Forcepoint

Web Security On-prem and URL Filtering

v8.5.x

**Log Server Troubleshooting Guide**

Contents

Introduction

If you are using web protection solutions, the Log Server service (Log Server) must be installed to enable creation of Internet activity reports. Log Server:

- Receives browsing data from:
  - Filtering Service

    In Forcepoint Web Security deployments, Filtering Service forwards log information from Content Gateway to Log Server.
  - (*Web Security Hybrid module*) Sync Service
- Stores the data in temporary files on its local hard drive
- Forwards the data to the Log Database, where it is moved into database tables for use in generating reports
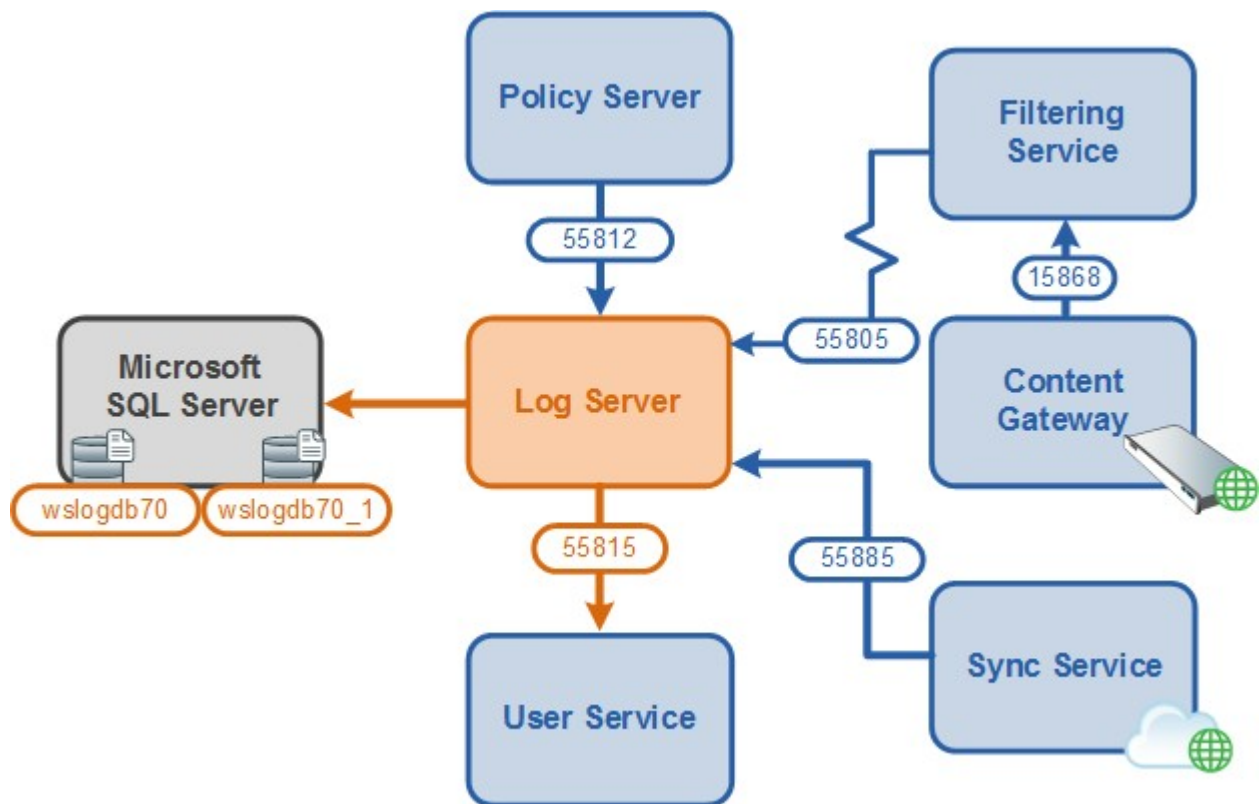
Log Server also requests and receives:

- User and group information from User Service
- Category, risk class, and protocol information from Policy Server

When a user generates browsing data for the first time, Log Server requests information about that user from User Service, which pulls the needed data from the directory server. From that point on, Log Server regularly requests user information for employee names, network login names and group membership, updating its stored data accordingly as changes are found in the directory.

Custom categories and protocols, as well as changes to risk class mappings are forwarded to Log Server and maintained in the Log Database.

When there is a problem with Log Server, none of this data is sent to the Log Database. Reports do not include the most recent browsing data, user information, or customized policy enforcement information.

This collection contains the following articles to help you identify and resolve the underlying cause of reporting problems. Click a link to jump to an article, or use the arrows at the top of the content pane to browse through the articles in this collection.

- *Log Server installation: Error connecting to SQL Server*
- *Log Server installation: Error creating the Log Database*
- *Log Server stops unexpectedly or will not start*
- *Log Server and Windows registration*
- *Incorrect or missing data in reports*
- *Log Database permissions*

Additional troubleshooting and reference articles are also available:

- Manually Creating the Log Database
- Using TestLogServer for Troubleshooting
- Log Server Error Reference

Related concepts

Related tasks

Log Server installation: Error connecting to SQL Server

Before you begin

When the installer displays a SQL Server connection error, you can either:

- Exit the installer, correct the problem and re-run the installer.
- Leave the installer open, correct the problem and return.

To address the problem:

Steps

1) Make sure the Microsoft SQL Server machine is running and available on the network.

2) Use the Windows Services tool (**Start** > **Administrative Tools** > **Services or Server Manager** > **Tools** > **Services**) to make sure the following services are running:

   - **SQL Server**

     If you are using the default instance, the full service name is **SQL Server (MSSQLSERVER)**.

   - **SQL Server Browser**

   - (*SQL Server Standard* or *Enterprise*) **SQL Server Agent**

     If you are using the default instance, the full service name is **SQL Server Agent (MSSQLSERVER)**.

     SQL Server Express does not require the SQL Server Agent service.

3) Double-check the SQL Server host name or IP address, instance name, and port:

   - If you entered the hostname, try using the IP address.

   - The instance name (if any) is entered as part of the hostname or IP address. For example, 10.201.55.13\instance_name.

   - The default port is 1433.

4) Verify the authentication method used to connect to the database:

- ◼ To specify a Windows trusted connection, the logon account used when running the installer must be a trusted account with appropriate permissions.
- ◼ To specify a SQL Server account, verify that the account name and password are correct and the account has the appropriate permissions.

  See *Log Database permissions*.

5) Make sure you are running a supported version of Microsoft SQL Server.

The supported SQL Server versions are listed in the Certified Product Matrix.

Related tasks

Log Server installation: Error creating the Log Database

Before you begin

If the installer encounters problems creating the Log Database, you can either:

- ◼ Exit the installer, correct the problem, and re-run the installer.
- ◼ Complete the installation, then correct the problem and manually create the Log Database (see Manually Creating the Log Database).

  If you choose this option, note that Log Server cannot start until the Log Database has been created.

To address the problem:

Steps

1) Make sure the database location that you specified currently exists on the SQL Server machine.

2) Verify that the account used to run the installer has read and write permissions to the database location.

If a custom path has been selected, the SQL Server process must have adequate file system permissions for database file creation in the specified location.

3) Make sure there is sufficient disk space on the SQL machine to create the Log Database files.

This may mean creating the Log Database on a drive other than C.

4) Check to see if a file or files with the default Log Database names (wslogdb70 and wslogdb70_1) already exist.

- In order for existing database files to be used by the installer, they must be properly connected to the database engine.
- If the files exist but are not connected, either connect the files to the database engine, or remove them before continuing.

5) If you are installing v8.4 or v8.5, use SQL Server Management Studio to make sure the Initial Size defined for the model database does not exceed 10MB. (This requirement was removed in v8.5.3.)

Log Server stops unexpectedly or will not start

Before you begin

If you have installed Log Server, but the service will not start or continues to stop, first verify that Log Server is connected to the Log Database.

Steps

1) Log on to the Forcepoint Security Manager with Global Security Administrator or unconditional Super Administrator permissions.

2) Go to the **Web** > **Settings** > **Reporting** > **Log Server** page.

3) Under Log Database Connection, click **Test Connection**.

If the test fails

Perform the following steps:

Steps

1) Make sure the Microsoft SQL Server machine is running and connected to the network.

2) Make sure the connection port entry is correct, and that there is no firewall blocking the port.
The default port is 1433, but other ports can be used.

3) Use the Windows Services tool to verify that the following services are running:

- **SQL Server**

  If you are using the default instance, the full service name is **SQL Server (MSSQLSERVER)**.

- **SQL Server Browser**

- (*SQL Server Standard* or *Enterprise*) **SQL Server Agent**

  For the default instance, the full service name is **SQL Server Agent (MSSQLSERVER)**.

  SQL Server Express does not require the SQL Server Agent service.

4) Make sure that your authentication settings are correct.

- If you are using SQL Authentication, make sure that the password in the **Log Database Connection** section of the **Settings** > **Reporting** > **Log Server** page is correct.

  If the password has been changed within SQL Server, it also needs to be changed here.

- If you are using Windows Authentication, make sure that Log Server is set up to run as a trusted account:

  a) Open the Windows Services tool on the Log Server machine.

  b) Scroll down to find the **Websense Log Server** service.

  c) Right-click the service name, then select **Properties**.

  d) Select the **Log On** tab to view and change account information.

5) To recreate the database connection, re-enter the database information on the **Settings** > **Reporting** > **Log Server** page.

- If you are using a SQL instance, make sure the instance name is included as part of the SQL Server location (for example, IP_address\instance_name).

- Double-check the port entry.

6) Make sure that the network connection between the Log Server and Log Database machines has not been interrupted.

7) Make sure Log Server can connect to the DSN server.

An error indicating that Log Server cannot connect to the DSN server may occur:

- If Windows User Account Control (UAC) is enabled. Disable UAC.

- If a hostname, rather than IP address, is specified for the SQL Server location. Use the IP address so that access to the DSN server is not required.

If the test succeeds

If the connection test passes but Log Server does not start, or continues to stop:

Steps

1) Make sure that Policy Server is running and that Log Server can connect to Policy Server.

2) Navigate to the **bin** directory on the Log Server machine (`C:\Program Files\Websense\Web Security\bin`, by default) and verify the Policy Server IP address and UID in the **websense.ini** file.

The Policy Server UID in **websense.ini** should match the one in the **config.xml** file on the Policy Server machine.

3) Still in the **bin** directory, make sure the **logserver.ini** file exists and has not been corrupted.

If an error occurs when you try to open the file in a text editor, replace the corrupted file with a good file from backup.

4) Make sure the Log Server machine has not run out of disk space.

5) Verify that the folders defined for ODBC cache and BCP files on the **Web** > **Settings** > **Reporting** > **Log Server** page in the Forcepoint Security Manager exist, and that Log Server has permission to write to them.

6) If Log Server is defined to run as a domain administrator account, set the service to run as **Local System**:

    a) Open the Windows Services tool on the Log Server machine.

    b) Scroll down to find the **Websense Log Server** service, then right-click the service name and select **Properties**.

    c) Select the **Log On** tab to view and click **Local System account**, then click **OK**.

7) Make sure Log Server is registered properly with the Windows operating system. See *Log Server and Windows registration*.

Related tasks

Log Server and Windows registration

To verify that the Log Server service is properly registered with the Windows operating system, or to register or re-register the service:

Steps

1) Use the Windows Services tool to stop the **Websense Log Server** service.

2) Open a command prompt and navigate to the **bin** directory (`C:\Program Files\Websense\Web Security\bin`, by default).

3) Enter the following command.

```
logserver.exe -c
```

If no errors display, the service is registered correctly. If an error that contains "Initialization: -1" displays, continue with the next step.

4) With the Log Server service stopped, delete the **LogServer.exe.p12** file from the **bin** directory

5) Use the Windows Services tool to start the Log Server service. If other errors display, continue with the next step.

6) To remove the Log Server service, enter:
   ```
   logserver.exe -u
   ```

7) To register the executable, enter:
   ```
   logserver.exe -i
   ```

8) Once again, enter the following command. Verify that no errors appear.
   ```
   logserver.exe -c
   ```

Next steps

You can add the **-debug** parameter to the **logserver.exe -c** command to gather more advanced diagnostic information (see *Run Log Server in debug mode*).

Related tasks
Run Log Server in debug mode on page 16

Incorrect or missing data in reports

If Log Server is installed and the Log Database was created successfully, but reports contain no data or no recent data, use the following steps to identify and address the problem.

Related tasks
Make sure Filtering Service is sending data on page 10
Look for problems when temporary files not created on the Log Server machine on page 11
Check for Log Database problems on page 12
Run Log Server in debug mode on page 16

Make sure Filtering Service is sending data

Before you begin

Log Server receives Internet usage data from Filtering Service. If there are problems with Filtering Service, data is not sent, and log records cannot be created.

Steps

1) Make sure that Filtering Service is running.

   ■ *Windows*: Use the Services tool to verify that **Websense Filtering Service** is Started.

   ■ *Linux*: Use the `/opt/Websense/WebsenseDaemonControl` command to make sure that **Filtering Service** is running.

2) Go to the **Settings** > **General** > **Logging** page in the Web Security module of the Forcepoint Security Manager and click **Check Status** to verify that Log Server is listening at the specified IP address or hostname, and on the specified port.

   If the status check fails:

   ■ Verify the Log Server IP address or hostname and port values. The values on the **Settings** > **General** > **Logging** page must match those on the **Settings** > **Reporting** > **Log Server** page.

   ■ Make sure no firewall is blocking the port (**55805**, by default).

   ■ Open a Windows Command Prompt or PowerShell on the Log Server machine and run the following command to verify that Log Server is listening on the port:

   ```
   netstat -ban > port.txt
   ```

   Open **port.txt** and find **LogServer.exe** in the list. The logging port should be listed.

   ■ Use a utility like **telnet** or **ping** to verify that the Log Server and Filtering Service machines can communicate.

3) Verify that Content Gateway, Network Agent, or a third-party integration product has been properly configured to communicate with Filtering Service, and that Internet traffic is being seen.

   If all of the following are true:

   a) You have either deployed Forcepoint Web Security or integrated Forcepoint URL Filtering with a third-party product.

   b) Users requests are being managed correctly.

   c) No records are being sent to Log Server.

   Stop Network Agent. If Log Server begins to receive Internet usage data, port spanning was not configured in your network, or port spanning was interrupted. See the Network Agent Quick Start paper for information about how to position Network Agent in your network.

4) Make sure that Filtering Service is associated with a Policy Server that has its own Log Server instance (is configured for logging), and that data is not being diverted to the TestLogServer utility for troubleshooting purposes.

- In Web Security module of the Forcepoint Security Manager, make sure the expected Policy Server IP address appears in the toolbar, and that there is no alert indicating that no Log Server is installed for the Policy Server.

- If TestLogServer has been started, make sure it has been set up to forward records to Log Server. (See Using TestLogServe r for Troubleshooting for more information.)

Look for problems when temporary files not created on the Log Server machine

Before you begin

Log Server receives information from Filtering Service and stores it in temporary files before sending it to the Log Database. Problems on the Log Server machine can interfere with that process.

First, monitor the cache or BCP folder on the Log Server machine (`C:\Program Files\Websense\Web Security\bin\Cache or bin\Cache\BCP`, by default) to verify that temporary files are being created. If temporary files are being created and processed normally, files appear in the directory only briefly before the data is processed into the Log Database and the temporary file is deleted.

If temporary files are not being created, and there are no problems with Filtering Service communication:

Steps

1) In the Web Security module of the Forcepoint Security Manager, verify that the Log Server IP address or hostname and port values on the **Settings** > **General** > **Logging** page are correct and match the IP address or hostname and port values shown on the **Settings** > **Reporting** > **Log Server** page.

- If your deployment includes appliances, the Log Server IP address must be used.
- Make sure that the actual IP address appears, and not 127.0.0.1.

2) Check for firewalls that might be blocking the logging port (55805, by default).

3) Make sure the Log Server executable version is correct:

a) Navigate to the **bin** directory on the Log Server machine (`C:\Program Files\Websense\Web Security\bin`, by default).

b) Right-click the **LogServer.exe** file and select **Properties**.

c) Select the **Details** tab, and verify that the **Product Version** matches your current web protection product version. Find current version information on the **Help** > **About Forcepoint Security Manager** page in the Forcepoint Security Manager.

4) Check the file paths set up for cache and BCP files on the **Settings** > **Reporting** > **Log Server** page to make sure the folders exist, and that Log Server has permission to write to them.

5) If TestLogServer is being used, make sure it is set up to forward data to Log Server. (See Using TestLogServer forTroubleshooting for more information.)

Look for problems when temporary files created on the Log Server machine

If Log Server is creating temporary files, but data is not being processed and sent to the Log Database:

Steps

1) If Log Server has been configured to use BCP insertion, go to the **Settings** > **Reporting** > **Log Server** page and change the insertion method to ODBC.

This issue may occur if **bcp.exe** or one of its support files has been removed from the system. Correct the problem with bcp.exe to restore the ability to use BCP insertion.

2) If the Log Database was installed using Windows Authentication, make sure Log Server is running as a trusted user.

3) Make sure no other applications, such as antivirus software, a backup utility, or log file analyzers, are running that might be locking the temporary files.

4) Make sure there is only one copy of **bcp.exe** on the Log Server machine.

5) If the **Websense Log Server** service is listed as **Started** in the Windows Services tool, and the alert "Service was not found" appears, follow the steps listed in *Log Server and Windows registration*.

> **Related tasks**
> Log Server and Windows registration on page 8

Check for Log Database problems

> **Before you begin**
>
> Some of the troubleshooting steps make changes to the Log Database. Back up the database before proceeding.

After backing up the database:

Steps

1) Make sure that there is enough disk space for the ETL (Extract, Transfer, and Load) job to create a new standard logging partition when rollover conditions occur.

- If necessary, add additional disk space to the machine.

  Remember to change the File Path entries on the **Web** > **Settings** > **Reporting** > **Log Database** page in the Forcepoint Security Manager if this process changes the database location.

- Use the **Settings** > **Reporting** > **Log Database** page to delete or move older partitions. To do this, scroll to Available Partitions, mark each partition to be deleted and click **Delete**.

  Contact your Database Administrator or IT department if you want to keep the partitions but need to move them to free up disk space.

- As a temporary fix, until more disk space can be added, shrink all standard logging partitions except the current active partition. This does impact reporting speed.

- Make sure **tempdb** is not full. Tempdb filling up is often a symptom of other SQL Server problems. Check for SQL Server errors about tempdb to resolve the underlying issue. Once the issue is resolved, ask your Database Administrator or IT department to stop and restart the Microsoft SQL Server services to clear tempdb. (If the underlying issue is not resolved, tempdb may grow again very quickly.)

  Be sure to determine the impact to other applications before restarting SQL Server services.

2) If you are using Microsoft SQL Server Standard or Enterprise, make sure the **SQL Server Agent** service is running for the database instance that hosts the Log Database.

3) Verify that the ETL job has the correct SQL Server permissions to create the database (see *Log Database permissions.*

4) In order to ensure that the ETL job can create a new standard logging partition make sure that:

- The initial size (**Init Size** field value) for the data and log files (set on the **Settings** > **Reporting** > **Log Database** page) is not greater than maximum size set by your Database Administrator.

- The **File Path** entries for the data and log files on the **Settings** > **Reporting** > **Log Database** page is correct and the folders exist.

- The SQL Server service instance hosting the Log Database has write permissions on the **File Path** folders.

5) Verify that there is at least one current, active partition (a partition neither disabled nor marked for deletion) listed on the **Settings** > **Reporting** > **Log Database** page.

6) Make sure there are no other processes running that use significant resources (such as an antivirus scan).

7) If you are using Microsoft SQL Server Standard or Enterprise, verify that the SQL Agent jobs (Websense_AMT_ETL_wslogdb70, Websense_ETL_Job_wslogdb70, Websense_IBT_DRIVER_wslogdb70, Websense_Maintenance_Job_wslogdb70, and Websense_Trend_DRIVER_wslogdb7) exist and are running.
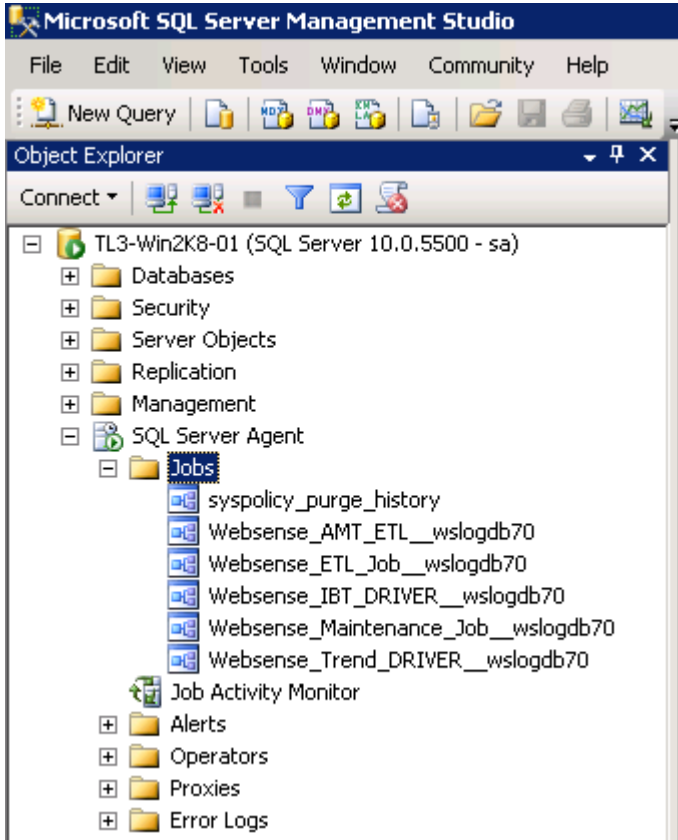
- If one or more jobs is not running, see *Database jobs are not running*.
- If the jobs are running, but the error "Could not obtain information about Windows NT group/user 'server \admininstrator'" appears, see *Database jobs are running, but an error appears*.

Related tasks

Database (ETL) jobs are not running

If the ETL job (Websense_ETL_Job_wslogdb70) is not running:

Steps

1) Use SQL Server Management Studio to make sure the current, active logging partition is not flagged as "suspect."

If the "suspect" flag appears, notify your Database Administrator or IT department and request that data and disk recovery be performed, if necessary. When the recovery process is complete, start the ETL job.

2) Use SQL Management Studio to see if records exist in the **dbo.incomingbuffer** table under **wslogdb70**. If there are records in dbo.incomingbuffer:

   a) Locate the **dbo.wse_etl_config** table.

   b) Right click the table name and select **Edit top 200 rows** or **Select top 1000 rows**.

   c) Check the value under **max_buffer_size**. If the value is negative, revert it to a positive value.

Database (trend) jobs are not running

If the trend job (Websense_Trend_DRIVER_wslogdb70) is not running:

Steps

1) Make sure you have enabled trend data retention on the **Web** > **Settings** > **Reporting** > **Log Database** page.

2) Verify that the retention values are not all zero.

3) Make sure the trend job has the correct SQL Server permissions to update the database. (See *Log Database permissions*).

> **Related tasks**
> Log Database permissions on page 17

Database jobs are running, but an error appears

> **Before you begin**
>
> The error "Could not obtain information about Windows NT group/user 'server\admininstrator'" indicates a problem with the account that owns the Microsoft SQL Server jobs. If the jobs are running as a user other than the account used by the ODBC connection, there may be a problem authenticating the user.

To find out which account is used to run the database jobs in SQL Server Standard or Enterprise:

Steps

1) Log on to SQL Server Management Studio.

2) Expand the SQL Serer Agent tree.

3) Right-click a web protection database job, then select **Properties**.

4) Look for the value in the **Owner** field.

Next steps

Refer to the instructions for your SQL Server version to change the owner of all web protection jobs to the trusted account used by the ODBC connection (Log Server) **or** a standard SQL Server user (like **sa**).

Run Log Server in debug mode

Before you begin

If you are having issues with Log Server and are not able to identify or correct the problem using the steps offered in this guide, run the Log Server service in debug mode to collect additional information.

Steps

1) On the Log Server machine, open the Windows Services tool.

2) Locate **Websense Log Server** service.

3) Right-click the service name, then select **Properties**.

4) On the General tab, click **Stop**.

5) In the Start Parameters box, enter **-debug**.

6) Click **Start**, then close the Properties window.

Next steps

Log Server starts and creates the file **debug.txt** in the **bin** directory (`C:\Program Files\Websense\Web Security \bin`, by default). Log Server writes tracing data to the file. Open debug.txt in a text editor for information about any issues Log Server encounters as it starts and runs.

If the problem is that Log Server continues to stop, the last entry of the file generally indicates the point of failure.

The debug.txt file can become very large if Log Server is left to run in debug mode. When you have finished troubleshooting your Log Server issue, Use the Windows Services tool to once again stop the service. Remove the "-debug" parameter, then start the service again.

Stopping and restarting Log Server does not remove an existing debug.txt file.

Log Database permissions

Before you begin

Microsoft SQL Server Standard and Enterprise editions define SQL Server Agent roles that govern accessibility of the job framework. The SQL Server Agent jobs are stored in the SQL Server **msdb** database.

To install Log Server successfully, the user account that owns the web protection database must have adequate permissions to create the Log Database. This account then becomes database owner.

If you are using Microsoft SQL Server 2008, 2008 R2, 2012, 2014, or 2016 Standard or Enterprise, the database owner account must:

1) Be a member of the **dbcreator** fixed server role.

2) Have membership in one of the following roles in the **msdb** database:
   - **SQLAgentUserRole**
   - **SQLAgentReaderRole**
   - **SQLAgentOperatorRole**

3) Have membership in the **db_datareader** role

For SQL Server Express, the account requires the **sysadmin** server role.

Use Microsoft SQL Server Management Studio to grant the database user account the necessary permissions to successfully install Log Server.

Steps

1) On the SQL Server machine, launch **SQL Server Management Studio**.

2) Select the **Object Explorer** tree, and then select **Security** > **Logins**.

3) Select the login account to be used during Log Server installation.

4) Right-click the login account and select **Properties** for this user.

5) Select **User Mapping** and do the following:

    a) Select **msdb** in database mapping.

    b) Grant membership to one of these roles:
- SQLAgentUserRole
- SQLAgentReader Role
- SQLAgentOperator Role

    c) Grant membership to the **db_datareader** role.

    d) Click **OK** to save your changes.

6) Select **Server Roles**, and then select **dbcreator**. The dbcreator role is created.

7) Click **OK** to save your changes.