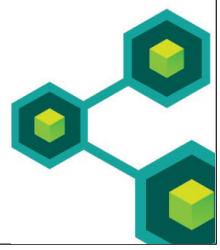
Examine Audit Logging and Indication Processing Facility Logging

IBM Cognos BI 10.2.2



Business Analytics software

Business Analytics software

IBM

Objectives

- At the end of this module, you should be able to:
  - describe installation logs and configuration logs
  - explore audit logging
  - explore IPF logging

Business Analytics software

IBM

What are Installation Logs?

- record activities performed by installation wizard transferring files
  - Install
  - Error summary
  - Installer specification

Creation of these log files is enabled by default. They provide details of the installation activities of the product.

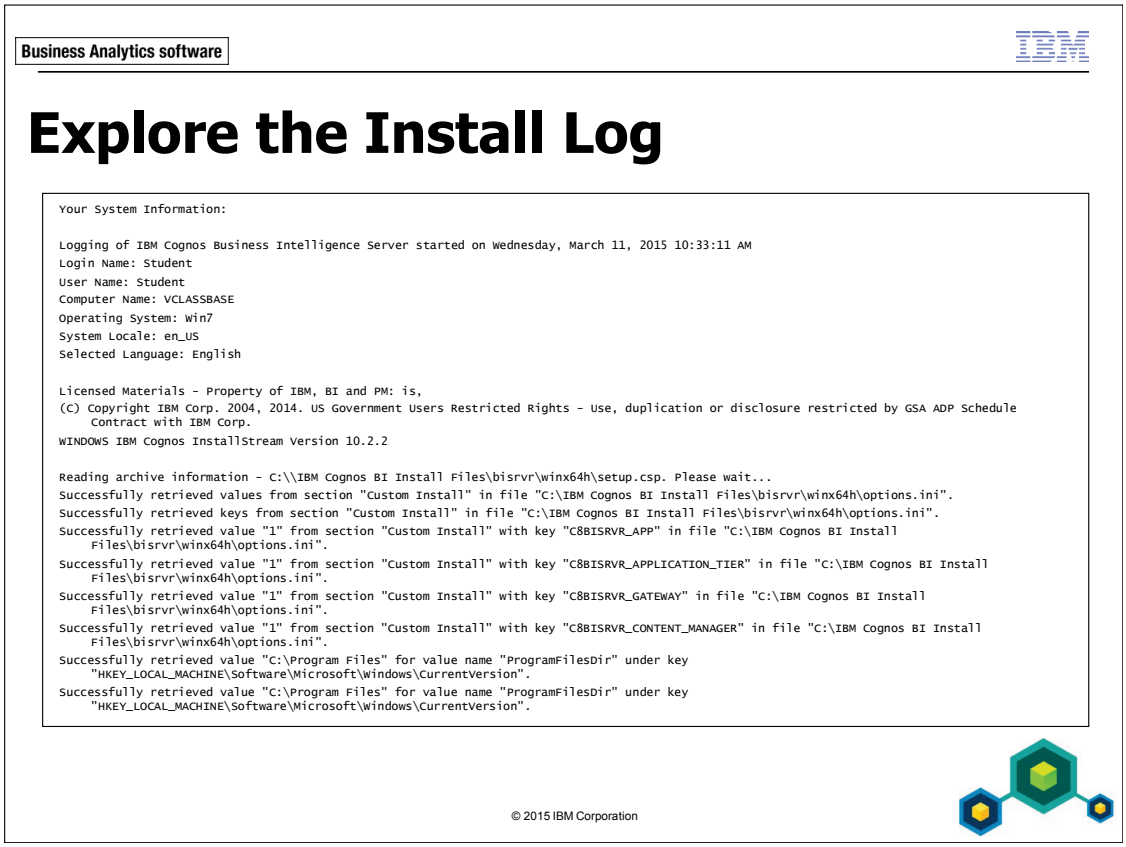
Business Analytics software

IBM

Review Installation Logs

- Install Log
- Error Log
- Specification Log
- Content Manager Result Logs

You will review the installation logs over the next few pages.



The tl-<component>-<version>-<date>_<time>.txt file is located in the ..\instlog directory and contains information on the files that were copied and the registry keys that have been altered by the installation.

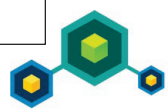
The example in the slide represents a section of the file contents.

Business Analytics software

IBM

Explore the Error Log

```
Your System Information:

Logging of IBM Cognos Business Intelligence Server started on Wednesday, March 11, 2015 10:33:11 AM
Login Name: Student
User Name: Student
Computer Name: VCLASSBASE
Operating System: Win7
System Locale: en_US
Selected Language: English

Licensed Materials - Property of IBM, BI and PM: is,
(C) Copyright IBM Corp. 2004, 2014. US Government Users Restricted Rights - Use, duplication or disclosure restricted
    by GSA ADP Schedule Contract with IBM Corp.
WINDOWS IBM Cognos InstallStream Version 10.2.2

Selected Components:
  IBM Cognos Business Intelligence Server
    Application Tier Components
    Gateway
    Content Manager

Local disk space information:

Drive:     Available:      Required Estimate:
C:\        25.22 GB        3.15 GB

Dialog Entry Information:
[Installation Location]
C:\Program Files\IBM\cognos\c10_64full

[Shortcut Folder]
IBM Cognos 10 - 64 Full
```

The tl-<component>-<version>-<date>_<time>_summary_error.txt file is located in the ..\instlog directory and contains any error that may have been encountered during the copy or apply phase of the install.

The example in the slide represents a section of the file contents.

Business Analytics software

IBM

Explore the Specification File

```
; Licensed Materials - Property of IBM
; BI and PM: is
; (C) Copyright IBM Corp. 2004, 2014
; US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract
    with IBM Corp
[Dialog1]
Title=Welcome to the Installation Wizard
DE=0
EN=1
FR=0
JA=0
ES=0
NL=0
SV=0
FI=0
IT=0
PT_BR=0
KO=0
ZH_CN=0
ZH_TW=0
[Dialog2]
Title=IBM License Agreement
;Failure to accept the license agreement and non-IBM terms, if any, will abort the installation.
;Please return the software to the point of acquisition and obtain a refund, if applicable.
```


The tl-<component>-<version>-<date>_<time>.ats file is located in the ..\instlog directory and contains the selections made by the user within the installation wizard.

This file can also be used to pre-select installation items when performing a silent install.

The example in the slide represents a section of the file contents.

Business Analytics software

IBM

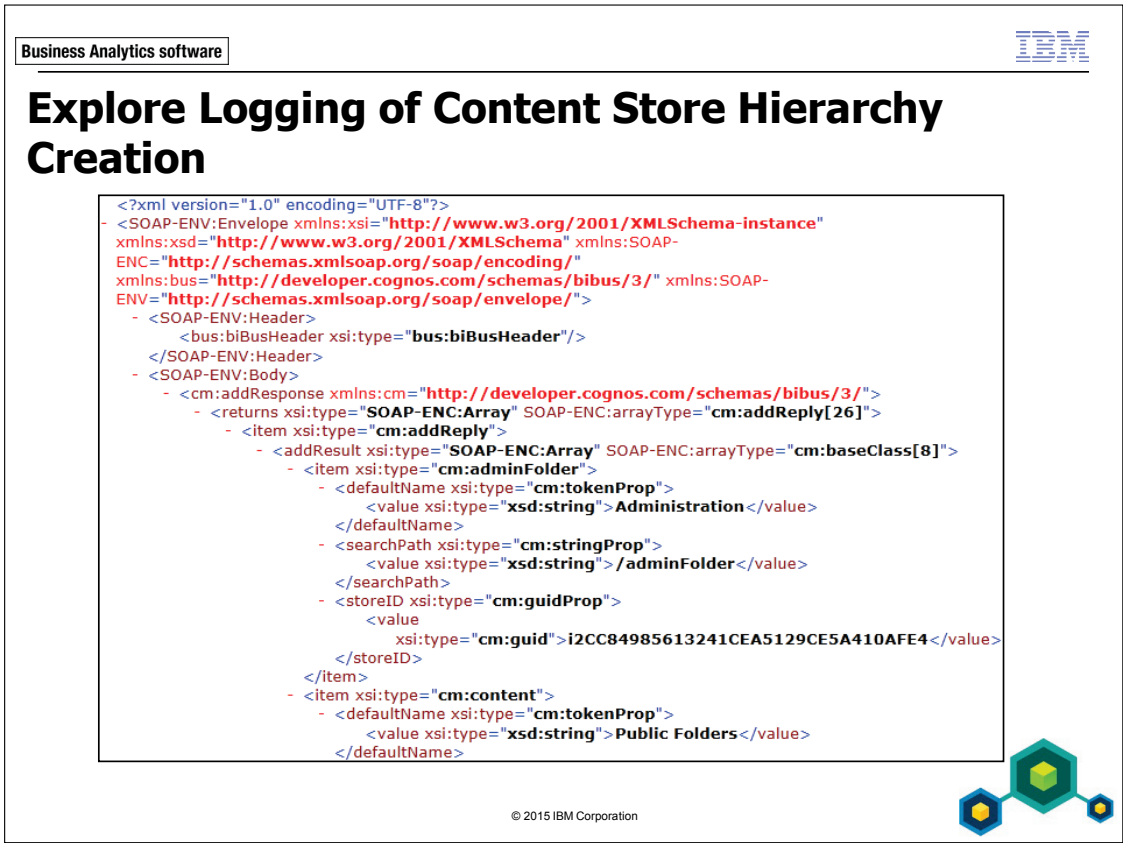
Explore the Content Manager Results Logs

- records activities product performed creating initial Content Store hierarchy and objects
- activities are logged to files CMCreateBaseObjectsScript_results.xml and CMCreateScript_results.xml in the ..\logs directory

If you see these logs, you will know that Content Manager was created.

The Content Manager Results logs may include log files that start with 00x. These include additional setup information of the Content Store. For example, 002.CMCreatePageletObjects_results.xml shows the setup of the portlets for IBM Cognos Administration.

Note: In the lab environment used in this course, the logs directory has been cleared, so you will not see these files.



The CMCreateBaseObjectsScript_results.xml contains the results of the creating the initial content hierarchy.

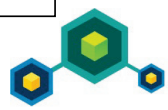
If you receive a message that an error was detected while creating the initial content objects, to troubleshoot the problem, check the ..\logs\CMCreateBaseObjectsScript_results.xml log file to see what was created.

Business Analytics software

IBM

Explore Logging of Creation of Initial Content Store Objects

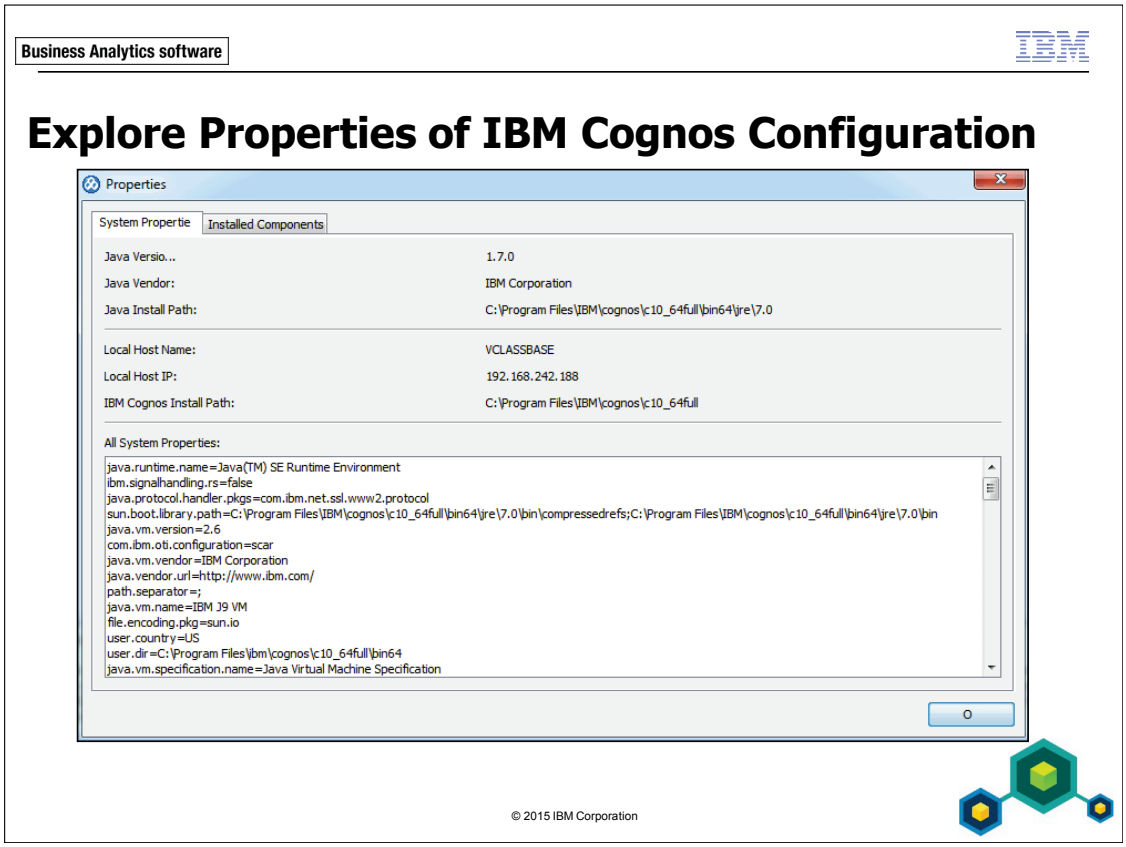
```
<?xml version="1.0" encoding="UTF-8"?>
- <SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:bus="http://developer.cognos.com/schemas/bibus/3/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
  - <SOAP-ENV:Header>
      <bus:biBusHeader xsi:type="bus:biBusHeader"/>
    </SOAP-ENV:Header>
  - <SOAP-ENV:Body>
    - <cm:updateResponse xmlns:cm="http://developer.cognos.com/schemas/bibus/3/">
      - <updateResult xsi:type="SOAP-ENC:Array" SOAP-ENC:arrayType="cm:baseClass[125]">
        - <item xsi:type="cm:adminFolder">
          - <defaultName xsi:type="cm:tokenProp">
              <value xsi:type="xsd:string">Administration</value>
            </defaultName>
          - <searchPath xsi:type="cm:stringProp">
              <value xsi:type="xsd:string">/adminFolder</value>
            </searchPath>
          - <storeID xsi:type="cm:guidProp">
              <value xsi:type="cm:guid">i2CC84985613241CEA5129CE5A410AFE4</value>
            </storeID>
          </item>
        - <item xsi:type="cm:content">
          - <defaultName xsi:type="cm:tokenProp">
              <value xsi:type="xsd:string">Public Folders</value>
            </defaultName>
```

The CMCreateScript_results.xml contains the results of the creation of the initial Content Store objects, including security objects.

The element <updateResult xsi:type="SOAP-ENC:Array" SOAP-ENC:arrayType="cm:baseClass[125]"> tells us that 125 objects (items) were created in the initial Content Store.

The SOAP message in the slide displays the SOAP response.



You can explore the properties of IBM Cognos Configuration to obtain system information such as Java version, Java vendor, Java install path, local host name, local IP address, IBM Cognos 10 install path, Java system properties, selected environment variables and installed IBM Cognos 10 components.

In IBM Cognos Configuration, press Ctrl+ F3, and the results will be written to a dialog box. Here you can review system properties and installed components.

Business Analytics software

IBM

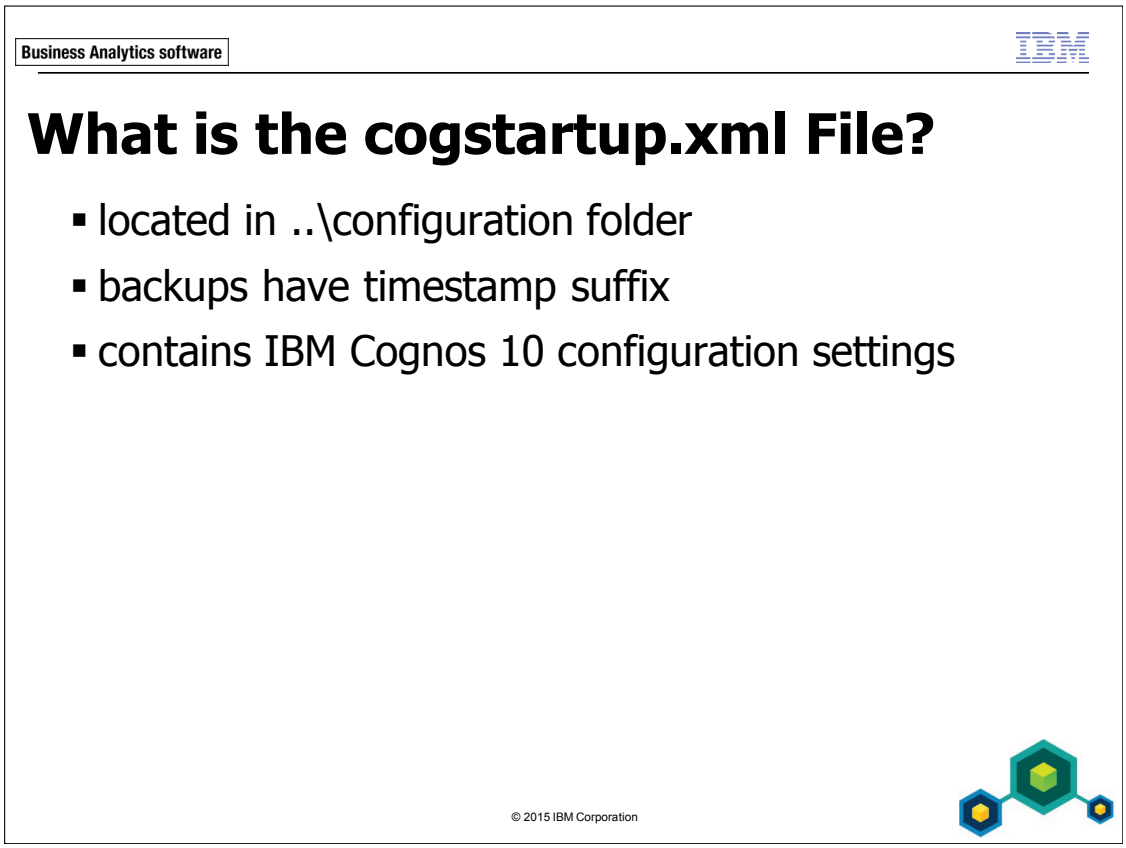
Logging of IBM Cognos Configuration

- obtain information on Java path and the loading of JAR files on launch of IBM Cognos Configuration

```
Looking for JRE in: \bin...
Looking for JRE in: \jre\bin...
Looking for JRE in: jre\7.0\bin...
Using CLASSPATH:
   .;..\bin\cclcfgmcf_mcf.jar;cogconfig.jar;configcnfm.jar;..\bin\cogconfigi.jar;..\bin\cogcn
   fm.jar;..\bin\bcprov-jdk14-145.jar;..\bin\dom4j-1.6.1.jar;..\bin\jaxen-
   1.1.1.jar;..\bin\cclcfgmcf.jar;..\bin\cclcfgapi.jar;..\bin\jcam_crypto.jar;..\bin\i18nj.ja
   r;..\bin\icu4j.jar;..\bin\commons-httpclient-3.1.jar;..\bin\commons-codec-
   1.3.jar;..\bin\commons-logging-1.1.jar;..\bin\commons-logging-api-1.1.jar;..\bin\commons-
   logging-adapters-1.1.jar;..\bin\CognosIPF.jar;..\bin\log4j-
   1.2.17.jar;..\bin\jcam_jni.jar;..\bin\jdxslt.jar;..\bin\ant.jar;..\bin\ant-
   launcher.jar;..\bin\jcam_config_test.jar;..\bin\cclcoreutil.jar;..\bin\CognosCCL4J.jar
Using J_HOME:    jre\7.0
Using J_OPTS:
```


If you cannot open IBM Cognos Configuration, you can double-click cogconfig.bat or cogconfig.sh in the ..\bin directory (in the ..\bin64 directory for 64-bit installations). You may encounter this if there is a JVM/JRE issue. The output will be written to a command window.

To obtain additional information on the launch of IBM Cognos Configuration, in a command window, run cogconfig.bat or cogconfig.sh with the parameters –log and –d. This creates a cogconfig_<timestamp>.log in the ..\logs directory, and will provide more detail on why IBM Cognos Configuration did not load.



This file contains all of the IBM Cognos configuration settings for a specific installed instance of IBM Cognos 10.

Business Analytics software

IBM

What is the coglocale.xml File?

- located in..\configuration folder
- backups have time stamp suffix
- records configuration choices made in IBM Cognos Configuration for product and content locales, locale mapping, and currency support

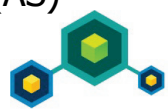
If you experience problems with language support in the user interface or in reports, use these files to track your changes.

Business Analytics software

IBM

What is Auditing in IBM Cognos 10?

- audit logging provides basic information about user and system activity
  - user login/logoff
  - report executions
  - schedule executions
  - services start/stop
  - agent execution
  - authorization actions (add/remove permissions)
  - threshold violations (IBM Cognos Administration defined metrics)
  - Human Task Service (HTS), Annotation Service (AS) activity

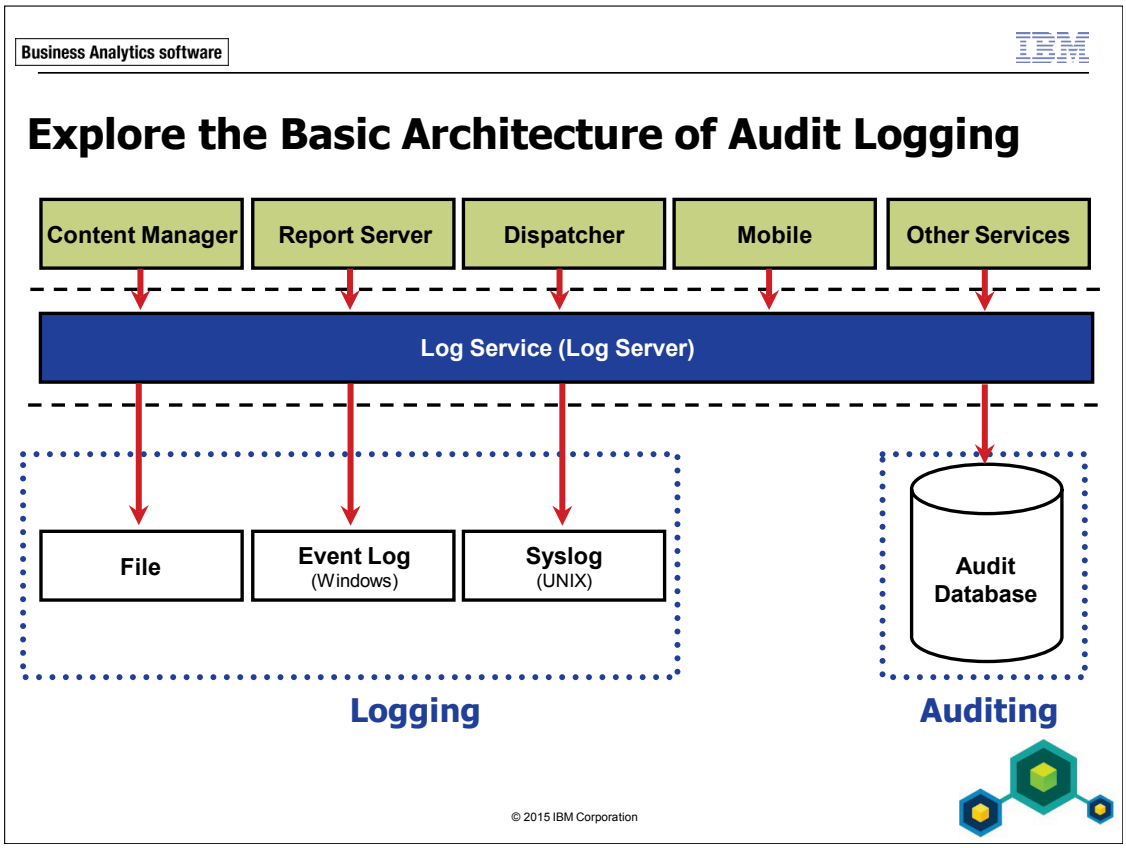


Audit logging can answer the following questions: Who? When? What? Affecting what object?

Audit logging is used to:

- audit the operation of a system or users
- monitor usage of reports and studios
- gather usage statistics
- troubleshoot issues in conjunction with other log files

What about reports of users by role, in order to be SOX compliant? This functionality is not available out of the box. However, the Audit Extension utility can be used to accomplish this task. It is available from the IBM developerWorks Web site at http://www.ibm.com/developerworks/data/library/cognos/development/utilities/page574.html.



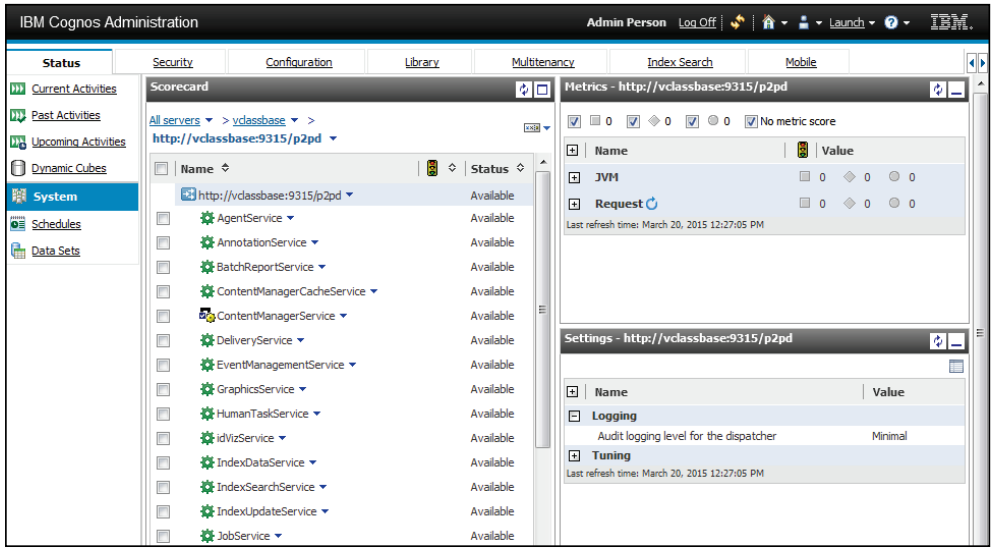
Components and services provide output generated locally to a local instance of Log Service which runs on every installed instance and is the first service to start. This service will collect the input and output it to local destinations.

The log messages are not sent through the BIBus, but are instead passed to the local service through other means, such as direct port to port communication.

LogService is implemented by a component called Log Server.

Business Analytics software

Set Logging Levels



Logging levels are configurable through the IBM Cognos Administration UI for each service. In IBM Cognos Administration, on the Status tab, the System page reveals a scorecard, metrics, and settings. In the Scorecard pane, click on the server name that you want to set logging on; for example, click http://<server_name>:port/p2pd for properties at the dispatcher level.

Logging levels are set based on a service for audit logging in the UI. Since this UI only reflects services (this is SOA), this is used as the base for defining the settings. Internally the log level specified for the service will be mapped to components.

Business Analytics software

IBM

Explain Audit Logging Levels

- Minimal (default)
- Basic
- Request
- Trace
- Full

The Trace and Full levels can generate huge files in a short time, and therefore can degrade server performance significantly, and should never be used during peak periods. Because of this, once you gather your required information, you should then reduce the log level.

The Minimal level is the default, which logs start and stop service logs and runtime errors.

The Basic level logs the same as the Minimal level and also tracks the following: Logon/Logoff/Logon Expired logs, Report and query execution logs, Schedule execution logs, Agent mail, and Build and execution logs.

In addition to logging the same as the Basic level, the Request level logs also includes SOAP request and response logs.

The Trace level logs the same as the Basic level and includes requests to components with parameter values or function calls.

The Full level logs all of the above.

Demo 1: Set Logging Levels

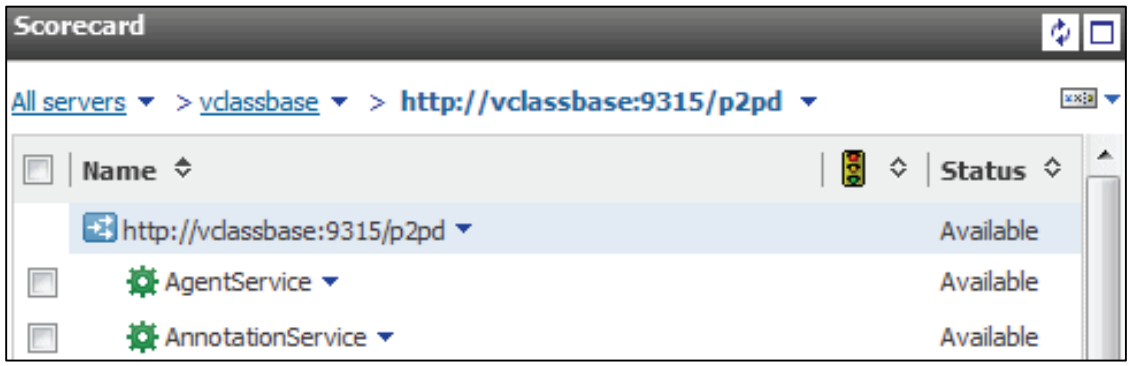
The IBM Cognos 10 Full:9315 dispatcher and the IBM Cognos 10 DispCM:9320 dispatcher should be running at the beginning of this demo.

Purpose:
You want to configure logging for the system. To become familiar with the logging available, you will use the IBM Cognos Administration tool.

Task 1. Select a dispatcher to configure.

1. Launch **Internet Explorer**, go to **http://vclassbase:88/C10Full**, log on to the **LDAP_Dev** namespace with **admin/Education1** credentials, and then launch **IBM Cognos Administration**.
2. On the **Status** tab, click **System**.
3. In the **Scorecard** pane, click **vclassbase**, and then click **http://vclassbase:9315/p2pd**.

   A section of the result appears as follows:



Task 2. Configure the Logging settings.

1. In the **Settings** pane, expand **Logging**.

   The current logging level is displayed, which is minimal logging for the dispatcher.
2. To access logging settings at the dispatcher level, click the **Set properties** icon on the **Settings** pane title bar.
3. In the **Category** list click **Logging**.

   There are many entries to configure logging for. Each service can be configured independently across the system.

4. Click **Next Page** to review more entries, and then click **First Page**.

   Leave IBM Cognos Administration open.

Task 3. Review the results of minimal logging for the dispatcher.

1. Launch **Windows Explorer**, navigate to **C:\Program Files\IBM\cognos\c10_64full\bin**, and then double-click **logviewV2.exe**.

   Optionally, you may want to create a shortcut for IBM Cognos Log Viewer on the desktop, for your convenience, as it will be used a few times in the course.
2. In **IBM Cognos Log Viewer**, from the **File** menu, click **Load Cognos Log File(s)**, and then double-click **cogserver.log**.
3. Near the bottom left, click the **cogserver.log** tab, and then scroll to the bottom of the log, and click the last entry, scrolling through the lower pane to read the entry details.

   You may see information similar to the following (the exact message will differ, depending on the actions that have occurred in your environment):

Component ID:	DISP
Build Number:	6100
Level:	1
Logger:	Audit.Other.dispatcher.DISP.com.cognos.pogo.logging.SystemEventLogger
Operation:	Start
Object Type:	Dispatcher
Object Path:	
Status:	Success

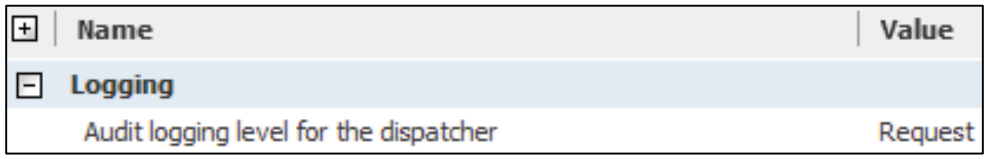
   Minimal tracing logs start and stop service logs and runtime errors. The most recent entries that you see should include these types of messages. Notice that there are no entries for logging on or off, or query executions, as that is not traced at the minimal level.
4. Close **IBM Cognos Log Viewer**.

   You will work more with this application later.

Task 4. Modify the logging level to request level tracing.

1. Switch to **IBM Cognos Administration**, on the **Set properties** page, for the **Audit logging level for the dispatcher** entry, change the value from **Minimal** to **Request**, and then click **OK**.
2. In the **Settings** pane, expand **Logging**.

   The new logging level is displayed.



Task 5. Log on, run a report, and observe the results.

1. Log off **Admin Person**, and then log on again with **admin/Education1** credentials.
2. Launch **IBM Cognos Connection**, navigate to **Public Folders\Samples_DQ\Models\GO Sales (query)\Report Studio Report Samples**, and run the **Horizontal Pagination_DQ** report.
3. When the report displays, log off **Admin Person**.
4. Launch **IBM Cognos Log Viewer**.

   In Windows Explorer, navigate to C:\Program Files\IBM\cognos\c10_64full\bin, and double-click logviewV2.exe, or use the Desktop shortcut if you created one.
5. From the **File** menu, click **Load Cognos Log File(s)**, and then double-click **cogserver.log**.

6. Near the bottom left, click the **cogserver.log** tab, maximize the window, and then scroll to the bottom of the log, reviewing the most recent entries.

   You may see a message similar to the following:

Component ID:	DISP
Build Number:	6100
Level:	4
Logger:	Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler
Operation:	
Object Type:	
Object Path:	
Status:	
Message:	

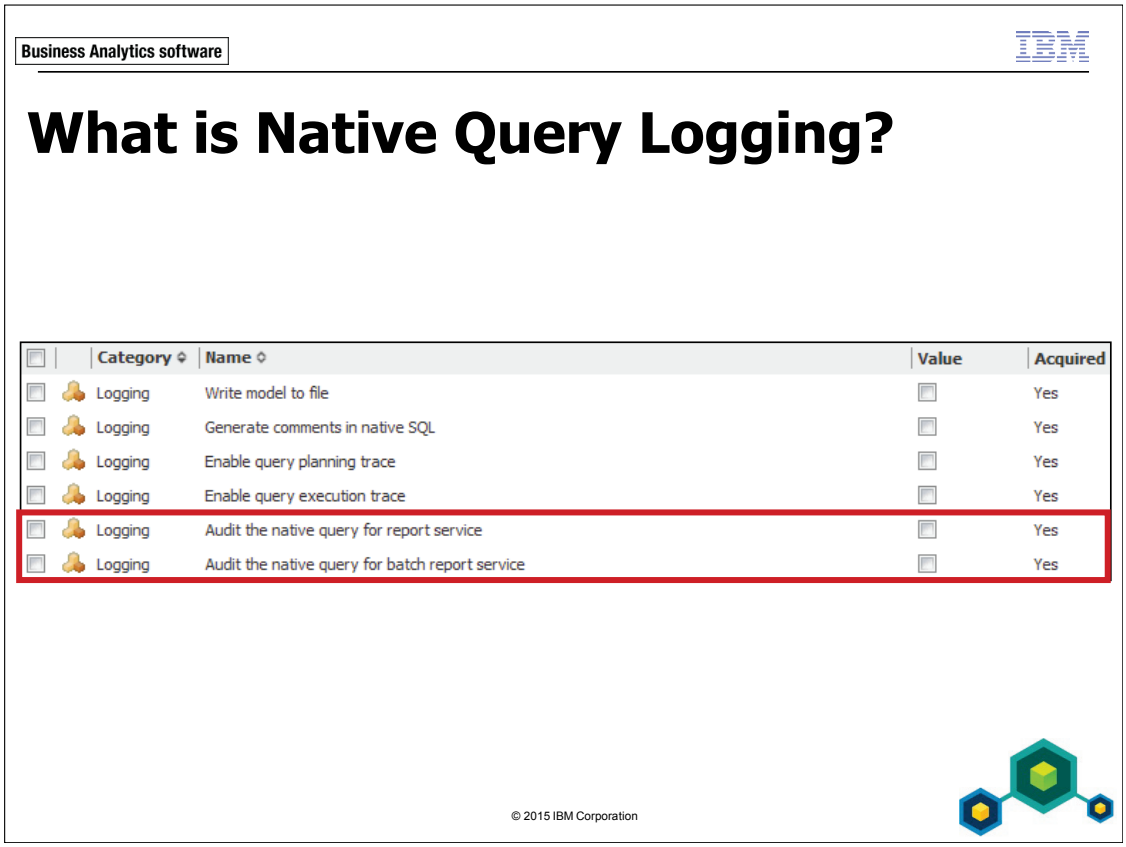
   Notice that there are many more entries that are tracked at this level of logging. The Request level logs start and stop service logs and runtime errors, tracks Logon/Logoff/Logon Expired logs, Report and query execution logs, Schedule execution logs, Agent mail, and Build and execution logs, and includes SOAP request and response logs.

7. Close all open windows.

   At this point, if logging was completed, you would return the logging state back to minimal, but in this case, you will need this detailed logging for a workshop later in this course, so you will leave the logging state as request.

8. To prepare the environment for the upcoming workshop, from the **Taskbar**, launch **Services**, and stop the **IBM Cognos DispCM:9320** dispatcher.

Results:
You used IBM Cognos Administration to explore the logging available in IBM Cognos 10, and set the audit logging for the Dispatcher service to Request tracing level.



For Report service, Batch report service and PowerPlay service, there is an additional setting to enable capturing the SQL/MDX sent to the query engine in audit logging. The captured SQL/MDX is not necessarily the one sent to the database, as the query engine might apply changes for various reasons.

The true native SQL/MDX can only be captured at the database side or in UDA trace (SQL for relational) or MDX debug output.

Business Analytics software

IBM

Explain Audit Logging Destinations

- target for audit logging data
- several types of destinations supported for different purposes
- multiple destinations can be used at the same time
- not every destination will output the same data

Several types of destinations are supported for different purposes, including database, files, Windows Event log, UNIX System log (Syslog), and Remote log service.

Depending on the destination, the generated log data will be filtered. Information that will vary includes the level of detail and the services and components that will be included.

For information on tables that are available in the audit logging database and what they are used for, refer to the IBM Cognos BI: Administration (v10.2.2) course, and the IBM Cognos Business Intelligence 10.2.2 Administration and Security Guide.

Business Analytics software

IBM

Where are Destinations Stored?

- audit database
  - stores audit logging data in a relational database schema for reporting on it
- filtering
  - only stores messages at Basic level or above
  - does not store system errors
- enable native query logging to capture SQL/MDX being sent to the query engine

Destinations are defined in IBM Cognos Configuration. The default destination is File. Additional destinations can be defined as required.

The destination database is commonly referred to as the audit database. Currently supported databases are DB2, SQL Server, Oracle, Informix, and Sybase.

A business reason for audit logging would be to gather usage statistics for reports and studios, track report, agent, and schedule executions, and to determine user activity.

IBM Cognos 10 provides a sample Framework Manager model and deployment that is included in the BI Samples install component. Model files can be found in the ..\webcontent\samples\models\Audit directory. Sample reports are provided in a deployment archive file located at ..\webcontent\samples\content\IBM_Cognos_Audit.zip.

Additional Information:

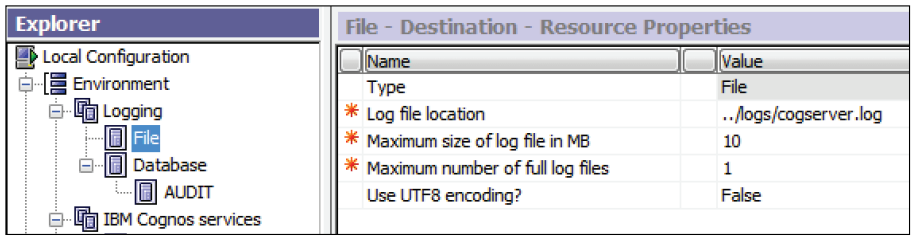
- The BI Samples are a separate install and do not come with the base IBM Cognos 10 server install.
- The Apache Derby that is used for the Cognos Content Store is not supported as an audit database.
- By default, the logging levels are set to Minimal.

Business Analytics software

IBM

Explore the File Log

- stores output in flat tab delimited file(s)
- no filtering
- default configuration out of the box
  - log file name is cogserver.log, size 10 MB, single file only



The destination File stores output in flat tab delimited file(s), for which you can configure the number and size of the log files. If all files are filled, the oldest one will get deleted and a new one is created for the most recent output (rolling windows). You will need to stop, and then start the IBM Cognos service to apply the new configuration settings.

The output is not filtered at all, and contains SQL/MDX if native query logging has been enabled.

cogserver.log should be the first place to look if something does not work or stops working. It is unusual to change the default destination, and it is recommended that name cogserver.log be used for this file.

The configuration fields are as follows:

- **Type**: The destination type (not modifiable).
- **Log file location**: location and file name of the log file. The ../ indicates the install directory.
- **Maximum Size of Log File in MB**: Maximum size before a new file will be created.
- **Maximum Number of Full Log Files**: The number of log files created. Can be a value between 1 and 10,000.

If multiple log files get created then the name of the files would be cogserver.1.log, cogserver.2.log.

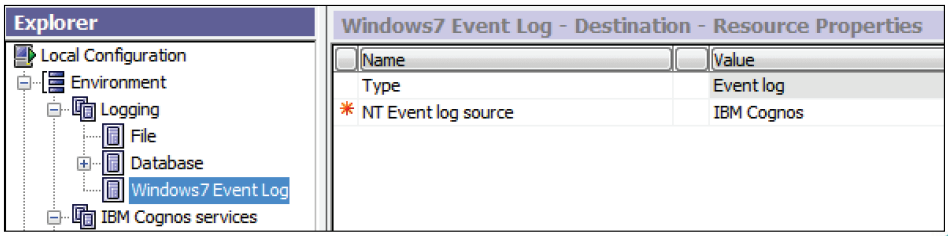
The file without any .#.log, for example cogserver.log, will always have the most recent information.

Business Analytics software

IBM

Explore the Windows Event Log

- send audit logging messages to the Windows Event log
- no filtering
- requires IBM Cognos 10 to be started as a Windows service

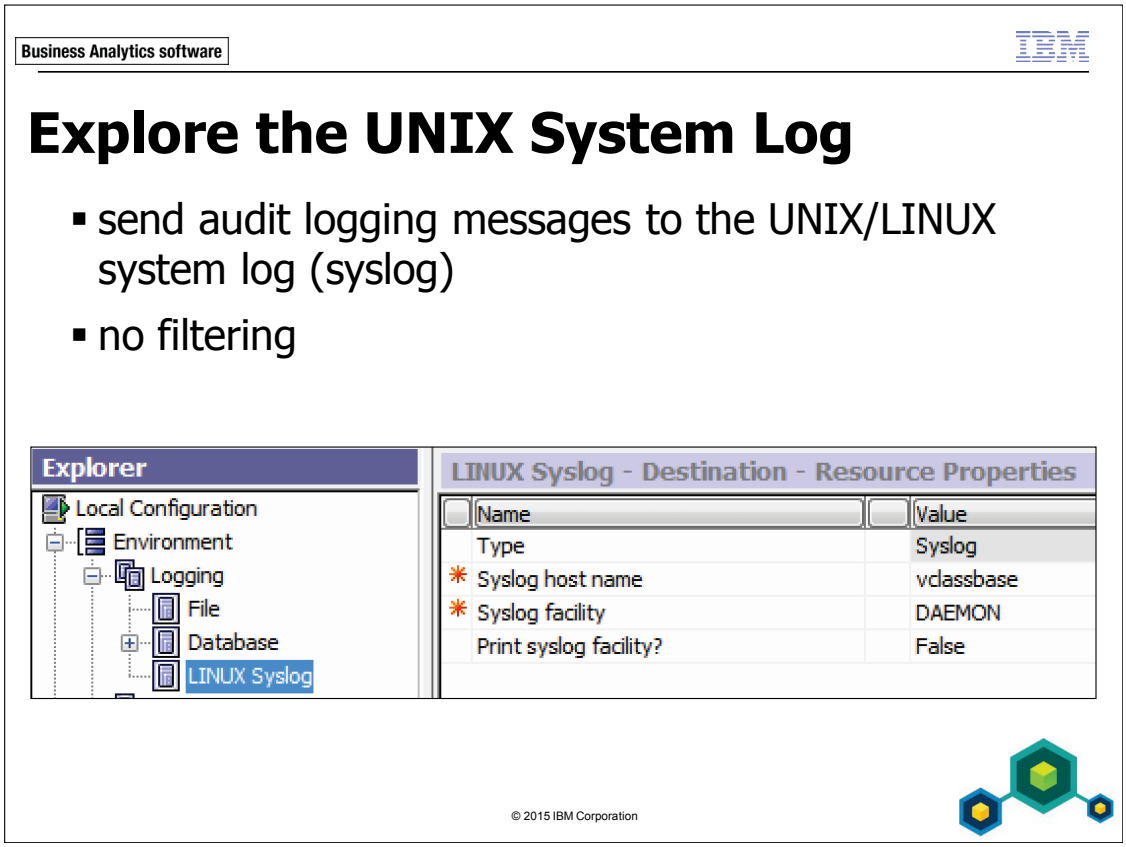


Logging messages are sent to the Application log; you may have to adjust the maximum size of the log to suit your environment. Use this when running as a Windows service to support integration with an Event Log based system management.

No filtering is applied, and it will not include SQL/MDX even if native query logging has been enabled.

This logging requires IBM Cognos 10 to be started as a Windows service, and does not work if IBM Cognos 10 is launched with startup.bat. The NT Event log source field is going to be the name that shows under the Source Column in the Windows Event Log. This value is modifiable.

If the Event Log source name changes in IBM Cognos Configuration, then the service will be unregistered with the old name, and the new name will get registered. Restarting the Windows service is necessary for these settings to take effect. Use startup.bat in test environments for a quick startup; it will run in a command window.



Use this logging mechanism when running on UNIX/Linux to support integration with syslog based system management.

No filtering is applied, and it will not include SQL/MDX even if native query logging has been enabled.

The configuration fields are as follows:

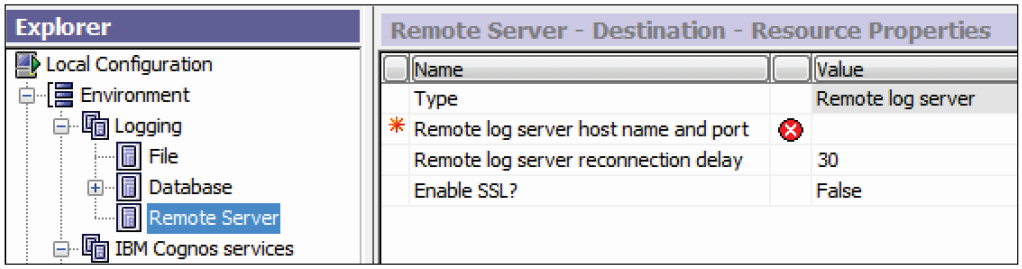
- Syslog host name: The name of the machine for the log file to be generated on.
- Syslog facility: The system component generating the system log. Possible values are KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, FTP, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7.

Business Analytics software

IBM

What is the Remote Log Server?

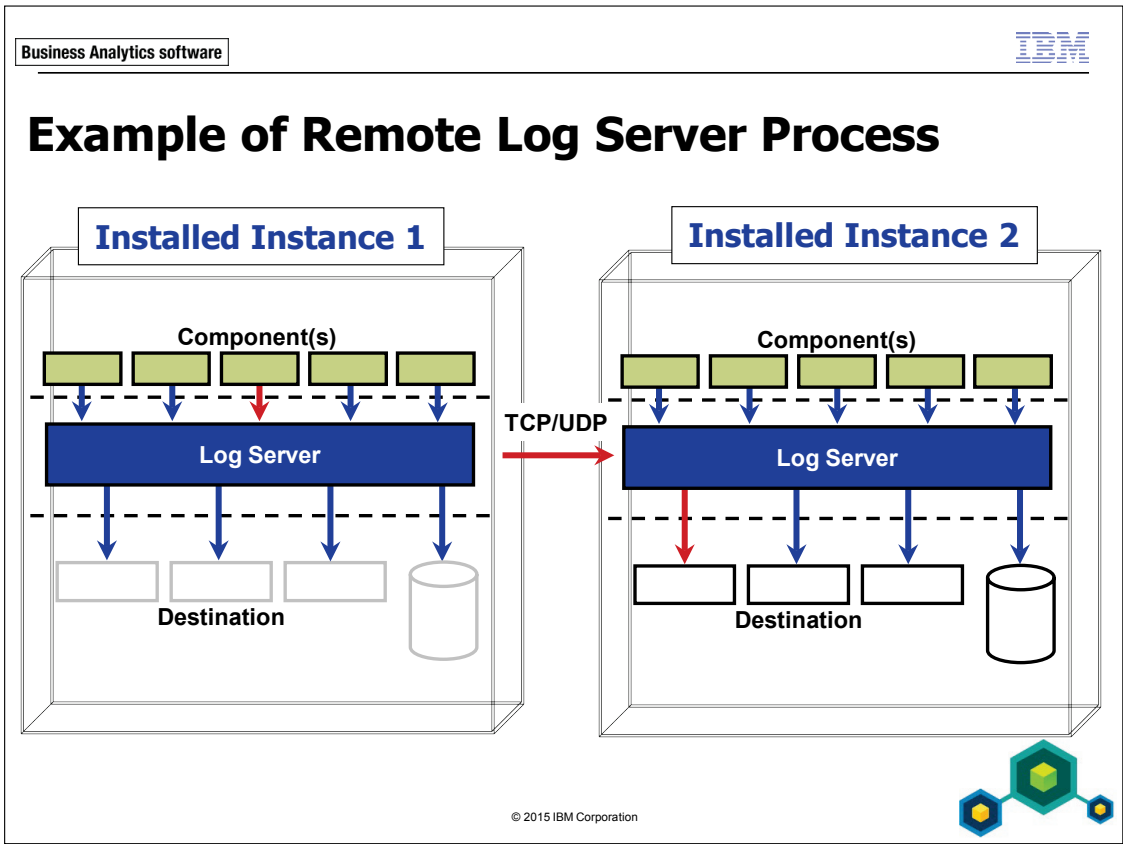
- sends locally generated audit logging messages to remote instance of Log Server through IP protocol
- no filtering
- federating logs is ambivalent



Use this method to collect and merge log messages from IBM Cognos 10 servers in a distributed install into one location. Log messages are sent to a remote instance of Log Server as UDP (User Datagram Protocol) by default, but could be sent by TCP as an alternative. SSL encryption can be applied.

No filters are applied, and all output is forwarded to the destination Log Server.

Federating, or joining logs is ambivalent, so you get the advantage of all logs in one location, but this will require more effort to identify an issue on a certain installed instance. It is suggested to keep local file based destinations and specify Remote Log Service destinations additionally. If the connection to the remote Log Server is lost, local recovery files will get created.



A component of installed instance 1 sends information to the local Log Service which sends it to the remote Log service on installed instance 2. Installed instances may not necessarily be on different servers. The Log service on installed instance 2 will send the info to one of the output destinations defined for installed instance 2.

Transmission is by TCP or UDP. TCP and UDP are both OSI layer 4 protocols and part of the Internet Protocols (IP) suite. While TCP is a reliable protocol which supports integrity checking, preserving the sequence of transmitted data and the confirmation from the receiver if the data was received completely, this is not supported by UDP. UDP is a protocol that sends the message and forgets about it on the client side. In practice UDP is faster but does not guarantee that data reaches the recipient in the right order or integrity. This can imply losing log messages or receiving them in the wrong order. Under high loads however, UDP might be a practical choice.

Workshop 1: Configure a Windows Event Log and Review Audit Information

You want to familiarize yourself with the information which is tracked in an audit database and logged to the cogserver.log file, and compare that to information logged in a Windows Event log for IBM Cognos 10. There is an audit database already configured in your environment which logs to cogserver.log, so you will have to configure a Windows Event log, and then run some activities in IBM Cognos 10, so that you can compare results between the two logs.

To do this you will:

- in IBM Cognos Configuration of the IBM Cognos 10 Full instance, create a new resource: Destination, named Windows7; type: Event log
- save the configuration, and restart the services
- perform activities such as running DQM reports in IBM Cognos 10 to populate the audit tables; logged on with admin/Education1 credentials (you will use DQM as this is the only server currently running, in the interest of time stopping and restarting the servers)
- review the logged results in Event Viewer
- review the logged results in C:\Program Files\IBM\cognos\c10_64full\logs\cogserver.log, using Microsoft Excel

For more information about where to work and the workshop results, refer to the Tasks and Results section that follows. If you need more information to complete a task, refer to earlier demos for detailed steps.

Workshop 1: Tasks and Results

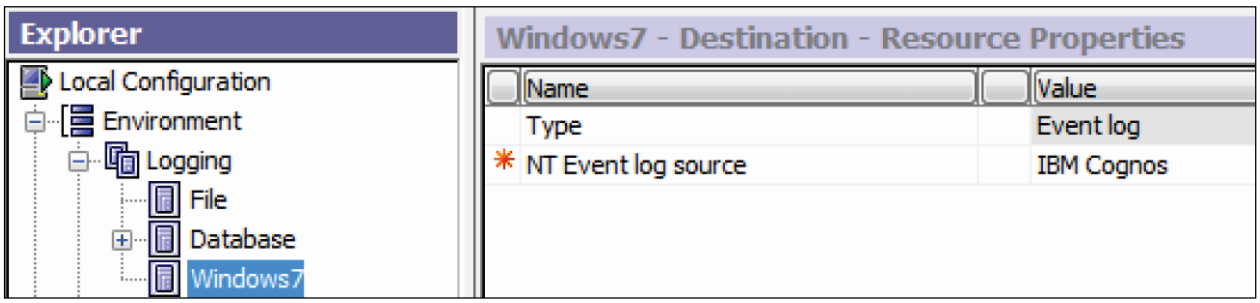
At the beginning of this workshop, the IBM Cognos Full:9315 dispatcher is running; the IBM Cognos DispCM:9320 dispatcher is not running. This is solely to reserve system resources. Stop the IBM Cognos DispCM:9320 dispatcher if it is running.

Task 1. Configure logging to the Windows Event log.

Currently, your environment is logging to an audit database, and you also want to log to a Windows destination, to compare the results.

- From the **Start** menu, click **All Programs**, click **IBM Cognos 10 - 64 Full**, and then click **IBM Cognos Configuration**.
- In the **Explorer** pane, navigate to **Environment\Logging**.
- Right-click **Logging**, click **New resource**, and then click **Destination**.
- In the **New Resource - Destination** dialog box, name the destination **Windows7**.
- From the **Type** list, select **Event log**, and then click **OK**.

  You have configured logging to the Windows Event log destination.



- Save the configuration and restart it, closing all messages that appear.

  Be patient, as it will take a few minutes for all the underlying services to restart. If the Lotus Domino Server (CProgramFilesx86IBMLotusDominodata) service is not running in the Services window, you will see a message in IBM Cognos Configuration indicating that the mail server cannot be reached. This is acceptable because you are not using the mail server at this time.

- Close **IBM Cognos Configuration** when the services have successfully started.

Task 2. Perform activities in IBM Cognos 10 to populate cogserver.log.

- Launch **Internet Explorer**, go to **http://vclassbase:88/C10Full**, log on to the **LDAP_Dev** namespace with **admin/Education1** credentials, and then launch **IBM Cognos Connection**.
- In **My Folders**, run the job called **Run Multiple Chart Reports DQM**.

  If you did not perform the demo earlier in this course that created this job, you can run a few random dynamic query reports of your choice. You have configured auditing for the 9315 dispatcher only, and that is the dispatcher which services dynamic queries, so run dynamic query reports to ensure results.

  When you run the job, you can monitor the execution by selecting the option to view run history details before clicking OK.
- After the reports run (this will take a few moments), close the browser window.

Task 3. Review the logged results in Event Viewer.

- To open **Event Viewer**, from the **Start** menu, navigate to **Control Panel\Administrative Tools**, and then double-click **Event Viewer**.
- Maximize the window, and then in the navigation pane on the left, expand the **Windows Logs** folder.

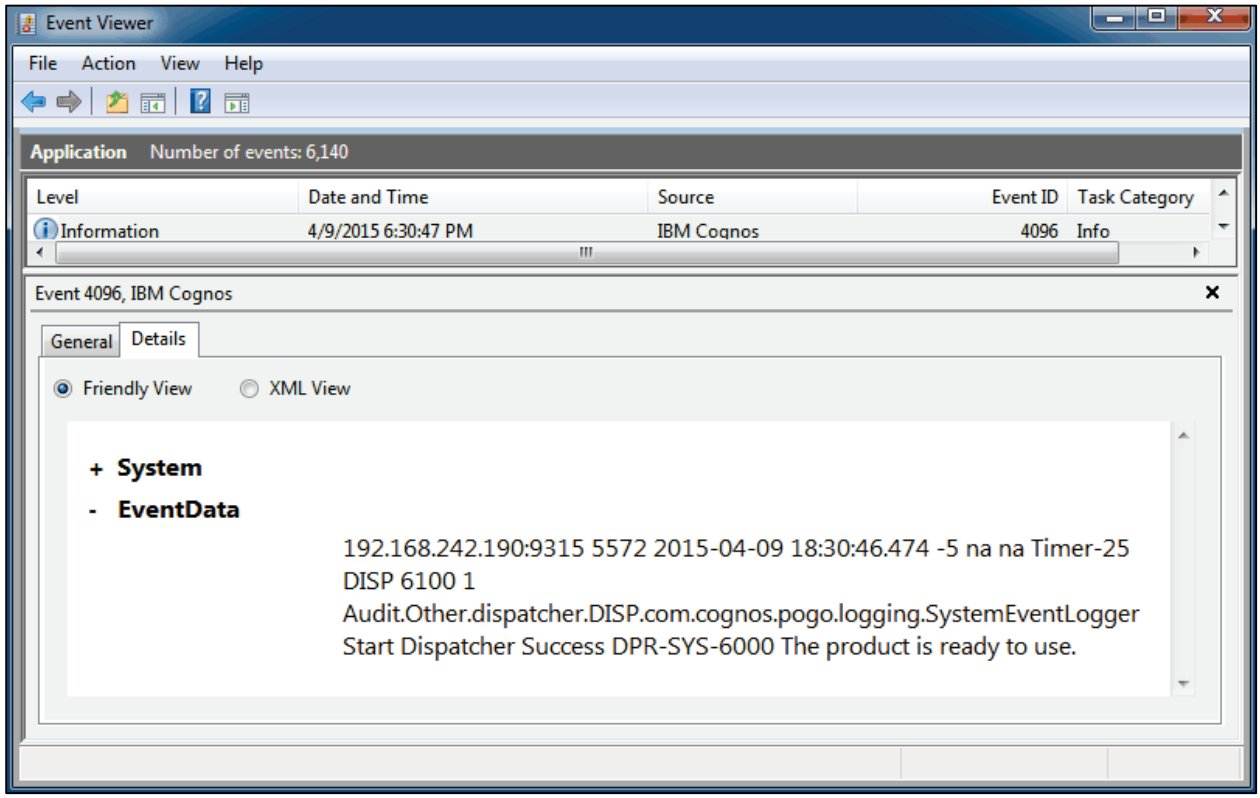
  There are five categories of messages for you to view: Application, Security, Setup, System, and Forwarded Events.
- Click **Application**.

  The logged entries are displayed. It may take some time for the entries to display.
- Under the **Source** column, double-click an **IBM Cognos** entry.

  The information is displayed for the entry.

- In the **Event Properties** window, click the **Details** tab, click **+** to expand **System**, review the information, and then close the **Event Properties** dialog box.

  The results appear similar to the following:



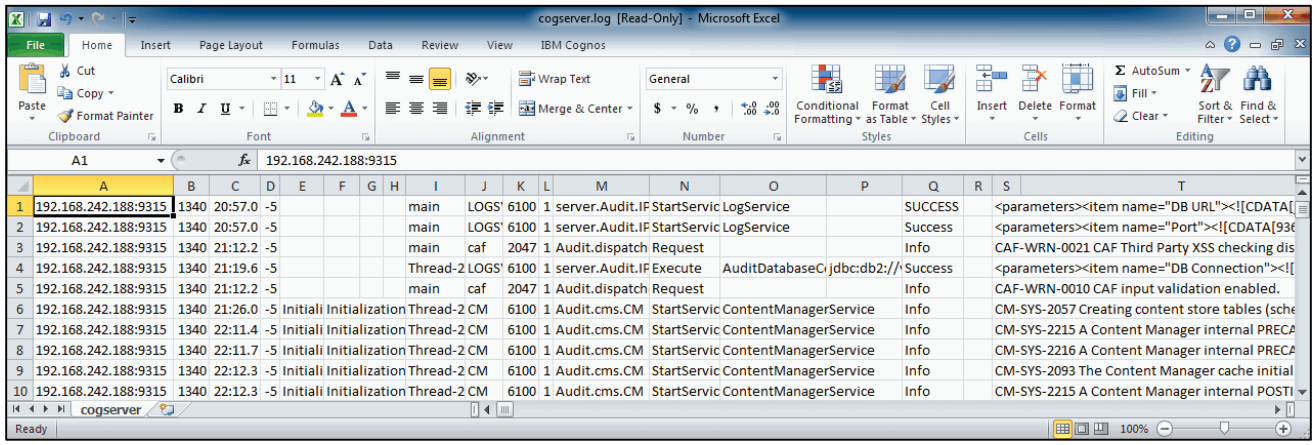
- Scroll through the list of entries in the **Application** pane, opening an IBM Cognos entry for each of the following types: **Information**, **Warning**, and **Error** (if applicable)
- When you have finished reviewing the events, close the **Event Viewer** window, close the **Administrative Tools** window, and then close the **Control Panel** window.

Task 4. Review the logged results in cogserver.log.

- Launch **Windows Explorer**, navigate to **C:\Program Files\IBM\cognos\c10_64full\logs**, and then open **cogserver.log** with **Microsoft Excel**.

  The file will be locked, as the server is using it, so open as read only when prompted. You may also be prompted about the file not loading completely; accept this message.

  The results appear similar to the following:



- Scroll through the messages, and notice that they include different information than what was tracked in the Windows Event log.

  The information tracked in cogserver.log is collected at a lower level of detail.

- When you have finished reviewing this file, close **Microsoft Excel** without saving changes, and then close **Windows Explorer**.

Business Analytics software

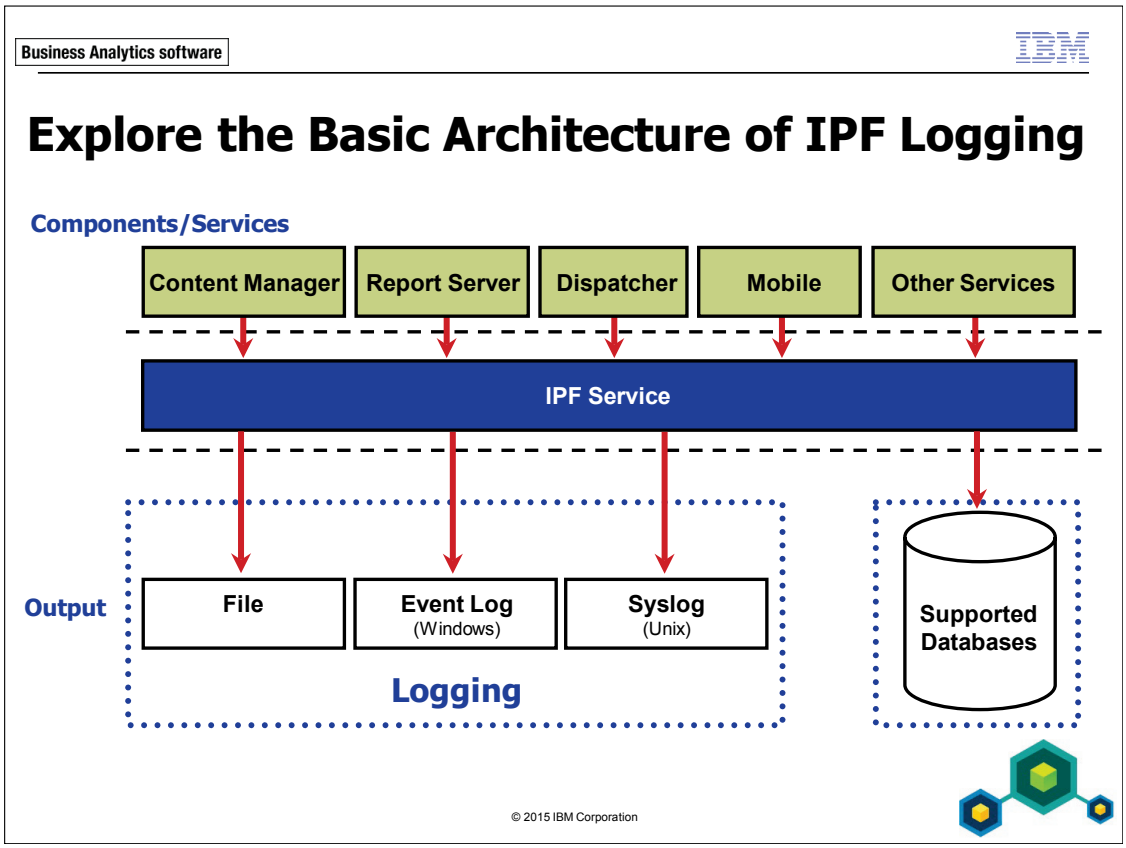
IBM

What is IPF Logging?

- based on Indication Processing Facility (IPF)
- IPF is thin wrapper around log4j
  - many applications use log4j as logging framework
  - update log4j default configuration file for applications that integrate with IBM Cognos 10 integrates
- Java and C++ interfaces
  - IBM Cognos interfaces

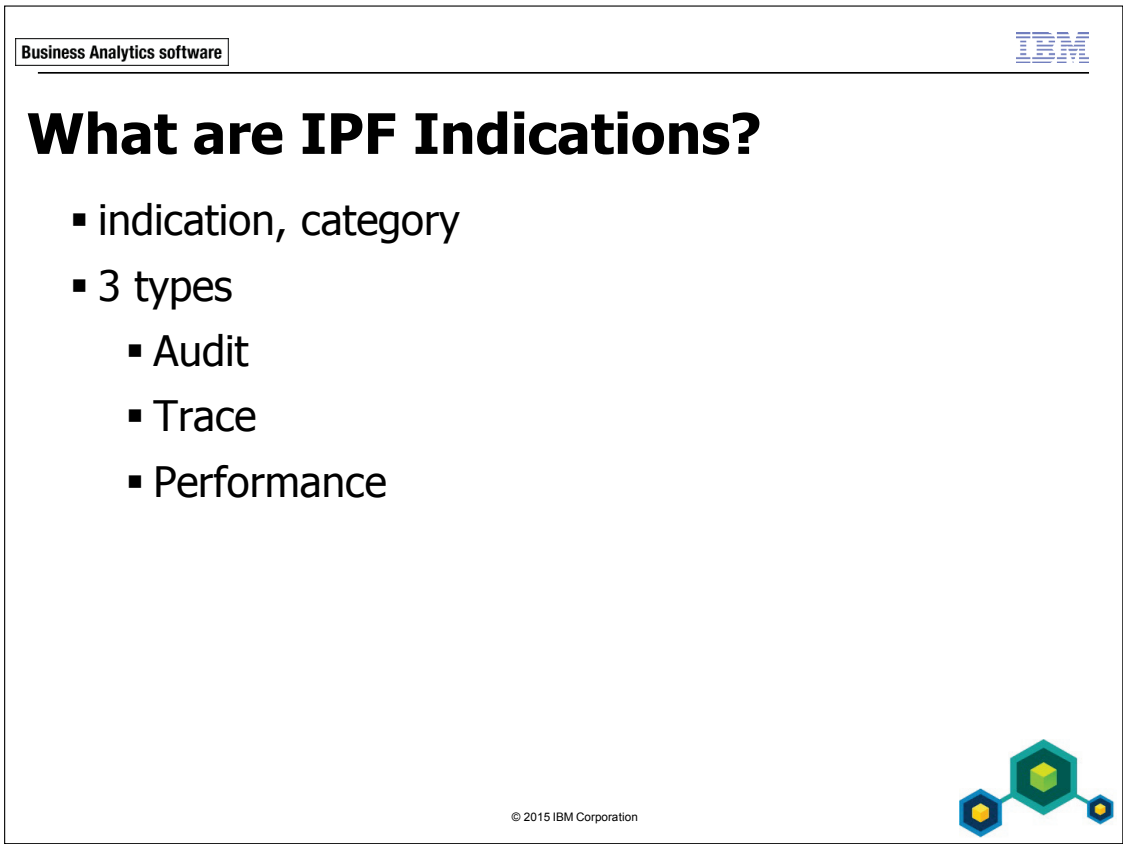
log4j is a Java-based logging utility that allows configuration of what information is output to log files. It is used primarily as a debugging tool, and is one of several Java logging frameworks. log4j is part of the Jakarta project of the Apache Software Foundation.

Although the Apache Jakarta Project has been retired, more information is available at http://jakarta.apache.org and http://logging.apache.org/log4j/1.2/.



IPF has a client-server architecture. The IPF Server is configured through IBM Cognos Configuration and IBM Cognos Connection, and IPF clients use their own configuration files.

In the diagram, the IPF Clients are the Components/Services.



Another word for indication is category. There are 3 types of indications:

- Audit: shows calls that are made from components
- Trace: shows what tasks and function calls are being performed
- Performance: shows the amount of system resources taken for a task

Business Analytics software

IBM

What are the Fields of Audit and Trace Indications?

- Host Identity
- Process ID
- Time
- TimeZone Offset
- Session ID
- Request ID
- SubRequest
- Step ID
- Thread ID
- Component ID
- Build Number
- Level
- Logger Name
- Operation
- Object Type
- Object Path
- Status
- Message
- Log Data

These fields are what is parsed out to logviewerV2.

Host Identity: Identifies the system on which the indication was generated. It is expressed as an IP address.

Process ID: The operating system assigned Process ID (PID). The Process ID provides information that aids in the analysis of process flow and the correlation of the actions within a component.

Time: Local system time of the event.

TimeZone Offset: Offset from GMT.

Session ID: Represents the session where the definition of a session is the lifetime of a passport ID and its passport.

Request ID: An ID representing the request.

SubRequest ID:	Subrequest ID of a component.
Step ID:	An ID representing the step within a job execution, otherwise it is empty.
Thread ID:	An ID representing the thread where the request is executing.
Component ID:	The four character name of the component generating the indication.
Build Number:	Build number of component.
Level:	Logging level that this indication was created with.
Logger Name:	Component that is processing the indication.
Operation:	Action being performed on an object.
Object Type:	Object on which the action is being performed. It depends on the context but often it will be the name of a service that the Component ID is calling.
Object Path:	Path of the object on which the action is being performed. This field is often empty but when populated it is usually a Content Store search path or a connection string.
Status:	Operations where a start and end indication are written.
Message:	Content of what was performed.

Business Analytics software

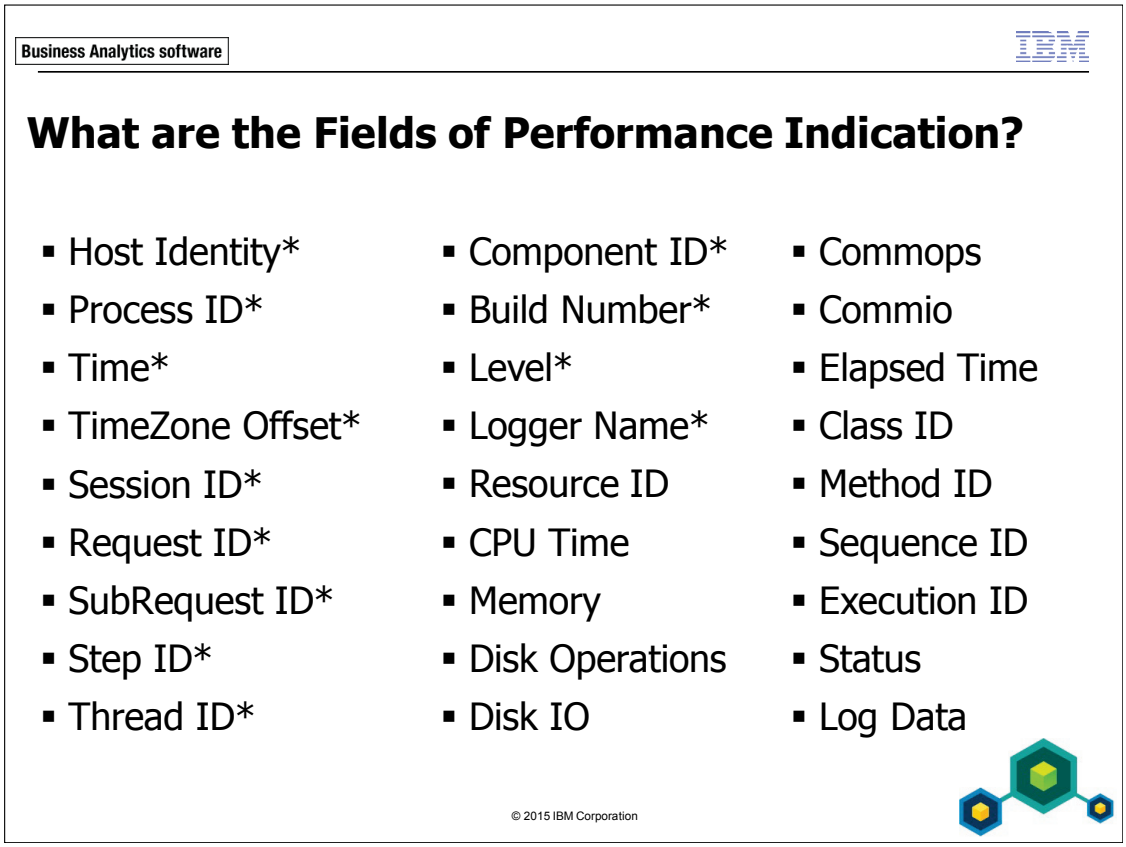
IBM

Applicability of Audit and Trace Indication Fields

Field Name	Minimal	Basic	Request	Trace	Full
Host Identity	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
Process ID	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
Time	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
TimeZone	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
Session ID	N/A	Mandatory	Mandatory	Mandatory	Mandatory
Request ID	Optional	Optional	Mandatory	Mandatory	Mandatory
SubRequestID	N/A	Optional, Conditional Mandatory*	Mandatory	Mandatory	Mandatory
StepID	N/A	N/A	Conditional Mandatory**	Conditional Mandatory**	Conditional Mandatory**
Thread ID	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
Component ID	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
Build Number	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
Level	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
LoggerName	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
operation	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
logData	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
objectType	Optional	Mandatory	Mandatory	N/A	N/A
objectPath	Optional	Optional	Mandatory	N/A	N/A
status	Mandatory	Mandatory	Mandatory	N/A	N/A
Message	Optional, Conditional Mandatory***	Optional, Conditional Mandatory***	Optional, Conditional Mandatory***	N/A	N/A

* if RequestID exists **only for jobs *** if error occurs

This indicates what fields will show in an indication for specific levels. N/A represents a field that is not applicable for the given level.



Fields with an asterisk are identical to audit and trace indications, and the other fields are specific to performance indications.

There are other logs and traces that do performance, such as Perf.QFS, UDA.

Resource ID: ID used for internal purposes

CPU Time: Amount of time used by the CPU for processing

Memory: Current memory used by object.

Disk Operations: Count of disk operations made by object.

Disk IO: Total bytes read and written by the object.

Commops: Count of network operations made by an object.

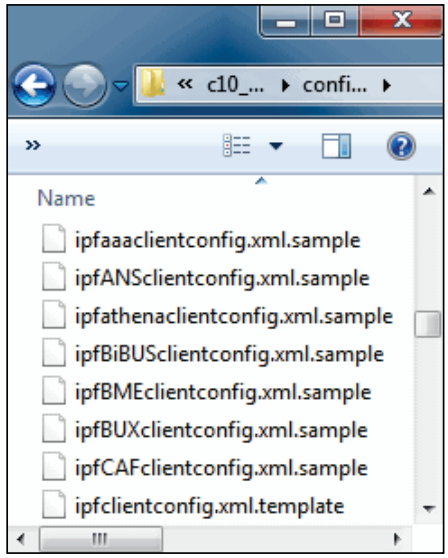
Commio:	Total bytes read and written over network links.
Elapsed time:	Amount time taken in total to process.
Class ID:	Name of object creating the indication.
Method ID:	The name of the method/function from where the indication is being generated.
Sequence ID:	Value to distinguish multiple indications being logged in the same context.
Execution ID:	Unique ID for the indication to distinguish a given indication from another due to a call to the same component.
Status:	Current action represented by the indication.
Log Data:	Any custom data that a component wants to log.

Business Analytics software

IBM

What are IPF Client Logs?

- component-specific IPF logs
- configuration files have the form ipfXXXXclientconfig where XXXX represents component name
- ipfClientConfig.xml
- files reside in ..\configuration folder



Component specific IPF logs cannot be configured in the IBM Cognos 10, but instead configuration is done to a file named ipfClientConfig.xml. As more IBM Cognos components are installed, more ipfXXXXclientconfig files will be installed. Some component specific IPF files may have different layouts or verbosity levels regarding comments in them. Most important though, is that they may differ in the way they are used. Some files require modification beyond renaming them to get output.

When employing internal IPF based logging, enabling a client configuration file will disable the audit logging configured, including audit DB.

IPF Client logs can be useful to troubleshoot components (all tracing and debugging), or to troubleshoot performance issues of a component.

Business Analytics software

IBM

Explain IPF Client Logging (1 of 2)

- IPF maintains watch on the ipfclientconfig.xml file pinging for it every 60 seconds
- rename the required ipfXXXXclientconfig.xml.sample file to ipfclientconfig.xml
- if ipfclientconfig.xml file is found, logging instantly is reconfigured according to file contents
- logs tracing and performance indications

It is best practice to make a copy of the ipfXXXXclientconfig.xml.sample first before you rename (and edit) the required ipfXXXXclientconfig.xml.sample file to ipfclientconfig.xml.

If the ipfclientconfig.xml file is found, logging in the system is automatically reconfigured according to file contents and no restart of IBM Cognos 10 is required. To disable the logging, rename the file back to what it was before it was renamed to ipfclientconfig.xml.

Only Tracing and Performance indications are generally logged in IPF client logging. Audit indications must be explicitly enabled and special configuration must be applied so that Audit indications are sent back to the IPF Server where they are properly written to the configured Audit output targets.

Business Analytics software

IBM

Explain IPF Client Logging (2 of 2)

- client configurations impose complete override of audit logging settings
- mapping file (..\configuration\ipfstartup.xml) loaded at LogService startup maps services to components

```
<service id="dispatcher">
  <component id="DISP"/>
  <component id="dispatcher"/>
  <component id="CAF"/>
</service>
```

Mapping file

Client configurations impose a complete override of the audit logging settings. Audit logging configures the IPF Server only and does so only for audit categories, and ipfclientconfig.xml overrides at the IPF Client.

You may need to customize an ipfclientconfig.xml file to incorporate the audit logging settings to have tracing and audit logging in parallel. Changes to the files may be required if your are not running in Tomcat, or if the default log port has been changed.

If Audit logging been enabled, it is best to try to replicate issues in a non-production environment, so that IPF client logs can be taken without impacting the audit information in the production environment.

Audit logging is simply a UI-enabled subset of IPF functionality. Internal logging is more sophisticated and detailed, and its main purpose is for troubleshooting.

Business Analytics software

When to Use ipfXXXXclientconfig.xml (1 of 2)

Component	File to Use	Helps Troubleshoot
DISP	ipfdispclientconfig.xml.sample	Start-up problems (including services started by the Dispatcher), load balancing, performance
BIBUS	ipfBiBusclientconfig.xml.sample	Low level communication between Dispatchers and Report Services
CM	ipfCMclientconfig.xml.sample	Content Store database access problems
CRP	ipfcryptoclientconfig.xml.sample	Keystore access and synchronization, access to AutoCA, SSL/Trust issues, Trusted Request problems
AAA	ipfaaaclientconfig.xml.sample	Security issues
CAF	ipfCAFclientconfig.xml.sample	Database access problems, get error details strip by the CAF secure error feature, get details about CAF validation failures, get textual descriptions of CAF configuration failures, debug CAF internal failures
XTS	ipfXTSclientconfig.xml.sample	Query Studio UI issues, Cognos Portal Service (CPS) issues, Agent Studio UI issues
JSM, DLS, JS, MS, ASV, EMS	ipfSDSclientconfig.xml.sample	Scheduling (JSM, JS), E-mail delivery (DLS), Agents (ASV), Future scheduled events or schedules (EMS), Background tasks currently running (MS)

Business Analytics software

IBM

When to Use ipfXXXXclientconfig.xml (2 of 2)

Component	File to Use	Helps Troubleshoot
RSVP	ipfRSVPclientconfig.xml.sample	Report Service / Batch Report Service, reports and queries, performance
CQE	ipfCQEclientconfig.xml.sample	See notes
MDDS	ipfMDDSconfig.xml.sample	Interaction with 3rd party OLAP providers such as SAP, MSAS and DB2OLAP
UDA	ipfUDAclientconfig.xml.sample	Runtime Queries
CRX	ipfCRXclientconfig.xml.sample	Report Expressions
DMB	ipfDMBclientconfig.xml	See notes
FM	ipfFMclientconfig.xml.sample	Framework Manager
ANS	ipfANSclientconfig.xml.sample	Analysis Studio issues
XQE	ipfXQEclientconfig.xml.sample	Dynamic Query Mode issues
BUX	ipfBUXclientconfig.xml.sample	Cognos Workspace specific issues
HTS	ipfHTSclientconfig.xml.sample	Human Task Service issues
MOB	ipfMOBclientconfig.xml.sample	Cognos Mobile issues

For CQE troubleshooting using the ipfCQEclientconfig.xml.sample file:

- Trace logging records the input received by CQE (such as governor settings), warnings, and detailed information about input query translation to CQE internal logical and physical query trees.
- Performance logging records the time spent in CQE functions.
- Audit logging records all CQE query service API calls.

For DMB (Dynamic Molap Builder) troubleshooting using the ipfDMBclientconfig.xml file:

- Audit data: Audit.RTUsage.DAM.DMB records information about Public API function call (names and parameters): the XML model definition, the data streams, and the request to build the cube.
- Trace data: Trace.DAM.DMB records information about the Exceptions thrown in DMB, policy implementation, and specific failures.
- Performance data: Perf.DAM.DMB records information about the time spent to build the cube (time spent in DMB and PPDS).

Business Analytics software

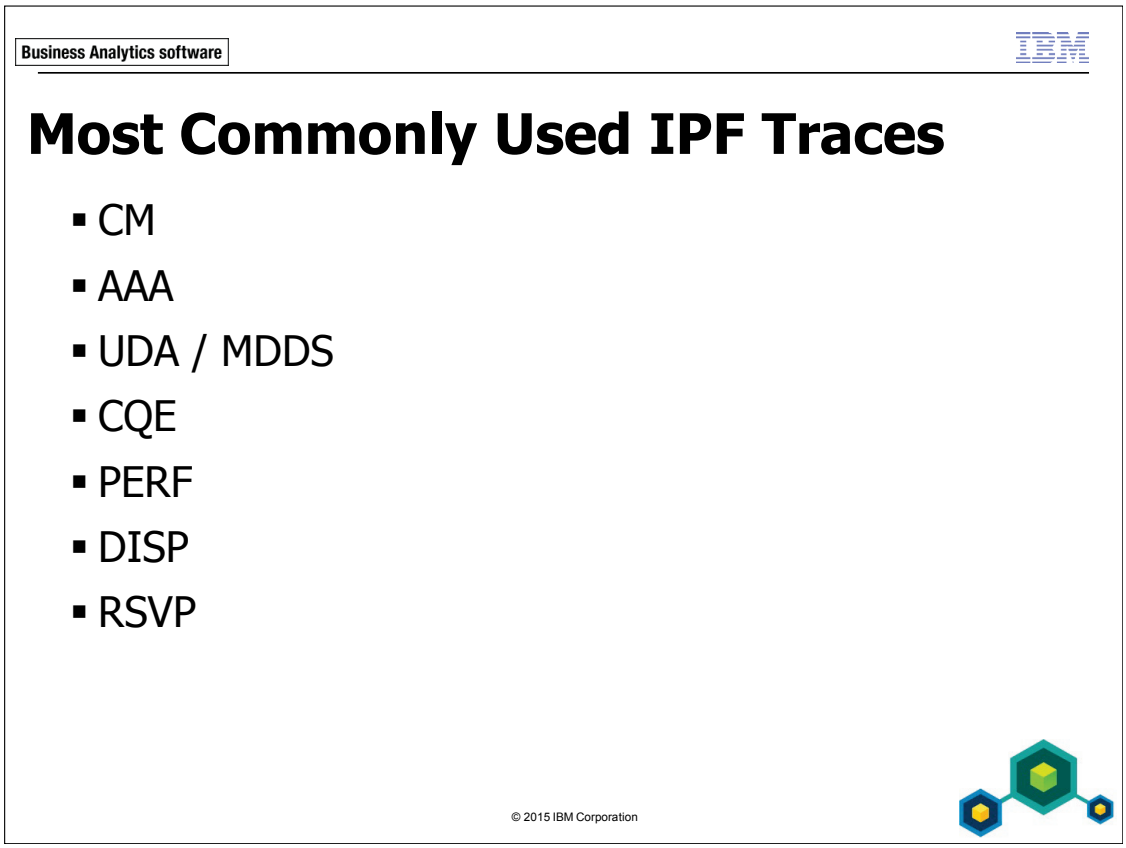
IBM

Describe SDS Logging

- ipfSDSclientconfig controls logging of several services
- to turn on trace logging for the Agent Service in ipfSDSclientconfig.xml
  - search for <level value="warn">
  - change <level value="warn"> to <level value="debug">

```
<category name="Trace.ASV" class="com.cognos.indications.LogTypedLogger">
                <level value="warn"/>
                <appender-ref ref="clientFlatFile"/>
</category>
```


The slide provides an example of turning on trace logging for the Agent service.



These are the most common IPF traces that are used on a regular basis.

Some new IPF Client files as of IBM Cognos 10.2.0 include: XQE, BUX, HTS, SPSS.

Business Analytics software

IBM

Summary

- At the end of this module, you should be able to:
  - describe installation logs and configuration logs
  - explore audit logging
  - explore IPF logging

Workshop 2: Configure IPF Logging

You need to configure log files to get additional logging information for Cognos 10 components. These log files are useful in getting additional information for specific Cognos 10 Components. Specifically, you will implement IPF logging on the dispatcher and Content Manager components. You will be working with the IBM Cognos 10 - 64 Full instance only, in this workshop.

To do this you will:

- open ipfdispclientconfig.xml in Internet Explorer, examine elements of the file, and focus on the <appender> sections, noting the target file names and locations
    - What is the difference between the <appender> sections named fileWithFilter and clientFlatFile?
- implement IPF logging on the dispatcher
    - stop services for the IBM Cognos Full:9315 instance
    - rename the file appropriately and start the services
    - stop services and examine the log file in Microsoft Excel
    - disable IPF logging on the dispatcher
- repeat as above for the Content Manager using the ipfCMclientconfig.xml file

For more information about where to work and the workshop results, refer to the Tasks and Results section that follows. If you need more information to complete a task, refer to earlier demos for detailed steps.

Workshop 2: Tasks and Results

At the beginning of this workshop, the IBM Cognos Full:9315 dispatcher is running; the IBM Cognos DispCM:9320 dispatcher is not running. This is solely to reserve system resources.

Task 1. Open the ipfdispclientconfig.xml file and examine the elements of the file.

When IPF logging is implemented on the ipfdispclientconfig.xml file, it can be used to troubleshoot start-up problems, including services started by the dispatcher, load balancing issues, and performance issues.

- In **Windows Explorer**, navigate to **C:\Program Files\IBM\cognos\c10_64full\configuration**, copy **ipfdispclientconfig.xml.sample**, and then paste to the same directory.
- Rename **ipfdispclientconfig.xml - Copy.sample** to **ipfdispclientconfig.xml**, from the file properties, ensure that the **Read-only** attribute is not selected, and then open the file in **Internet Explorer** (iexplore.exe).

  If the Information Bar displays a message about running scripts, click the Information Bar, click Allow Blocked Content, and then click Yes.

- Locate the following section:

```
- <appender class="org.apache.log4j.RollingFileAppender"
name="fileWithFilter">
  <param name="File" value="../logs/crnclientWarn.log"/>
  <param name="MaxBackupIndex" value="1"/>
  <param name="MaximumFileSize" value="10485760"/>
- <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%m%n"/>
  </layout>
- <filter class="org.apache.log4j.varia.LevelRangeFilter">
    <param name="LevelMin" value="WARN"/>
    <param name="LevelMax" value="WARN"/>
  </filter>
</appender>
```

  This section is used to define a log file that includes a filter as defined by **<param name="LevelMin" value="WARN" />** and **<param name="LevelMax" value="WARN" />**. As a result this file will only capture WARN messages if they are generated.

- Locate the following section:

```
<appender class="org.apache.log4j.RollingFileAppender"
name="clientFlatFile" >
  <param name="File" value="../logs/crnclient.log"/>
  <param name="MaxBackupIndex" value="1"/>
  <param name="MaximumFileSize" value="10485760"/>
- <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%m%n" />
  </layout>
</appender>
```

  This section is used to define a log file that is not filtered. As a result this file will capture WARN messages and all lower messages, such as STOP and START, if they are generated.

  Notice that both sections include parameters for defining:

  - a target file name and location for log output, for example:
    - <param name="File" value="../logs/crnclient.log" />
  - file properties, for example:
    - **<param name="MaxBackupIndex" value="1" />** - maximum number of log files that will ever exist
    - **<param name="MaximumFileSize" value="10485760" />** - maximum size of the log file in KB

    Note: With these property settings, when the file reaches its maximum size, log data begins to be overwritten. If MaxBackupIndex value is set to > 1, then once the maximum file size is reached additional log files will be created as <name>.log.1, <name>.log.2, <name>.log.3 depending on the set value.

- Close **Internet Explorer**.

Task 2. Implement IPF logging on the dispatcher using ipfdispclientconfig.xml.

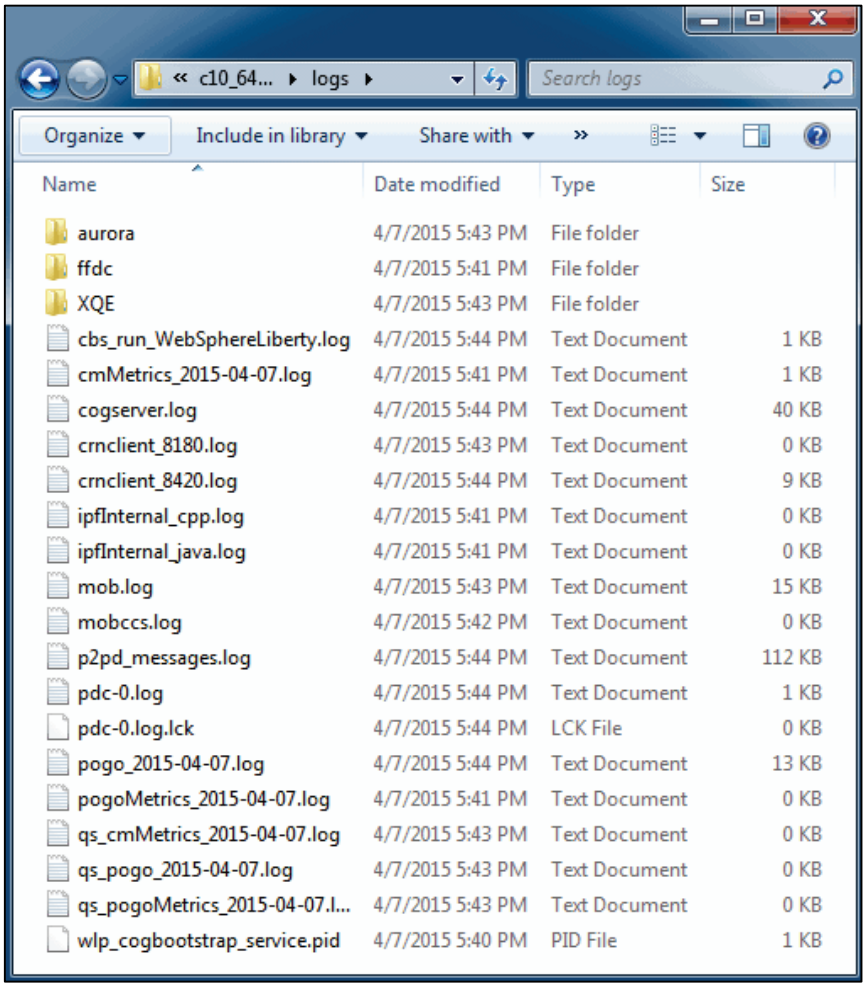
- On the **Taskbar**, click **Services**, and then stop **the IBM Cognos Full:9315** service.
- In **Windows Explorer**, rename **ipfdispclientconfig.xml** to **ipfclientconfig.xml**.
- Navigate to **C:\Program Files\IBM\cognos\c10_64full\logs**.
- Delete all files from the root of the **logs** folder, and then start the **IBM Cognos Full:9315** service.

  Do not delete the XQE directory or its contents.

  If a message displays, indicating that the service did not start in a timely fashion, click OK to dismiss this message. Wait until this instance has fully started (you may do a refresh of the display every two minutes) before proceeding to the next step.

- When the service has successfully started, navigate to **C:\Program Files\IBM\cognos\c10_64full\logs** to identify the log files that are generated as a result of the start operation, including the **crnclient_xxxx.log** files.

  The results appear similar to those shown below:



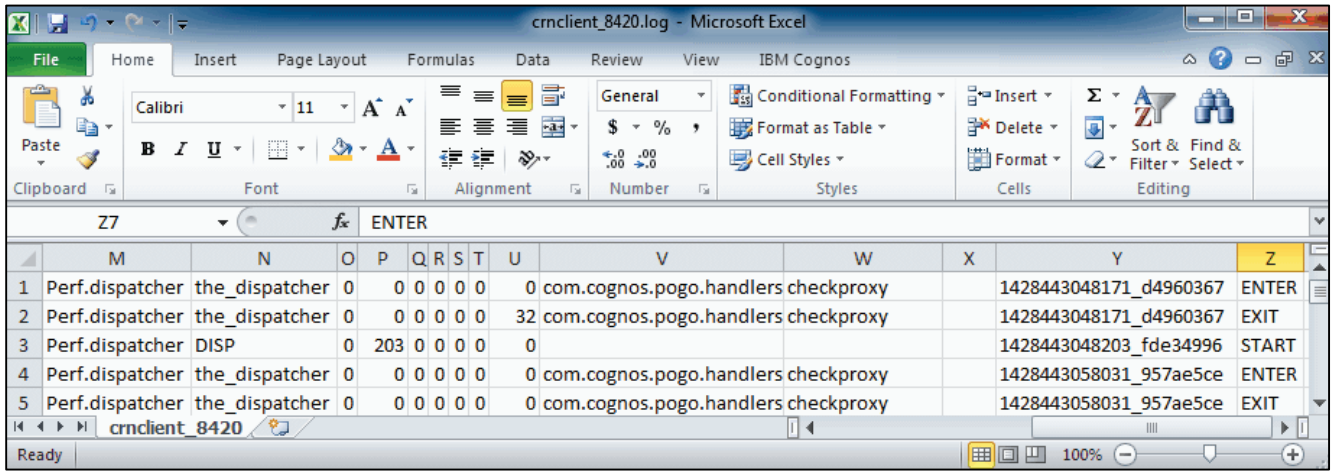
- Stop the **IBM Cognos Full:9315** service.
- Open the most recent **crnclient_xxxx.log** file with **Microsoft Excel** (the other crnclient_xxxx.log file will be empty).

  If an activation message appears for Microsoft Excel, dismiss the message, and continue.

  In Microsoft Excel, you may have to click the crnclient_xxxx tab to see the results display.

  At this point the crnclient_xxxx.log file contains start up information only, as that is the only operation you have performed. Notice that columns map to the indication fields seen earlier in the content of this module.

The results appear similar to the following:



	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	Perf.dispatcher	the_dispatcher	0	0	0	0	0	0	0	com.cognos.pogo.handlers	checkproxy		1428443048171_d4960367	ENTER
2	Perf.dispatcher	the_dispatcher	0	0	0	0	0	0	32	com.cognos.pogo.handlers	checkproxy		1428443048171_d4960367	EXIT
3	Perf.dispatcher	DISP	0	203	0	0	0	0	0				1428443048203_fde34996	START
4	Perf.dispatcher	the_dispatcher	0	0	0	0	0	0	0	com.cognos.pogo.handlers	checkproxy		1428443058031_957ae5ce	ENTER
5	Perf.dispatcher	the_dispatcher	0	0	0	0	0	0	0	com.cognos.pogo.handlers	checkproxy		1428443058031_957ae5ce	EXIT

- Close **Microsoft Excel** without saving changes.
- At **C:\Program Files\ibm\cognos\c10_64full\configuration**, delete the **ipfclientconfig.xml** file.

Task 3. Open the ipfCMclientconfig.xml file and examine the elements of the file.

- Copy **ipfCMclientconfig.xml.sample** and paste to the same directory.
- Rename **ipfCMclientconfig.xml - Copy.sample** to **ipfCMclientconfig.xml**, and then open it in **Internet Explorer**.

  Disregard the running scripts message if it appears in the browser, or allow the blocked content.

- Locate the following section:

```
  <appender class="org.apache.log4j.RollingFileAppender"
name="cmFlatFile">
  <param name="File" value="../logs/cm_trace.log"/>
  <param name="MaxBackupIndex" value="1"/>
  <param name="MaximumFileSize" value="10485760"/>
- <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%m%n"/>
  </layout>
  </appender>
```

  Again, notice that this section includes parameters for defining a target file name and location for log output, and file properties.

- Close **Internet Explorer**.

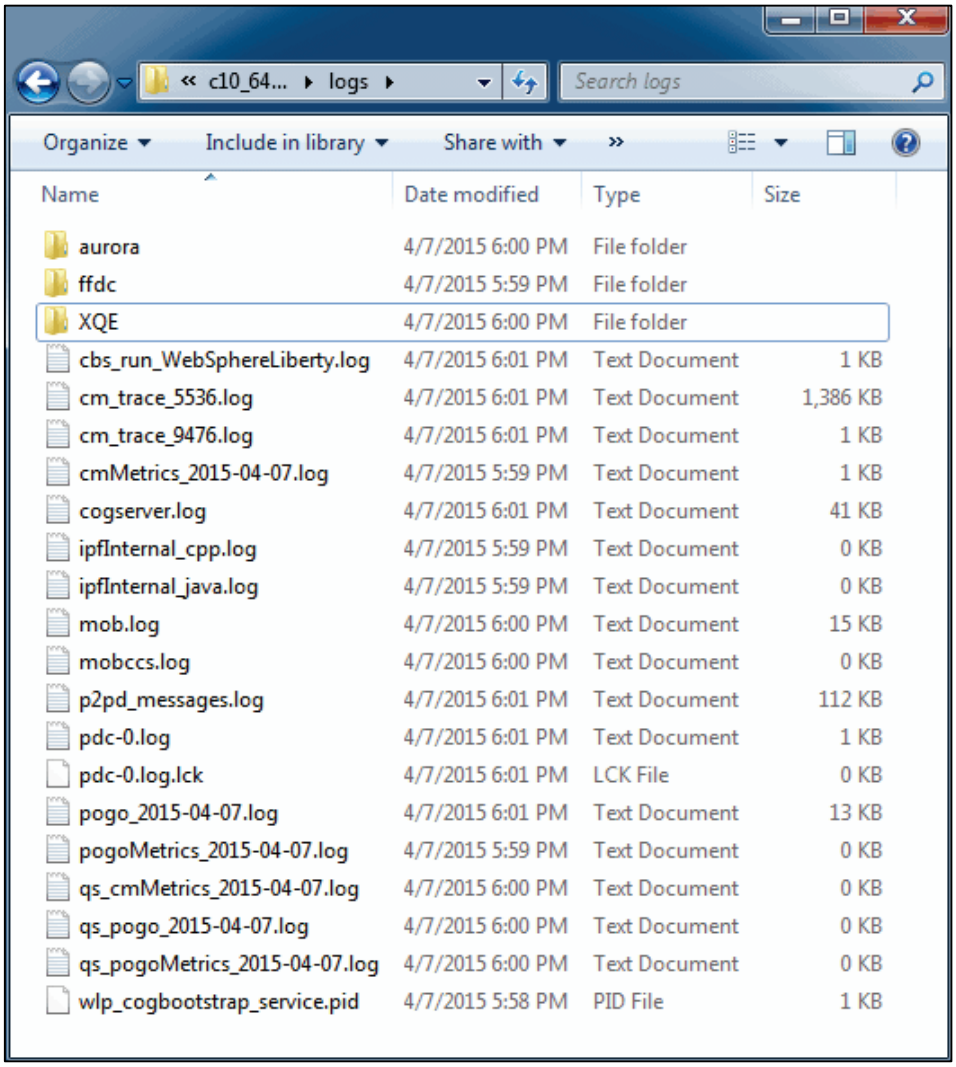
Task 4. Implement logging on the Content Manager using ipfCMclientconfig.xml.

- Open the **Services** window and ensure that the **IBM Cognos Full:9315** service is not running (stop it if necessary).
- In **Windows Explorer**, rename **ipfCMclientconfig.xml** to **ipfclientconfig.xml**.
- Navigate to **C:\Program Files\ibm\cognos\c10_64full\logs**, and then delete all files from the root of the **logs** folder.

  Do not delete the XQE directory or its contents.
- Start the **IBM Cognos Full:9315** service.

- When the service has successfully started, navigate to **C:\Program Files\IBM\cognos\c10_64full\logs** to identify the log files that are generated as a result of the start operation, including the **cm_trace_xxxx.log** files.

  The results appear similar to the following:

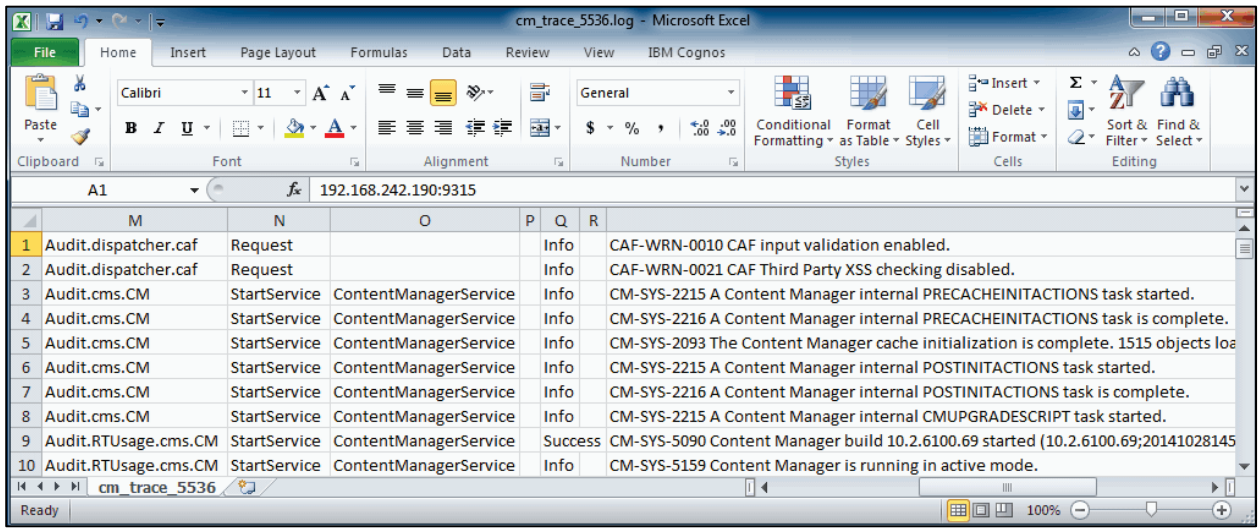


- Stop the **IBM Cognos Full:9315** service, and when it has stopped, open the largest **cm_trace_xxxx.log** file in **Microsoft Excel**, and review the contents.

  If an activation message appears for Microsoft Excel, dismiss the message, and continue.

  At this point the cm_trace_xxxx.log file contains start up information only, as that is the only operation you have performed. Again, notice that columns map to the indication fields seen earlier in this module.

  The results appear similar to those shown below:



	M	N	O	P	Q	R	
1	Audit.dispatcher.caf	Request			Info		CAF-WRN-0010 CAF input validation enabled.
2	Audit.dispatcher.caf	Request			Info		CAF-WRN-0021 CAF Third Party XSS checking disabled.
3	Audit.cms.CM	StartService	ContentManagerService		Info		CM-SYS-2215 A Content Manager internal PRECACHEINITACTIONS task started.
4	Audit.cms.CM	StartService	ContentManagerService		Info		CM-SYS-2216 A Content Manager internal PRECACHEINITACTIONS task is complete.
5	Audit.cms.CM	StartService	ContentManagerService		Info		CM-SYS-2093 The Content Manager cache initialization is complete. 1515 objects loa
6	Audit.cms.CM	StartService	ContentManagerService		Info		CM-SYS-2215 A Content Manager internal POSTINITACTIONS task started.
7	Audit.cms.CM	StartService	ContentManagerService		Info		CM-SYS-2216 A Content Manager internal POSTINITACTIONS task is complete.
8	Audit.cms.CM	StartService	ContentManagerService		Info		CM-SYS-2215 A Content Manager internal CMUPGRADESCRIPT task started.
9	Audit.RTUsage.cms.CM	StartService	ContentManagerService		Success		CM-SYS-5090 Content Manager build 10.2.6100.69 started (10.2.6100.69;20141028145
10	Audit.RTUsage.cms.CM	StartService	ContentManagerService		Info		CM-SYS-5159 Content Manager is running in active mode.

  Note: If you see messages regarding "runTimeState" is unknown, it could be due to the dispatcher being too busy when starting, to be able to return a value.

- Close **Microsoft Excel** without saving.
- At **C:\Program Files\ibm\cognos\c10_64full\configuration**, delete the **ipfclientconfig.xml** file.

  Leave the IBM Cognos Full:9315 service stopped for the next module.

- Close all open windows