Tranalyzer2

ntpDecode

Network Time Protocol (NTP)

Tranalyzer Development Team

Contents

1 ntpDecode

1.1 Description

The ntpDecode plugin produces a flow based view of NTP operations between computers for anomaly detection and troubleshooting.

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
NTP_TS	1	0: no time stamps, 1: print NTP time stamps	
NTP_LIVM_HEX	0	Leap indicator, version and mode: 0: split into three values, 1: aggregated hex number	

1.3 Flow File Output

The ntpDecode plugin outputs the following columns:

Name	Type	Description	Flags
ntpStat	H8	NTP status, warnings and errors	
ntpLiVM	H8	NTP leap indicator, version number and mode	NTP_LIVM_HEX=1
ntpLi_V_M	U8_U8_U8	NTP leap indicator, version number and mode	NTP_LIVM_HEX=0
ntpStrat	H8	NTP stratum	
ntpRefClkId	IP4	NTP root reference clock ID (stratum ≥ 2)	
ntpRefStrId	SC	NTP root reference string (stratum ≤ 1)	
ntpPollInt	U32	NTP poll interval	
ntpPrec	F	NTP precision	
ntpRtDelMin	F	NTP root delay minimum	
ntpRtDelMax	F	NTP root delay maximum	
ntpRtDispMin	F	NTP root dispersion minimum	
ntpRtDispMax	F	NTP root dispersion maximum	
ntpRefTS	TS	NTP reference timestamp	NTP_TS=1
ntpOrigTS	TS	NTP originate timestamp	NTP_TS=1
ntpRecTS	TS	NTP receive timestamp	NTP_TS=1
ntpTranTS	TS	NTP transmit timestamp	NTP_TS=1

1.3.1 ntpStat

The ntpStat column is to be interpreted as follows:

ntpStat	Description
2^0 (=0x01)	NTP port detected
2^1 (=0x02)	—
2^2 (=0x04)	—
2^3 (=0x08)	—
2^4 (=0x10)	—
2^5 (=0x20)	—
2^6 (=0x40)	—
2^7 (=0x80)	—

1.3.2 ntpLiVM

The ntpLiVM column is to be interpreted as follows (refer to Section 1.6 for some examples):

ntpLiVM	Description
xx..	Leap indicator
..xx x...	Version number
.... .xxx	Mode

The Leap Indicator bits are to be interpreted as follows:

Leap Indicator	Description
0x0	No warning
0x1	Last minute has 61 seconds
0x2	Last minute has 59 seconds
0x3	Alarm condition, clock not synchronized

The Mode bits are to be interpreted as follows:

Mode	Description
0x0	Reserved
0x1	Symmetric active
0x2	Symmetric passive
0x3	Client
0x4	Server
0x5	Broadcast
0x6	NTP control message
0x7	Private use

1.3.3 ntpStrat

The `ntpStrat` column is to be interpreted as follows:

ntpStrat	Description
`0x00`	Unspecified
`0x01`	Primary reference
`0x02-0xff`	Secondary reference

1.3.4 ntpRefStrId

The interpretation of the `ntpRefStrId` column depends on the value of ntpStrat. The following table lists some suggested identifiers:

ntpStrat	ntpRefStrId	Description
`0x00`	`DCN`	DCN routing protocol
`0x00`	`NIST`	NIST public modem
`0x00`	`TSP`	TSP time protocol
`0x00`	`DTS`	Digital Time Service
`0x01`	`ATOM`	Atomic clock (calibrated)
`0x01`	`VLF`	VLF radio
`0x01`	`callsign`	Generic radio
`0x01`	`LORC`	LORAN-C
`0x01`	`GOES`	GOES UHF environment satellite
`0x01`	`GPS`	GPS UHF positioning satellite

1.4 Monitoring Output

In monitoring mode, the ntpDecode plugin outputs the following columns:

Column	Type	Description	Flags
`ntpPkts`	U64	Number of NTP packets	

1.5 Plugin Report Output

The following information is reported:

- Aggregated `ntpStat`
- Number of NTP packets

1.6 Examples

- Extract the NTP leap indicator:

```
tawk 'NR > 1 { print rshift(and(strtonum($ntpLiVM), 0xc0), 6) }' out_flows.txt
```

- Extract the NTP version:
  ```
  tawk 'NR > 1 { print rshift(and(strtonum($ntpLiVM), 0x38), 3) }' out_flows.txt
  ```
- Extract the NTP mode:
  ```
  tawk 'NR > 1 { printf "%#x\n", and(strtonum($ntpLiVM), 0x7) }' out_flows.txt
  ```