

Kubernetes نم رركم لال ليجستللة ةظحال م متت في تاباختنالل ايلعللة ةنجلللا لالخل نم Splunk

قيبطتلة ةيلباق

Splunk Enterprise Kubernetes

فصولا

ءاشناب موقت اهنأ امك ،عقوتم وه امك تاباختنالل ايلعللة ةنجلللا تانايب ةسرهف متي ال
Kubernetes نم ددحم ردصم هل ددحم سرهفل ةددعتم مداوخ ربع تاراركت

ءالجتسإ

في فيلاتل رمألل مءاختساب تاباختنالل ايلعللة ةنجلللا زيمملا زمرلا ةلاح نم الوأ ققحت 1.
Splunk SH ب ةصاخال (GUI) ةيموسرلا مدختسملا ةهجاو

```
|rest /services/data/inputs/http/http  
| table name, token , disabled
```

ةددعتم رءاصم عاونأل ةححص ريغ تامال ع عضوب موقبي ردصملا ناك اذإ تاراركتلله رهظت دق. 2.
ححص ريغ رءاصملا عاونأ وأ ردصملا نيوكت ناك اذإ امم ققحت اذل

```
index=
```

```
| stats count by source ,sourcetype
```

3. نرم نم رثكأ ةدراو ةرركملا ثادحلأا تناك اذا ام دكأت.

```
index=
```

```
| stats count by _time, source, host | where count > 1
```

4. تادادعإلا ىلإ لاقتنالال لالخنم Splunk في تاباختنالال ايلعلال ةنجللال تالاخلإا تادادعإا صحنف . دكأت Splunk في (GUI) ةيموسرلا مدختسملال ةهجاو في HTTP ثادحأ عمجم > تانايبلا تالخدم > وأ ردصملا سفنل نيترم تاباختنالال ايلعلال ةنجللاب ةصاخ تالخدم يأ ديدحت مدع نم قيبطتلا.

5. HEC لوانتب ةقلعتم تاريذحت وأ ءاطخأ يأ دوجو نم ققحتلل ةيلخادل Splunk تالجس عجار . لكاشم وأ تانيوكتلا في ءاطخأ دوجو ىلإ ريشت دق يتلاو .

```
index=_internal spource*splunkd.log* component-HttpEventCollector*
```

رارق

- "1 > دعال بولسأ هيف نوکي يذلا لقحلا... ماخ_ ب ةلود ددع" رمألا، Kubernetes ردصمل لوقح ياً نمضتت ال يتلا ثادحألا ىلإ عجري اذه نأل هب قوئوم ريغ تاراركتلا فاشتكال دنع اهراركت متي ثادحألا عيجم نأ ودبي كلذل. كلذل ىلإ امو ثدحل فرعم لثم ةديرف لقح نيئمضت متي مل ام. Splunk ب ةصاخلا (GUI) ةيموسرلا مدختسملا ةهجاو يفا هعايدىل ةيلاوألا تانايبلا يفا kubernetes.pod_id وأ kubernetes.docker_id لثم ايبسن ديرف ردصملا ةيانهن نم تاراركتلا نم ققحتلاو.

- لامحألا ةنزاوم نيوكت نم دكأت. لامحألا تانزاوم نم ديدعلا دوجول ارظن تاراركتلا تثدح دق ةحيجصل ريغ تادادعلا نأل ةحيجصل سراهفلا ىلإ تانايبلا هيجوتل حيجصل لكشب تاراركت ىلإ يدؤيس امم ةددعتم تاسرهفم ىلإ تانايبلا سفن نييعت ىلإ يدؤت.

ةلص تاذاطباور

[ةبركم ثادحأ ىلع روثعلا يئبنكمي فيك](#)

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