

Table of Contents

User logs

Log Details

Job logs

.....

.....

.....

3

4

4

User logs

All actions within netYCE are logged to offer an audit trail. These are actions performed by the users and of some of the back-end functions (e.g. tftp server). User actions like the editing of variables are logged extensively as are the additions and deletes. The actions performed by the (scheduled) Jobs are not included in this log although the submission of these jobs by the users are. The Job execution results have their own log, the Job Logs.

The user action Log can accessed from the '**Operate - Logs**' or from '**Admin - Logs**' menus. The 'Change Logs' form shows the historical Logs in pages of 100 entries, the most recent at the top.

By default the logs are filtered for the entries of the current user (or **Operator**), but can be modified to any other known user or for – All – users. New Log entries inserted while the form is open are not shown.

User Action logs

Users:

-all-

Me

All

Month: Day:

Operator	Action	Name	Message	Timestamp
sanjay	Delete complianc...	2685	Delete 'I records from table 'NCCM.Cmpl_condition' Keys: Rule_id = 2685 Rule_id = 2685 Condition_L...	2022-04-28 20:08:49
sanjay	Delete complianc...	2683	Delete ' records from table 'NCCM.Cmpl_rule' Keys: Rule_id = 2683 Policy_id = 1647 Rule_id = 2683 R...	2022-04-28 20:08:49
sanjay	Delete complianc...	2683	Delete ' records from table 'NCCM.Cmpl_condition' Keys: Rule_id = 2683 Rule_id = 2683 Condition_L...	2022-04-28 20:08:49
sanjay	Delete complianc...	2681	Delete 'I records from table 'NCCM.Cmpl_rule' Keys: Rule_id = 2681 Policy_id = 1647 Rule_id = 2681 Ru...	2022-04-28 20:08:49
sanjay	Delete complianc...	2681	Delete 'I records from table 'NCCM.Cmpl_condition' Keys: Rule_id = 2681 Rule_id = 2681 Condition_id ...	2022-04-28 20:08:49
sanjay	Delete complianc...	2679	Delete 'I records from table 'NCCM.Cmpl_rule' Keys: Rule_id = 2679 Policy_id = 1647 Rule_id = 2679 R...	2022-04-28 20:08:49
sanjay	Delete complianc...	2679	Delete 'I records from table 'NCCM.Cmpl_condition' Keys: Rule_id = 2679 Rule_id = 2679 Condition_id...	2022-04-28 20:08:49
sanjay	Delete complianc...	2677	Delete 'I records from table 'NCCM.Cmpl_rule' Keys: Rule_id = 2677 Policy_id = 1647 Rule_id = 2677 Ru...	2022-04-28 20:08:49
sanjay	Delete complianc...	2677	Delete '3 records from table 'NCCM.Cmpl_condition' Keys: Rule_id = 2677 Rule_id = 2677 Condition_L...	2022-04-28 20:08:49
sanjay	Delete complianc...	2675	Delete 'I records from table 'NCCM.Cmpl_rule' Keys: Rule_id = 2675 Policy_id = 1647 Rule_id = 2675 R...	2022-04-28 20:08:49
sanjay	Delete complianc...	2675	Delete 'I records from table 'NCCM.Cmpl_condition' Keys: Rule_id = 2675 Rule_id = 2675 Condition_id...	2022-04-28 20:08:49
sanjay	Delete complianc...	2673	Delete 'I records from table 'NCCM.Cmpl_rule' Keys: Rule_id = 2673 Policy_id = 1647 Rule_id = 2673 Ru...	2022-04-28 20:08:49
sanjay	Delete complianc...	2673	Delete 'I records from table 'NCCM.Cmpl_condition' Keys: Rule_id = 2673 Rule_id = 2673 Condition_id...	2022-04-28 20:08:49
sanjay	Delete complianc...	2671	Delete 'I records from table 'NCCM.Cmpl_rule' Keys: Rule_id = 2671 Policy_id = 1647 Rule_id = 2671 Ru...	2022-04-28 20:08:49
sanjay	Delete complianc...	2671	Delete 'I records from table 'NCCM.Cmpl_condition' Keys: Rule_id = 2671 Rule_id = 2671 Condition_id ...	2022-04-28 20:08:49
sanjay	Delete complianc...	2669	Delete 'I records from table 'NCCM.Cmpl_rule' Keys: Rule_id = 2669 Policy_id = 1647 Rule_id = 2669 R...	2022-04-28 20:08:49
sanjay	Delete complianc...	2669	Delete 'I records from table 'NCCM.Cmpl_condition' Keys: Rule_id = 2669 Rule_id = 2669 Condition_L...	2022-04-28 20:08:49
sanjay	Delete complianc...	2667	Delete 'I records from table 'NCCM.Cmpl_rule' Keys: Rule_id = 2667 Policy_id = 1647 Rule_id = 2667 R...	2022-04-28 20:08:49
sanjay	Delete complianc...	2667	Delete 'I records from table 'NCCM.Cmpl_condition' Keys: Rule_id = 2667 Rule_id = 2667 Condition_id...	2022-04-28 20:08:49
sanjay	Delete complianc...	2665	Delete 'I records from table 'NCCM.Cmpl_rule' Keys: Rule_id = 2665 Policy_id = 1647 Rule_id = 2665 R...	2022-04-28 20:08:49

◀

◀

24

/ 14885

▶

▶

20

Items per page

461 - 480 of 297688 items

View

Three categories of Filters can be used search logs. The **Action** column defines the type of action performed, the **Name** column the relevant object name or names (e.g. site name or node name). The most detail is available in the **Message** column, although only the first line of the message is displayed. when using a Message filter, the entire message is searched.

The filter strings support wildcard searches but will rarely be needed since the entered string will be treated as a case insensitive substring. To use wildcards, use the SQL characters % and _ for 'none or several characters' (like '*') and 'one character' (like '?') respectively. When using multiple filters, the resulting logs will meet all criteria.

Using the date filter, results can now be sorted both by month, and by day in order to narrow down the searches.

Log Details

The Log Details are opened by double clicking any Log entry. Many logs offer additional details using multiple lines in the message. If the operator has sufficient access rights, these are displayed in the Log Details.

The kind of details available differ per message type. For the logs resulting from editing variables in the various forms, the next format is used:

```
o 1st line = "Updated <object> (<table>)"
o 2nd line = "Keys: <key> = <value>, <key> = <value>, ..."
o 3rd line = ""
o 4th line = <variable>:
o 5th line = "  <old-value> => <new-value>"
o remaining lines as #4, #5 for other changed variables
```

When the variable contains a multiline value, the 5th line is replaced by a more elaborate section that consists of the **diff** (formatted differences) between the old and new values followed by the full new value. Various lines with – – are used for demarcation of the sections.

Action Log 4543029 ✕

Operator: sanjay

Name: 2675

Action: Delete compliance rule

Message

```
Delete '1' records from table 'NCCM.Cmpl_rule'
Keys: Rule_id = 2675

Policy_id      = 1647
Rule_id        = 2675
Rule_name      = "Check on NPA accounts"
Rule_description = "Check on Non Personal Accounts"
Rule_type      = 0
Rule_scope     = 0
Rule_severity  = 1
Vendor_type    = "Checkpoint_Mgmt"
Rule_start     = ""
Rule_end       = ""
Command       = ""
Template       = ""
Timestamp     = "2022-02-02 13:37:23"

To restore the record(s):
INSERT INTO NCCM.Cmpl_rule
(
`Policy_id`,`Rule_id`,`Rule_name`,`Rule_description`,`Rule_type`,`Rule_scope`,`Rule_severity`,`Vend
```

Close

Job logs

The logs of specific command jobs can be found in the operate section under Operate → Jobs → Job logs. When clicking on the link in the lower right corner of each row, the job details will be displayed in a separate window.

From:

<https://labs-wiki.netyce.com/> - **Technical documentation**

Permanent link:

https://labs-wiki.netyce.com/doku.php/menu:admin:action_logs:action_logs

Last update: **2022/04/29 11:50**

