Adabas Auditing on Mainframe

Concepts

Version 221

October 2021

ADABAS & NATURAL

This document applies to Adabas Auditing on Mainframe Version 221 and all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: ALA-INTRO-TBD-20211008

Table of Contents

1 About this Documentation

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
`Monospace font`	Identifies service names and locations in the format *`folder.subfolder.service`*, APIs, Java classes, methods, properties.
`Italic`	Identifies: Variables for which you must supply values specific to your own situation or environment. New terms the first time they occur in the text. References to other documentation sources.
`Monospace font`	Identifies: Text you must type in. Messages displayed by the system. Program code.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
|	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the | symbol.
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Online Information and Support

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at **https://documentation.softwareag.com**.

Software AG Empower Product Support Website

If you do not yet have an account for Empower, send an email to empower@softwareag.com with your name, company, and company email address and request an account.

Once you have an account, you can open Support Incidents online via the eService section of Empower at **https://empower.softwareag.com/**.

You can find product information on the Software AG Empower Product Support website at **https://empower.softwareag.com**.

To submit feature/enhancement requests, get information about product availability, and download products, go to **Products**.

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the **Knowledge Center**.

If you have any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory at **https://empower.softwareag.com/public_directory.aspx** and give us a call.

Software AG Tech Community

You can find documentation and other technical information on the Software AG Tech Community website at **https://techcommunity.softwareag.com**. You can:

- Access product documentation, if you have Tech Community credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

Data Protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.

2 Introducing Adabas Auditing on Mainframe

This chapter provides information on Adabas Auditing for z/OS, a selectable unit of Adabas that enables specific Adabas files to be monitored for auditing purposes.

What is Adabas Auditing?

Adabas Auditing helps you to:

Maintain data security and compliance with a simple, powerful way to track and audit all activity on your Adabas databases.
Maintain full visibility into your database activity while enhancing cybersecurity efforts by detecting unauthorized access.
Track and trace who is accessing, reading and changing your data.

Organizations running Adabas on IBM z/OS have generated valuable information such as financial data, personnel files and proprietary business material over decades.

Common business operations require this data to be accessed regularly by multiple applications, end-users and services.

To maintain security and comply with regulations, you need to know:

Who is reading or changing your data.
Which changes were made.
When were changes made.
Where did the activity occur.
Which applications were used to access your data.

This calls for a solution that delivers efficient and comprehensive ways to track and trace both read and edit activities in your databases.

Adabas Auditing for z/OS tracks and stores audit data safely in secure, indexed, long-term archives, helping you stay on top of data security and compliance regulations, including HIPAA, SOX and GDPR, and to keep your Adabas systems secure and reliable for years to come.

Features

Audit all Adabas applications
Use Adabas Auditing for z/OS on all Adabas applications, including Natural, COBOL, Assembler, PL/1 and Fortran.

Track all Adabas database operations
Track and audit all commands for user files on the database including read, search, browsing, insert, delete and update commands for all user files on a database.

Customize audit tracks

Select your choice of data from many Adabas databases, then apply filters to focus only on relevant Adabas events.

Protect audit data

Ensure audit data is only available to authorized persons. Prevent alterations to audited data and mask sensitive archived information.

Archive and retrieve audit data

Retain audit data with long-term archiving capabilities to comply with both regulations and internal standards. Index archived data to quickly retrieve and search data logs.

Easy-to-use web-based user experience

Enable fast deployment and use by multiple stakeholders including auditors, security officers, and database administrators.

Enable Database Administrators to track all access and activity on the database

Know what data is being captured or exported. Trace specific users and applications for each event. Resolve data inconsistencies. Fix production outages and provide proper access rights.

Support Data Protection Officers with infrastructure and tools for security audits

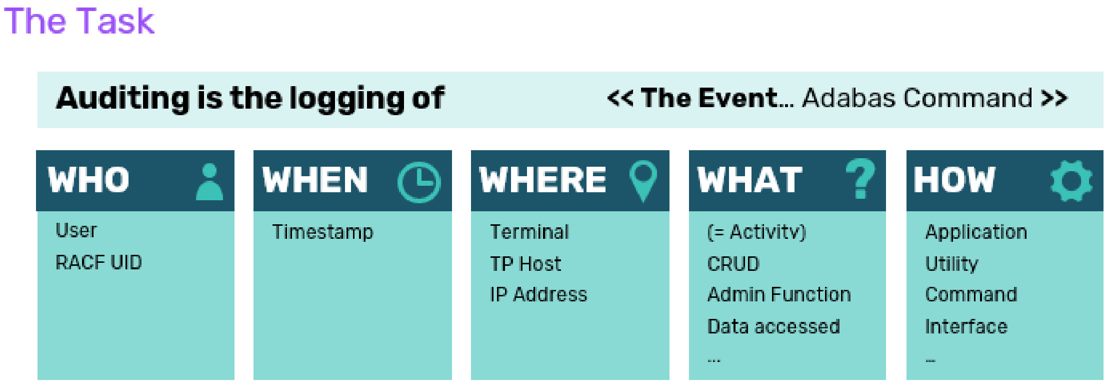
Ensure data is available to external auditors, archived consistently and separately from production data; stored for specific periods to comply with regulations, with access limited to authorized personnel.

3 Concepts

In an Adabas environment, providing audit data means capturing events that 'touch' your Adabas data. You may not want, or need, to capture all events, so the ability to define filters and rules to reduce the amount of data captured is critical to maintaining existing performance levels.

Not only do you need to capture the events that affect your data, but you also need to make sure you capture all necessary associated information (the 'who', 'when', 'where', 'what', and 'how') in order to provide you with the correct information for analysis.

Pictured below is a diagram relating to the concepts of auditing in the Adabas environment.



The Task

Auditing is the logging of **<< The Event...** Adabas Command **>>**

WHO	WHEN	WHERE	WHAT	HOW
User RACF UID	Timestamp	Terminal TP Host IP Address	(= Activity) CRUD Admin Function Data accessed ...	Application Utility Command Interface ...

- Audit modification in data
- Track and Select (Read/Find) of any data access
- Trigger the auditing of data based on rules
- Auditing can be at file level or Userview level
- Subscriptions can be used to group sets of data, e.g. Transactions across files
- This is not an archiving system, i.e. logging the whole record
- Audit Data is what the auditor wants to see - Set the right keys for that
- Auditing can be used to view the history of change to resolve logical applications
- Researching a security violation - Deep dive

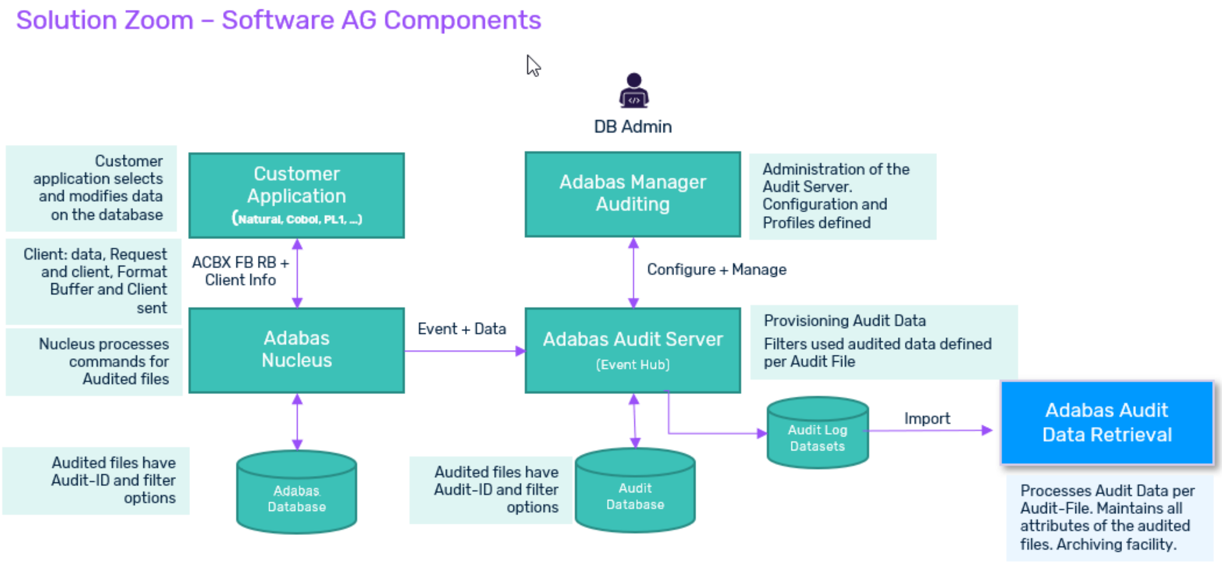
Adabas Auditing for z/OS provides a 2-stage filtering process to ensure only the data you want is collected and made available for subsequent analysis. Initial filtering is performed within each auditing enabled Adabas nucleus before sending the audit data to a centralized Audit Server. There additional filtering is performed.

This filtering (and associated rules) results in only required audit data being collected and processed. This way you ensure your day-to-day Adabas activities can continue without being affected.

Architecture

Adabas Auditing is not an application in the traditional sense. Rather, it is made up of several components that work together to audit data without disrupting normal Adabas operations. A portion of the auditing process occurs within the Adabas nucleus address space, while another portion of the task occurs within an address space known as the Adabas Audit Server.

Pictured below is a diagram showing the Adabas Auditing architecture and the main components involved.


Solution Zoom – Software AG Components
DB Admin
Customer application selects and modifies data on the database
Customer Application
(Natural, Cobol, PL1, ...)
Client: data, Request and client, Format Buffer and Client sent
ACBX FB RB + Client Info
Adabas Nucleus
Nucleus processes commands for Audited files
Event + Data
Adabas Manager Auditing
Administration of the Audit Server. Configuration and Profiles defined
Configure + Manage
Adabas Audit Server
(Event Hub)
Provisioning Audit Data
Filters used audited data defined per Audit File
Audited files have Audit-ID and filter options
Adabas Database
Audited files have Audit-ID and filter options
Audit Database
Audit Log Datasets
Import
Adabas Audit Data Retrieval
Processes Audit Data per Audit-File. Maintains all attributes of the audited files. Archiving facility.

- Customer Application
- Adabas Nucleus
- Adabas Audit Server
- Adabas Auditing Configuration and Administration
- Adabas Audit Data Retrieval Server

- Adabas Audit Data Viewer

Customer Application

The user application can be anything that can issue Adabas calls/commands. The commands may be any command that either access or modify business data on the databases. Access also includes Histograms.

When the command is sent to the Adabas nucleus; format buffers, record buffers, search buffers and value buffers, as well as client information, can be captured as audit information for the command event.

Detailed aspects of the command event (e.g. ACB/ACBX type) are captured as well.

Adabas Nucleus

For each file that is registered for Auditing, it is allocated a unique Audit-ID. That file will keep that Audit-ID for the life of the file, even if the file gets moved to another database and file number.

When a command is issued to a file registered for Auditing, the Adabas nucleus performs some initial processing before it is sent to the Audit Server. Unlike Replication, the event is not transaction oriented.

There are various filters, per file, to reduce the number of commands being sent to the Audit Server. These filters enable only the important audit data to be collected by the Audit Server thus improving performance.

Adabas Audit Server

For each file that is registered to an Adabas nucleus, there must be a corresponding registration of the file on the Audit Server side.

On the Audit Server, there are also filters and rules. Some of these filters may be set on either the Audit Server side or the Adabas nucleus. Some of the reasons for this are described below:

- For auditing based on update type commands

  Since there are typically a lot fewer update type commands than read type commands, filtering performed on the Adabas nucleus side will be better for performance.

- For auditing based on the use of certain fields

  If records, for a file, need to be audited, provided a certain field is specified in the User Format Buffer, filtering performed on the Adabas nucleus side will be better for performance.

- For auditing based on changing field values

If a specified field(s) only needs to be audited for value changes, filtering should be done on the Audit Server side.

These filters (and their associated rules) enable the customer to use complex logic to exclude data from being collected. In addition, within these filters, the customer can identify those command buffers and Adabas fields that need to be audited.

Each record that passes the rules and filtering process is identified as an Audit Event. All associated data relating to this Audit Event (e.g. Request and Client information) is written to the Audit Log datasets for subsequent processing by the Audit Data Retrieval Server.

Note: The data collected in the Audit Log datasets is not intended to be used for the auditing of whole records for an Adabas file. It is there to provide only the necessary information to enable an Auditor to fulfil their auditing role.

Adabas Auditing Configuration and Administration

The creation and maintenance of auditing definitions are performed using Adabas Auditing Configuration via the Natural application SYSALA.

Administration of the Adabas Audit Server and Adabas nuclei enabled for auditing is performed via the Natural application SYSALAA. This includes various Operator commands and Admin functions (e.g. Show statistics or parameters, Deactivate a Subscription, etc.).

For the administration of the Auditing System file on the Audit Server database, this can be via SYSAOS or SYSALAA. Maintaining the Auditing System file is a DBA maintenance task.

Adabas Audit Data Retrieval Server

The Audit Data Retrieval Server is the target to which all Audit Events are sent, made available via the Audit Logs.

Each Audit Event is processed by the Retrieval Server and stored in its own database. Each Audit Event is timestamped with the date-time that the originating Adabas nucleus processed the command.

The Retrieval Server will also store ‘key’ information (i.e. indices) about each Audit Event. These indices can subsequently be used as search criteria to retrieve individual events, the viewing of which is facilitated by the Adabas Audit Data Viewer.

The Audit Event keys may be descriptors, as defined on the Source Adabas file (type DE), or new key values, as defined via the Audit Server (i.e. GFFT Definitions).

Customers may define the retention period of any or all audit data information stored in the Retrieval Server’s database.

Adabas Audit Data Viewer

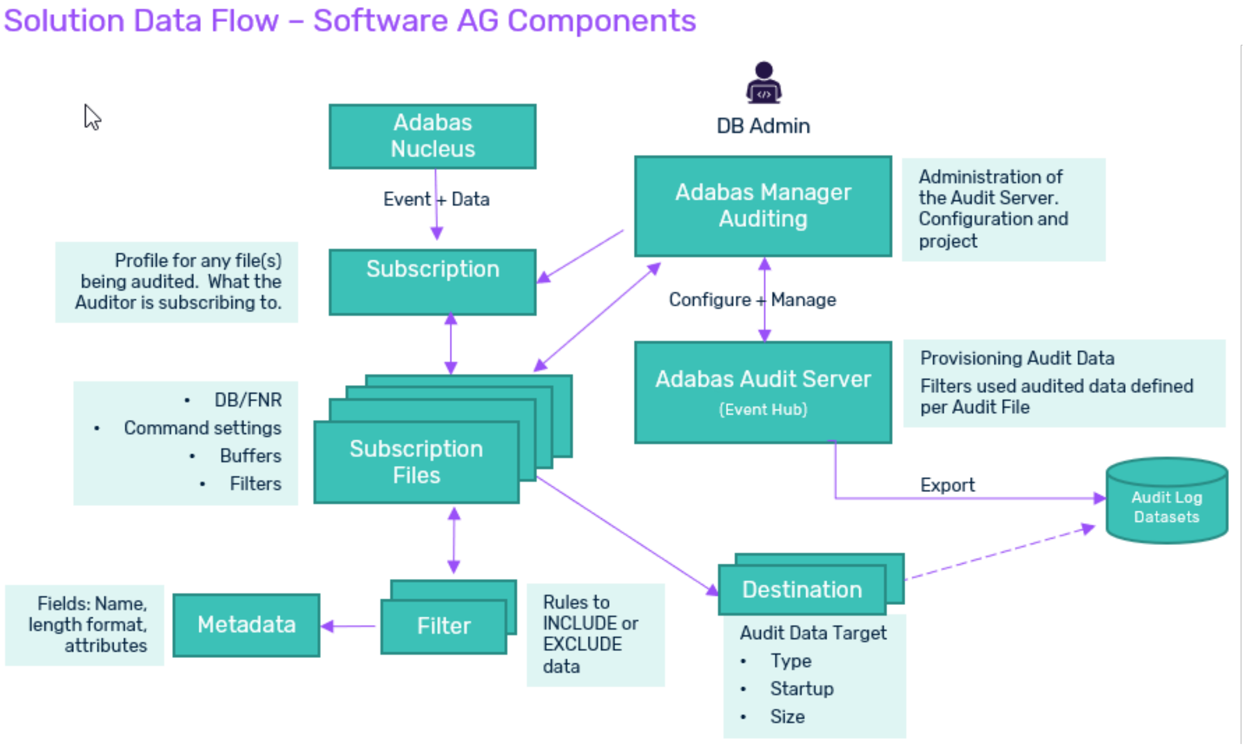
The Data Viewer is the key tool for the Auditor. Here, the Auditor can analyze Audit Events using whatever criteria they wish to verify the integrity of the data and how it is being used.

The Data Viewer has a powerful search engine, necessary due to the potential for very large volumes of data This way the customers can search at various levels: File level, User-view level, and Subscription level.

Additional options are available such as creating folders allowing searches to be expanded across individual files and subscriptions.

Auditing Processing

This section describes how the different processing phases support the flow of audit data from the source Adabas nucleus to the Adabas Audit Server and the Audit Logs.


Solution Data Flow – Software AG Components
DB Admin
Adabas Nucleus
Event + Data
Adabas Manager Auditing
Administration of the Audit Server. Configuration and project
Profile for any file(s) being audited. What the Auditor is subscribing to.
Subscription
Configure + Manage
Adabas Audit Server
(Event Hub)
Provisioning Audit Data
Filters used audited data defined per Audit File
DB/FNR
Command settings
Buffers
Filters
Subscription Files
Export
Audit Log Datasets
Destination
Audit Data Target
Type
Startup
Size
Fields: Name, length format, attributes
Metadata
Filter
Rules to INCLUDE or EXCLUDE data

Phase 1: Application Processing

The application issues an Adabas command to an Adabas database. The command (or request) buffers and client information is sent to the Adabas nucleus.

Phase 2: Adabas Nucleus Processing

The Adabas nucleus processes the command as normal. At command end, it checks to see if the Adabas file has been defined for Auditing. If so, initial filtering is performed to determine if this command is eligible for auditing. If that is the case, an event is triggered which sends all relevant command buffers and client information over to the Adabas Audit Server.

Phase 3: Adabas Audit Server Processing

The Audit Server receives the auditing data and checks to see if it matches any of the defined subscriptions that are currently active in the Audit Server. If a subscription match occurs, then within the subscription definition is a list of fields identifying what information should be extracted from the received data to create an Audit Event. This Audit Event is stored in the Audit Log.

Auditing Definition Overview and Maintenance

To use Adabas Auditing and customize its processing, you must supply various auditing definitions.

These auditing definitions reside in the Auditing system file (loaded onto the Adabas Audit Server as part of the installation process). The definitions are created and maintained using Adabas Auditing Configuration. For more information about how to configure the Auditing definitions, refer to the *Adabas Auditing Configuration* chapter.

At Adabas Audit Server start-up, these auditing definitions are read from the Auditing system file.

The following sections relate to the different types of definitions required for auditing.

- Definition Descriptions
- Definition Specification Sequence

Definition Descriptions

Once you install Adabas Auditing, you specify a set of definitions that drive its audit processing. These definitions are described in the following table in order of importance to auditing (required definitions are listed first).

Definition Type	Defines	How many definitions are required?
Destination	The destination of the audited data. Refer to section *Maintaining Destination Definitions* in chapter *Adabas Auditing Configuration*.	Required. At least one destination definition is required for auditing to occur. Create one definition for every Adabas Auditing destination you intend to use.

Definition Type	Defines	How many definitions are required?
Subscription	A set of specifications to be applied to the auditing of the data. These include (but are not limited to): ■ architecture key, output alpha and wide-character keys that should be used ■ various settings relating to the availability of the subscription in specific circumstances Subscription definitions identify subscription file definitions that should be used.	Required. At least one subscription definition is required for auditing to occur. Refer to *Maintaining Subscription Definitions* in chapter *Adabas Auditing Configuration*.
Subscription File (SFILE)	Subscription Files are referenced by subscription definitions. A subscription file definition identifies (among other things): ■ the Adabas database ID and file number that should be audited ■ whether select, insert, delete, and update commands should be audited ■ if any, the file's alpha character encoding ■ the Format Buffer definitions that should be used for auditing	Required. At least one subscription file is required for auditing to occur. Refer to *Maintaining Subscription Definitions* in chapter *Adabas Auditing Configuration*.
Format Buffer	A Format Buffer definition stored separately for use in Subscription definitions. You can specify Format Buffers manually or generate them using Predict file definitions. When you generate them, a field table is also generated.	Required. A Format Buffer is required for Request, Client and File data. Refer to *Maintaining Format Buffer Definitions* in chapter *Adabas Auditing Configuration.*.
Audit Filters	A filter definition that filters the records used for auditing based on the values of the fields in those records.	Not required. No filter definition is required. Refer to *Maintaining Filter Definitions* in chapter *Adabas Auditing Configuration*.

Definition Specification Sequence

The applicable definitions have a sequence in which they should be set up for destination type Audit. The following table lists the definitions that apply to the destination in the order in which they should be defined.

Destination Type	Description	Definition List and Order of Creation
Audit	Audited data is written to the Audit Log of the Audit Server.	1. Destination definitions, as necessary (referenced by Subscription definitions) 2. Format Buffer definitions, if needed (can be referenced by the Subscription File definitions) 3. Subscription definitions, including at least one Subscription File definition 4. One or more Subscription File definitions (included in the Subscription definition)

Use Cases

For the purposes of the following use cases, it is assumed that Adabas Auditing has been installed into the Adabas Database. It is also assumed that the Adabas Audit Server has been installed. For information regarding the installation of the Auditing function into the Adabas Database and for Audit Server installation, refer to the *Installation* chapter.

Adabas Auditing Use Case 1

The Auditor would like to audit all data activities relating to their Payroll system.

- The Payroll application uses files 100,110, 200 and 280 on database ID 1420.

  No other files exist on database ID 1420.
- Auditing of all (!) the files used by the Payroll application is required.
- All the files contain PII (Personal Identifiable Information) and other information sensitive to employees.
- All relevant information concerning any update, delete or access of any data elements must be made available.

Relevant information should include:

- the user/job initiating the Adabas command
- the data accessed, inserted, or deleted
- for an update, the before and after values of all fields

The following are the steps required to enable Adabas Auditing to implement the above use case.

Adabas Database preparation	Adabas Audit Server preparation
Prepare database 1420 as follows: ■ Add required Adabas nucleus (ADARUN) parameters ■ Assign an Audit Name to each of the files 100, 110, 200 and 280 ■ Add required Adabas Nucleus Parameter (ADAANP) statements	Prepare the Audit Server as follows: ■ Create an Auditing Destination with SYSALA (if necessary) ■ Create Format Buffers or Format Buffers with associated Field Tables (GFFTs*) for files 100, 110, 200 and 280 ■ Create an Auditing Subscription for files 100, 110, 200 and 280

Note: GFFT is the Global Format File Table that defines the metadata related to the auditing of a particular Format Buffer (or 'view').

- Adabas Database preparation: Add required ADARUN parameters
- Adabas Database preparation: Assign an Audit Name to files 100, 110, 200 and 280
- Adabas Database preparation: Add required ADAANP statements
- Adabas Audit Server preparation: Create an Auditing Destination
- Adabas Audit Server preparation: Create Format Buffers or Format Buffers with associated Field Tables (GFFTs) for files 100, 110, 200 and 280
- Adabas Audit Server preparation: Create an Auditing Subscription for files 100, 110, 200 and 280

Adabas Database preparation: Add required ADARUN parameters

The minimum required ADARUN parameters to be added to database 1420 are:

```
ADARUN AUDITING=YES
ADARUN LAP=<size of Auditing pool>
```

For a description of these and other auditing related ADARUN parameters, refer to the *Reference* chapter > section *Pertinent ADARUN Parameters for Auditing*.

Adabas Database preparation: Assign an Audit Name to files 100, 110, 200 and 280

Each file participating in auditing must have an Audit Name. This is a user assigned 8-character value allowing audit information to be tracked. The Audit Name should be unique across all files participating in auditing. There are 2 ways to assign an Audit Name to a file:

1. Use the `AUDITNM=` parameter when the file is loaded with ADALOD.
2. Use the MODFCB function of ADADBS with the `AUDITNM=` parameter.

For more information about the use of the `AUDITNM=` parameter with ADALOD LOAD and ADADBS MODFCB, refer to the *Reference* chapter > section *Utilities Used with Adabas Auditing*.

Adabas Database preparation: Add required ADAANP statements

The files participating in auditing in database 1420 are defined using ADAANP statements that are read from the ADAANP DD. The Adabas nucleus JCL must be modified to contain a //ADAANP DD statement.

For more information on the ADAANP statements, refer to the *Reference* chapter > section *Adabas Nucleus Auditing Parameters*.

To implement this use case, the following ADAANP statements may be used:

```
ADAANP GLOBAL
ADAANP GCONNECTCOUNT=5         # connection attempts after first fails
ADAANP GCONNECTINTERVAL=300    # seconds between connection attempts
ADAANP GAPWARNINTERVAL=60      # seconds audit pool warnings supressed
ADAANP GAPWARNMESSAGELIMIT=20  # audit pool messages before supressed
ADAANP GAPWARNINCREMENT=10     Percent audit pool increment before warning
ADAANP GAPWARNPERCENT=50       Percent audit pool used before warning
ADAANP GSERVERID=1702          # default audit server to connect to
*
ADAANP FILE
ADAANP FLIST=100-300           All files between 100 and 300
*
* Adabas Access command audit collection
ADAANP    FACCACBX=YES         Collect Adabas Control Block info
ADAANP    FACCDS=YES           Collect data storage (compressed record)
ADAANP    FACCINFO=YES         Collect user info
ADAANP    FACCFB=YES           Collect format buffer
ADAANP    FACCSB=YES           Collect search buffer
ADAANP    FACCVB=YES           Collect value buffer
*
* Adabas Delete command audit collection
ADAANP    FDELACBX=YES         Collect Adabas Control Block info
ADAANP    FDELDS=YES           Collect data storage (compressed record)
ADAANP    FDELINFO=YES         Collect user info
*
* Adabas Insert command audit collection
```

```
ADAANP    FINSACBX=YES        Collect Adabas Control Block info
ADAANP    FINSDS=YES          Collect data storage (compressed record)
ADAANP    FINSINFO=YES        Collect user info
ADAANP    FINSFB=YES          Collect format buffer
*
* Adabas Update command audit collection
ADAANP    FUPDACBX=YES        Collect Adabas Control Block info
ADAANP    FUPDAI=YES          Collect data storage after image
ADAANP    FUPDBI=YES          Collect data storage before image
ADAANP    FUPDINFO=YES        Collect user info
ADAANP    FUPDFB=YES          Collect format buffer
```

Adabas Audit Server preparation: Create an Auditing Destination

The Audit Server must have a destination of type Audit defined for the auditing information to be available for analysis by auditors. An existing destination may be used or a new one may be created specifically for Payroll auditing.

Use Adabas Auditing Configuration to ensure there is a Destination of type Audit. If not, add one.

For more information pertaining to managing Audit Destinations, refer to the *Adabas Auditing Configuration* chapter.

Adabas Audit Server preparation: Create Format Buffers or Format Buffers with associated Field Tables (GFFTs) for files 100, 110, 200 and 280

A Format Buffer or GFFT must be created for each Adabas file.

A Format Buffer identifies the Adabas fields that are to be taken from the compressed record when before and/or after images from Adabas access, insert, delete, or update commands are written to the destination.

A GFFT is the Global Format File Table that defines the metadata related to the auditing of a particular Format Buffer (or ‘view’).

The format buffer or GFFT is created in Adabas Auditing Configuration and associated with the file it represents when the subscription is defined.

For information pertaining to creating format buffers and GFFTs, refer to the *Adabas Auditing Configuration* chapter.

For information pertaining to the syntax and content of a format buffer, refer to the *Adabas for Mainframes* documentation > *Command Reference* manual > section *Format Buffers*.

Adabas Audit Server preparation: Create an Auditing Subscription for files 100, 110, 200 and 280

The Audit Server must have at least one subscription containing the Payroll application files to map the incoming Audit data to a destination.

Use Adabas Auditing Configuration to add a subscription and associate the Adabas files with the subscription.

In the example below, the Adabas Auditing Configuration File-related Parameters screen has all the audit data types set to Y (yes) for all files, so that all auditing information received from the database will be written to the destination.

```
22:36:23        ***** A D A B A S  AUDITING CONFIGURATION *****      2021-01-06
                          List of Subscription SFILEs                M-RP1415
Subscription  PAYROLL     Current
      Name   PAYROLL_APPLICATION_SUBSCRIPTION                                      ↩

                    send Data        send FB   send Request  send Client
 Sel   DBID  File   S  D  I  U  BI   S  I  U   S  D  I  U    S  D  I  U
 ----------------------------------------------------------------------------
  _    1420   100   Y  Y  Y  Y  Y    Y  Y  Y   Y  Y  Y  Y    Y  Y  Y  Y
  _    1420   110   Y  Y  Y  Y  Y    Y  Y  Y   Y  Y  Y  Y    Y  Y  Y  Y
  _    1420   200   Y  Y  Y  Y  Y    Y  Y  Y   Y  Y  Y  Y    Y  Y  Y  Y
  _    1420   280   Y  Y  Y  Y  Y    Y  Y  Y   Y  Y  Y  Y    Y  Y  Y  Y
```

For more information pertaining to the creation of Audit subscriptions, refer to the *Adabas Auditing Configuration* chapter.

Adabas Auditing Use Case 2

The Payroll application from Use Case 1 has 2 new requirements.

1. File 115 was added to this application. File 115 has IRS provided data concerning tax brackets, withholding percentages and other static data. File 115 is to be excluded from auditing.
2. The data in file 280 has been determined to not contain PII or otherwise sensitive data requiring access auditing. Access auditing is to be removed for file 280, although update, add and delete auditing must remain in effect.

The following information describes the changes necessary to enable Adabas Auditing to implement this new use case.

Use Case 1 has the following file group defined for database 1420 via its ADAANP nucleus parameter statements:

```
ADAANP FILE
ADAANP FLIST=100-300          All files between 100 and 300
```

If this existing file group was kept then:

- The new file 115 would automatically be audited similarly to the other files.
- File 280 would continue to send access audit information to the audit server.

Therefore, modifications to the existing configuration are necessary to meet the auditing requirements for Use Case 2.

- Option 1: Restrict the audit data collected by database 1420 and sent to the Audit Server
- Option 2: Restrict the audit data consumed by the Audit Server subscription

Option 1, 2, or both may be implemented.

Option 1 – Restrict the audit data collected by the database 1420 and sent to the Audit Server

Adabas Database changes	Adabas Audit Server changes
Modify ADAANP statements (see below).	No modifications are necessary.

Note:

Option 1 is to control the flow of the audit information from the Adabas database to the Adabas Audit Server.

To restrict the collection of audit data as required, two changes must be made to the ADAANP configuration.

The first change is to the existing file group.

Change:

```
ADAANP FLIST=100-300
```

To:

```
ADAANP FLIST=100,110,200
```

This change eliminates file 150, and it also eliminates file 280 which will be handled by a new file group.

The second change is to add a new file group for file 280.

This file group starts like this:

```
ADAANP FILE
ADAANP FLIST=280
```

It then has the same insert, delete, and update file parameters as the existing file group. However, we change the following access file parameters to eliminate the collection of auditing information from any access (Read, Find, Histogram) commands to file 280:

```
ADAANP    FACCACBX=NO
ADAANP    FACCDS=NO
ADAANP    FACCINFO=NO
ADAANP    FACCFB=NO
ADAANP    FACCSB=NO
ADAANP    FACCVB=NO
```

Option 2 – Restrict the audit data consumed by the Audit Server subscription

Adabas Database changes	Adabas Audit Server changes
No modifications are necessary.	Modify the subscription to exclude access audit information for file 280 (file 115 is not defined to the subscription so no action is needed for file 115).

Note:

Option 2 is to allow the flow of all audit information from the Adabas database to the Adabas Audit Server and restrict the unneeded audit information from the Audit Destination with Audit Subscription changes.

To restrict the auditing information as required:

- No changes are made for file 150 as it was not defined in the subscription in the previous use case and is already restricted.
- Alter the access (referred to as S for select in Adabas Auditing Configuration) audit information for file 280 as shown below in the example Adabas Auditing Configuration File-related Parameters screen (mind, Select being of value N).

```
22:36:23        ***** A D A B A S  AUDITING CONFIGURATION *****      2021-01-06
                          List of Subscription SFILEs                M-RP1415
Subscription  PAYROLL     Current
       Name   PAYROLL_APPLICATION_SUBSCRIPTION                                  ↩

                    send Data         send FB   send Request  send Client
 Sel   DBID  File   S  D  I  U  BI    S  I  U   S  D  I  U    S  D  I  U
 -----------------------------------------------------------------------------
  _    1420   100   Y  Y  Y  Y  Y     Y  Y  Y   Y  Y  Y  Y    Y  Y  Y  Y
  _    1420   110   Y  Y  Y  Y  Y     Y  Y  Y   Y  Y  Y  Y    Y  Y  Y  Y
  _    1420   200   Y  Y  Y  Y  Y     Y  Y  Y   Y  Y  Y  Y    Y  Y  Y  Y
  _    1420   280   N  Y  Y  Y  Y     N  Y  Y   N  Y  Y  Y    N  Y  Y  Y        ↩
```

For more information pertaining to modifying Audit subscriptions, refer to the *Adabas Auditing Configuration* chapter.

Option Considerations

	Option 1: Adabas Database changes	**Option 2: Adabas Audit Server changes**
Pros	■ Removes the burden on the Adabas Database of collecting, queuing, and transferring auditing information that is unlikely to be used. ■ Removes the burden on the Adabas Audit Server of receiving and queuing auditing information that is unlikely to be used.	■ No changes to Adabas Database required. ■ Flexibility if the restricted auditing data is required at a future time.
Cons	■ More complex ADAANP configuration.	■ No reduction in the burden of the Adabas Database or Adabas Audit Server.

Adabas Auditing Use Case 3

The Payroll application from Use Case 2 has 2 new requirements:

1. Access auditing for file 110 is to be changed such that the access auditing is limited to Adabas commands where at least one of SOCIAL-SECURITY-NBR, DATE-OF-BIRTH, and ZIP-CODE (Adabas fields AC, AF and AQ) is accessed.
2. For file 200, only include the file data (compressed record) if the PAYROLL-TYPE (Adabas field AB) is ‘B’ (bonus) or ‘R’ (regular hours).

The required configuration changes are:

Adabas Database changes	Adabas Audit Server changes
Modify ADAANP statements to add a new FILE group for file 110.	Add a filter for file 200 to the Subscription.

- Adabas Database changes: Modify ADAANP statements to add a new FILE group for file 110
- Adabas Audit Server changes: Add a Filter for file 200 to the Subscription

Adabas Database changes: Modify ADAANP statements to add a new FILE group for file 110

The first change is to the existing file group.

Change:

```
ADAANP FLIST=100,110,200
```

To

```
ADAANP FLIST=100,20
```

This change eliminates file 110 which will be handled by a new file group.

The second change is to add a new file group for file 110. This file group starts like this:

```
ADAANP FILE
ADAANP FLIST=110
```

It then has the same insert, delete, and update file parameters as the FILE group for files 100 and 200. However, change the following access file parameters to restrict the access auditing information to access commands where at least one of fields AC, AF and AQ is accessed:

```
ADAANP    FACCACBX=FIELDS
ADAANP    FACCDS=FIELDS
ADAANP    FACCINFO=FIELDS
ADAANP    FACCFB=FIELDS
ADAANP    FACCSB=FIELDS
ADAANP    FACCVB=FIELDS
ADAANP    FACCFIELDS= 'AC,AF,AQ'
```

This implements the first requirement.

Adabas Audit Server changes: Add a Filter for file 200 to the Subscription

In Adabas Auditing Configuration, add a filter that includes records if field AB is equal to ‘R’ or ‘B’. The following example is a filter named FILE200.

```
19:38:34        ***** A D A B A S  AUDITING CONFIGURATION *****      2021-01-14
                              Filter Definition                      M-RP1150

Filter Name ... PAYROLL_APPLICATION_SALARY_FILE                      1 of 1
Filter ID ..... FILE200_  Exclude or Include Records .. I

          ------  Source  --------------------            -----  Target  -----
Sel Group Field   PE    MU Image  Begin Length    Cond    Field Value
--- ----- ------------------------------------    ----    --------------------
 _     1   AB                                      EQ            R,B
```

Next, associate the filter with data records for file 200 in the subscription. Modify the subscription in Adabas Auditing Configuration.

The example below adds the filter named FILE200 to the subscription used for Payroll. The filter is applied to all data records (before-image and/or after images from access, insert, delete, or update commands).

```
20:28:54        ***** A D A B A S  AUDITING CONFIGURATION *****      2021-01-14
                           File-Related Parameters                   M-RP1420

Subscription Name ............ PAYROLL_APPLICATION_SUBSCRIPTION
Subscription ID .............. PAYROLL   Current
Description .................. FILES FOR PAYROLL
DBID / File Number ........... _1420  _200
                           Format and Filter Settings
                                           Request FB ID ........... REQUEST
Data Format Buffer ID ........ FIL200FB    Request Filter ID ....... _______
Data Filter ID ............... FILE200_    MF Client FB ID .... .... ________
Data Filter FB ID ............ _______     MF Client Filter ID ..... _______
Data Origin (Mf,Luw,Both) ....             LUW Client FB ID ........ ________
                                           LUW Client Filter ID .... ________
Buffers       Data BI FB SB VB UB Req Clnt
Select cmd ...  Y      Y  N  N  N  Y   Y
Insert cmd ...  Y      Y           Y   Y
Update cmd ...  Y   Y  Y           Y   Y
Delete cmd ...  Y                  Y   Y
```

This implements the second requirement.

For detailed information pertaining to filters, refer to the *Adabas Auditing Configuration* chapter.

Product Requirements

With a basic understanding of how Adabas Auditing works, you can begin to install, configure, and run the system.

This section describes the products you need to install, implement, and operate Adabas Auditing.

- Adabas
- Natural
- Adabas Online System (AOS)
- Predict (Optional)
- Adabas Auditing

Adabas

A supported version of Adabas should already be available, with all ZAPs applied from the `ALAvrs.MVSZAPS` data set and any subsequent `ALAvrs.MVSZXnn` data sets (if they have been provided).

Note: The Adabas Audit Server must run with a minimum Adabas version of 8.5 SP1 or, if the Adabas version is greater than 8.5 SP1, the same (or later) version of Adabas as the Adabas database(s) whose data is being audited. Adabas databases whose data is to be audited may run with Adabas version 8.4 SP2 or later.

For information on installing Adabas, refer to the *Adabas for Mainframes* documentation.

Natural

A supported version of Natural should already be available to support the installation of Adabas Auditing Configuration (SYSALA) and Adabas Auditing Administration (SYSALAA).

For information on installing Natural, refer to the *Natural for Mainframes* documentation.

Adabas Online System (AOS)

A supported version of Adabas Online System (AOS) should already be available to support the installation of Adabas Auditing Configuration (SYSALA) and Adabas Auditing Administration (SYSALAA).

Be sure to follow the installation instructions in the Adabas Online System manual for licensed versions.

If you only use a demo version of Adabas Online System, note that only limited information concerning Adabas Auditing is available to you.

For information on installing the Adabas Online System, refer to the *Adabas Online System* documentation.

Predict (Optional)

If you will be using the Adabas Auditing feature that allows you to generate Format Buffers and a field table (GFFT) using Predict, a supported version of Predict must be available.

Otherwise, Format Buffers and an associated field table (GFFT) can be generated using the Adabas Auditing Configuration.

For information on installing Predict, refer to the *Predict* documentation.

Adabas Auditing

Install Adabas Auditing, as described in the *Installation* chapter.

The Installation chapter describes the following procedures in detail:

- How to install the Adabas Auditing software?
- How to create and start the Adabas Audit Server?
- How to customize Adabas nuclei for auditing?