/**********************

The following is a set of example filters that can be created for use with the MySQL Enterprise Audit product to meet STIG requirements.

Before being used, auditing must first be configured to be enabled within the MySQL 8.0 Enterprise Edition Server.

The MySQL audit filters are capable of coarse or very fine-grained auditing for all or specific users. For more information, go to https://dev.mysql.com/doc/refman/8.0/en/audit-log-filtering.html.

For specifics on the JSON filters, go to https://dev.mysql.com/doc/refman/8.0/en/audit-log-filter-definitions.html#audit-log-filtering-enabling-logging.

Once enabled, the DBA can assess what to audit. This could be broad, for example every connection, statement, and action by every user whether a success or failure; or narrow, watching specific actions or action types on specific tables, etc.

This supplement will start with filter examples, which will audit more items, including much of what is required by many auditing STIG requirements, recognizing that sometimes systems cannot handle the storage overhead of auditing every action, and providing specific filtering examples.

Each example shows setting a MySQL variable string:

```
SET @<filter parameter name>=<JSON Filter>;
```

That JSON sting is used in the process of creating an audit filter:

```
SELECT audit_log_filter_set_filter('<a name for the filter>',@<filter parameter name>);
```

Next, the filter is set as the default for all users in the MySQL Server by binding it to "'%'".

For example:

```
SELECT audit_log_filter_set_user('%',' failpermissionreadfilter ');
```

OR

The filter is set to a specific user.

```
SELECT audit_log_filter_set_user('user1@localhost', 'log_user1_access');
```

**************************/

/*****

Filter Example 1: This filter is for full logging and will log every event. This would satisfy any STIG auditing requirement. However, use with caution as the audit log will grow quickly on an active system.

******/

```
SET @log_all ='{ "filter": { "log": true } }';
```

/*****

Filter Example 2: This filter is for full logging of all connection attempts.

******/

```
SET @log_all_connection_attemtps = '{ "filter": { "class": { "name": "connection" } } }';
```

/***

Filter Example 3: Only audit failed connections.

******/

```
set @filter_failed_connections = '{ "filter": { "class": { "name": "connection",
                       "event": { "name": "connect",
                             "log": { "not": { "field": { "name": "status",
                                              "value": 0 } } } } } } }';
```

/*****

Filter Example 4: Generate audit records when any unsuccessful accesses to objects occur.

*****/

```
set @fl='{
 "filter": {
   "class": {
   "name": "general",
     "event": {
       "name": "status",
       "log": {
         "not": { "field": { "name": "general_error_code", "value": 0 }}
       }
     }
   }
 }
}';
```

```
/*****

Filter Example 5: This filter is used specifically to audit failed attempts to read, insert, delete, or
update details on the mysql schema tables related to users, permissions, and privileges.

The JSON example below looks for read failures by using:

"event": { "name": "read" ,
You could modify for just insert
"event": { "name": "insert" ,
Or use a JSON array to look for one or more from read, insert, delete, update:
"event": { "name": [ "delete", "insert", "update" ],

The filter example is looking for non-zero status values. This indicates a failure as the audit
writes only when an error code occurs.

"log" : { "not": { "field": { "name": "general_error_code", "value": 0 } }

*****/

SET @fail_permissionobj_read_filter =
'{ "filter": { "id": "main",
            "class": [ { "name": "connection",
                       "log": true,
                       "event": { "name": "change_user", "log": false } },
                     { "name": "table_access",
                       "event": { "name": "read" ,
                                "log": false,
                                "filter": { "activate": { "or":
                                { "and": [ { "field": { "name": "table_database.str", "value": "mysql" } },
                                { "field": { "name": "table_name.str", "value": "user" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value":
"information_schema" } },
                                { "field": { "name": "table_name.str", "value": "user_privileges" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value": "mysql" } },
                                { "field": { "name": "table_name.str", "value": "db" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value": "mysql" } },
                                { "field": { "name": "table_name.str", "value": "global_grants" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value": "mysql" } },
                                { "field": { "name": "table_name.str", "value": "tables_priv" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value": "mysql" } },
                                { "field": { "name": "table_name.str", "value": "procs_priv" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value": "mysql" } },
                                { "field": { "name": "table_name.str", "value": "proxies_priv" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value": "mysql" } },
                                { "field": { "name": "table_name.str", "value": "columns_priv" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value": "mysql" } },
                                { "field": { "name": "table_name.str", "value": "procs_priv" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value": "mysql" } },
                                { "field": { "name": "table_name.str", "value": "role_edges" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value": "mysql" } },
                                { "field": { "name": "table_name.str", "value": "default_roles" } } ] }
                                ] },
                                "class": { "name": "general",
                                "event": { "name": "status",
                                "log" : { "not": { "field": { "name": "general_error_code", "value": 0 } } },
                                "filter": { "ref": "main" } } } } } } ] } }';
```

/*****

Filter Example 6: This filter is used specifically to audit calls to MySQL Statements within the following command types. This filter looks at the specific type of actions, versus examples 4 and 5, which look at internal MySQL tables. This example audits both successful and failed attempts.

For a complete list of general_sql_command values, run the following SQL:

```
SELECT NAME FROM performance_schema.setup_instruments
    WHERE NAME LIKE 'statement/sql/%' ORDER BY NAME;
```

The example filter below can be modified by adding or removing lines or substituting sql_command names desired.

*****/

```
set @filter_dcl_command_types = '{
  "filter": {
    "class": {
      "name": "general",
      "event": {
        "name": "status",
        "log": {
          "or": [
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "alter_user" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "alter_user_default_role" } } ]
},
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "alter_user" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "create_role" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "create_user" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "create_user" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "drop_role" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "drop_role" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "drop_user" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "drop_user" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "grant_roles" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "grant_roles" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "grant" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "rename_user" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "revoke" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "revoke_all" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "revoke_roles" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "set_role" } } ] },
{ "and": [ { "field": { "name": "general_sql_command.str",    "value": "show_create_user" } } ] }
     ]
    }
   }
  }
 }
}';
```

/*****

Filter Example 7: This is a general example for watching specific tables, in this case for reads, but "insert", "update", or "delete" could be added to the line.

```
"event": { "name": "read" ,
```

This can be modified for just insert:

```
"event": { "name": "insert" ,
```

Or use a JSON array to look for 1 or more from read, insert, delete, update

```
"event": { "name": [ "delete", "insert", "update" ],
```

The database and table name should be completed to match the specifics desired.

****/

```
SET @filter_fail_table_reads =
'{ "filter": { "id": "main",
       "class": [ { "name": "connection",
             "log": true,
             "event": { "name": "change_user", "log": false } },
            { "name": "table_access",
             "event": { "name": "read" ,
                   "log": false,
                   "filter": { "activate": { "or":
                   { "and": [ { "field": { "name": "table_database.str", "value":
"<schema/database name>" } },
                   { "field": { "name": "table_name.str", "value": "<tablename1>" } } ] },
                   { "and": [ { "field": { "name": "table_database.str", "value":
"<schema/database name>" } },
                   { "field": { "name": "table_name.str", "value": "<tablename1>" } } ] }
                   ] },
                   "class": { "name": "general",
                   "event": { "name": "status",
                   "log" : { "not": { "field": { "name": "general_error_code", "value": 0 } } },
                   "filter": { "ref": "main" } } } } } } ] } }';
```

/****

Filter Example 8: The following is a more complex filter example. In this case, it generates audit records when security objects are deleted. (Denoted by looking for “drop_table” or “rename_table” command types for the list of security objects within MySQL.)
*****/

```
SET @filter_seccurity_objects_deleted = '
{ "filter":
 { "id": "main",
 "class":
 [
   { "name": "connection" },
   { "name": "general",
     "event":
     { "name": "status",
       "log":
       {
         "and":
         [
           {
             "or":
             [
               {"field": { "name": "general_command.str", "value": "Query" }},
               {"field": { "name": "general_command.str", "value": "Execute" }}
             ]
           },
           {
             "or":
             [
               {"field": { "name": "general_sql_command.str", "value": "drop_table" }},
               {"field": { "name": "general_sql_command.str", "value": "rename_table" }}
             ]
           }
         ]
       }
     }
   },
   { "name": "table_access",
     "event":
     { "name": "update",
       "log": true,
       "filter":
       {
         "activate":
         {
           "or":
           [ { "and":
               [
                 { "field": { "name": "table_database.str", "value": "mysql"}},
                 { "field": { "name": "table_name.str", "value": "user"} }
               ]
             },
             { "and":
               [
                 { "field": { "name": "table_database.str", "value": "information_schema"}},
                 { "field": { "name": "table_name.str", "value": "user_privileges"} }
               ]
             },

             { "and":
               [
                 { "field": { "name": "table_database.str", "value": "mysql"}},
                 { "field": { "name": "table_name.str", "value": "db"} }
               ]
             },

             { "and":
               [
                 { "field": { "name": "table_database.str", "value": "mysql"}},
                 { "field": { "name": "table_name.str", "value": "global_grants"} }
               ]
             },

             { "and":
               [
                 { "field": { "name": "table_database.str", "value": "mysql"}},
                 { "field": { "name": "table_name.str", "value": "tables_priv"} }
               ]
             },

             { "and":
               [
                 { "field": { "name": "table_database.str", "value": "mysql"}},
                 { "field": { "name": "table_name.str", "value": "procs_priv"} }
               ]
             },

             { "and":
               [
                 { "field": { "name": "table_database.str", "value": "mysql"}},
                 { "field": { "name": "table_name.str", "value": "proxies_priv"} }
               ]
             },

             { "and":
               [
                 { "field": { "name": "table_database.str", "value": "mysql"}},
                 { "field": { "name": "table_name.str", "value": "columns_priv"} }
               ]
             },

             { "and":
                     [
                      { "field": { "name": "table_database.str", "value": "mysql"}},
                      { "field": { "name": "table_name.str", "value": "role_edges"} }
                     ]
                    },
                    { "and":
                     [
                      { "field": { "name": "table_database.str", "value": "mysql"}},
                      { "field": { "name": "table_name.str", "value": "default_roles"} }
                     ]
                    }
                   ]
                  },
                  "class":
                  {
                   "name": "general",
                   "event":
                   {
                    "name": "status",
                    "log": false,
                    "filter": { "ref": "main"}
                   }
                  }
                 }
                }
               }
              ]
             }
             }
             ';
```

/*****

Filter Example 9: This filter generates audit records when successful access to specified objects occurs. Below is a JSON example to filter only successfully executed INSERT/UPDATE/DELETES statements for some specific database/tables. (Read could also be added to audit selects.)

```
@filter_successful_access=
{
 "filter":
 {
  "id": "main",
  "class":
  {
    "name": "table_access",
    "event":
   {
    "name": [ "delete", "insert", "update" ],
    "log": false,
      "filter":
      {
        "activate": { "or": [ { "and": [ { "field": { "name": "table_database.str", "value": "db_1" } },
                                           { "field": { "name": "table_name.str", "value": "table_1" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value": "db_2" } },
                                           { "field": { "name": "table_name.str", "value": "table_2" } } ] },
                                { "and": [ { "field": { "name": "table_database.str", "value": "db_3" } },
                                           { "field": { "name": "table_name.str", "value": "table_3" } } ] }
                             ]
                     },
        "class": { "name": "general",
          "event":
            {
              "name": "status",
              "log": { "field": { "name": "general_error_code", "value": 0 } },
              "filter": { "ref": "main" }
            }
        }
      }
    }
   }
  }
}

/*
Example to STIG Cross-Reference: If specific filters are needed for the list below, see the
referenced example. Note the example may need slight modification. How to modify is noted in
those examples.
*/

/***
AU-12 c     CCI-000172       SRG-APP-000492-DB-000333
Filter Example 5

AU-12 c     CCI-000172       SRG-APP-000494-DB-000344
Filter Example 7

AU-12 c     CCI-000172       SRG-APP-000494-DB-000345
Filter Example 7

AU-12 c     CCI-000172       SRG-APP-000495-DB-000326
Filter Example 6

AU-12 c     CCI-000172       SRG-APP-000495-DB-000327
Filter Example 6

AU-12 c     CCI-000172       SRG-APP-000495-DB-000328
Filter Example 6

AU-12 c     CCI-000172       SRG-APP-000495-DB-000329
Filter Example 6
```

AU-12 c CCI-000172 SRG-APP-000496-DB-000334
Filter Example 5

AU-12 c CCI-000172 SRG-APP-000496-DB-000335
Filter Example 5

AU-12 c CCI-000172 SRG-APP-000498-DB-000346
Filter Example 5

AU-12 c CCI-000172 SRG-APP-000498-DB-000347
Filter Example 6

AU-12 c CCI-000172 SRG-APP-000499-DB-000330
Filter Example 5

AU-12 c CCI-000172 SRG-APP-000499-DB-000331
Filter Example 5

AU-12 c CCI-000172 SRG-APP-000501-DB-000336
Filter Example 8

AU-12 c CCI-000172 SRG-APP-000501-DB-000337
Filter Example 8

AU-12 c CCI-000172 SRG-APP-000502-DB-000348
Filter Example 6

AU-12 c CCI-000172 SRG-APP-000502-DB-000349
Filter Example 6

AU-12 c CCI-000172 SRG-APP-000503-DB-000350
Filter Example 2

AU-12 c CCI-000172 SRG-APP-000503-DB-000351
Filter Example 2

AU-12 c CCI-000172 SRG-APP-000504-DB-000354
Filter 1 or Filter Example 6

AU-12 c CCI-000172 SRG-APP-000504-DB-000355
Filter 1 or Filter Example 6

AU-12 c CCI-000172 SRG-APP-000505-DB-000352
Related to audit data format – meets.

AU-12 c CCI-000172 SRG-APP-000506-DB-000353
Related to audit data format – meets.

AU-12 c CCI-000172 SRG-APP-000507-DB-000356
Filter Example 7

AU-12 c CCI-000172 SRG-APP-000507-DB-000357
Filter Example 4

AU-12 c CCI-000172 SRG-APP-000508-DB-000358
Filter Example 4

AU-14 (1) CCI-001464 SRG-APP-000092-DB-000208
Filter Example 2

AU-3 CCI-001487 SRG-APP-000100-DB-000201
Related to audit data format – meets.

***/