Auditing

Auditing is the ability to monitor selected user actions according to a defined security policy. In Jethro, audit messages are logged in an audit log file per server.

Audit log file name:

jethro_audit.log

The Audit message are divided into categories (Can be turned on/off in jethrolog.properties):

AUDIT.AUTHENTICATION

AUDIT.AUTHORIZATION

Audit message properties

Property	Value
Event timestamp	<timestamp>
Category	AUTHENTICATION | AUTHORIZATION
Session	<session_id>
Request id	<request_id>
Operation	LOGIN | RECONNECT | <sql-command-type>
User	<username>
IP	<client_ip_address>
Object type	INSTANCE | SCHEMA | TABLE | VIEW
Resource	<object-identifier> | other
Required permission	SELECT | INSERT | ALL
Allowed	True | False

Events triggering audit messages

AUTHENTICATION:

- Upon user first connect attempt, logs the logging attempt: operation LOGIN, the available details, and marks allowed true/false.
- Upon reconnect attempt, logs the reconnect attempt: operation RECONNECT, the available details, and marks allowed true/false.

AUTHORIZATION:

- Upon check of permission to an object issue, log message with all the available details.

See also

Authorization

Authentication