How to integrate Netop Security Server log events collection with Syslog

Article Number: 529 | Last Updated: Thu, Oct 15, 2020 12:52 PM

The Netop Security Server is a service that provides centralized authentication and authorization in a LAN/WAN environment of users that are to access remote devices where privileged access management is required. Apart from managing remote access the Netop Security Server also acts as a centralized service for log events. These events are sent by Host and/or Guest and are always stored in the Security Server's database for review and post-processing, but in some cases you would want these events also to be sent to your Syslog server. In order for the Netop Security Server to be able to send log events to a Syslog server you need the following: A Syslog Agent that grabs log event entries as they appear in a directory; Configure the Netop Security Server to send log events to the defined directory; If you already have a Syslog Server in operation you probably also have a Syslog Agent that you can use for the Security Server. And you would also know how to configure it. If not take a look at KIWI Syslog Server, which is available in a freeware version. And a free Syslog agent is provided by Datagram. The configuration of the Netop Security Server is as follows: Create the directory where you want the log events to go; Open the text file C:\Windows\netop.ini for edit; Find the section [NSS]

Add the following line:

NETOPLOG_DIRECTORY="PATH"

  The default format of the log entry is YYYY-MM-DD HH:MM:SS, HOSTNAME, EVENTTYPE , DESCRIPTION, SERIAL, DTLERR, ERROR

This format will be used unless you define a custom format. The default format definition would be defined like this:

NETOP_LOG_FORMAT=%4.4d-%2.2d-%2.2d %2.2d:%2.2d:00, %s, %s, %s, %d, %d, %d A sample event for Syslog using the default format may look like this: 2020-10-15 08:53:00, DK-GSÂ , *CFGWUCHK , 0, 26, 0, 0

If you want to use a custom definition it must exist in the same section as the definition under [NSS]. After the changes in the netop.ini file you must restart the Netop Helper Service in order for it to take effect.

Posted - Thu, Oct 15, 2020 12:25 PM.
Online URL:
https://kb.netop.com/article/how-to-integrate-netop-security-server-log-events-collection-with-syslog-529.html