Manage logging

The Content Platform Engine, which is the main component of IBM FileNet P8 Platform, provides logging capabilities for tracking functional issues and troubleshooting. In this section, you will learn how to monitor the system logs and configure trace logging for troubleshooting.

Content Platform Engine System Logs

Content Platform Engine produces several log files during normal operation. Following are the primary troubleshooting tools for the administrator:

- p8_server_error.log
- pesvr_system.log
- p8_server_trace.log

You must become familiar with normal log entries and monitor these log files to observe changes in behavior that might indicate a problem and to ensure that log files are managed. Keep the files to a reasonable size, roll over to new files and delete old ones when you no longer need them.

If the organization uses workflows, the following tools are available to monitor the workflow system:

- vwtool
- vwmsg
- pelog
- peverify

The IBM Case Foundation administration courses will help you use these tools effectively.

Default location of logs

By default the Content Platform Engine logs are stored in the following locations:

- WebSphere Application Server:

  <install_root/profiles/profile_name/FileNet/server_instance_name>

  Example:

  C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1
- WebLogic Server:

  bea/user_projects/domains/domain_name/FileNet/AdminServer

You can change the location where the files are stored. The Content Engine Startup Content page (CE Ping page) shows the path configured for the log files. In a clustered environment, each server will contain its own Content Platform Engine log files. They are located in the server_instance_name under the current working directory of the deployed application.

Web application server logs

When troubleshooting IBM FileNet P8 Platform, you will need to collect the logs from the Content Platform Engine as well as the logs from the web application server. IBM Content Navigator, which provides the user interface for IBM FileNet P8 Platform, logs errors and entries in the web application server's logs.

Each web application server generates its own logs.

The following list contains supported web application servers, default path for the log files, and the name of the log files in the order of importance.

WebSphere

- Location: install_root/profiles/profile_name/logs/server_name
- Examples of log locations:

  WebSphere (Windows): C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1

  WebSphere (Linux): /opt/ibm/WebSphere/AppServer/profiles/AppSrv01/logs/server1
- Log files:
  - SystemOut.log
  - SystemErr.log
  - startServer.log
  - stopServer.log

WebLogic

- Location: oracle_home/admin/domain_name/aserver/servers/AdminServer/logs
- Examples of log location:

  C:\bea\user_projects\domains\base_domain\servers\AdminServer\logs

- Log files:
  - AdminServer.log
  - access.log
  - Base_domain.log

Note that the MustGather technote (https://www.ibm.com/support/docview.wss?uid=swg21308231) provides suggestions for what data and logs to collect when reporting an issue with support. If your organization has a dedicated web application server administrator, you will need to collaborate to capture the requested web application server logs.

Trace logs

Trace logs are used to troubleshoot specific issues. Trace logging is typically implemented to collect and record information about application failures in test or production environments. If you open a support call, the representative might request that you enable trace logging and reproduce the issue. In that situation, the representative recommends which subsystem flags to enable and what level of detail to collect.

You can configure trace logging at the domain level or the site level. The site-level configuration takes precedence over any domain level settings. Site level configuration is used in organizations that have servers and users in more than one geographical location. For details about Domain and Site, refer to the *Architecture and domain structures* section in this course.

Use Administration Console for Content Platform Engine to configure trace logging, including configuring the level of details for server trace logging and setting the location of the trace log file. The configuration is done on the Trace Subsystem tab of the domain properties. The default file name is p8_server_trace.log.

Disable trace logging when you no longer need it. Trace logs can grow quickly and impact system performance and disk space.

Guidelines for monitoring log files

- Establish a baseline and know what to expect.

  Part of detecting problems is being aware of what normal activity looks like. If you establish a baseline of activity and you are familiar with the normal error messages that your system generates, you can better detect anomalies, such as new or more frequent error messages.

- Monitor logs regularly.

  Watch for new error messages and any change in error log size.

  Example: If the size of a log file is normally 64 KB, and on one day it shows 100 KB

  Log level sizes can be a clue that something is wrong. For instance, a single error might produce a new log entry every 5 minutes. This new log entry causes the log file to grow much more quickly, which you first detect by observing the change in the log file size.

  Tools such as ECM System Monitor can be used to generate alerts when unusual activity occurs.

- Increase monitoring after any system changes.

  Example: Patches applied

- Keep records of normal logs for comparison purposes.

  If you keep a week of logs each month, you have comparison information to use in case of a change. If you keep more than that, you might be using more space than you need. If there no major changes to the log behavior after a year or so, you might decide to keep a week of logs for the whole year.

Activity: View and archive system logs

In this activity, you locate the Content Platform Engine logs and the WebSphere Application Server logs. You shut down the web application server to archive the logs. You restart the web application server and examine the new logs created.

In this activity, you will accomplish the following:

- Locate the Content Platform Engine logs.
- Locate the WebSphere Application Server logs.
- Disable WebSphere Application Server trace logging.
- Archive old log files.
- Examine the new log files.

Locate the Content Platform Engine logs.

- Ensure that the IBM FileNet P8 Platform components are started.

  If you have not started them earlier, start the components by using the earlier activity: *Prepare your system - Start IBM FileNet P8 Platform.*

- In the **Mozilla Firefox** browser, open **Content Engine Startup Context (Ping Page)**.
  - Use the bookmark in the **Bookmarks** menu > **System Health** > **CE Ping** or enter the following URL: **http://vclassbase:9080/FileNet/Engine**
- On the Ping page, scroll down and then note down the value for the **Log File Location** key.

Log File Location	C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1

- In a **Windows Explorer** window, navigate to that folder path: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1**

  You can copy the value from the Ping page and paste it on Windows Explorer.

- Notice that there are four log files:
  - p8_server_error.log
  - p8_server_trace.log
  - pesvr_system.log
  - pesvr_trace.log

- Minimize the Windows Explorer window.

Locate the WebSphere Application Server logs.

- In a **Windows Explorer** window, navigate to the **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1** folder and notice that there many log files:
  - SystemOut.log
  - SystemErr.log

  These two files are most often referenced.

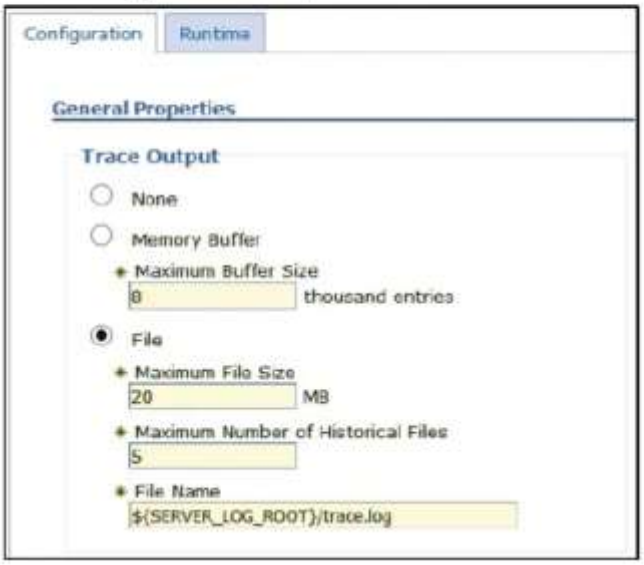
Disable WebSphere Application Server trace logging.

In this task, you disable trace output for the WebSphere Application Server. The student system is configured with the trace output enabled.

- In the **Mozilla Firefox** browser, click the **WAS** bookmark or enter the following URL: **https://localhost:9043/ibm/console/**
- Type the following values for user ID and password and click **Log in**.
  - User name: **wasadmin**
  - Password: **FileNet1**
- On the left navigation pane, expand **Troubleshooting** and then click **Logs and trace**.

- Click the **Diagnostic Trace** link under **General Properties** section.

  On the Configuration tab of the Diagnostic trace service page, notice that you can control the Maximum File Size, Maximum Number of Historical Files to keep before overwriting, File Name, and location of the trace log.



- On the **Configuration** tab, select **None** to disable the trace output and then click **OK** at the end of the page.
- In the **Messages** section, click **Save** to save the configuration.
- Log out of the **WebSphere Integrated Solutions Console** and close the browser.

  The change does not take effect until WebSphere Application Server is restarted. You restart WebSphere Application Server in the next task.

Archive old log files.

In this task, you stop the server and archive the WebSphere Application Server and Content Platform Engine logs.

- Open the **WebSphere Admin** folder on the desktop, right-click the **_4 Stop server1.bat** file, and then select **Run as administrator** from the list.
- Click **Yes** when you are prompted with the **User Account Control** dialog box to allow the program to run.

  Wait for the operation to complete (the command window closes).
- Minimize the **WebSphere Admin** folder window.

- Maximize the **Windows Explorer** window where you viewed the Content Platform Engine log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1**.
- Create a folder that is called **Archived_CPE_Logs** (this name is not critical) in this directory to store the archived Content Platform Engine logs and then move all the four ***.log** files to the new folder.
- On the **File Access Denied** dialog box, select the **Do this for all current items** option and then click **Continue** to move the files.
- Minimize the **Windows Explorer** window.

  Maximize the Windows Explorer window where you viewed the WebSphere Application Server log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1** folder.
- Create a folder that is called **Archived_WAS_Logs** (this name is not critical) in this directory to store the archived WebSphere Application Server logs and move the **SystemOut.log, startServer.log**, and **SystemErr.log** files to the new folder.
- On the **File Access Denied** dialog box, select the **Do this for all current items** option and then click **Continue** to move the files.
- Minimize the **Windows Explorer** window.

- Open the **WebSphere Admin** folder on the desktop, right-click the **_1 Start server1.bat** file, and then select **Run as administrator** from the list.
- Click **Yes** when you are prompted with the **User Account Control** dialog box to allow the program to run.

  Wait for the operation to complete (the command window closes).
- Minimize the **WebSphere Admin** folder window.

Examine the new log files

If no log files exist, the Content Platform Engine (CPE) and the WebSphere Application Server create new logs at startup.

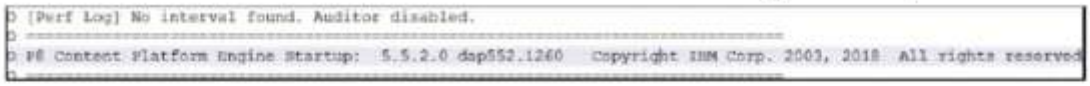
- Maximize the **Windows Explorer** window where you viewed the CPE log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1**.
- Notice the four log files that are created with the current date and time.

- Right-click the **p8_server_error.log** file, select **Edit with Notepad++,** and examine the log entries that are created during startup.

  Cancel any prompts to update to the Notepad++ version.

  Normally, there are no errors and only INFO entries are found on the page.
- Maximize the **Windows Explorer** window where you viewed the WebSphere Application Server log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1** folder.
- Notice that the log files (that were archived) are created with the current date and time.
- Open **SystemOut.log** with **Notepad++** and examine the log entries that are created during startup.
- Scroll down the log file to the text **P8 Content Platform Engine Startup: 5.5.2.0** as shown in the following screen capture.

  You can also search for the text: P8 Content Platform Engine Startup



  This text indicates the Content Platform Engine startup.

  Errors are logged as Java stack traces. There are a couple of errors such as the following one:

  "ResourceMgrIm E WSVR0017E: Error encountered binding the J2EE resource, CNMailSession, as mail/CNMailSession"

  These errors can be ignored because the components are not being used. However, it is important that you monitor your organization's log files regularly and learn to recognize errors that might indicate a serious issue.
- Open **SystemErr.log** with **Notepad++** and then examine the log entries that are created during startup.

  Notice that this log file does not have as many entries as the SystemOut.log.
- Open **startServer.log** with **Notepad++** and examine the log entries.

  Notice the last entry that includes the text: *Server 1 open for e-business.*

  This log entry indicates that the WebSphere Application Server started successfully.
- When you are done examining the log files, click **File** > **Close All** and then exit **Notepad++**.

Activity: Configure trace logging

Trace logging options can be set on the domain or at the site level. If the settings are configured on the site, they override the settings on the domain.

In this activity, you configure trace logging on the Content Platform Engine at the domain level and site level. You log in to an IBM Content Navigator desktop to create security entries in the trace log and then examine the entries in the trace log.

In this activity, you will accomplish the following:

- View and configure initial trace configuration.
- Configure trace logging on the domain.
- Configure trace logging at the site level.
- Inspect the trace log files.
- Create trace log entries.
- Disable trace logging.

Configure trace logging on the domain.

In this task, you will first view the trace log file before enabling the trace logging. You will configure trace logging at the domain level, and then configure the site to inherit these settings.

- Maximize the **Windows Explorer** window where you viewed the Content Platform Engine log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1**.
- Right-click the **p8_server_trace.log** file, select **Edit with Notepad++,** and examine the initial log entries.

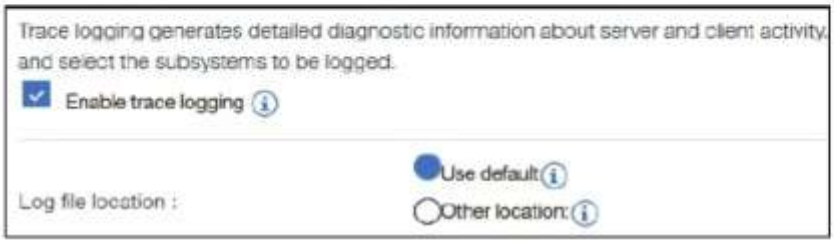
  Since the trace logging is not yet enabled, there may not be much text.
- Close the **p8_server_trace.log** file.
- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or enter the following URL: **http://vclassbase:9080/acce**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the right pane, from the **EDU_P8** tab, select the **Trace Subsystem** subtab.

  Use the forward arrow on the right to scroll to find the tab. You can also use the down arrow to select the subtab from the list.

If the contents of the tab is displayed, click the tab or click Refresh and the content will be refreshed.

- On the **Trace Subsystem** subtab, select the **Enable trace logging** option.
- For the **Log file location** field, select the **Use default** option.

  The trace log is saved in the same folder as the Content Platform Engine log files.



- Scroll down to the **Subsystems** section and select the **Detail** level trace options for the following subsystems:
  - **Error Trace Flags**
  - **Search Trace Flags**

  Moderate and Summary levels are automatically selected.

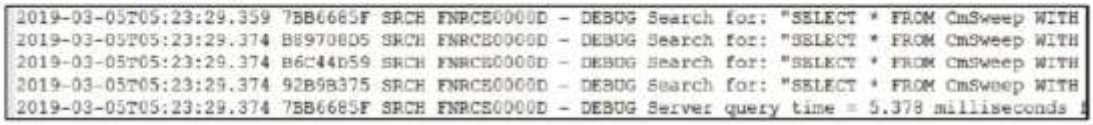
  Log files at the Detail level grow quickly. Enable only the subsystems that you need. Remember to disable trace logging when you no longer need it.
- Click **Save** to save the **EDU_P8** domain configuration and then click **Refresh**.
- On the left navigation pane, expand the **Global Configuration** > **Administration** > **Sites** node and select **Initial Site (Default)**.
- From the **Initial Site** tab on the right pane, select the **Trace Subsystem** subtab and verify that **EDU_P8 (server hierarchy object)** as the **Configuration source.**
- If it is not already selected, select the option, click **Save**, and then click **Refresh.**

  Ensure that Enable trace logging is selected.
- Log out of the administration console and close the browser.

- Maximize the **Windows Explorer** window where you viewed the Content Platform Engine log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1**.
- Open the **p8_server_trace.log** file in **Notepad++** and then verify that the file contains a few of **DEBUG** level entries at the end of the file.

  The Debug value is on the Sev column of the log file.

  If the entries are not listed, close the file, refresh on the Windows Explorer window and then open again.



- Close the trace log file and minimize the Notepad++ window.

Configure trace logging at the site level.

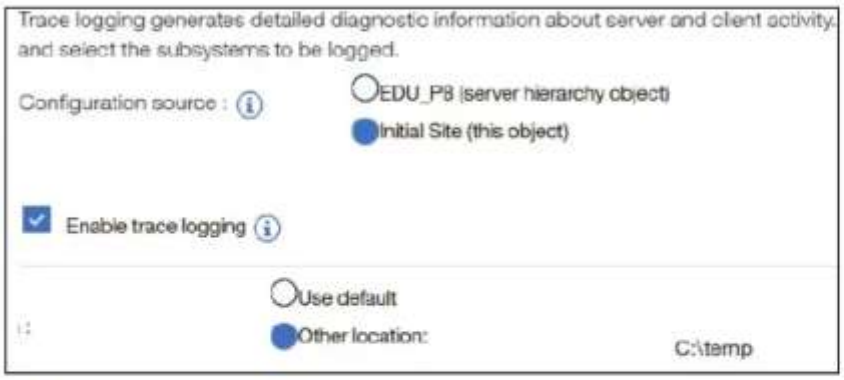
In the previous task, you enabled trace logging at the domain level. In this task, you configure the trace logging at the site level and it will override the domain settings.

- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- In the **ACCE**, on the left navigation pane, expand the **Global Configuration** > **Administration** > **Sites** folder and click **Initial Site (Default)**.
- From the **Initial Site** tab on the right, select the **Trace Subsystem** subtab and then select **Initial Site (this object)** for the **Configuration source** field.
- When you are prompted with a dialog box **Selecting this option means…**, click **OK** and then verify that **Enable trace logging** is selected.

  The parent (domain) configuration values that apply to child objects will not apply to this node (site). Since the settings are configured on the site, it will override the settings on the domain, and so domain configurations values will not apply.

- For the **Log file location** field, select the **Other location** option and then type **C:\temp**.

  The trace log will be saved to this new folder.



- Click **Save** and then click **Refresh**.
- From the **Trace Subsystem** subtab, scroll down to the **Subsystems** section, select the **Detail** level trace options for the **Security trace flags** subsystem.

  If you are unable to select, log out of the administration console to clear the cache and log back in.

  The Error Trace Flags and Search Trace Flags entries are already selected because of the previous configuration. For the site level, you can modify them.

- Click **Save,** click **Refresh**, and then click **Close** to close the **Initial Site** tab.
- Log out of the administration console and close the browser.
- In **Windows Explorer**, navigate to the folder location (**C:\temp)** that you specified for the trace log and verify that the **p8_server_trace.log** file generated.
- Refresh the display and then open the file in **Notepad++** and verify that the file contains **DEBUG** level entries.
- Close the file.

Create trace log entries.

You enabled security trace logging. You will log in to IBM Content Navigator as Olivia and then check the trace log file for this entry.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator**.
- Type **Olivia** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.

- In **Windows Explorer**, navigate to the **C:\temp** folder and open the **p8_server_trace.log** file again in **Notepad++**.
- Search for the word **Olivia** and review the log entry.

  Some log entries show Olivia's login event.
- Close the trace log file and then exit **Notepad++**.
- Log out of the **IBM Content Navigator desktop** and close the browser.

Disable trace logging.

Trace logging affects system performance and uses disk space. It is a good practice not to leave trace logging enabled for long periods of time.

- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the **EDU_P8** tab, open the **Trace Subsystem** subtab.
- Clear the **Enable trace logging** option, click **Save**, and then click **Refresh**.

  Even if you configured trace logging at the Site level and those settings override any global (domain) settings, you still have to disable trace at the domain level.
- On the left navigation pane, expand the **Global Configuration** > **Administration** > **Sites** folder and click **Initial Site (Default)**.
- From the **Initial Site** tab on the right pane, select the **Trace Subsystem** subtab and then clear the **Enable trace logging** option.
- Click **Save**, and then click **Refresh**.
- Log out of the administration console and close the browser.

  Optionally, you can repeat the earlier *Create trace log entries* task with a different user (Oscar, FileNet1) and check the trace log file. You will not find any entries for Oscar since you disabled the trace logging.
- Close all the open Windows Explorer windows.