

IBM Cognos Open Mic Notification and Auditing in Cognos BI



3rd July, 2013

IBM Cognos Open Mic Team



Gracy Mendonca – IBM Cognos Support Engineer

Presenter / Facilitator



Amit Desai – IBM Cognos Support Engineer

Technical Panel Member

Agenda

Audit Store:

1. What is an audit store and what kind of information is stored in it ?
2. How to configure an audit store ?
3. How to create your own Audit package and create reports ?
4. Simple checks that can be looked into when auditing stops working.

Notification Store:

1. What is a notification store? What kind of information is stored in it?
2. How to config a Notification Store ?
3. What is a NC drop script ?
4. Symptoms that indicate a problem in the Notification Store Configuration.

Note: All screen shots are with reference to Cognos BI 10.2

What is a Cognos Audit Store?

IBM Cognos Platform provides a complete auditing capability that permits administrators to report on and manage system usage.

By default, system messages, errors, and other product details are logged to flat files that reside in the <c8_install>/logs directory.

Although the information provides the ability to identify possible errors that have occurred in the environment, the information is volatile because of the versioning mechanism (that is, file rollover parameter in IBM Cognos Configuration).

6 Simple Steps to Configure Auditing

Step 1:

- Create a new DB or new schema inside an existing DB on the Database server that will be used for audit information logging.
- It has the same specification as the content store.

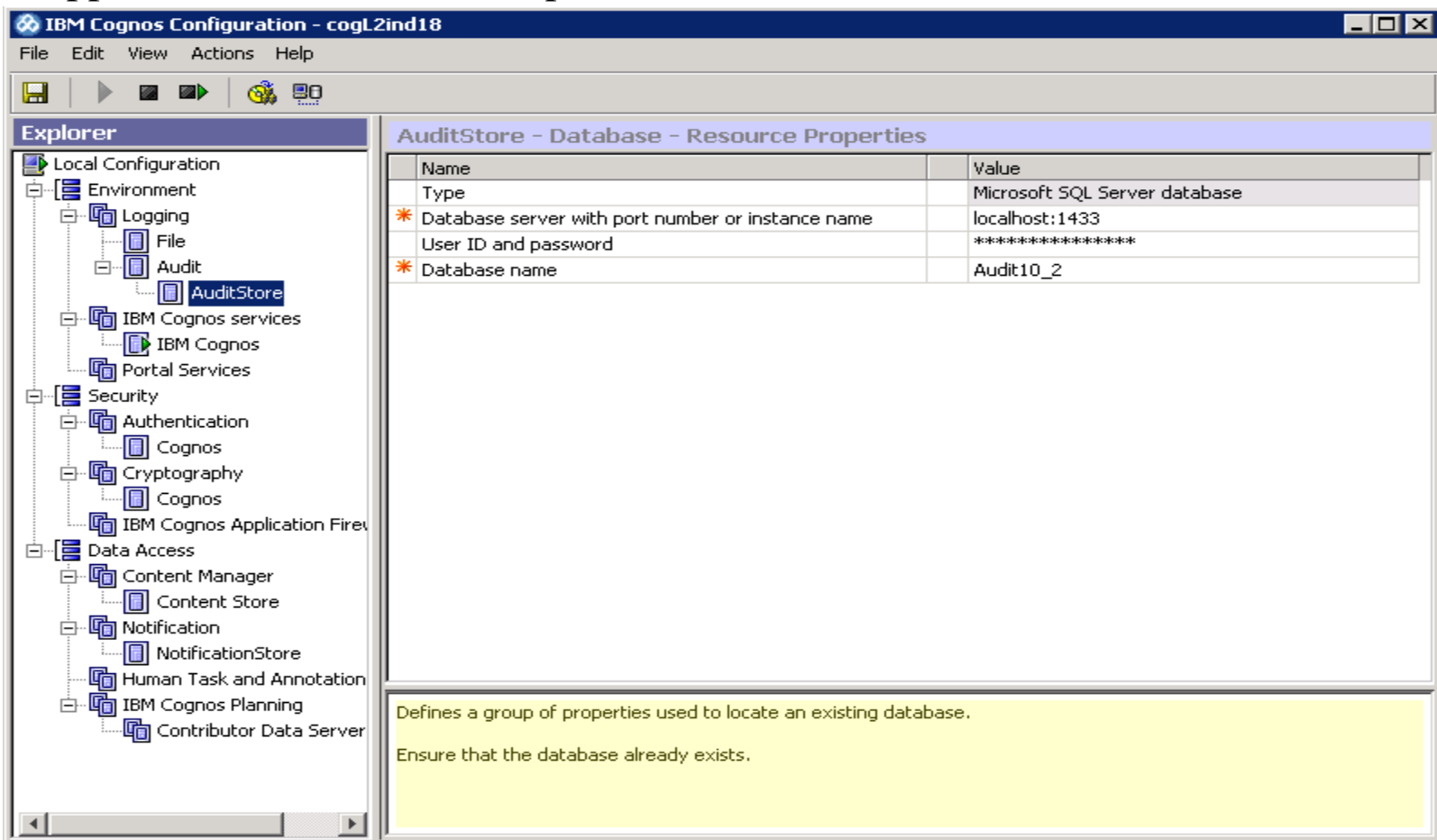
Details to create an audit store can be found on Page 265 of the Installation and Configuration Guide of 10.2

- In a distributed environment, the local log server on an Application Tier Component computer sends log messages to the logging database.
- For Oracle, Sybase, and DB2, the appropriate JDBC driver and database client software (DB2 only) is required only on the Application Tier Components computer with the remote log server that connects to the logging database.

6 Simple Steps to Configure Auditing

Step 2 :

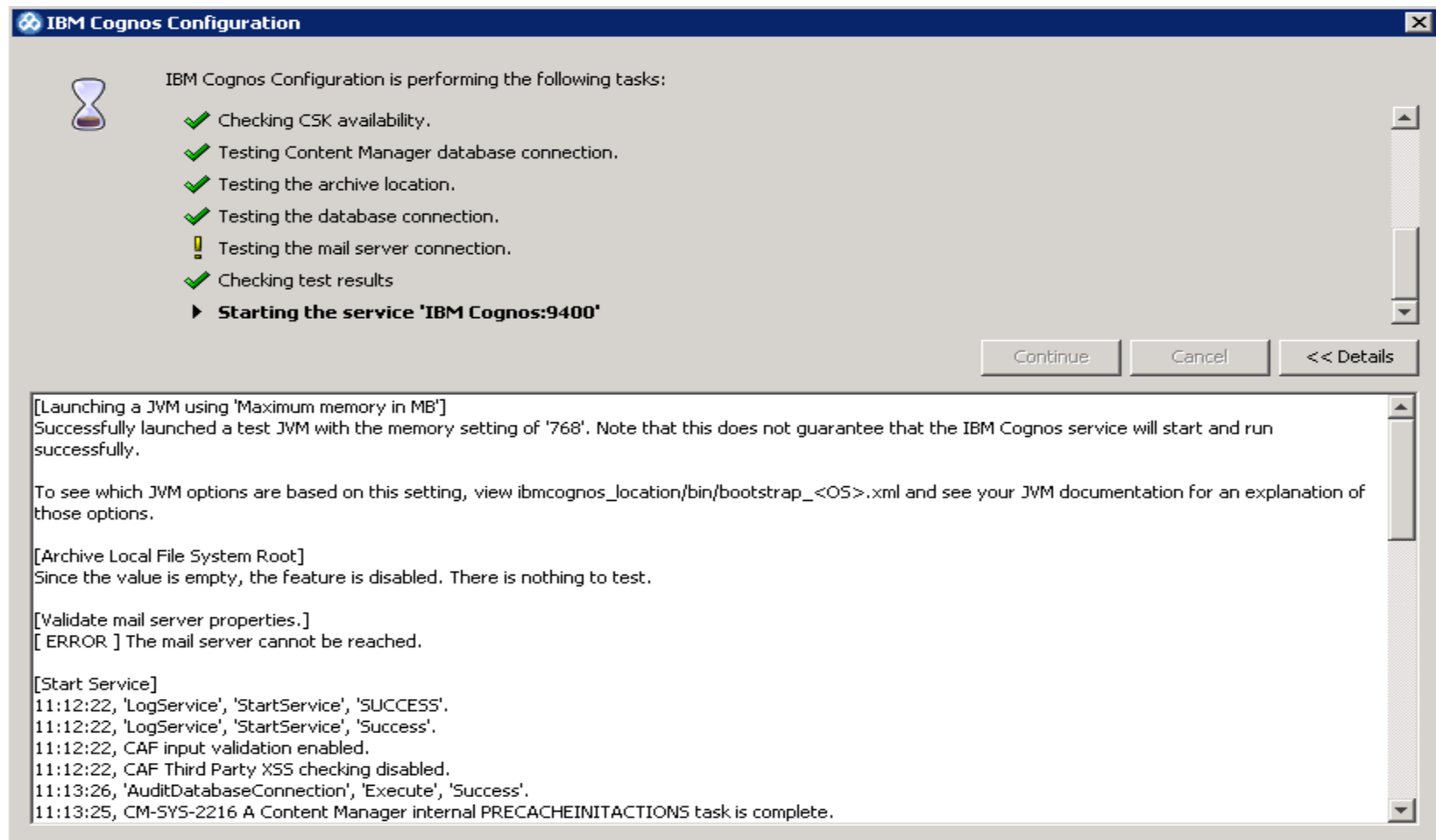
Configure it in Cognos Configuration of every Content Manager (active and standby) and Application Tier machine(dispatcher)



6 Simple Steps to Configure Auditing

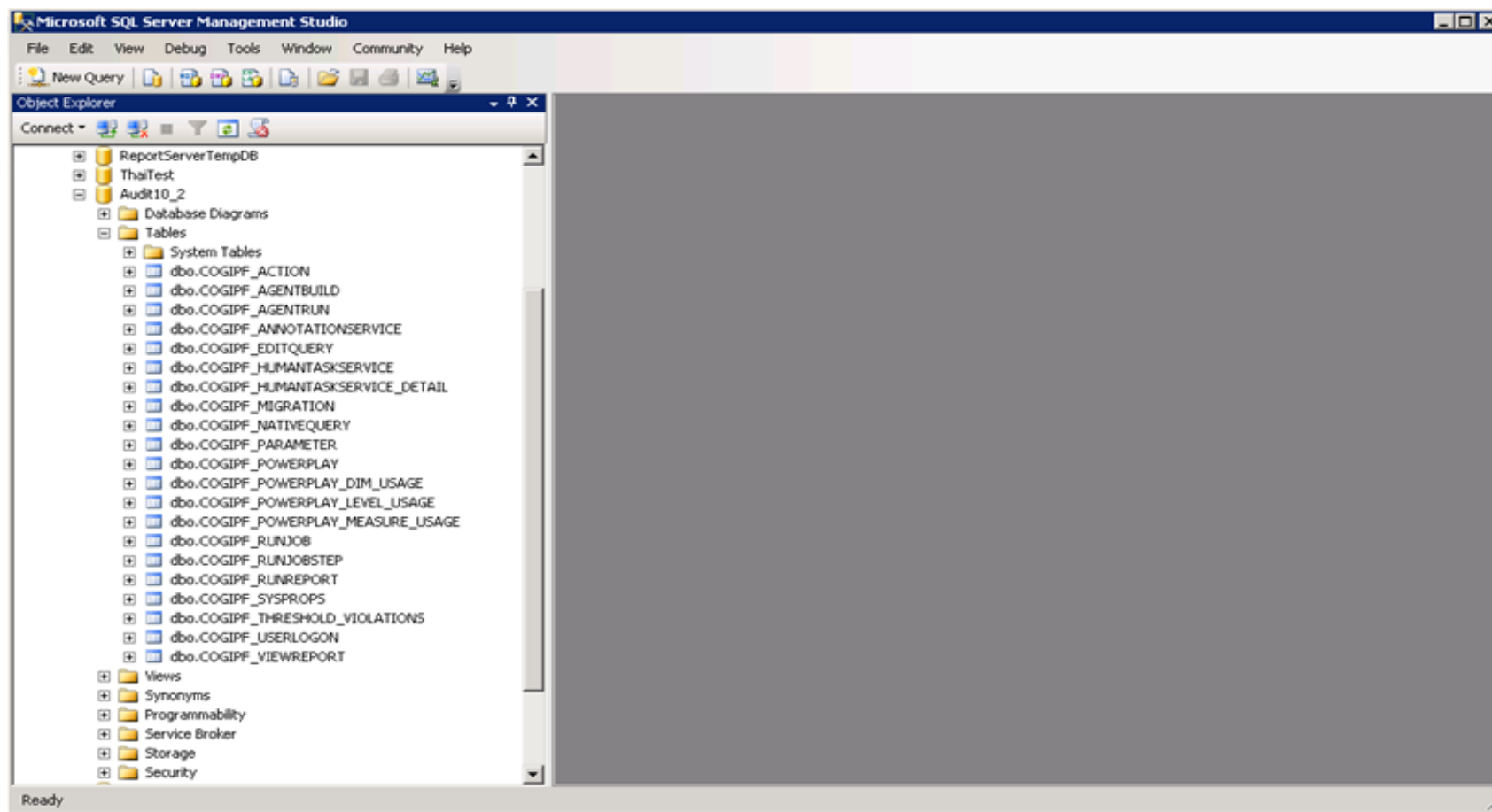
Step 3:

Starting the Cognos Service. (The screen shot below is in reference to Tomcat)



6 Simple Steps to Configure Auditing

Tables created in the audit DB



Tables used for logging audit info for BI

<u>Cognos BI Audit Tables</u>	
COGIPF_ACTION	Stores information about operations performed on objects
COGIPF_AGENTBUILD	Stores information about agent mail delivery
COGIPF_AGENTRUN	Stores information about agent activity including tasks and delivery
COGIPF_ANNOTATIONSERVICE	Stores audit information about annotation service operations
COGIPF_EDITQUERY	Stores information about query runs
COGIPF_HUMANTASKSERVICE	Stores audit information about human task service operations (tasks and corresponding task states)
COGIPF_HUMANTASKSERVICE_D ETAIL	Stores additional details about human task service operations (not necessarily required for every audit entry eg. Notification details and human role details)
COGIPF_NATIVEQUERY	Stores information about queries that IBM <u>Cognos</u> software makes to other components
COGIPF_PARAMETER	Stores parameter information logged by a component
COGIPF_RUNJOB	Stores information about job runs
COGIPF_RUNJOBSTEP	Stores information about job step runs
COGIPF_RUNREPORT	Stores information about report runs
COGIPF_USERLOGON	Stores user logon and logoff information
COGIPF_VIEWREPORT	Stores information about report view requests

Other tables

Audit System Tables	
COGIPF_THRESHOLD_VIOLATIONS	Stores information about threshold violations for system metrics
COGIPF_SYSPROPS	Table contains a single record that indicates logging version detail
COGIPF_MIGRATION	Table is reserved for an upcoming migration application
<u>Cognos Powerplay Audit Tables</u>	
POWERPLAY	Stores information about <u>PowerPlay</u> package, report and report view requests
POWERPLAY_DIM_USAGE	Stores information about dimensions used in <u>PowerPlay</u> package, report and report view requests
POWERPLAY_LEVEL_USAGE	Stores information about levels used in <u>PowerPlay</u> package, report and report view requests
POWERPLAY_MEASURE_USAGE	Stores information about <u>PowerPlay</u> measures used in <u>PowerPlay</u> package, report and report view requests

6 Simple Steps to Configure Auditting

Step 4:

Importing the audit sample package

The sample audit package IBM_Cognos_Audit is provided with the Cognos Server Installation and is present at\webcontent\samples\content

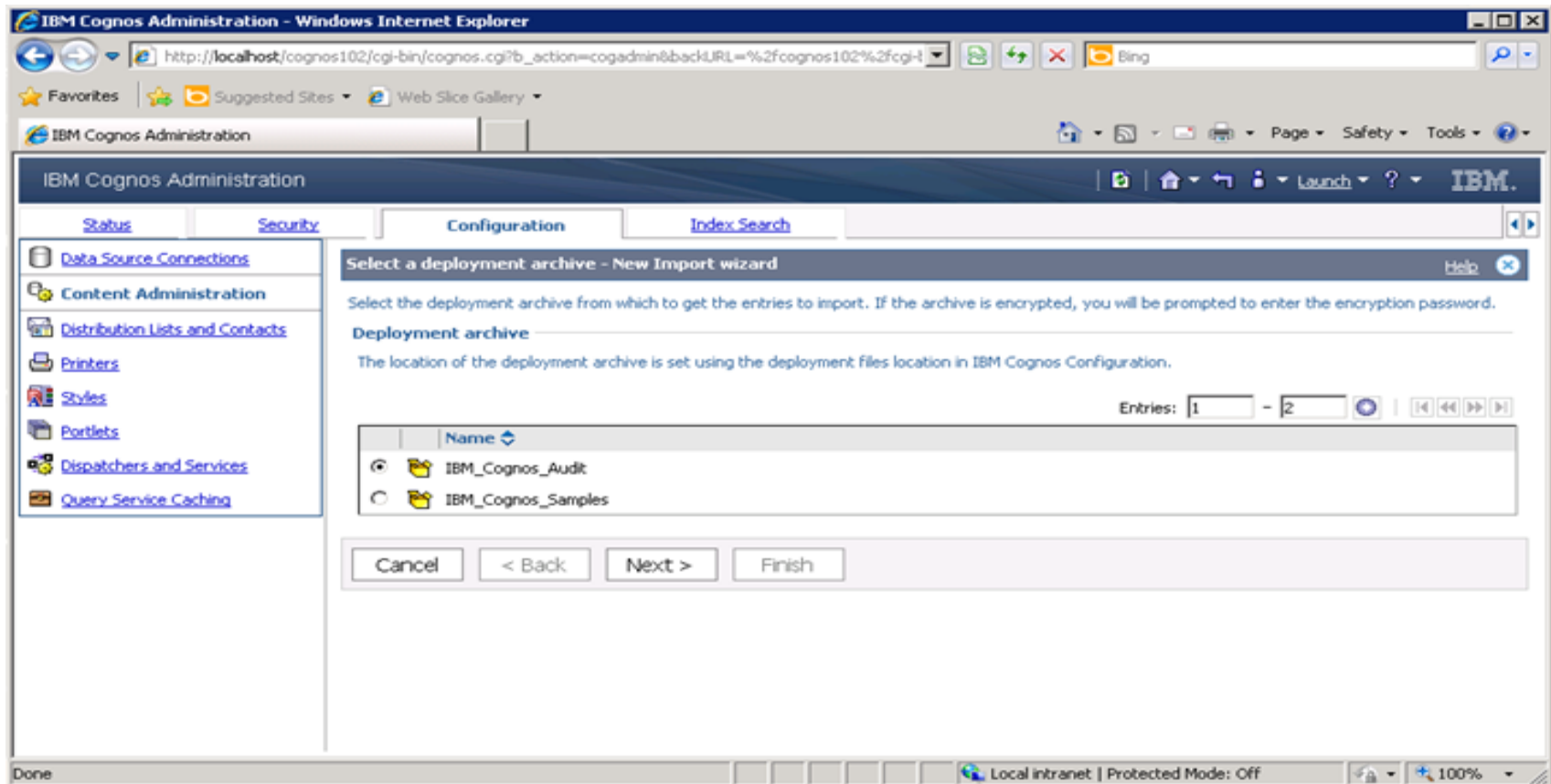
a. a. Copy the IBM_Cognos_Audit (zip file) from
...\CognosSamples\c10\webcontent\samples\content\
to C:\Cognos102\c10\deployment\ (BI server)

6 Simple Steps to Configure Auditting

b. Open the Cognos Portal, go to Cognos Administration
Configuration Tab → Content Administration

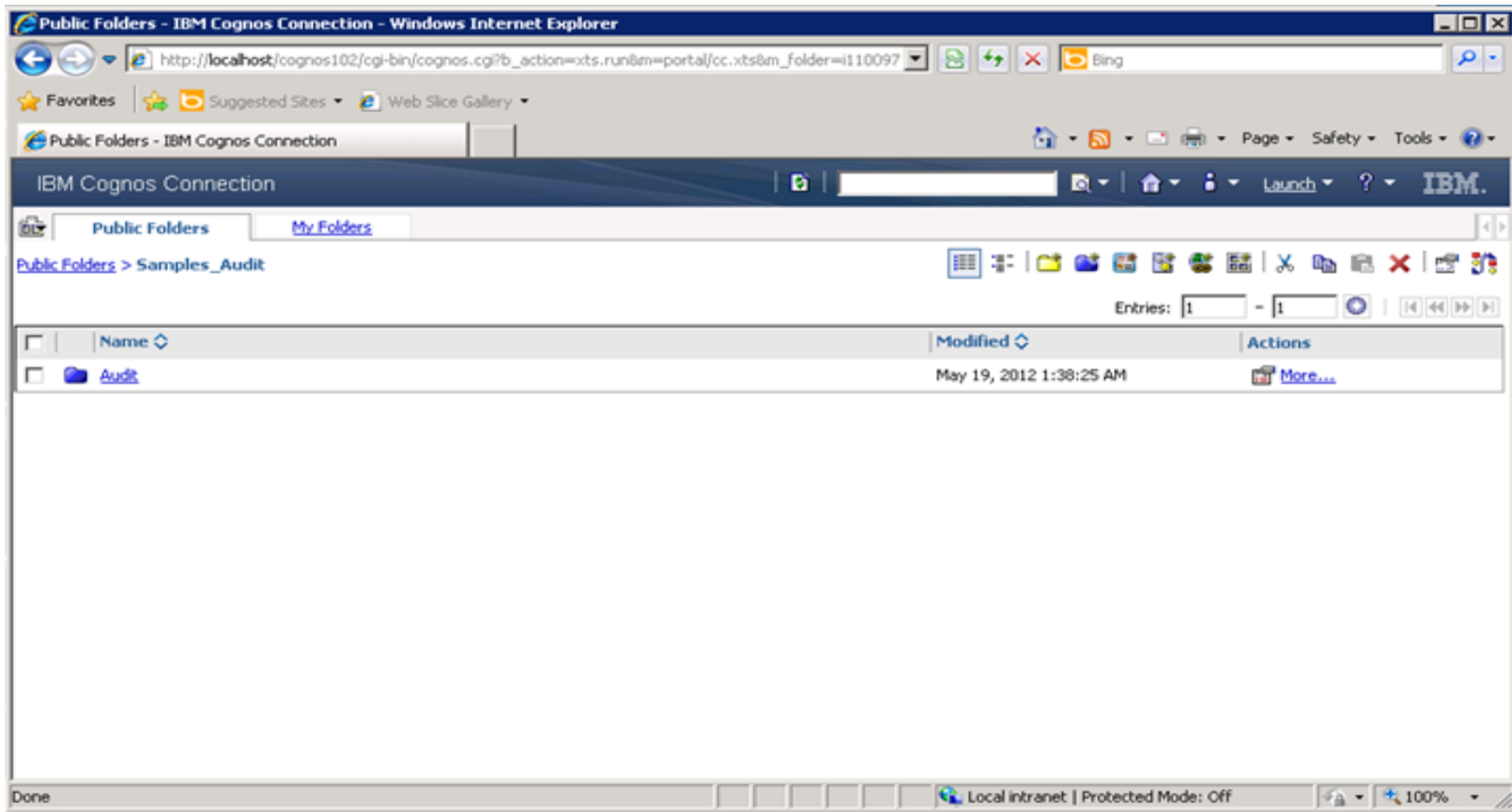
Click on new import from the list of icons on the right top.

Follow the import wizard by clicking on next to finish the deployment import process.



6 Simple Steps to Configure Auditting

The package is now imported in Cognos Connection.



6 Simple Steps to Configure Auditing

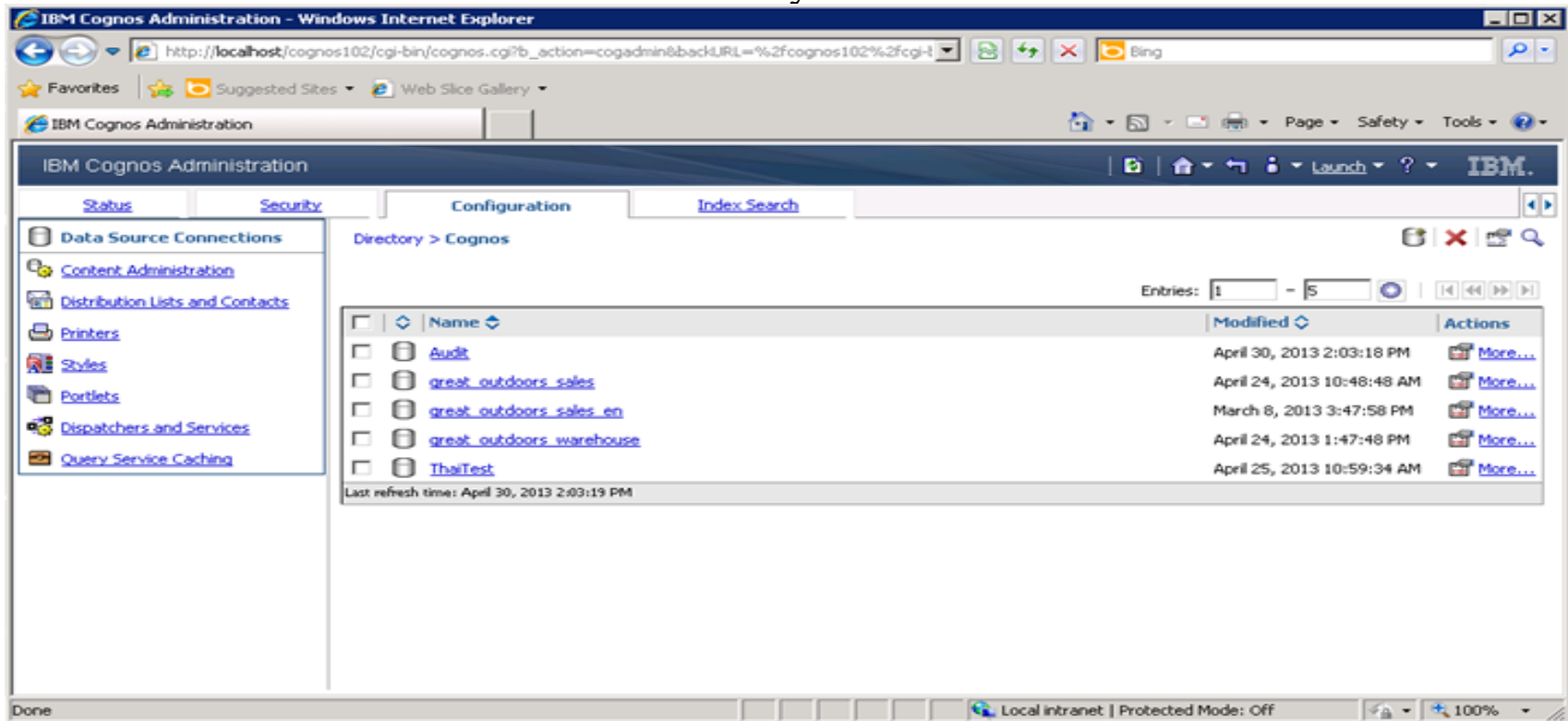
Step 5:

Creating a data source connection to the Audit DB

Open the Cognos Portal, go to Cognos Administration

Configuration Tab → Data Source Connections

Create a new connection and follow the wizard to give the connection information to connect to the DB. Name should be Audit only



The screenshot shows the IBM Cognos Administration web interface in a Windows Internet Explorer browser. The address bar shows the URL: http://localhost/cognos102/cgi-bin/cognos.cgi?b_action=cogadmin&backURL=%2fcognos102%2fcgi-1. The page title is "IBM Cognos Administration". The navigation bar includes tabs for Status, Security, Configuration, and Index Search. The left sidebar shows a tree view with "Data Source Connections" selected. The main content area displays a table of existing data source connections. The table has columns for Name, Modified, and Actions. The entries are:

Name	Modified	Actions
Audit	April 30, 2013 2:03:18 PM	More...
great_outdoors_sales	April 24, 2013 10:48:48 AM	More...
great_outdoors_sales_en	March 8, 2013 3:47:58 PM	More...
great_outdoors_warehouse	April 24, 2013 1:47:48 PM	More...
ThaiTest	April 25, 2013 10:59:34 AM	More...

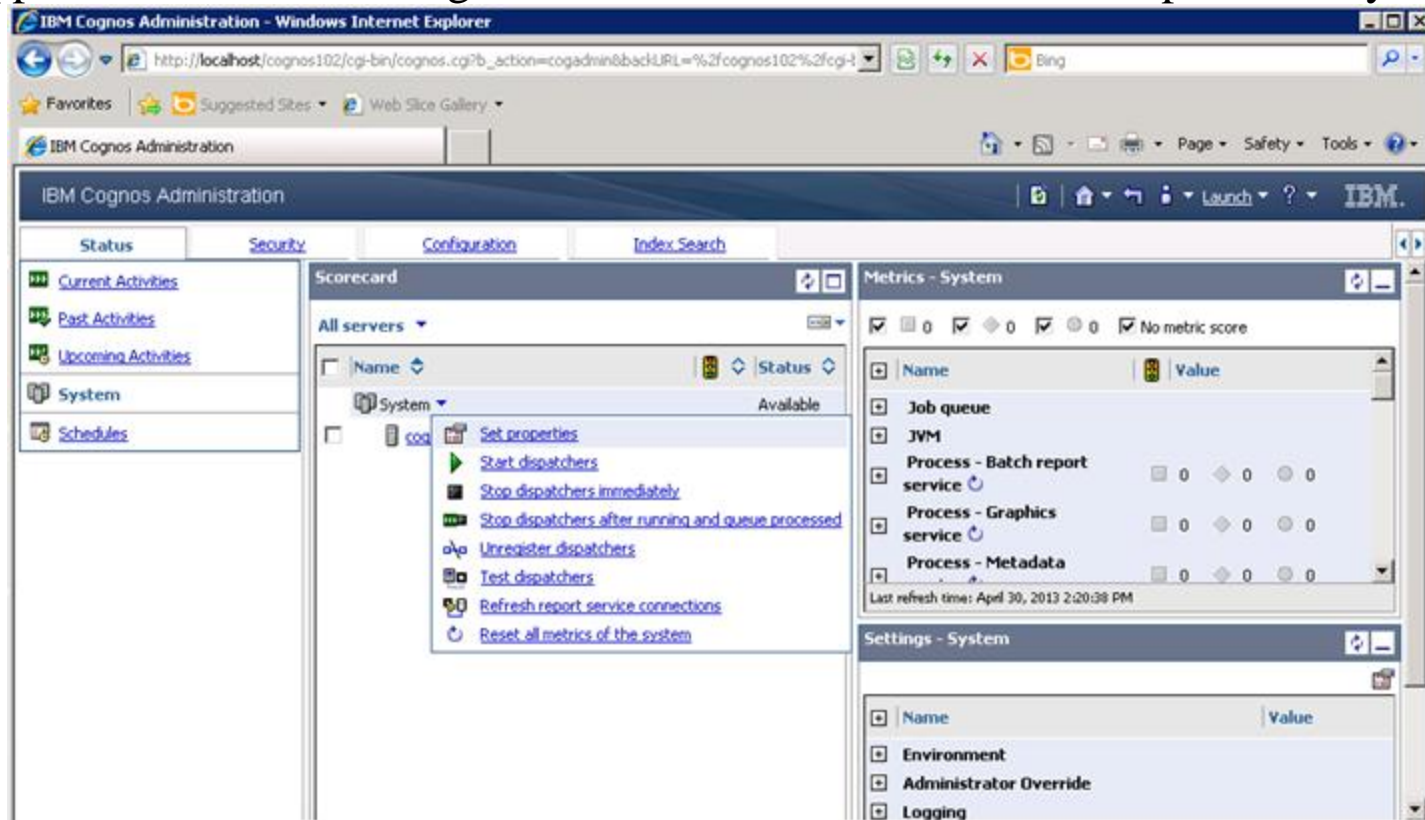
Below the table, it says "Last refresh time: April 30, 2013 2:03:19 PM". The status bar at the bottom indicates "Local intranet | Protected Mode: Off" and "100%".

6 Simple Steps to Configure Auditing

Step 6:

Increasing the logging level to Basic to start logging.

Further levels Request, Trace and Full are not recommended unless requested by support for troubleshooting and when done should be service specific only.



6 Simple Steps to Configure Auditing

Set properties - Configuration

Help

General Settings Permissions

Specify the configuration settings for this entry. By default, an entry acquires its configuration settings from a parent. You can override those settings with the settings set explicitly for this entry.

Category:
Logging

Entries: 1 - 15

<input type="checkbox"/>	Category	Name	Value	Default
<input type="checkbox"/>	Logging	Audit logging level for annotation service	Minimal	Yes
<input type="checkbox"/>	Logging	Audit logging level for agent service	Minimal	Yes
<input type="checkbox"/>	Logging	Audit logging level for batch report service	Basic	No
<input type="checkbox"/>	Logging	Audit the native query for batch report service	<input type="checkbox"/>	Yes
<input type="checkbox"/>	Logging	Audit logging level for the Content Manager Cache Service	Minimal	Yes
<input type="checkbox"/>	Logging	Audit logging level for Content Manager service	Minimal	Yes
<input type="checkbox"/>	Logging	Audit logging level for the dispatcher	Minimal	Yes
<input type="checkbox"/>	Logging	Audit logging level for delivery service	Minimal	Yes
<input type="checkbox"/>	Logging	Audit logging level for event management service	Minimal	Yes
<input type="checkbox"/>	Logging	Audit logging level for graphics service	Minimal	Yes

OK Cancel

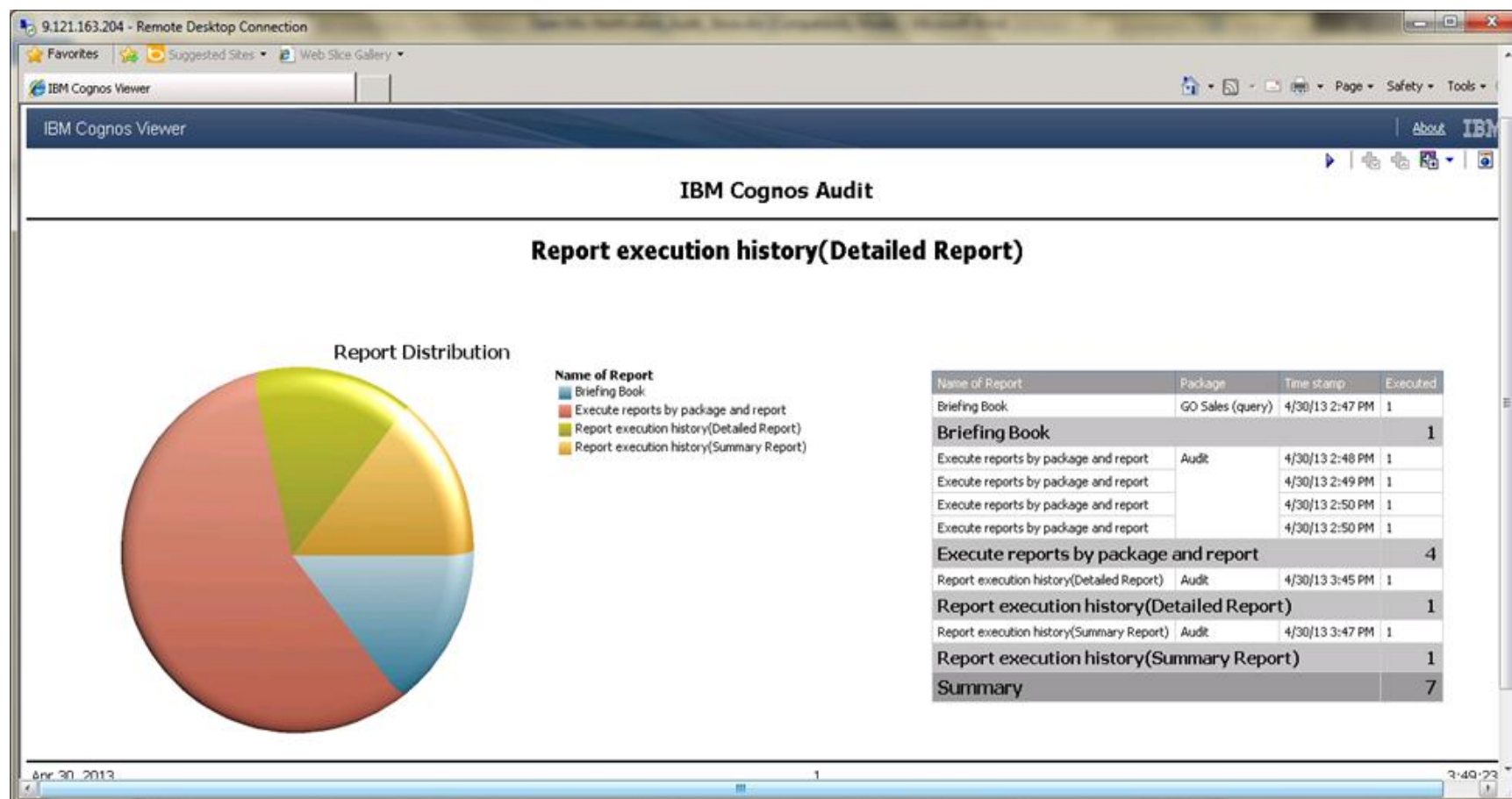
What logging level records what kind of info?

System activity type	Minimal	Basic	Request	Trace	Full
System and service startup and shutdown, runtime errors	Y	Y	Y	Y	Y
User account management and runtime usage		Y	Y	Y	Y
User requests		Y	Y	Y	Y
Service requests and responses			Y		Y
All requests to all components with their parameter values				Y	Y
Other queries to IBM Cognos components (native query)				Y	Y

Sample Audit Report

Execute Cognos reports

Then execute the audit report (Report Execution History – Detailed report) that will give us information on which reports were run



Detailed example of an audit report and table

Authentication:

Authentication is handled through the IBM Cognos Content Manager Service. Therefore, recording authentication-related detail requires auditing to be enabled for the IBM Cognos Content Manager Service.

In the following scenario, auditing is set to minimal for all services except the IBM Cognos Content Manager Service.

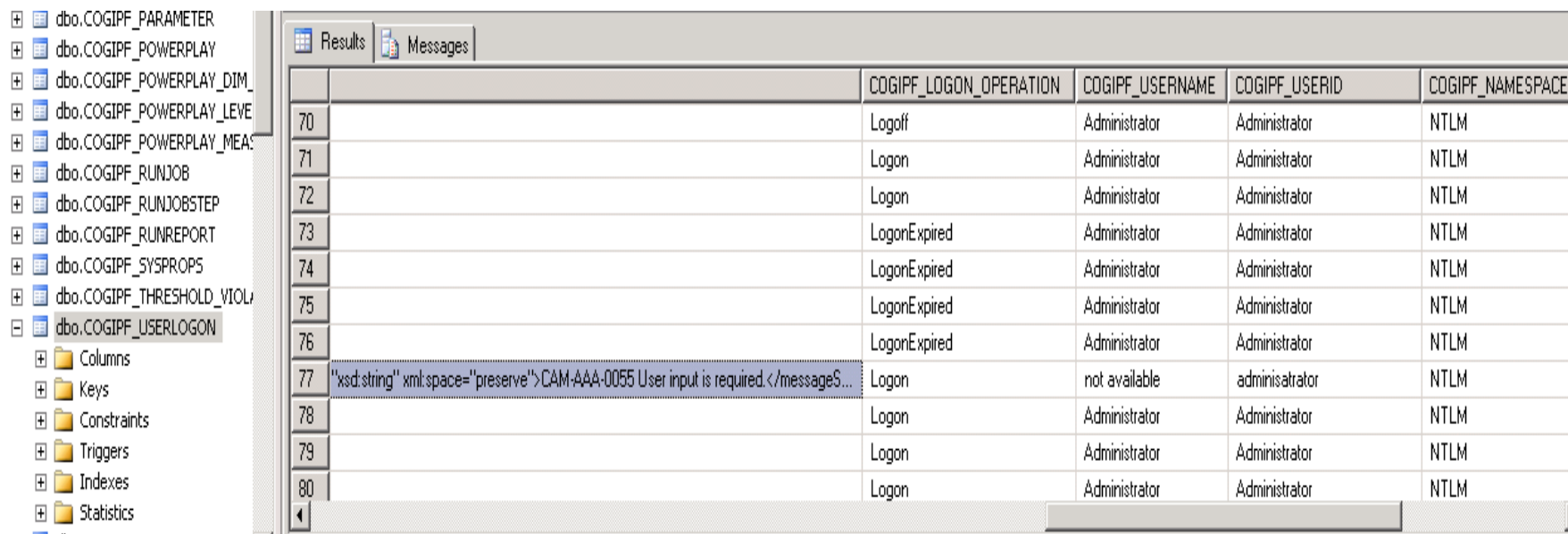
Logging into IBM Cognos Connection causes audit data to be written into two tables:

- COGIPF_USERLOGON
- COGIPF_ACTION

The primary information related to the user logon (that is, user name and authenticating namespace) is contained in the COGIPF_USERLOGON table

Secondary information such as group membership is recorded in the COGIPF_ACTION table.

The COGIPF_USERLOGON tables has various columns holding user name, namespace, and the error message occurred if any while the user tried to login. If the user clicked ok without providing the login credentials, a message “ User input is required” is logged in the DB for that user



		COGIPF_LOGON_OPERATION	COGIPF_USERNAME	COGIPF_USERID	COGIPF_NAMESPACE
70		Logoff	Administrator	Administrator	NTLM
71		Logon	Administrator	Administrator	NTLM
72		Logon	Administrator	Administrator	NTLM
73		LogonExpired	Administrator	Administrator	NTLM
74		LogonExpired	Administrator	Administrator	NTLM
75		LogonExpired	Administrator	Administrator	NTLM
76		LogonExpired	Administrator	Administrator	NTLM
77	"<xs:string xmlns:space='preserve'>CAM-AAA-0055 User input is required.</messageS...	Logon	not available	adminisatrator	NTLM
78		Logon	Administrator	Administrator	NTLM
79		Logon	Administrator	Administrator	NTLM
80		Logon	Administrator	Administrator	NTLM

What affects audit logging ?

Ipf tracing –

While troubleshooting support requests that an advanced level of logging be enabled to capture detailed traces. This is called an ipf trace

This trace is enabled by editing files called ipfxxxclientconfig.xml.sample present inside the Cognos configuration dir.

xxx stands for the component eg. Rsvp-report service

If this trace is enabled incorrectly, it will stop auditing

Changes in logging level –

Audit level “Minimal” will disable audit logging to the database

If the appropriate logging level is not set, then the kind of information you wish to see would not be captured in the tables.

Deleting only part of audit tables -

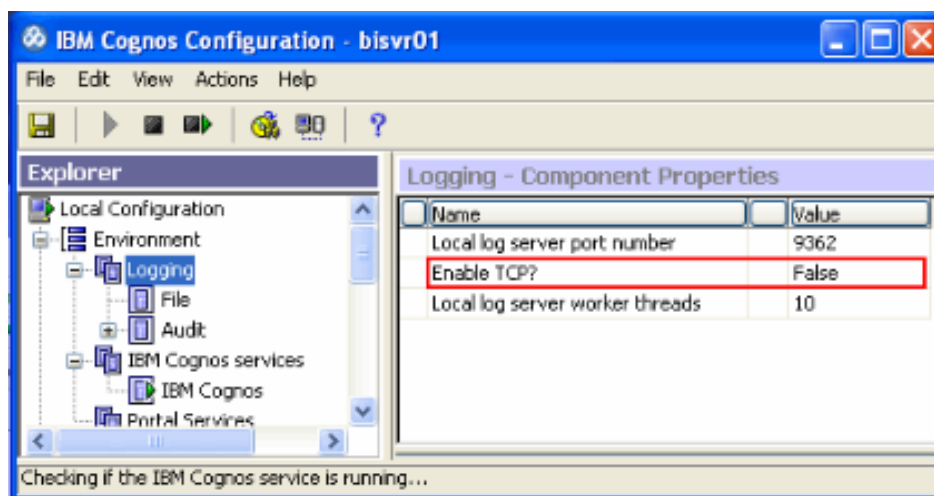
Audit tables are created when the service start after we configure it in cognos config, however if a table gets deleted inside the audit table it cannot be recreated. So there is inconsistency in the tables as a result the auditing will not work properly

How to make sure that ipf tracing does not affect audit logging ?

Highlighted fields are important to ensure that audit logging is not interrupted during IPF trace activities. As long as the TCP connectivity parameters are correct and the audit level is set to warn, the IPF client trace functions and audit records continue to be logged to the audit Database.

```
<appender name="clientTCP" class="com.cognos.indications.LogTCPSocketAppender">
<param name="remoteHost" value="127.0.0.1"/>
<param name="Port" value="9362"/>
<param name="LocationInfo" value="false"/>
<param name="ReconnectionDelay" value="30000"/>
</appender>
<appender name="clientRemote"
class="com.cognos.indications.LogLocalUDPAppender">
<param name="Port" value="9362"/>
</appender>
<category name="Audit" class="com.cognos.indications.LogTypedLogger">
<level value="warn"/>
<appender-ref ref="clientRemote"/>
</category>
```

- Change the remoteHost value and the Port value to match the log server host and port number in IBM Cognos Configuration
- Change the appender reference within the <category name="Audit"> section to match the Log Server Enable TCP value in IBM Cognos Configuration.
- To verify whether clientRemote or clientTCP needs to be used as the appender-ref value, the parameters within IBM Cognos Configuration need to be examined.
- If the Enable TCP? parameter is set to False, then the clientRemote must be used. If the value is set to True, the clientTCP will be the require entry in the IPF file.

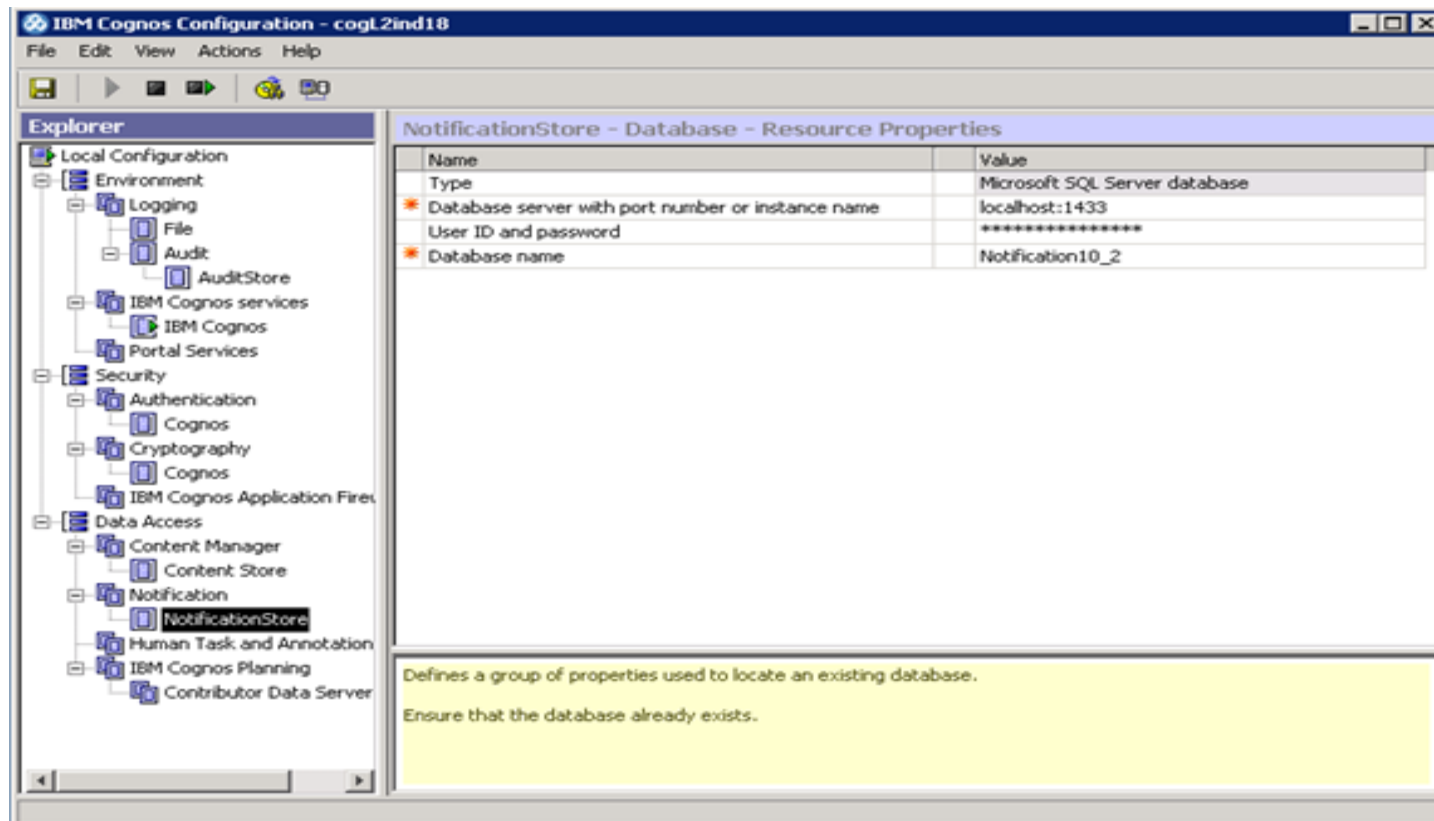


Notification Store
















































- IBM Cognos uses a notification database for job scheduling and for email notifications.
- If Application tier (dispatcher) and the Content Manager are installed on one computer and one directory (that makes it single server installation), then by default content store database is used for the notification database.
- You can change it to point to a different DB. This should be preferred because if the Notification Store and Content Store are one, then the number of connections to it is large. Separating them would reduce the number of connections to the content store.
- If you install the server components on different computers, you must manually configure the notification database connection information on every content manager machine and every application tier (dispatcher) machine.

Configure a Notification Store

1. Stop Cognos Service
2. Configure the Notification Store
3. Start the services



Tables inside the Notification Store

[-]  Notification10_2	
[-]  Database Diagrams	
[-]  Tables	
[-]  System Tables	
[+]  dbo.ANN_ANNOTATION	[+]  dbo.NC_CONFIGURATION
[+]  dbo.ANN_ANNOTATION_PROPS	[+]  dbo.NC_CTMAP
[+]  dbo.ANN_ANNOTATION_TEXT	[+]  dbo.NC_DB_VERSION
[+]  dbo.ANN_CONTEXT	[+]  dbo.NC_DELIVERYADDRESS
[+]  dbo.ANN_CONTEXT_DIMENSIONMEMBER	[+]  dbo.NC_EVENTSTATUS
[+]  dbo.ANN_DATAITEM	[+]  dbo.NC_JMSQUEUE
[+]  dbo.ANN_DIMENSION	[+]  dbo.NC_JOBQUEUE
[+]  dbo.ANN_DIMENSION_METADATAITEM	[+]  dbo.NC_MESSAGELINE
[+]  dbo.ANN_DIMENSIONMEMBER	[+]  dbo.NC_MESSAGELINE_ELEMENT
[+]  dbo.ANN_DIMENSIONMEMBER_DATAITEM	[+]  dbo.NC_MESSAGESTRUCT
[+]  dbo.ANN_IDTABLE	[+]  dbo.NC_METRICS
[+]  dbo.ANN_METADATAITEM	[+]  dbo.NC_OBJECTCATALOGUE
[+]  dbo.ANN_MODEL	[+]  dbo.NC_OBJECTID
[+]  dbo.ANN_MODEL_DIMENSION	[+]  dbo.NC_PERMISSION
[+]  dbo.ANN_VERSION	[+]  dbo.NC_RECIPIENT
[+]  dbo.HTS_ATTACHMENT	[+]  dbo.NC_SCHEDULE
[+]  dbo.HTS_CALLBACK	[+]  dbo.NC_SCHEDULE_QUEUE
[+]  dbo.HTS_CALLBACKPARAM	[+]  dbo.NC_SCHEDULED_EVENT_OVERRIDE
[+]  dbo.HTS_DEADLINE	[+]  dbo.NC_SDS_INSTANCE
[+]  dbo.HTS_DEADLINE_INSTANCE	[+]  dbo.NC_TASK
[+]  dbo.HTS_ESCALATION	[+]  dbo.NC_TASK_ANCESTOR_STOREIDS
	[+]  dbo.NC_TASK_HISTORY_DETAIL

NC Drop Script

What is an NC drop script ?

Cognos provides a script that drops only a few tables in the Notification Store (names have a prefix as NC). These tables hold metadata related to schedules.

Script is provided for every Database and is located at the below location
<Cognos Install Location>\configuration\schemas\delivery\

What does this script do and does it harm the existing schedule information?
Do we have to recreate schedules after the script is run?

- This script does not affect or alter your schedules.
- You do not have to recreate any schedule after the execution of this script.
- Note: If your notification store is same as the content store, then a little care needs to be taken while executing this script and only after taking a complete content store backup

Steps to run the NC drop script:

1- Stop Cognos Service

2- Have the Database Administrator back up the Complete Cognos content store database.

3- a. If notification store is same as the content store then connect to content store database using a database tool and with the same login as provided for Content store in Cognos configuration run the NC_DROP script
b. If notification store and content store are different then you should connect to the notification store and the script should be run on the notification store only

<Install Location>\configuration\schemas\delivery\oracle\NC_DROP_ORA.sql

<Install Location>\configuration\schemas\delivery\db2\NC_DROP_DB2.sql

<Install Location>\configuration\schemas\delivery\sqlserver\NC_DROP_MS.sql

You should not receive any error message in the script that you execute.

4- Start the Cognos service. This will recreate all the NC tables.

Indications that something is wrong with the Notification Store

If something unusual is noticed for schedules, then it is related to the Notification Store

Problem : Schedules are gone missing from the future activities

Inconsistent output seen in the current activities

Schedules go into pending state

Solution : Run the NC drop script on the Notification Store

Problem: Notification configured incorrectly or not configured on one of the servers in the distributed environment

Id and password incorrect in the configuration

Solution:

If database credentials are not known, export the configuration of a content manager server to determine the proper credentials needed to connect to the content store. (if notification store is same as content store)

Export the config from all dispatcher machines and check the credentials to connect to the notification store (if notification store is different from content store)

References

Audit Store:

<http://www.redbooks.ibm.com/redbooks/pdfs/sg247912.pdf>

Installation and Configuration Guide

http://public.dhe.ibm.com/software/data/cognos/documentation/docs/en/10.2.0/inst_cr_winux.pdf

Notification Store:

<http://www-01.ibm.com/support/docview.wss?uid=swg21429773>

2 & A



Thank You

