```
#   Version 9.0.0
# DO NOT EDIT THIS FILE!
# Changes to default files will be lost on update and are difficult to
# manage and support.
#
# Please make any changes to system defaults by overriding them in
# apps or $SPLUNK_HOME/etc/system/local
# (See "Configuration file precedence" in the web documentation).
#
# To override a specific setting, copy the name of the stanza and
# setting to the file where you wish to override it.
#
# This file contains possible attributes and values you can use to
# configure inputs, distributed inputs and file system monitoring.


[default]
index        = default
_rcvbuf       = 1572864
host = $decideOnStartup
evt_resolve_ad_obj = 0
evt_dc_name=
evt_dns_name=

[blacklist:$SPLUNK_HOME\etc\auth]

[blacklist:$SPLUNK_HOME\etc\passwd]

[monitor://$SPLUNK_HOME\var\log\splunk]
index = _internal

[monitor://$SPLUNK_HOME\var\log\watchdog\watchdog.log*]
index = _internal

[monitor://$SPLUNK_HOME\var\log\splunk\license_usage_summary.log]
index = _telemetry

[monitor://$SPLUNK_HOME\var\log\splunk\splunk_instrumentation_cloud.log*]
index = _telemetry
sourcetype = splunk_cloud_telemetry

[monitor://$SPLUNK_HOME\etc\splunk.version]
_TCP_ROUTING = *
index = _internal
sourcetype=splunk_version

[monitor://$SPLUNK_HOME\var\log\splunk\configuration_change.log]
index = _configtracker
```

```
[batch://$SPLUNK_HOME\var\run\splunk\search_telemetry\*search_telemetry.json]
move_policy = sinkhole
index = _introspection
sourcetype = search_telemetry
crcSalt = <SOURCE>
log_on_completion = 0

[batch://$SPLUNK_HOME\var\spool\splunk]
move_policy = sinkhole
crcSalt = <SOURCE>

[batch://$SPLUNK_HOME\var\spool\splunk\tracker.log*]
index = _internal
sourcetype = splunkd_latency_tracker
move_policy = sinkhole

[batch://$SPLUNK_HOME\var\spool\splunk\...stash_new]
queue      = stashparsing
sourcetype  = stash_new
move_policy = sinkhole
crcSalt    = <SOURCE>
time_before_close = 0

[batch://$SPLUNK_HOME\var\spool\splunk\...stash_hec]
sourcetype  = stash_hec
move_policy = sinkhole
crcSalt    = <SOURCE>

[fschange:$SPLUNK_HOME\etc]
disabled = false
#poll every 10 minutes
pollPeriod = 600
#generate audit events into the audit index, instead of fschange events
signedaudit=true
recurse=true
followLinks=false
hashMaxSize=-1
fullEvent=false
sendEventMaxSize=-1
filesPerDelay = 10
delayInMills = 100

[udp]
connection_host=ip
```

```
[tcp]
acceptFrom=*
connection_host=dns

[splunktcp]
route=has_key:_replicationBucketUUID:replicationQueue;has_key:_dstrx:typingQueue;has_key:_linebre
aker:rulesetQueue;absent_key:_linebreaker:parsingQueue
acceptFrom=*
connection_host=ip

[script]
interval = 60.0
start_by_shell = false

[SSL]
# SSL settings
# The following provides modern TLS configuration that guarantees forward-
# secrecy and efficiency. This configuration drops support for old Splunk
# versions (Splunk 5.x and earlier).
# To add support for Splunk 5.x set sslVersions to tls and add this to the
# end of cipherSuite:
#     DHE-RSA-AES256-SHA:AES256-SHA:DHE-RSA-AES128-SHA:AES128-SHA
# and this, in case Diffie Hellman is not configured:
#     AES256-SHA:AES128-SHA

sslVersions = tls1.2
cipherSuite = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-
AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256
ecdhCurves = prime256v1, secp384r1, secp521r1

allowSslRenegotiation = true
sslQuietShutdown = false
logCertificateData = true
certLogMaxCacheEntries = 10000
certLogRepeatFrequency = 1d

[script://$SPLUNK_HOME\bin\scripts\splunk-wmi.path]
disabled = 0
interval = 10000000
source = wmi
sourcetype = wmi
queue = winparsing
persistentQueueSize=200MB
```

```
# default single instance modular input restarts

[admon]
interval=60
baseline=0

[MonitorNoHandle]
interval=60

[WinEventLog]
interval=60
evt_resolve_ad_obj = 0
evt_dc_name=
evt_dns_name=

[WinNetMon]
interval=60

[WinPrintMon]
interval=60

[WinRegMon]
interval=60
baseline=0

[perfmon]
interval=300

[powershell]
interval=60

[powershell2]
interval=60
```