

لي لحت لكاشم لح - ةزت هملا ثادحأل دق ف مت لوح ةلح ةسارد Splunk: في ينمزل عباطل WinHostMon

قبطتال ةيلباق

Splunk ةسسؤم

فصولا

عباطل نيب ةريبك تافال تخا ةظحالم مت WinHostMon، نم صرقلا تانايب ةبقارم دن ع
ضعب تقو نيي عت مت. (_indexTime) عالتبال ةينمزل عباطل او (_time) ثدلل ةينمزل
ثحب جئاتن و ةسرهفلا في ريخأت الى دا امم، يضاملا في ةديعب خيراوت الى ع ثادحأل
ةللضم.

لى ع 'FreeSpaceKB' لقحلا في ةيمقرلا ةميقرلا ريسفت ةعاسا ببسب ةلكشملا هذه تاشن
في 'DATETIME_CONFIG=etc\datetime.xml' يضارثفالا دادعإل ببسب epoch تقو اهنأ
PROPS.conf.

عالتسا

ضارعال:

- قالاتل الى ع جئاتن ةيأ 'index=windows sourcetype=WinHostMon' نع ثحبلا جئاتن عجرت مل -
- '<time' و '<indexTime' نيب اريبك اريخأت SPL سفن نع تقولا لوط ثحبلا رهظأ -
- تايلمع في لكاشم دوجو مدع نم مغلرلا الى رهظت يضاملا في "time" اهل يتل ثادحأل تناك -
- ةسرهفلا و اينبثلا.
- مداخل سفن الى ةسرهفالو لوانتلا ةيلمع ثودح نم مغلرلا الى ةلكشملا ترمثسا -

ةيسيئرلا جئاتنلا:

- Splunkd OK: لي لخدال لجلسلا ثادحأ الى ع روثعال مت -

INFO ExecProcessor [4664 ExecProcessorSchedulerThread] - message from ""C:\Program Files\Splunk

ريغ 'time' ميقي شحبل تاي لمع ترهظأ نكلو، شادألأ باعيتسا ةحص نم لجسلا اذه دكأت -
ةحيحصلا.
عم قفاوتي يذلا، 'FreeSpaceKB=1607839214' لقحل نع ةيلوالأ شادألأ تالجس صحف فشك -
2020 ربمسي د 13 ل ةينمزل ةبقحل
حمسي امم، '\etc\datetime.xml' ل ريشي props.conf DATETIME_config فلم ليلحت رهظأ -
ينمز عباطك ئطاخ وحن لىل 'FreeSpaceKB' ريسفتب Splunk.

رارق

1. شحلم نيوكتل:

- props.conf ردصم عونل لدع م WinHostMon:

```
[WinHostMon]  
DATETIME_CONFIG = CURRENT
```

الدب شحلل ينمز عباطك (_indexTime) كالتةإل تقو مادختسإل Splunk هيچوتب ريغيغتال ماق
ةيلوالأ تانايبل نم دحاو ليلحت نم.

2. ةحصلا نم ققحتل تاوطخ:

- شحلم نيوكتل قيبطتل Splunk ليغشت ةداع مت -
- حالصإل نم ققحتلل اهتسرهف داعم رابتخإ تانايب -
- ةسرهلل تقو عم ةقسانت م ةقيقد ةينمز ميقي اهل نألأ شادألأ نأ ةطحال م -

ةيسيئرلا دئاولل

ذوذش وأ ةسرهلل تاريخأت ةهجاوم دنع ةينمزل عباوطل ليلحت ةيفيك نم امود ققحتل -
ةينمزل عباوطل.
ينمز عباط لوقح لىل شادألأ رقتفت ام دنع 'DATETIME_CONFIG = CURRENT' مدختسأ -
ةيمقرلا لوقحل ريسفت ةعاسا نكمي ام دنع وأ ةحلص.

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا