Monitor service log is continously growing with Zabbix on Windows with batch userparameter script and trigger Alert if log is unchanged

Author : admin

Recently we had an inteteresting **Monitoring work task to achieve**. We have an Application that is constantly **simulating encrypted connections traffic to a remote side machine** and sending specific data on TCP/IP ports.
Communiucation between **App Server A -> App Server B** should be continous and if all is working as expected App Server A messages output are logged in the Application log file on the machine which by the way Runs
Windows Server 2020.

Sometimes due to Network issues this constant reconnections from the Application S. A to the remote checked machine TCP/IP ports gets interrupted due to LAN issues or a burned Network Switch equipment, misconfiguration on the network due to some Network admin making stoopid stuff etc..

Thus it was important to **Monitor somehow whether the log is growing or not and feed the output of whether Application log file is growing or it stuck to a Central Zabbix Server.**
To be able to better understand the task, lets divide the desired outcome in few parts on required:

1. Find The latest file inside a folder C:\Path-to-Service\Monitoring\Log
2. Open the and check it is current logged records and log the time
3. Re-open file in a short while and check whether in few seconds new records are written
4. Report the status out to Zabbix
5. Make Zabbix Item / Trigger / Action in case if monitored file is not growing

In below article I'll briefly explain **how Monitoring a Log on a Machine for growing was implemented using a pure good old WIN .BAT (.batch) script and Zabbix Userparameter key**

1. Enable userparameter script for Local Zabbix-Agent on the Windows 10 Server Host

Edit Zabbix config file usually on Windows Zabbix installs file is named:

[**zabbix_agentd.win**]

Uncomment the following lines to enable userparameter support for **zabbix-agentd**:

```
# Include=c:\zabbix\zabbix_agentd.userparams.conf

Include=c:\zabbix\zabbix_agentd.conf.d\

# Include=c:\zabbix\zabbix_agentd.conf.d\*.conf
```

2. Create folders for userparameter script and for the userparameter.conf

Before creating userparameter you can to create the folder and grant permissions

Folder name under **C:\Zabbix -> zabbix_agentd.conf.d**

If you don't want to use Windows Explorer) but do it via cmd line:

```
C:\Users\LOGUser> mkdir \Zabbix\zabbix_agentd.conf\
C:\User\LOGUser> mkdir \Zabbix\zabbix_scripts\
```

3. Create Userparameter with some name file (Userparameter-Monitor-Grow.conf)

In the directory **C:\Zabbix\zabbix_agentd.conf.d** you should create a config file like: **Userparameter-Monitor-Grow.conf** and in it you should have a standard userparameter key and script so file content is:

```
UserParameter=service.check,C:\Zabbix\zabbix_scripts\GROW_LOG_MONITOR-USERPARAMETER.BAT
```

4. Create the Batch script that will read the latest file in the service log folder and will periodically check and report to zabbix that file is changing

notepad C:\Zabbix\zabbix_scripts\GROW_LOG_MONITOR-USERPARAMETER.BAT

```
REM "SCRIPT MONITOR IF FILE IS GROWING OR NOT"
@echo off

set work_dir=C:\Path-to-Service\Monitoring\Log\

set client=client Name

set YYYYMMDD=%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%

set name=csv%YYYYMMDD%.csv

set mytime=%TIME:~0,8%

for %%I in (..) do set CurrDirName=%%~nxI


setlocal EnableDelayedExpansion

set "line1=findstr /R /N "^^" %work_dir%\output.csv | find /C ":""

for /f %%a in ('!line1!') do set number1=%%a

set "line2=findstr /R /N "^^" %work_dir%\%name% | find /C ":""

for /f %%a in ('!line2!') do set number2=%%a


IF  %number1% == %number2% (

echo %YYYYMMDD% %mytime% MAJOR the log is not incrementing for %client%

echo %YYYYMMDD% %mytime% MAJOR the log is not incrementing for %client% >> monitor-grow_err.log

) ELSE (

echo %YYYYMMDD% %mytime% NORMAL the log is incrementing for %client%

SETLOCAL DisableDelayedExpansion

del %work_dir%\output.csv
```

```
FOR /F "usebackq delims=" %%a in (`"findstr /n ^^ %work_dir%\%name%"`) do (
  set "var=%%a"
  SETLOCAL EnableDelayedExpansion
  set "var=!var:*:=!"
  echo(!var! >> %work_dir%\output.csv
  ENDLOCAL
)
)
```

To download GROW_LOG_MONITOR-USERPARAMETER.BAT click here**.**

The script needs to have configured the path to directory containing multiple logs produced by the Monitored Application.
As prior said it will, list the latest created file based on DATE timestamp in the folder will output a simple messages:

If the log file is being fed with data the script will output to output.csv messages continuously, either:

```
%%mytime%% NORMAL the log is incrementing for %%client%%
```

Or if the Monitored application log is not writting anything for a period it will start writting messages

```
%%mytime%%mytime MAJOR the log is not incrementing for %client%
```

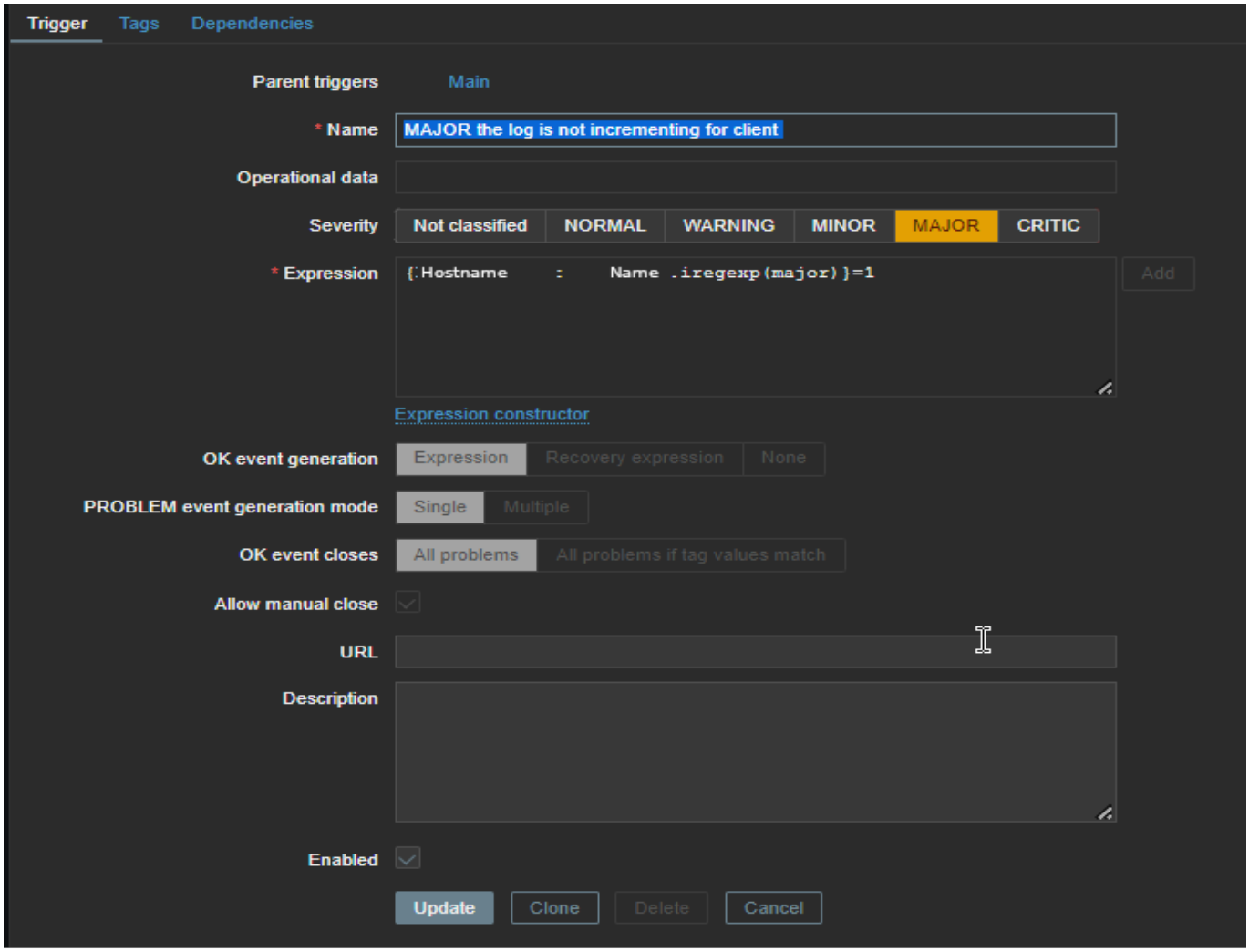
The messages will also be sent in Zabbix.

Before saving the script make sure you modify the Full Path location to the Monitored file for growing, i.e.:

```
set work_dir=C:\Path-to-Service\Monitoring\Log\
```

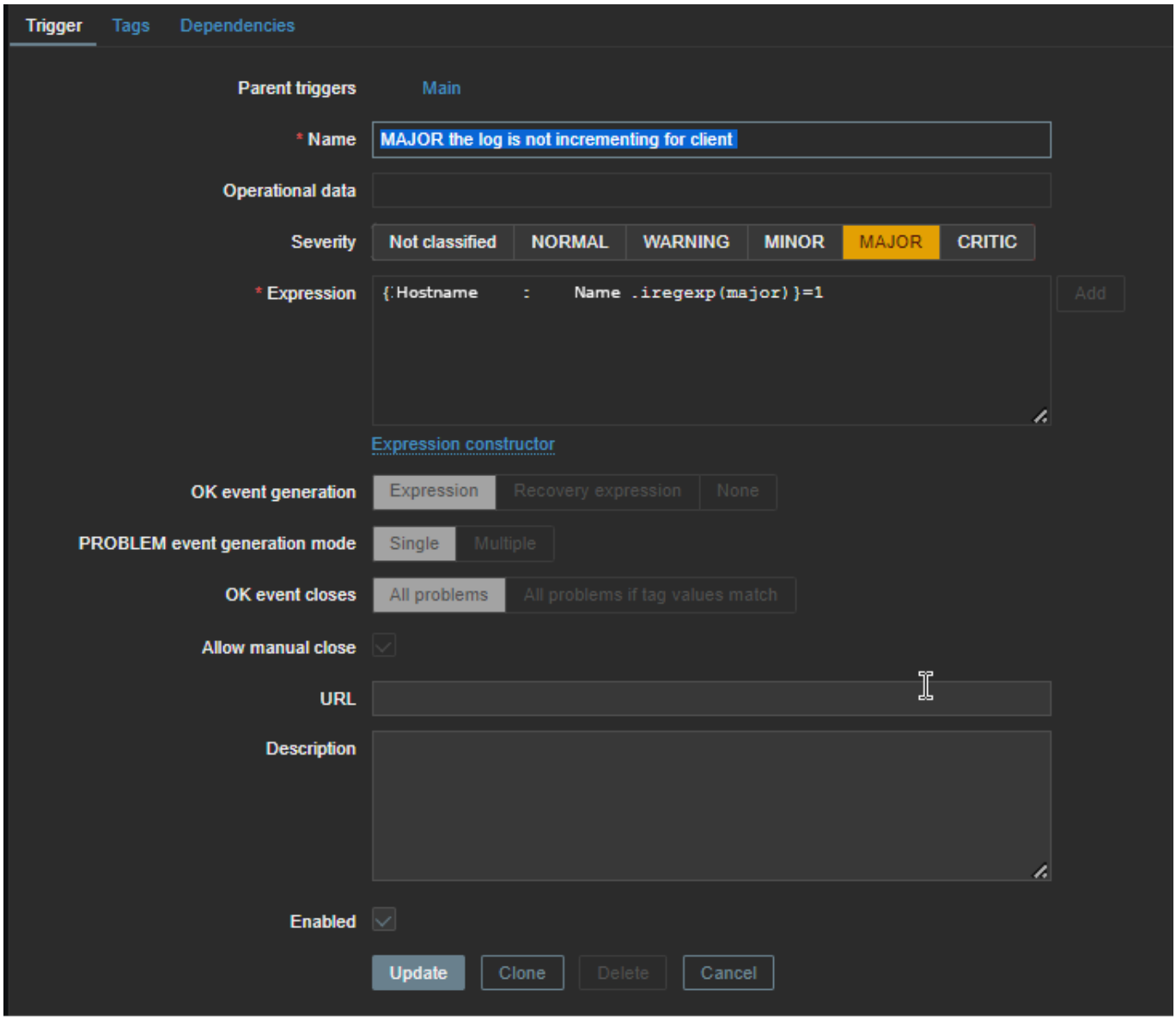
5. Create The Zabbix Item

*Set whatever **service.check name** you would like and a check interval to fetch the info from the userparameter (if you're dealing with very large log files produced by Monitored log of application, then 10 minutes might be too frequent, in most cases 10 minutes should be fine)*



6. Create Zabbix Trigger

You will need a Trigger something similar to below:



Now considering that zabbix server receives correctly data from the client and the monitored log is growing you should in Zabbix:

%%mytime%% NORMAL the log is incrementing for %%client%%

7. Lastly create an Action to send Email Alert if log is not growing