    - Log Server installation



Troubleshooting Logging

- Additional 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
  - Log Server FAQs
  - Log Server and Log Database issues
  - Ensure Proper Data Logging in Websense Enterprise and Websense Web Security Suite



Wrap-up

- Log Server and SQL Server requirements
- Installation and upgrade
- Management interfaces
- Logging flow diagram
- Where to start troubleshooting
- Identified key knowledge base articles
  - Article links are available in the presentation pdf

References

- Deployment and Installation Center
  - System Requirements (Chapter 2)
  - Migrating from MSDE to SQL Server 2008 R2 Express (Chapter 58)
- Detailed Websense component diagram
- Simplified Web filtering logging diagram
- Web Security default ports

Support Online Resources

websense
ESSENTIAL INFORMATION PROTECTION™

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

websense
ESSENTIAL INFORMATION PROTECTION™

Webinar Update

Title: **Achieving rapid success with WCCP and Web Security Gateway**

Date: **October 19th, 2011**

Time: **8:30 AM PDT (GMT -7)**

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

Customer Training Options

websense®
ESSENTIAL INFORMATION PROTECTION™

- 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

WEBSENSE®
Authorized Training Partner

WEBSENSE®
Certified Instructor