AUDIT TRAILS AND ITS ROLE IN BUILDING QUALITY APPLICATION

NIC Webinar- Knowledge Sharing among peers
PAN INDIA

on

14th Feb 2019

G. Mayil Muthu Kumaran
Scientist – F

NIC Software Quality Group

NATIONAL INFORMATICS CENTRE

DEFINITION

"Audit Trail/ Audit Log is a ***record of Actions and events*** that takes place on a computer system. Logs are the ***primary record keepers*** of system and network activity. Log provides a clear view of ***who owns the process, what action was initiated, when it was initiated, where the action occurred*** and ***why the process ran***."

certin
Handling Computer Security Incidents

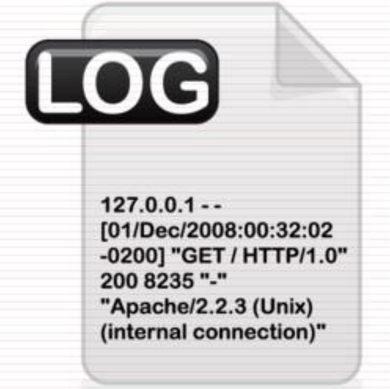
ISO/IEC 27001

ISO

ISO/IEC 27001

International Organization for Standardization and the International Electrotechnical Commission(ISO/IEC) in ISO/IEC 27001 states the standards of Information security.

Section A.10.10.2 states about Audit Trail and its monitoring, wherein the section enforces the maintenance of Audit trail or Audit Logs to assist in future investigations and access control monitoring



```
127.0.0.1 - -
[01/Dec/2008:00:32:02
-0200] "GET / HTTP/1.0"
200 8235 "-"
"Apache/2.2.3 (Unix)
(internal connection)"
```

It also demands the results to be reviewed regularly to identify possible security threats and incidents.

IMPORTANCE OF AUDIT TRAIL

- To ensure confidentiality, integrity and availability by reviewing and maintaining audit logs

- Investigate possible security incidents to reconstruct the sequence of events that preceded a problem and everything that occurred after it.

- Monitor user and system activity where appropriate, to prevent unauthorized accessing or disclosure of any sensitive information

- To ensure regulatory compliance or compliance to organization’s security policy

AUDIT LOG IN BUILDING QUALITY APPLICATION

Quality of an application greatly relies on the *security, authenticity, reliability and concurrency*.

Maintaining audit logs makes it possible to *detect and deter* penetration of any application and reveals the usage that identifies *misuse of the application*.

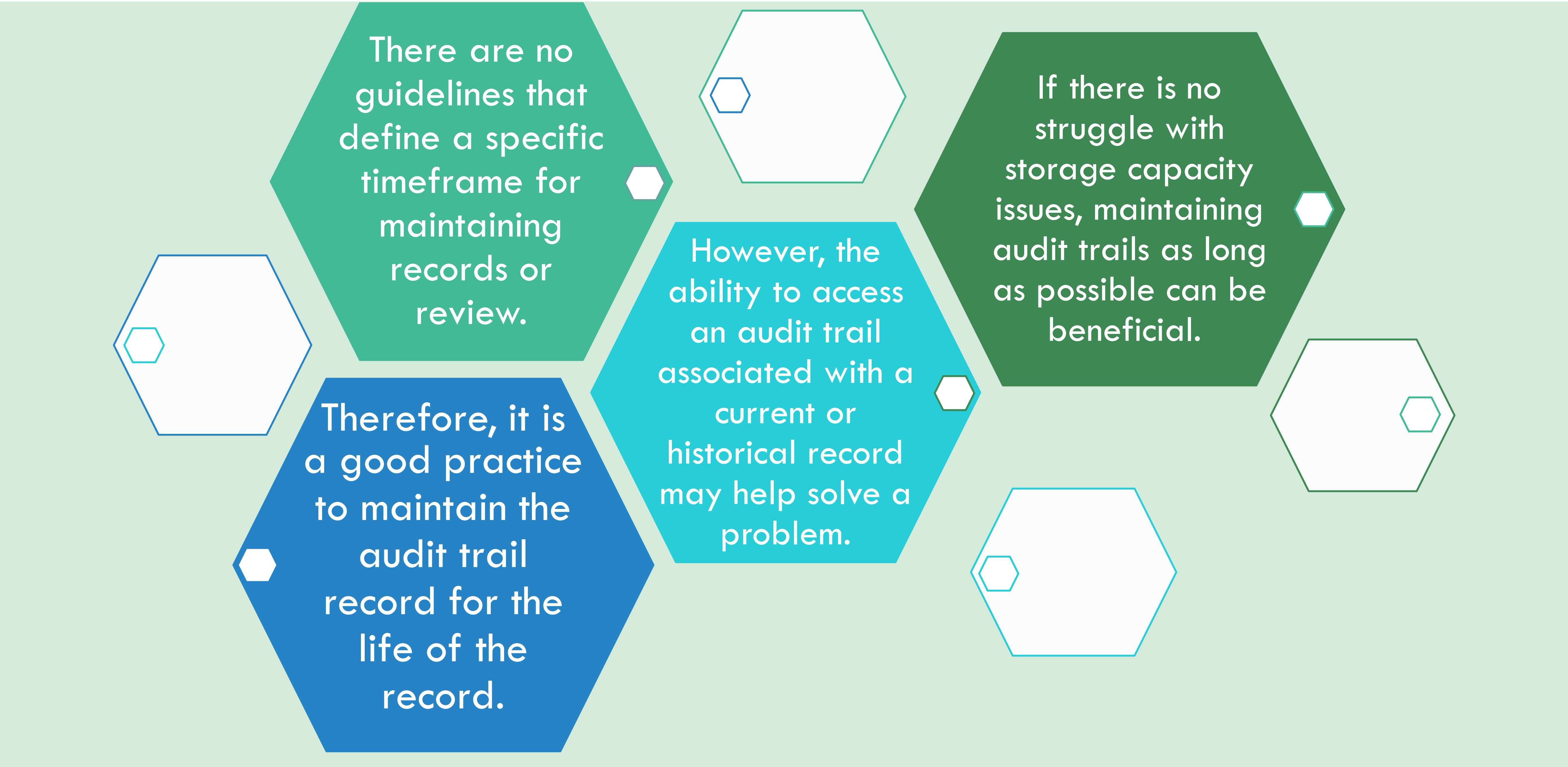
It is important that appropriate *Audit policies should be formulated* and implemented on all *Computer systems, servers and network devices* to facilitate collection of logs about all important events.

A *lapse in this area would result in deterioration in the quality* of the application as the application may not provide means of identifying mishappening.

WHAT TO LOG ?

- User IDs
- Date and time of log on and log off, and other key events
- Terminal identity
- Successful and failed attempts to access systems, data or applications
- Files and networks accessed
- Changes to system configurations and Use of system utilities
- Exceptions and other security-related events, such as alarms triggered

HOW LONG SHOULD LOGS BE KEPT ?



There are no guidelines that define a specific timeframe for maintaining records or review.

However, the ability to access an audit trail associated with a current or historical record may help solve a problem.

If there is no struggle with storage capacity issues, maintaining audit trails as long as possible can be beneficial.

Therefore, it is a good practice to maintain the audit trail record for the life of the record.

TYPES OF LOGS

System Logs

- Records system component events

Application Logs

- Logs all application level relevant activities into a system

Database Logs

- Log to track different database activities to ensure the data compliance

API Logs

- Logging API activities

SYSTEM LOGS

- The system logs entries has entries about authentication attempts, permission & privilege changes, file accesses and service starts & stops.

- These log systems facilitate application developers to diagnose application performance issues.

- Efficient system log analysis reduces system downtime, and helps in identifying unauthorized access or activity from a particular host.

WHAT IS CAPTURED (WINDOWS)

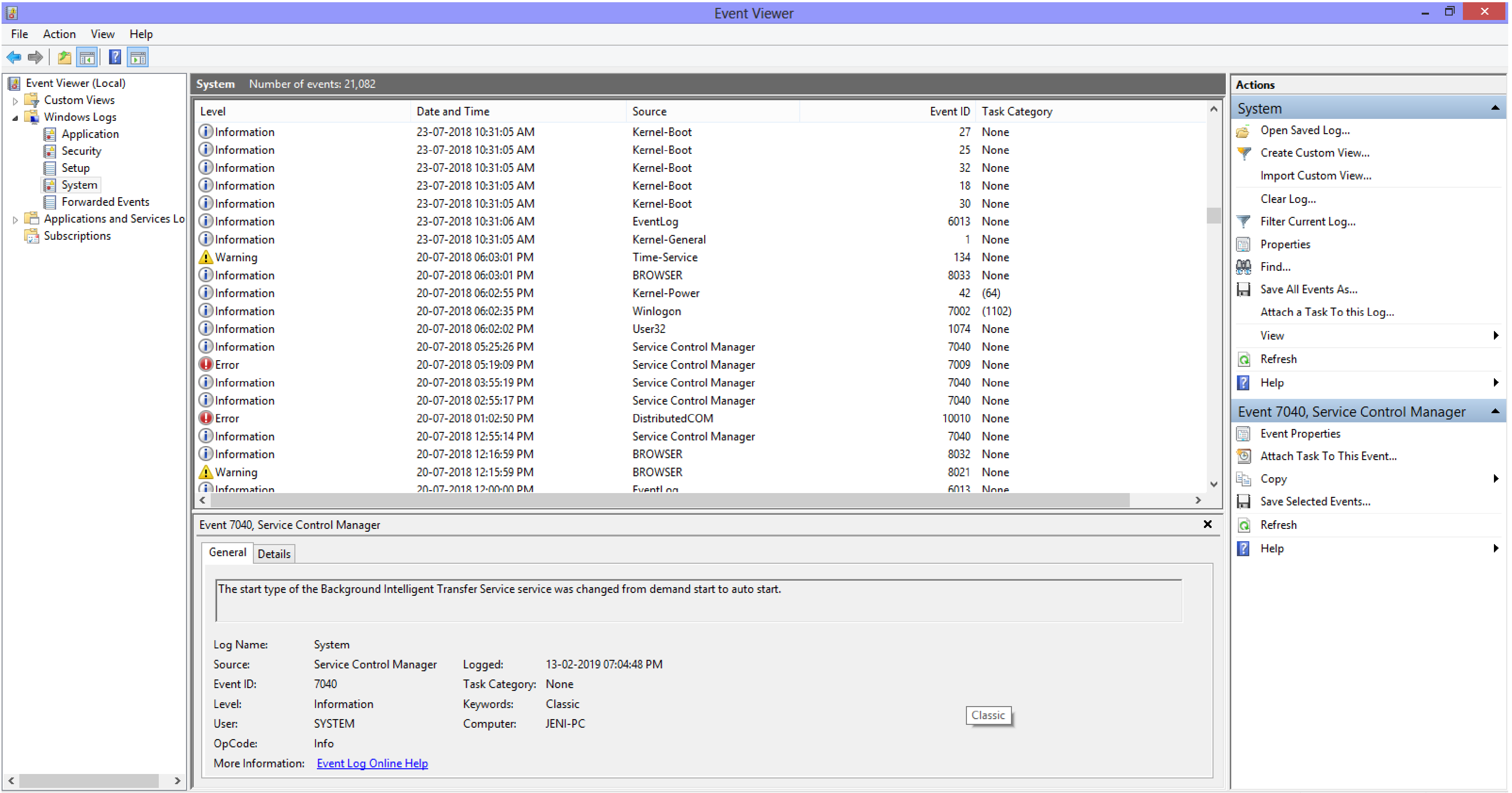
Date and Time

Source

Event ID

Level

Task Category



System Number of events: 21,082

Level	Date and Time	Source	Event ID	Task Category
Information	23-07-2018 10:31:05 AM	Kernel-Boot	27	None
Information	23-07-2018 10:31:05 AM	Kernel-Boot	25	None
Information	23-07-2018 10:31:05 AM	Kernel-Boot	32	None
Information	23-07-2018 10:31:05 AM	Kernel-Boot	18	None
Information	23-07-2018 10:31:05 AM	Kernel-Boot	30	None
Information	23-07-2018 10:31:06 AM	EventLog	6013	None
Information	23-07-2018 10:31:05 AM	Kernel-General	1	None
Warning	20-07-2018 06:03:01 PM	Time-Service	134	None
Information	20-07-2018 06:03:01 PM	BROWSER	8033	None
Information	20-07-2018 06:02:55 PM	Kernel-Power	42	(64)
Information	20-07-2018 06:02:35 PM	Winlogon	7002	(1102)
Information	20-07-2018 06:02:02 PM	User32	1074	None
Information	20-07-2018 05:25:26 PM	Service Control Manager	7040	None
Error	20-07-2018 05:19:09 PM	Service Control Manager	7009	None
Information	20-07-2018 03:55:19 PM	Service Control Manager	7040	None
Information	20-07-2018 02:55:17 PM	Service Control Manager	7040	None
Error	20-07-2018 01:02:50 PM	DistributedCOM	10010	None
Information	20-07-2018 12:55:14 PM	Service Control Manager	7040	None
Information	20-07-2018 12:16:59 PM	BROWSER	8032	None
Warning	20-07-2018 12:15:59 PM	BROWSER	8021	None
Information	20-07-2018 12:00:00 PM	EventLog	6013	None

Event 7040, Service Control Manager

General Details

The start type of the Background Intelligent Transfer Service service was changed from demand start to auto start.

Log Name:	System		
Source:	Service Control Manager	Logged:	13-02-2019 07:04:48 PM
Event ID:	7040	Task Category:	None
Level:	Information	Keywords:	Classic
User:	SYSTEM	Computer:	JENI-PC
OpCode:	Info		
More Information:	Event Log Online Help		

Classic

APPLICATION LOGS

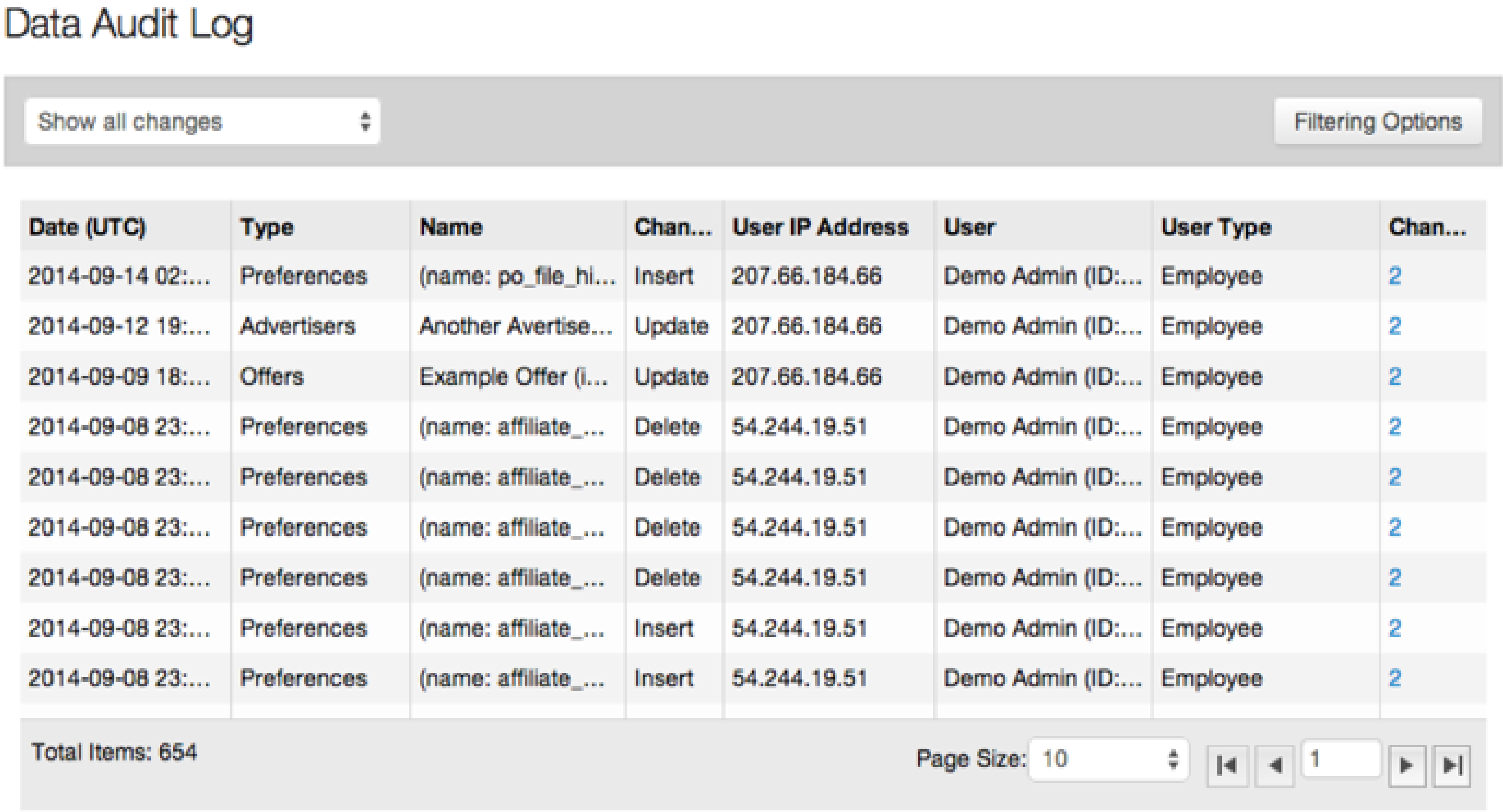
- These logs are built to be immutable, time synced and accessible by authorized users only.

- They can be maintained on a single server of application or can be distributed depending on the size and criticality of application.

- They should be planned and built such that the log information is fully exportable, available from an API and also searchable.

WHAT TO CAPTURE

- A Unique event ID and type
- Timestamp of the event
- Error message
- Success or failure of event
- IP address of the client
- User ID triggering the event
- Resources accessed
- Application Interface used by user
- Co-relation with audit trail entries



Data Audit Log

Date (UTC)	Type	Name	Chan...	User IP Address	User	User Type	Chan...
2014-09-14 02:...	Preferences	(name: po_file_hi...	Insert	207.66.184.66	Demo Admin (ID:...	Employee	2
2014-09-12 19:...	Advertisers	Another Avertise...	Update	207.66.184.66	Demo Admin (ID:...	Employee	2
2014-09-09 18:...	Offers	Example Offer (i...	Update	207.66.184.66	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Delete	54.244.19.51	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Delete	54.244.19.51	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Delete	54.244.19.51	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Delete	54.244.19.51	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Insert	54.244.19.51	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Insert	54.244.19.51	Demo Admin (ID:...	Employee	2

Total Items: 654

Page Size: 10

DATABASE LOGS

- Major categories of activities targeted by Database Logs include *Database Structure Changes, Data retrieval and modification, Authorization grants/changes* on database and other data accesses using database utilities for bulk loading or modification.

- Aim is to log and monitor all user's actions done on data and data structure thereby achieve data compliance.

MAINTAINING DATABASE AUDIT LOGS

Database security and compliance is a major concern for eGovernance applications as it not only handle citizen centric data but also most crucial and highly sensitive Ministries and other government department data.

Major Concerns in Database Security:

- Database structure and data access control
- Database data encryption and
- Database vulnerability analysis

Maintaining a database log system:

- Access control of the database and even who is viewing what data can be audited by a database log
- Data encryption can also be verified by database log review
- Database vulnerability exploitation can be traced back through a database log

AUDIT LOGS IN DIFFERENT DATABASES

Every database software provides its own built in logging options.

Oracle

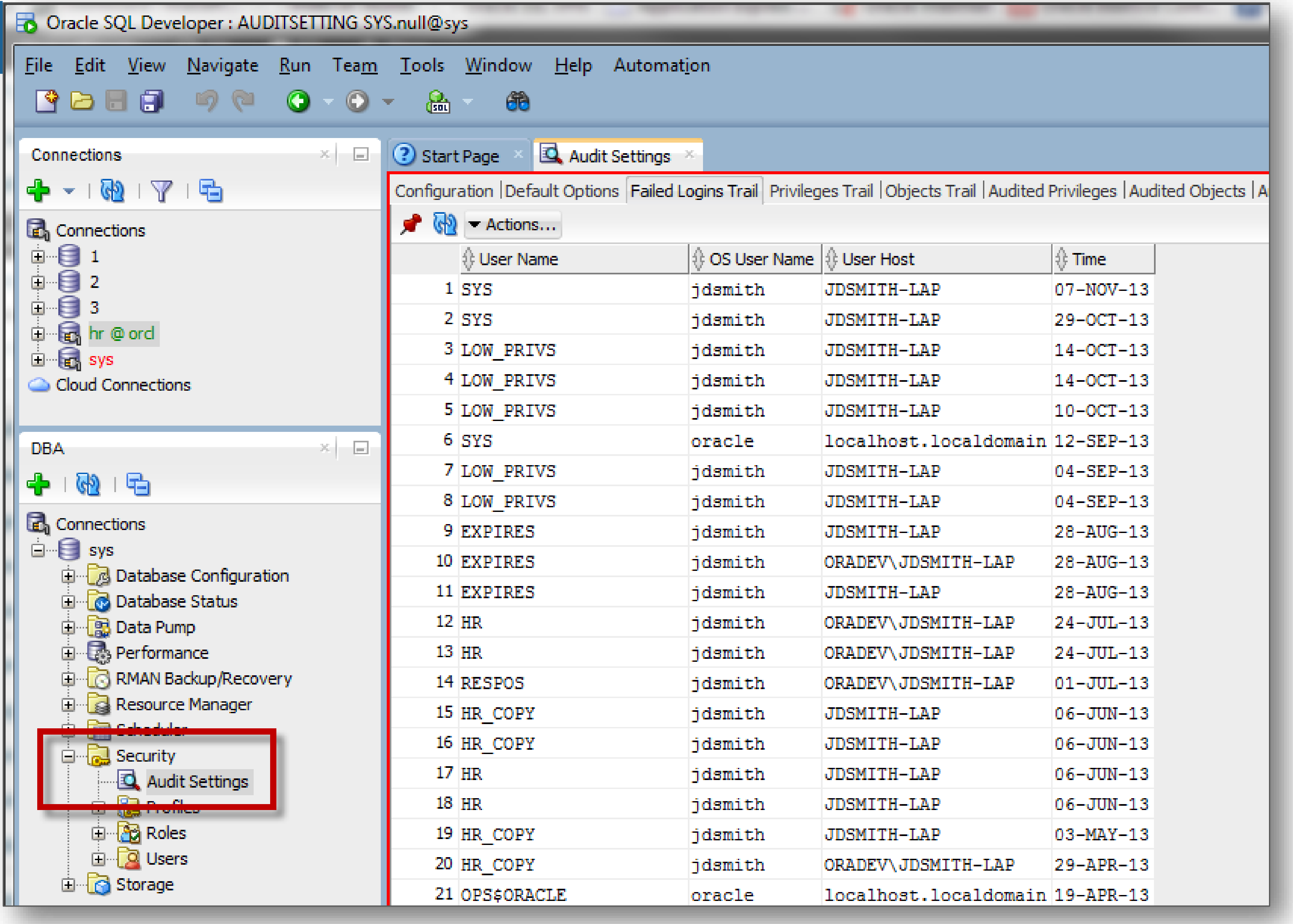
- Has built in mandatory, standard and fine-grained audit.
- Specifically, to enable mandatory auditing (off by default) one needs to set the audit_sys_operations parameter to true for the appropriate database instance.
- Enabling standard audit is done by setting the audit_trail parameter for the instance and then enabling the relevant audit options.

Postgres

- Open source database tool allows to maintain a log of activities and error messages.
- Until PostgreSQL 9.6, PostgreSQL log files were generated in pg_log directory (inside the data directory) by default.
- Since PostgreSQL 10, pg_log has been renamed to simply log.
- The parameters in file postgresql.conf can be customised as per logging requirement.

AUDIT LOGS IN DIFFERENT DATABASES

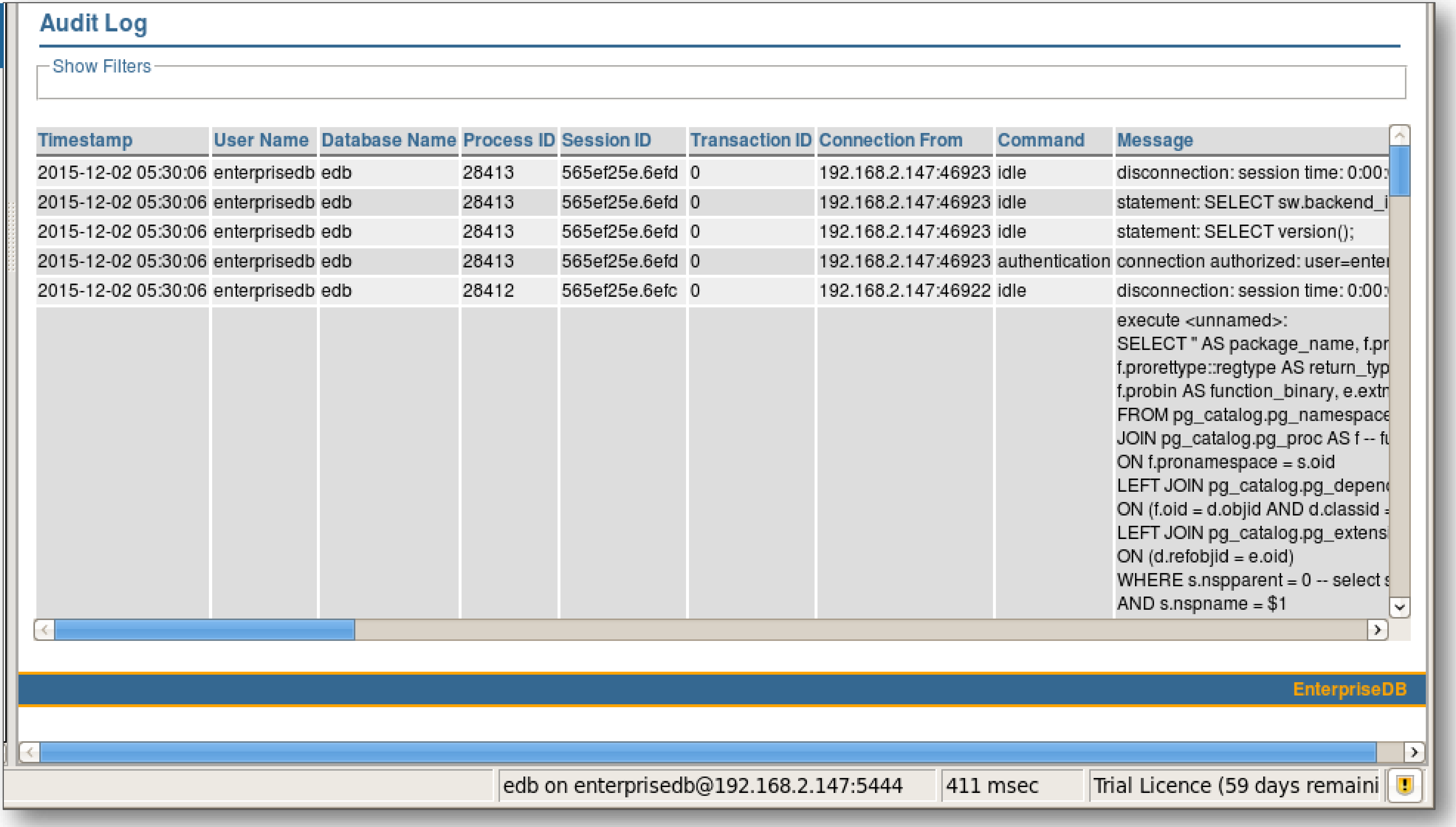
Oracle



	User Name	OS User Name	User Host	Time
1	SYS	jdsmith	JDSMITH-LAP	07-NOV-13
2	SYS	jdsmith	JDSMITH-LAP	29-OCT-13
3	LOW_PRIVS	jdsmith	JDSMITH-LAP	14-OCT-13
4	LOW_PRIVS	jdsmith	JDSMITH-LAP	14-OCT-13
5	LOW_PRIVS	jdsmith	JDSMITH-LAP	10-OCT-13
6	SYS	oracle	localhost.localdomain	12-SEP-13
7	LOW_PRIVS	jdsmith	JDSMITH-LAP	04-SEP-13
8	LOW_PRIVS	jdsmith	JDSMITH-LAP	04-SEP-13
9	EXPIRES	jdsmith	JDSMITH-LAP	28-AUG-13
10	EXPIRES	jdsmith	ORADEV\JDSMITH-LAP	28-AUG-13
11	EXPIRES	jdsmith	JDSMITH-LAP	28-AUG-13
12	HR	jdsmith	ORADEV\JDSMITH-LAP	24-JUL-13
13	HR	jdsmith	ORADEV\JDSMITH-LAP	24-JUL-13
14	RESPOS	jdsmith	ORADEV\JDSMITH-LAP	01-JUL-13
15	HR_COPY	jdsmith	JDSMITH-LAP	06-JUN-13
16	HR_COPY	jdsmith	JDSMITH-LAP	06-JUN-13
17	HR	jdsmith	JDSMITH-LAP	06-JUN-13
18	HR	jdsmith	JDSMITH-LAP	06-JUN-13
19	HR_COPY	jdsmith	JDSMITH-LAP	03-MAY-13
20	HR_COPY	jdsmith	ORADEV\JDSMITH-LAP	29-APR-13
21	OPS$ORACLE	oracle	localhost.localdomain	19-APR-13

AUDIT LOGS IN DIFFERENT DATABASES

Postgres



Audit Log

Show Filters

Timestamp	User Name	Database Name	Process ID	Session ID	Transaction ID	Connection From	Command	Message
2015-12-02 05:30:06	enterprisedb	edb	28413	565ef25e.6efd	0	192.168.2.147:46923	idle	disconnection: session time: 0:00:
2015-12-02 05:30:06	enterprisedb	edb	28413	565ef25e.6efd	0	192.168.2.147:46923	idle	statement: SELECT sw.backend_i
2015-12-02 05:30:06	enterprisedb	edb	28413	565ef25e.6efd	0	192.168.2.147:46923	idle	statement: SELECT version();
2015-12-02 05:30:06	enterprisedb	edb	28413	565ef25e.6efd	0	192.168.2.147:46923	authentication	connection authorized: user=ente
2015-12-02 05:30:06	enterprisedb	edb	28412	565ef25e.6efc	0	192.168.2.147:46922	idle	disconnection: session time: 0:00:
								execute <unnamed>: SELECT '' AS package_name, f.pr f.prorettype::regtype AS return_typ f.probin AS function_binary, e.extr FROM pg_catalog.pg_namespace JOIN pg_catalog.pg_proc AS f -- fu ON f.pronamespace = s.oid LEFT JOIN pg_catalog.pg_depend ON (f.oid = d.objid AND d.classid = LEFT JOIN pg_catalog.pg_extensi ON (d.refobjid = e.oid) WHERE s.nspparent = 0 -- select s AND s.nspname = $1

edb on enterprisedb@192.168.2.147:5444 | 411 msec | Trial Licence (59 days remaini

API LOGS

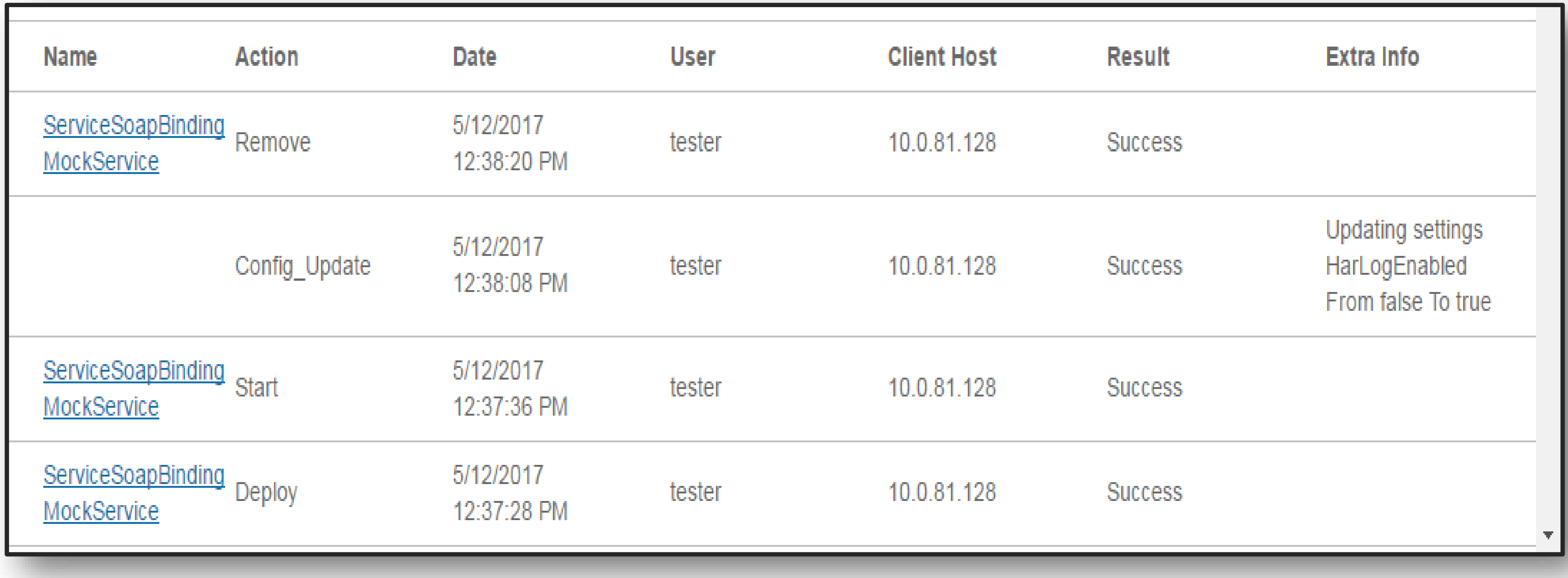
An API logging system should be able to provide information on how the API is used, who is using it, when its consumption reached the peak value, etc..

API Logging System features:

- Activity Logging captures and provides basic logging information for an API i.e.
  - ✓ Who is using the API
  - ✓ The IP address of the devices from where the request for API coming
  - ✓ Types of application(s) consuming API
  - ✓ Synced time and date when the request for consumption received and response was sent for every API call
  - ✓ Response / error Codes (if any generated)
- API Analytics
- Reports

WHAT TO CAPTURE

- Date with Timestamp
- Client IP Address
- Client Port
- Server IP Address
- Server Port
- Protocol Version
- URL + Query
- Protocol Status
- Response(type of error)



Name	Action	Date	User	Client Host	Result	Extra Info
ServiceSoapBinding MockService	Remove	5/12/2017 12:38:20 PM	tester	10.0.81.128	Success	
	Config_Update	5/12/2017 12:38:08 PM	tester	10.0.81.128	Success	Updating settings HarLogEnabled From false To true
ServiceSoapBinding MockService	Start	5/12/2017 12:37:36 PM	tester	10.0.81.128	Success	
ServiceSoapBinding MockService	Deploy	5/12/2017 12:37:28 PM	tester	10.0.81.128	Success	

TOOLS FOR AUDIT TRAILS

Database

- EventLog Analyzer (Oracle)
- Pgaudit (Postgres)
- audit-trigger 91plus (Postgres)
- CyanAudit (Postgres)

- Open Source Log Management Tool

syslog-ng
open source edition

GoAccess

- **GoAccess** is an open source **real-time web log analyzer** and interactive viewer that runs in a **terminal** in *nix systems or through the **browser.**

TOOLS FOR AUDIT TRAILS

- Free and open-source log management platform that supports in-depth log collection and analysis.

- Logmatic is an Open Source logging management software that integrates seamlessly with any language or stack.

Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. Fluentd helps you unify your logging infrastructure. (Open Source)

CHALLENGES ASSOCIATED WITH MANAGING AUDIT TRAIL

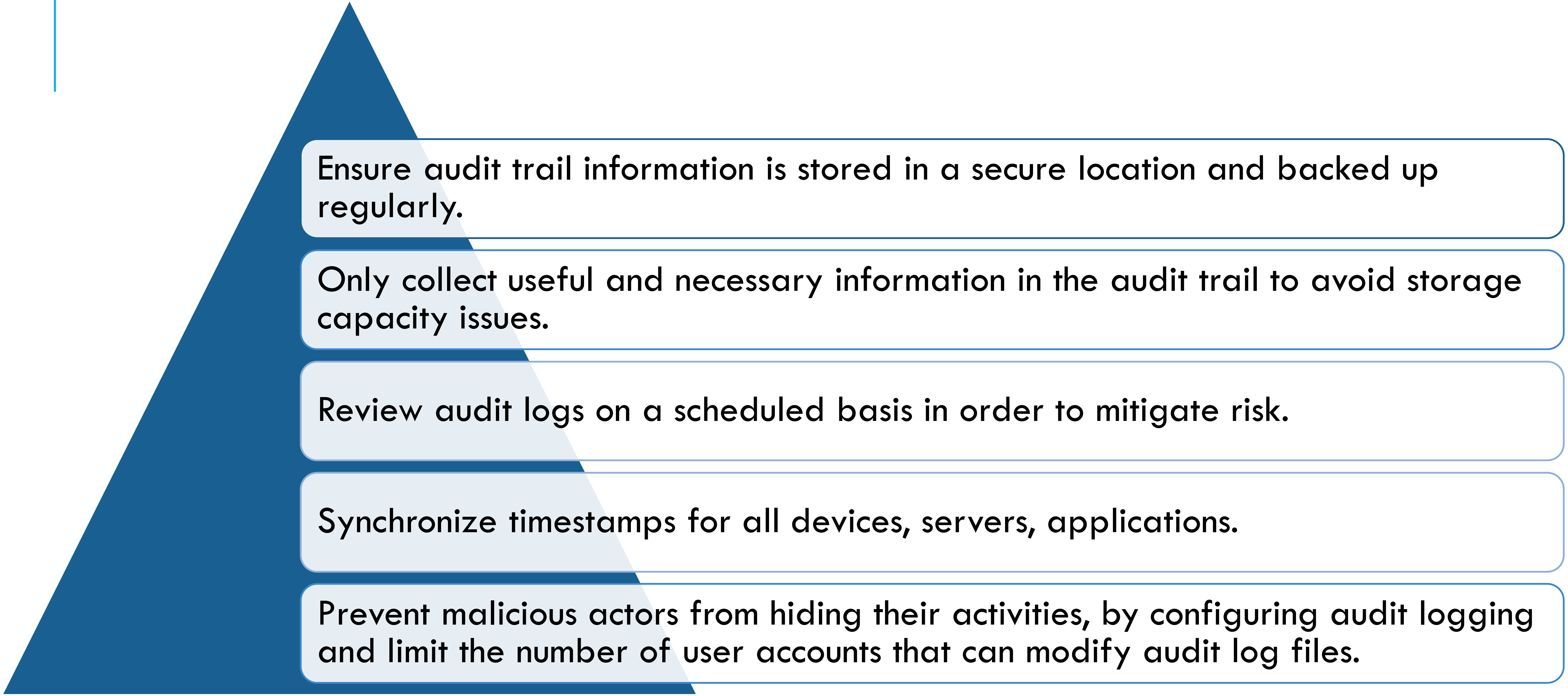
The logs may be cumbersome to navigate as they increase in size, which can cause storage cost challenges.

Access may be too broad, which can compromise the integrity of the data.

How long to keep records ?

Maintaining or managing an audit trail including the location used for storage, size, and access

BEST PRACTICES



Ensure audit trail information is stored in a secure location and backed up regularly.

Only collect useful and necessary information in the audit trail to avoid storage capacity issues.

Review audit logs on a scheduled basis in order to mitigate risk.

Synchronize timestamps for all devices, servers, applications.

Prevent malicious actors from hiding their activities, by configuring audit logging and limit the number of user accounts that can modify audit log files.

Thank you !

support-sqg@nic.in

IP : 5748