nmon-logger Documentation

Release 2.0

Guilhem Marchand

Sep 26, 2017

Contents

Nmon Performance is now associated with Octamis to provide professional solutions for your business, and professional support for the Nmon Performance solution.

CHAPTER 1

Overview:

About the nmon-logger

- Author: Guilhem Marchand
- First release was published on starting 2014
- Purposes:

The nmon-logger for the Nmon Performance application for Splunk implements the excellent and powerful nmon binary known as Nigel's performance monitor. Originally developed for IBM AIX performance monitoring and analysis, it is now an Open source project that made it available to many other systems. It is fully available for any Linux flavor, and thanks to the excellent work of Guy Deffaux, it also available for Solaris 10/11 systems using the sarmon project.

The Nmon Performance monitor application for Splunk will generate performance and inventory data for your servers, and provides a rich number of monitors and tools to manage your AIX / Linux / Solaris systems.

Nmon Performance is now associated with Octamis to provide professional solutions for your business, and professional support for the Nmon Performance solution.

For more information:

What does nmon-logger ?

The nmon-logger package provides out of the box performance and configuration logging of your systems, and will use syslog to transport these data to your central syslog servers.

For more information about Nmon for Linux, see: http://nmon.sourceforge.net/pmwiki.php

The nmon-logger package is provided for the 2 major syslog solutions:

- rsyslog, starting with version 8: nmon-logger-rsyslog
- syslog-ng: nmon-logger-syslog-ng

Its main purpose it to provide an alternative and agent free way of ingesting the Nmon data into Splunk Enterprise with the Nmon Performance application. Althought it could be used with other intelligence big data solution.

About Nmon Performance Monitor for Splunk

Nmon Performance Monitor for Splunk is provided in Open Source, you are totally free to use it for personal or professional use without any limitation, and you are free to modify sources or participate in the development if you wish.

Feedback and rating the application will be greatly appreciated.

- Join the Google group: https://groups.google.com/d/forum/nmon-splunk-app
- App's Github page: https://github.com/guilhemmarchand/nmon-for-splunk
- Videos: https://www.youtube.com/channel/UCGWHd40x0A7wjk8qskyHQcQ
- Gallery: https://flic.kr/s/aHskFZcQBn

Release notes

What has been fixed by release

V2.0.10:

- fix: reactivating the JFSFILE / JFSINODE collections until new core release is available to prevent missing features

V2.0.9:

- fix: Python parser - header detection correction for nmon external monitoring
- feature: Add df information for improved file system monitoring and storage capacity planning
- fix: Perl parser issue - UARG parsing issue for AIX #5

V2.0.8:

- fix: Python parser - preserve data ordering when possible during key value transformation

V2.0.7:

- fix: Python parser issue - epoch time stamp incorrectly parsed for dynamic data #4

V2.0.6:

- fix: corrections in hec_wrapper.sh (missing log_date function, check curl availability)

V2.0.5:

- fix: from TA-nmon - AIX - Better management of compatibility issue with topas-nmon not supporting the -y option #43
- fix: from TA-nmon - AIX - fix repeated and not justified pid file removal message #44
- fix: from TA-nmon - ALL OS - nmon_helper.sh code improvements #45
- feature: from TA-nmon - Optimize nmon_processing output and reduce volume of data to be generated #37
- fix: from TA-nmon - Linux issue: detection of default/nmon.conf rewrite required is incorrect #41
- fix: from TA-nmon - Error in nmon_helper.sh - bad analysis of external snap processes #42

V2.0.4:

- fix: nmon2kv.py issue when using the –use_fqdn option (useless call to get_fqdn function, undesired output)

Known Issues

Major or minor bug, enhancement requests will always be linked to an opened issue on the github project issue page:

https://github.com/guilhemmarchand/nmon-logger/issues

Please note that once issues are considered as solved, by a new release or support exchanges, the issue will be closed. (but closed issues can still be reviewed)

Current referenced issues:

- **fifo implementation not ready for Solaris on Sparc architectures:**

The sarmon binary for Sparc processor has not been released yet and is under compilation.

Once the binary will have been released, the TA-nmon using fifo will be compatible with Solaris Sparc processors.

Support

Octamis professional support for business

Nmon Performance is now available with professional support contract by Octamis limited.

Contact us at: sales@octamis.com

Community support

Nmon Performance Monitor for Splunk is provided in Open Source, you are totally free to use it for personal or professional use without any limitation, and you are free to modify sources or participate in the development if you wish.

This application and all of its components are provided under the Apache 2.0 licence, please remember that it comes with no warranty even if i intend to do my best in helping any people interested in using the App.

DISCLAIMER:

Unlike professional services, community support comes in "best effort" with absolutely no warranties.

Companies using this great piece are kindly invited to subscribe for a professional support contract to help us continuing developing the Nmon Performance solution!

Github

All the project components are hosted on Github:

- **Nmon Splunk core application:** https://github.com/guilhemmarchand/nmon-for-splunk
- **TA-nmon (technical addon for Splunk):** https://github.com/guilhemmarchand/TA-nmon
- **nmon-logger (agent less package for rsyslog/syslog-nr):** https://github.com/guilhemmarchand/nmon-logger

Use Github to open an issue for errors and bugs to be reported, or to ask for enhancements requests.

You can even provide your own improvements by submitting a pull request.

Splunk Answers

Splunk has a strong community of active users and Splunk Answers is an important source of information.

Access previous messages of users or open your own discussion:

https://splunkbase.splunk.com/app/3248

http://answers.splunk.com/answers/app/1753

Google Group Support

An App dedicated Google Group has been created:

https://groups.google.com/d/forum/nmon-splunk-app

This is also a great source of support from people using the Application, and you can also (if you subscribe to mailing news) receive important notifications about the App evolution, such as main release announcements.

Issues and enhancement requests

For any bug reporting, or enhancement request about the Nmon Performance application,you can:

- Open an issue on the Git project home page: https://github.com/guilhemmarchand/nmon-logger/issues
- Get in touch by mail: guilhem.marchand@gmail.com

Operating Systems compatibility

OS compatibility

The nmon-logger package is provided as:

- rpm package in the "rpm" directory, for Linux OS based on Redhat package manager
- deb package in the "deb" directory, for Linux OS based on Debian package manager
- raw files, to be implemented manually on any Linux OS

nmon-logger packages are widely tested against:

- CentOS
- Debian
- Ubuntu

Very few dependencies are required to run the nmon-logger package:

- rsyslog (minimal version 8) for nmon-logger-rsyslog / syslog-ng for nmon-logger-syslog-ng
- Python 2.7.x or any 2.x superior OR Perl with module Time:HiRes installed

Nmon binaries ?

The nmon-logger package has embedded binaries for most Linux OS on various processor architectures, see: http://nmon-for-splunk.readthedocs.io/en/latest/binaries.html

Introduction to Nmon processing

Nmon processing

The TA-nmon embeds different scripts to perform various tasks from starting nmon binaries to the creation of the final data to be indexed by Splunk.

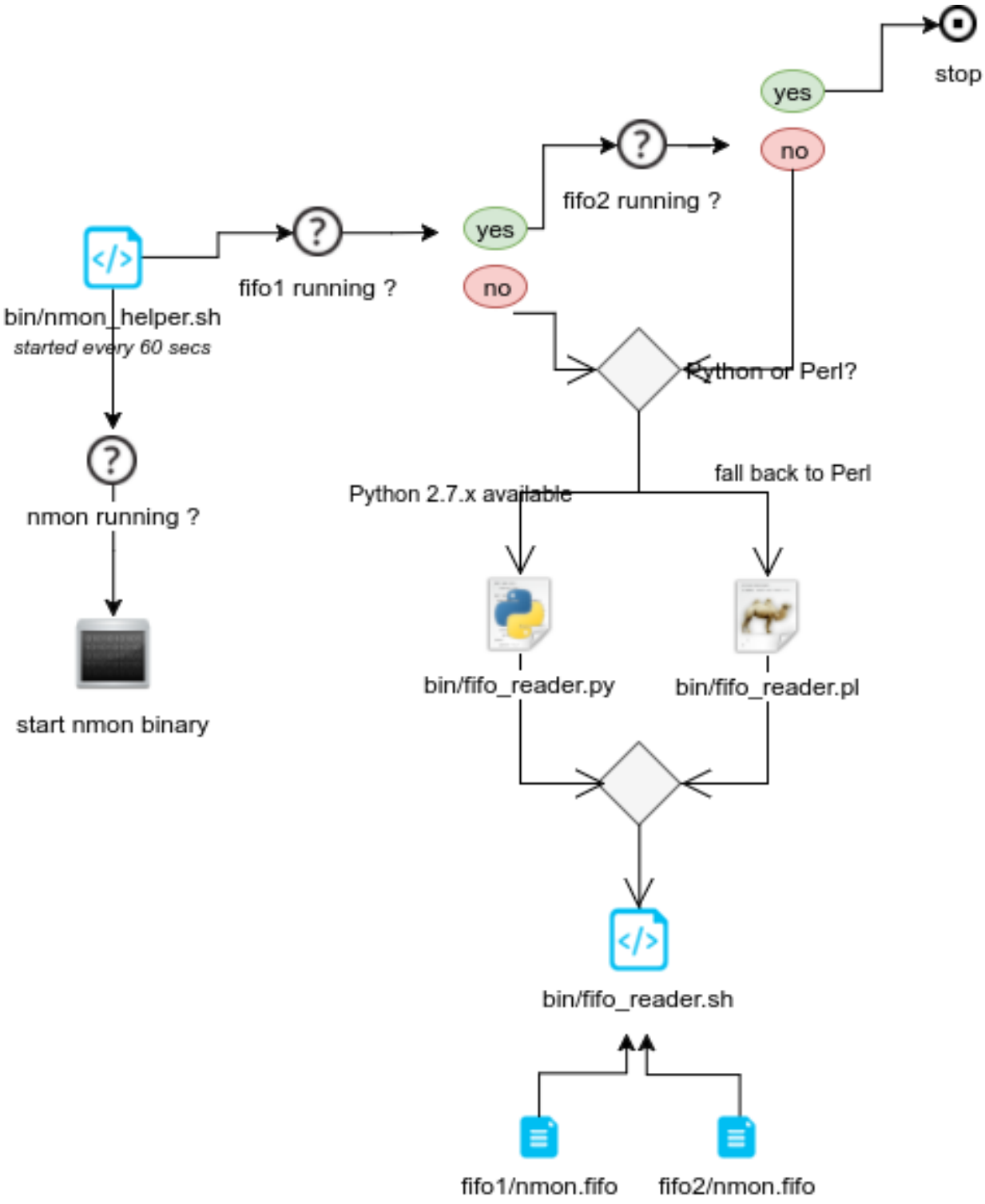
The following items expose the main steps of the processing, the technical details of each scripts and options are globally covered by the documentation.

bin/nmon_helper.sh

The "nmon_helper.sh" script is scheduled to be run every 60 seconds by Splunk, it is responsible for various tasks such as:

- identify the system (OS, processor architecture...)
- load default and custom configurations
- identify the best nmon binary candidate
- identify the running nmon process
- identify fifo_reader process running, and start the reader
- start the nmon binary

Simplified representation of the processing tasks:



bin/fifo_consumer.sh

The "fifo_consumer.sh" script is scheduled to be run every 60 seconds by Splunk, its purpose is consuming the dat files (different part of the nmon file) and stream its content to nmon2csv parsers:

- access the fifo files, wait at least 5 seconds since its last update

- Stream the content of the files to the nmon2csv parser
- empty the nmon_data.dat files for the next cycle

bin/nmon2kv.sh|.py|.pl

These are the nmon2kv parsers:

- the nmon2kv.sh is a simple wrapper which will choose between the Python and Perl parser
- the content is being read in stdin, and piped to the nmon2kv Python or Perl parser
- the Python or Perf parser reads the data, does various processing tasks and generate the final files to be read

Scripts and Binaries

Embedded Scripts in the nmon-logger

nmon_helper:

- bin/nmon_helper.sh:

This shell script is being used by the application to launch Nmon binaries whenever it is detected as required.

It is as well responsible in launching the fifo_reader scripts. (introduced in version 1.3.x)

fifo_reader:

- bin/fifo_reader.pl
- bin/fifo_reader.py
- bin/fifo_reader.sh

These scripts are continuously running as back ground processes on server running the technical addons. Their purpose is to read the fifo files (named pipe) nmon processes are writing to, and extract the different typologies of data from them nmon data

fifo_consumer:

- bin/fifo_consumer.sh

This script is scheduled by default to run every 60 seconds. Its purpose to recompose the nmon flaw of data to be parsed by the nmon parser scripts. (see bellow)

nmon_parser:

- bin/nmon2kv.sh | bin/nmon2kv.py | bin/nmon2kv.pl:

Shell / Python / Perl scripts used to manage and process Nmon raw data into multiple csv files being indexed by Splunk

The Shell script is a wrapper script to Python / Perl scripts. (decision is made on local interpreter avaibility with Python as the default choice)

nmon_cleaner:

- bin/nmon_cleaner.sh / bin/nmon_cleaner.py / nmon_cleaner.pl

Shell / Python / Perl scripts used to manage retention and purge of old nmon data.

Alternatively, it will also ensure that no outdated csv data is being left by Splunk in Performance and Configuration repositories

The Shell script is a wrapper script to Python / Perl scripts. (decision is made on local interpreter avaibility with Python as the default choice)

Embedded Binaries in the TA-nmon

The TA-nmon embeds Nmon binaries for Linux vendors and Solaris OS. AIX embeds by default its own version of Nmon, known as "topas-nmon".

For Linux OS:

- bin/linux: Main directory for Linux specific Nmon binaries
- bin/linux/amzn: 64 bits binaries for Amazon Linux (AMI)
- bin/linux/centos: 32/64 bits binaries for Centos
- bin/linux/debian: 32/64 bits binaries for Debian GNU/Linux
- bin/linux/fedora: 32/64 bits binaries for Fedora project
- bin/linux/generic: 32/64/ia64/power/mainframe binaries compiled for generic Linux
- bin/linux/mint: 32/64 bits binaries for Linux Mint
- bin/linux/opensuse: 32/64 bits binaries for Linux Opensuse
- bin/linux/ol: 32/64 bits binaries for Oracle Linux
- bin/linux/rhel: 32/64/ia64/mainframe/power binaries for Redhat Entreprise Server
- bin/linux/sles: 32/64/ia64/mainframe/power binaries for Suse Linux Entreprise Server
- bin/linux/ubuntu: 32/64/power/arm binaries for Ubuntu Linux
- bin/linux/arch: 32/64 bits binaries for Archlinux
- bin/raspbian: arms binaries for Raspbian Linux

Most of these binaries comes from the official Nmon Linux project site. On x86 processor and for Centos / Debian / Ubuntu / Oracle Linux these binaries are being compiled by myself using Vagrant and Ansible automation. (See https://github.com/guilhemmarchand/nmon-binaries)

Associated scripts resource (nmon_helper.sh) will try to use the better version of Nmon available, it will fall back to generic or system embedded if none of specially compiled versions can fit the system.

For Solaris OS:

sarmon binaries for Oracle Solaris x86 and Sparc:

- bin/sarmon_bin_i386: sarmon binaries for Solaris running on x86 arch
- bin/sarmon_bin_sparc: sarmon binaris for Solaris running on sparc arch

sarmon binaries comes from the official sarmon site project.

For AIX:

Nmon is shipped within AIX by default with topas-nmon binary.

CHAPTER 2

Processing:

CHAPTER 3

Deployment and configuration:

CHAPTER 4

Troubleshoot:

CHAPTER 5

Various: