

00000000	00	0000000000000000	0000000000000000	00	000000000000000000000000000000
44666373	BB	47657474696E67	53746172746564	BB	51756963687374617274

# Quickstart Guide

## Splunk setup

20	00000000000000	00000000	00000000000000000000	0000000000000000	0000000000000000	0000000000000000	00000000	00000000	00000000	0000	00000000
22	437265617465	746865	666F6C6C6F77696E67	64656661756C74	696E6465786573	74686174	617265	75736564	6279	53433453	

25	00	00	00	00	00
F6	65	6D	61	69	6C

25	00	00	00	00
E6	65	70	61	76

25	00	00	00	00	00	00	00
E6	6E	65	74	61	75	74	68

25	00	00	00	00	00	00
F6	6F	65	74	64	6C	70

25	00	00	00	00	00	00
E6	6E	65	74	64	6E	73

25	00	00	00	00	00
F6	6F	65	74	66	77

25	00	00	00	00	00	00
E6	6E	65	74	69	64	73

25	00	00	00	00	00	00
E6	6E	65	74	6F	70	73

25	00	00	00	00	00	00
E6	6E	65	74	77	61	66

25	00	00	00	00	00	00	00	00
E6	6E	65	74	70	72	6F	78	79

25	00	00	00	00	00	00	00
E6	6E	65	74	69	70	61	6D

25	00	00	00	00	00	00	00	00
E6	6F	73	77	69	6E	73	65	63

25	00	00	00	00	00
E6	6F	73	6E	69	78

25	00000000000000000000	00000000000000000000	00000000000000	00000000	00000000000000000000	0000000000000000	0000000000000000
E6	656D5F6D657472696373	284F7074696F6E616C	6F70742D696E	666F72	53433453	6F7065726174696F6E616C	6D6574726963733B656E73757265

00000000	0000	0000000000000000	0000	00	0000000000000000	00000000000000
74686973	6973	63726561746564	6173	61	60657472696373	696F64657829

20	00000000000000	00	000000	000000000000	000000	000000000000	00000000	0000000000000000	000000	000000	00000000	000000	00000000000000	
22	437265617465	61	484543	746F6B656E	666F72	534334532E	5768656E	66696C6C696E67	6F7574	746865	666F726D	666F72	746865	746F6B656E2C

0000	0000	000000000000000000000000	00000000	000000	20000000000000000000	000000000000000020	00000000	0000	00000000	0000000000	000000	00000000	0000000000	000000
6974	6973	7265636F6D6D656E646564	74686174	746865	1C53656C6563746564	496E64657865731D	70616E65	6265	6C656674	626C616E6B	616E64			

00000000	00	lastChanceIndex	0000	0000000000000000	0000	00000000	000000	00000000	00000000	0000000000000000	0000	00000000	00000000
74686174	61		6265	637265611746564	736F	74686174	616C6C	64617461	7265636569766564	6279	53433453	77696C6C	

6C	61
6F	64

73	6F	6D	65	77	68	65	72	65
----	----	----	----	----	----	----	----	----

69	6E
----	----

53	70	6C	75	6E	6B	20
----	----	----	----	----	----	----

## SC4S setup<sub>(using RHEL 7.6)</sub>

20	000000	000000	00000000	0000	00000000000000	0000	0000000000	000000	00000000000000	00000000000000	00000000000000	0000	00000000
22	536574	746865	686F7374	4F53	6865726E656C	746F	6D61746368	746865	64656661756C74	72656365697665	627566666572	6F66	73633473

00	00	00	00	00
77	68	69	63	68

00	00
69	73

00	00	00
73	65	74

00	00
74	6F

00	00	00	00
31	36	4D	42

[illegible]

```
net.core.rmem default = 1703936
```

```
net.core.rmem max = 1703936
```

25	00	00	00	00	00
F6	41	70	70	6C	79

```
sysctl -p
```

20	000000000000	000000	000000000000	0000	000000	000000000000000000	0000000000000000
22	456F73757265	746865	6865726F656C	6973	6F6F74	64726F7070696F67	70616368657473

```
netstat -su | grep "receive errors"
```

20	0000000000000000	0000000000000000	0000000000000000	00000000	00000000	0000000000000000	0000000000000000
22	496E7374616C6C	636F6E6E747261636B	285248454C	372E38	77697468	706F646D616E	6E6E6C7920

```
<dnf or yum> install connttrack
```