

ثحب ال ءارظن ةفاضا إىل ء رءاق رىغ : أطءال رىظن ال ءطساوب لاصتال نىىى ءءاع

قىب طتال ءىلباق

Splunk ءسسؤم

فصولا

ءء ، ءئىب ال فى ءءىء ءحب سؤؤر إىل ءفاضا إلب ءءىء سراهف ءفاضا ل ءلوا ءم فى
ءءومءم ءحب ال سؤؤر نىوكت مءى مل نكلو ءءومءم ال ماظن نم ءء سراهف ال

ءحب ال سؤؤر نكل ءلئس ال فى ءحب ال سؤؤرل ءارظن ءل ءللب ءرءا سراهف نىىى ءم
ءحب ال ءارظن ءرءا سراهف م إىل ءوئء

ءالءتسا

- لاصتال اب ءلءءم لكاشم ءوءو مءء نمو SSL ءاءء ءءص نم ققءء
- ءطساوب لاصتال نىىى ءءاع ، SSL لاصتا ءاشن رءء : `splunkd.log show` فى ءاطءا
سرهف لب صاءال IP ناوئء رىظن ال
- ءءاو ءاءء إىل ءفاضا إلب نىوكتال ءافلم ماءءسا بىوئىل نىوكتال لشف
ءىشال سففن ماىقل فى (GUI) ءىموسرل مءءسمل
- ماءءس ال ءىق SSL نال ارظن سراهف لب صاءال URI فرءم `https` ماءءسا نم ءكاأ
- ءءومءم ال ماظن ءضو فى ءنءم ال سراهف ال ءاءء نم ءكاأ
- ءاءومءم ءسلى ءحب ال سؤؤر

راق

مءى ءال ءحب ال سارءضو إىل ءحب ال سارءىوئءى نال بءى ، ءءىمءمء مء ءق سراهف ال نال امب
ضفرىو ءءص لكشب لىءم ال إىل سراهف ال ماظن فرءءى نل إىل `server.conf` فى ءنىءمء
رىظن ال بلط

ءءمءم رىغ ءحب ال سؤؤر نال نم مءرل إىل ءءىمءمء ءءومن إىل ءاءءى ءحب ال سارء نال امءاء ركءء

ىلى امء ءرءم `server.conf` ل ءلكش 1.

```
[clustering]
master_uri = https://x.x.x.x:xxxx (https://x.x.x.xxxxx)
mode = searchhead
pass4SymmKey= yourPass4SymmKey
```

س وؤر عيزوت متي، ****Indexers cluster**** ب صاخال ةومجم لماظن ل يساسأل URI Master_uri =
ةلحال هذل ةومجم ريغ ثحب ل
ةومجم لماظن تالاصتال ثحب ل س أ ر ع و ي ف م داخال ني ع ت ل ب ول ط م اذه = عض و ل ا
م ه ب صا خ ح ا ت ف م ة فاضا ني م د خ ت س م ل ا ل ع ب ج ي ، ةومجم لماظن ح ا ت ف م = pass4SymmKey
ةمسل هذل

ةي لم عل ح ج ن ت ن ا ب ج ي و ، ثحب ل ا ر ئ اظن ة فاضا ة داع ل لواحو ة م د خ ل ل ي غ ش ت ة داع ا ب م ق 2.

ةلص تا ذ ط باور

Splunk قئاثو

ثحب ل ا س أ ر ل ا ثحب ل ا ر ئ اظن ة فاضا :

<https://docs.splunk.com/Documentation/Splunk/7.3.0/DistSearch/Configuredistributedsearch>

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 ج 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 و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ظ 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 ج 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 ج 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 ج 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