
















# Showing Logs of a Containerized xUML Service

## Showing the Service Logs

Name	Type	Quick Actions
 ticketsystem	xuml-service	     
 ideamanagement	xuml-service	     

The administration application gives you access to the logs of a containerized xUML service.

You have two options to access the logs:

- Click **Open logs**  in the quick actions bar in the service's list.

### On this Page:

- [Showing the Service Logs](#)
- [Showing the Service History Log](#)

### Related Pages:

- [Working With the Administration](#)
  - [Working With the Deployment Wizard](#)
- [Controlling Containerized xUML Services](#)
  - [Adapting the Configuration of Containerized xUML Services](#)
  - [Changing the Log Level of a Containerized xUML Service](#)
  - [Persistent States of Containerized xUML Services](#)
- [Controlling Docker Container](#)

### Related Documentation:

- [BRIDGE Integration Platform User's Guide](#)

## Details of ticketsystem

← **running** ▶ ■ ↻

Information ▼

Details ▼

Documentation ▼

Logs ▲



Filter



Channel

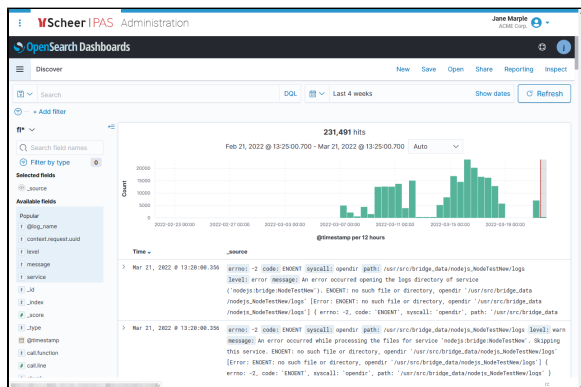
error

access

[Open Log Analyzer to inspect logs](#)



- Open the details page of the service, open section **Logs** and click on the Log Analyzer link.



Both ways will open the logs of the corresponding Docker container in the Log Analyzer where you can view, filter and search the platform logs for all services.



Reference to Analyzer Platform

transformations for further information. If you access the Log Analyzer for the first time on a newly installed platform,

y  
o  
u  
w  
ill  
h  
a  
v  
e  
t  
o  
cr  
e  
a  
t  
e  
a  
n  
in  
d  
e  
x  
p  
a  
tt  
e  
r  
n  
fi  
rs  
t,  
r  
e  
f  
e  
r  
t  
o  
C  
r  
e  
a  
ti  
ng  
a  
n  
I  
nd  
e  
x  
P  
a  
tt  
e  
rn  
.



#### Default Retention Time of Log Files

The following retention times are valid for log files of your PAS installation:

- **Container logs:** Log files inside all containers are deleted after 7 days.
- **Log Analyzer (OpenSearch) logs:**
  - Single cluster: Log files are deleted after 14 days.
  - High Availability cluster: Log files are deleted after 30 days.
- **Integration (Bridge) logs:** The default retention time for Bridge logs is 30 days. This is configurable in the UI, refer to [Integration Platform User's Guide > Node Instance Preferences](#).

## Showing the Service History Log

Details of ticketsystem



Information

Details

Documentation

Logs

History Log

Persistent State



The administration application gives you access to the history of a containerized xUML service ( **PAS 24.0** ).

To access the service history, open the details page of the service and go to section **History Log**.

History Log

Filter

Date	User	Action
28/02/2024 13:42	jane.marple	Restart Instance
13:41	jerry.cotton	AO_SRV_BPMN_RESTSERVICE_MAXREQUESTHEADERSIZE changed from 8 to 10
13:40	jane.marple	The following settings have been changed: <ul style="list-style-type: none"><li>G_SIMPLE_FORM_EXAMPLE_AUTORETRY changed from false to true</li><li>AO_SETTINGS_DEFAULTCONNECTIONPOOLSIZE changed from 10 to 11</li></ul>
13:39	jerry.cotton	Stop instance
13:33	jane.marple	Start instance
13:33	jane.marple	Service created (1.0)

Items 10 1 - 6 / 6

In the **History Log** section you can inspect the service history. The log shows all actions of the xUML service (creation, start, stop etc.) including setting changes.

The content of the history log is read-only.

Filter

max

Date	User	Action
28/02/2024 13:41	jerry.cotton	AO_SRV_BPMN_RESTSERVICE_MAXREQUESTHEADERSIZE changed from 8 to 10

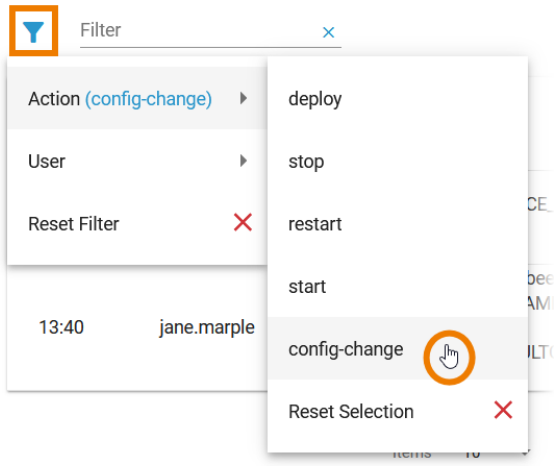
Use the filter field to search for a specific entry.


The content of the filter field is applied to the column **Action** only.

Click **Extended filter** to display the extended filter options:

- Action
- User

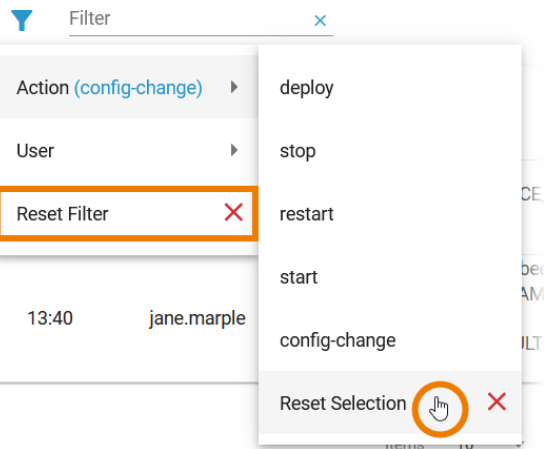
If a filter is applied, the extended filter changes to **Filter**.



 Both extended filter options are loaded dynamically:

- Option **Action** only lists actions that have already been executed in the service.

- Option **Users** only lists users who have already performed a transaction in the service.



In the main filter window, you can reset all selected filters. Click **Reset Filter**.

In the filter option window, you can also reset the selection.