splunk>

Administrative Tip Sheet

GuidePoint
SECURITY
YOUR MISSION. SECURED.

Rules of the PROPS!

(for extraction)

```
TIME_PREFIX = ^
MAX_TIMESTAMP_LOOKAHEAD = 25
TIME_FORMAT = %Y-%m-%d %H:%M:%S,%3N
LINE_BREAKER = ([\r\n]+)\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2},\d{3}
SHOULD_LINEMERGE = False
TRUNCATE = 10000
TZ = US/Eastern
```

props.conf

```
[my_sourcetype]
TRANSFORMS-foo=retwrite_host
EXTRACT-extract_ip = (?<ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})

FIELDALIAS-foo = user AS my,user id AS myid
REPORTS-foo2=my_report_name
LOOKUP-foo = mylookuptable userid AS myuserid OUTPUT username AS myusername
```

transforms.conf

```
[rewrite_host]
REGEX = abc(\w+)\s+
DEST_KEY= MetaData:Host
FORMAT = host::$1

[lookup_def]
filename = mylookup_table.csv

[my_report_name]
REGEX = abc\s+(\w+):\s+(\d+)
FORMAT = field1::$1 field2:$2
```

web.conf

(this should be default!)

```
[settings]
sslVersions=tls1.1,tls1.2
enableSplunkWebSSL=true
supportSSLV3Only=false
```

deploymentclient.conf

```
[deployment-client]
phoneHomeIntervalInSecs = 600

[target-broker:deploymentServer]
targetUri = deploymentserver.splunk.mycompany.com:8089
```

ui-prefs.conf

```
[search]
dispatch.earliest_time = -15m
dispatch.latest_time = now
```

inputs.conf

```
[monitor:///mnt/logs/hostname/logs]
disabled=1 |1=true, 0=false
host_segment = 3
index=abc
source=abc
sourcetype=abc123

[script://<cmd>]
```

outputs.conf

```
[tcpout]
defaultGroup = primary_indexers

[tcpout:primary_indexers]
server = server_one:9997, server_two:9997
autoLB = true
autoLBFrequency = 15
forceTimebasedAutoLB = true

sslCertPath = $SPLUNK_HOME/etc/auth/server.pem
sslRootCAPath = $SPLUNK_HOME/etc/auth/ca.pem
sslPassword = password
sslVerifyServerCert = true
```

indexes.conf

```
[volume:volume_name]
path =/opt/splunk/data
maxVolumeDataSizeMB = 1572864
# Frozen Volume is not configurable,
#must define per index the path.

[indexname]
homePath = volume:hot/indexname
coldPath = volume:cold/indexname
thawedPath = volume:cold/indexname/thaweddb

frozenTimePeriodInSecs =31540000
coldToFrozenDir = /opt/splunk/data/frozen/
indexname
#max size is unlimited unless defined here,

# this is max size of hot+warm+cold, before its frozen
maxTotalDataSizeMB = 4294967295

[indexAndForward]              (for all non-indexers)
index=false
```

Popular Commands and their Syntax

Oneshot

/opt/splunk/bin/splunk add oneshot /path/to/log_file.log -sourcetype log_fileA -index test -rename- source whatsmysource

CLI

Accept License on first Start	/opt/splunk/bin/splunk start --accept-license
Enable Splunk as a Service	/opt/splunk/bin/splunk enable boot-start -user splunk
Reload Deployment Server Apps	/opt/splunk/bin/splunk reload deploy-server
Push Apps from Index Master to Indexers	/opt/splunk/bin/splunk apply cluster-bundle
Initiate Rolling Restart for Indexers	/opt/splunk/bin/splunk rolling-restart cluster-peers
Enable Master Maintenance Mode	/opt/splunk/bin/splunk enable maintenance-mode
Push Apps from SH Deployer to SHC Peers Initiate	/opt/splunk/bin/splunk apply shcluster-bundle -target anyshcmemberip:8089
Rolling Restart for SHC	/opt/splunk/bin/splunk rolling-restart shcluster-members
Join license slave to license master	splunk edit licenser-localslave -master_uri https://<master>:<port>
Add / edit users in CLI	splunk < add | edit > user admin2 -password changeme2 -role admin
Show detailed deployment client info	splunk list deploy-clients

Debug Logging Settings

Defaults are: $SPLUNK_HOME/etc/log.cfg

Update this with new: $SPLUNK_HOME/etc/log-local.cfg

Via CLI: ./splunk set log-level TailingProcessor -level DEBUG

BTOOL

```
/opt/splunk/bin/splunk cmd btool --debug inputs list |grep [
/splunk cmd btool --app=<app_name> <conf_file_prefix> list
```

Splunk XML

NAVIGATION

app_name/data/ui/nav/default.xml

```
<nav>
  <collection label=”Dashboards”>
    <view name=”palo_alto_api” />
    <view name=”palo_alto_web_content_policies” default=’true’/>
    <view name=”domain_lookup”/>
  </collection>
  <collection label=”Other Views”>
    <view name=”search” default=’true’ />
    <view name=”data_models” />
    <view name=”reports” />
    <view name=”alerts” />
    <view name=”dashboards” />
  </collection>
</nav>
```

IP Tables 101

How to Redirect (at top of IP tables statement)

iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-ports 8000 iptables-save

General Rule

-A INPUT -m state --state NEW -m tcp -p tcp --dport 8000 -j ACCEPT -m comment --comment “splunk web interface”

Configure Use of Nonstandard Ports

```
[settings]  (web.conf)              change mgmt port
mgmtHostPort=127.0.0.1:8989         change web port
httpport = 8001

[replication_port://9877]       (server.conf)

[kvstore]  (server.conf)
port = 8191
```

Time Conversion/Syntax

Change from epoch	strftime(_time, “%H:%M”)
Change string to time	strptime(timeStr, “%H:%M”)

%H is 00-23 hours

%M is 00-59 minutes

%*x*N subseconds with number

%p AM or PM

%S is 00-60 as seconds

%T is 24 hour notation (%H:%M:%S) %A full weekday name

%a abbrev weeday name

%d day of month (01-31)

%e day of month (1-31)

%b abbrev month name (Jan)

%B full month name

%m month as decimal (01-12)

%y year as (00-99)

%Y 4 digit year (2017)

Common Splunk Ports

8000 web, 8089 management, 8080 index rep, 9997 uf listener, 8191 kv, 8000 web, 8089 Management, 9997 uf listener, 8191 kv, 8065 appserver, 9887 index/sh replication