

Eingesammelte Ereignisse fehlen - Beheben von Zeitstempelanalyseproblemen in Splunk: Anwenderbericht zu WinHostMon

Geltungsbereich

Splunk Enterprise

Beschreibung

Beim Überwachen von Datenträgerdaten von WinHostMon wurden erhebliche Diskrepanzen zwischen Ereigniszeitstempeln (`_time`) und Einzugstimestempeln (`_indextime`) beobachtet. Bei einigen Ereignissen wurde ihre `_time` auf einen früheren Zeitpunkt festgelegt, was zu Indexierungsverzögerungen und irreführenden Suchergebnissen führte.

Dieses Problem trat auf, weil der numerische Wert im Feld 'FreeSpaceKB' aufgrund der Standardeinstellung 'DATETIME_CONFIG=\etc\datetime.xml' in props.conf als Epochenzeit fehlinterpretiert wurde.

Untersuchung

Symptome:

- Die Suchergebnisse für 'index=windows sourcetype=WinHostMon' haben überhaupt keine Ergebnisse zurückgegeben.
- Bei der Suche nach der gleichen SPL traten große Verzögerungen zwischen ``_time`` und ``_indextime`` auf.
- Ereignisse mit ``_time`` weit in der Vergangenheit erschienen, obwohl keine Probleme mit der Aufnahme oder Indizierung Prozesse.
- Das Problem bestand weiter, obwohl die Aufnahme und Indizierung auf demselben Server stattfand.

Wichtigste Ergebnisse:

- Splunked internen Protokoll gefunden Ereignisse aufgenommen OK:

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

- Dieses Protokoll bestätigte die korrekte Erfassung von Ereignissen, aber die Suchvorgänge zeigten falsche `\_time` Werte.
- Die Untersuchung der Rohereignisprotokolle ergab das Feld 'FreeSpaceKB=1607839214', das der Epochenzeit für den 13. Dezember 2020 entspricht.
- Die Analyse der Datei props.conf ergab, dass DATETIME_CONFIG auf 'etc\datetime.xml' verweist, sodass Splunk 'FreeSpaceKB' fälschlicherweise als Zeitstempel interpretieren konnte.

Auflösung

1. Aktualisierte Konfiguration:

- Modifizierte props.conf für den WinHostMon-Quellentyp:

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

Die Änderung wies Splunk an, die Aufnahmezeit (_indextime) als Zeitstempel des Ereignisses zu verwenden, anstatt einen aus den Rohdaten zu analysieren.

2. Validierungsschritte:

- Splunk neu gestartet, um die aktualisierte Konfiguration anzuwenden.
- Testdaten zur Überprüfung der Fehlerbehebung neu deklariert.
- Beobachtete, dass Ereignisse nun genaue _Zeitwerte hatten, die auf _indextime ausgerichtet waren.

Wichtigste Punkte

- Überprüfen Sie stets, wie Splunk Zeitstempel analysiert, wenn Indizierungsverzögerungen oder Zeitstempelanomalien auftreten.
- Verwenden Sie `DATETIME\_CONFIG = CURRENT`, wenn Ereignisse keine gültigen Zeitstempelfelder haben oder wenn numerische Felder falsch interpretiert werden könnten.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.