Splunk® Enterprise
Getting Data In 9.0.4

List of pretrained source types

Generated: 2/28/2023 12:57 am

List of pretrained source types

Splunk software ships with built-in or pretrained **source types** that it uses to parse incoming data into events.

The Splunk platform can automatically recognize and assign many of these pretrained source types to incoming data. You can also manually assign pretrained source types that the Splunk platform doesn't recognize automatically. To assign source types manually, see Override automatic source type assignment.

From a heavy or universal forwarder, you can also configure source types from the inputs.conf configuration file. If you use Splunk Enterprise, you can assign source types from either Splunk Web or from the inputs.conf file.

Use a pretrained source type if it matches your data, as the Splunk platform already knows how to properly index pretrained source types. If your data doesn't fit any pretrained source types, you can create your own source types. See Create source types. The Splunk platform can also index virtually any format of data even without custom properties.

Automatically recognized source types

The following table shows automatically recognized source types:

Source type	Origin	Examples
access_combined	NCSA combined format http web server logs. Can be generated by Apache or other web servers.	`10.1.1.43 - webdev [08/Aug/2022:13:18:16 -0700] "GET / HTTP/1.0" 200 0442 "-" "check_http/1.10 (nagios-plugins 1.4)"`
access_combined_wcookie	NCSA combined format http web server logs. Can be generated by Apache or other web servers, with cookie field added at the end.	`"66.249.66.102.1124471045570513" 59.92.110.121 - - [19/Aug/2022:10:04:0 -0700] "GET /themes/splunk_com/images/logo_splunk.png HTTP/1.1" 200 994 "http://www.splunk.org/index.php/docs" "Mozilla/5.0 (X11; U; Linux i686 en-US; rv:1.7.8) Gecko/20220524 Fedora/1.0.4-4 Firefox/1.0.4" "61.3.110.148.1124404439914689"`
access_common	NCSA common format http web server logs. Can be generated by Apache or other web servers.	`10.1.1.140 - - [16/May/2022:15:01:52 -0700] "GET /themes/ComBeta/images/bullet.png HTTP/1.1" 404 304`
apache_error	Standard Apache web server error log	`[Sun Aug 7 12:17:35 2022] [error] [client 10.1.1.015] File does not exist: /home/reba/public_html/images/bullet_image.gif`
asterisk_cdr	Standard Asterisk IP PBX call detail record	`"","5106435249","1234","default","""James Jesse""<5106435249>","SIP/5249-1ce3","","VoiceMail","u1234","2022-05-26 15:19:25","2022-05-26 15:19:25","2022-05-26 15:19:42",17,17,"ANSWERED","DOCUMENTATION"`
asterisk_event	Standard Asterisk event log (management events)	`Aug 24 14:08:05 asterisk[14287]: Manager 'randy' logged on from 127.0.0.1`
asterisk_messages	Standard Asterisk messages log (errors and warnings)	`Aug 24 14:48:27 WARNING[14287]: Channel 'Zap/1-1' sent into invalid extension 's' in context 'default', but no invalid handler`
asterisk_queue	Standard Asterisk queue log	`1124909007|NONE|NONE|NONE|CONFIGRELOAD|`
cisco_syslog	Standard Cisco syslog produced by all Cisco network devices including	`Sep 14 10:51:11 stage-test.splunk.com Aug 24 2022 00:08:49: %PIX-2-106001: Inbound TCP connection denied from IP_addr/por to IP_addr/port flags TCP_flags on interface int_name Inbound TCP`

Source type	Origin	Examples
	PIX firewalls, routers, ACS, and so on. Usually through remote syslog to a central log host.	connection denied from 144.1.10.222/9876 to 10.0.253.252/6161 flags SYN on interface outside
db2_diag	Standard IBM DB2 database administrative and error log	2022-07-01-14.08.15.304000-420 I27231H328 LEVEL: Event PID : 2120 TID : 4760 PROC : db2fmp.exe INSTANCE: DB2 NODE : 000 FUNCTION: DB2 UDB, Automatic Table Maintenance, db2HmonEvalStats, probe:900 STOP : Automatic Runstats: evaluation has finished on database TRADEDB
exim_main	Exim MTA mainlog	2022-08-19 09:02:43 1E69KN-0001u6-8E => support-notifications@splunk.co R=send_to_relay T=remote_smtp H=mail.int.splunk.com [10.2.1.10]
exim_reject	Exim reject log	2022-08-08 12:24:57 SMTP protocol violation: synchronization error (input sent without waiting for greeting): rejected connection from H=gate.int.splunk.com [10.2.1.254]
linux_messages_syslog	Standard Linux syslog, located at /var/log/messages on most platforms	Aug 19 10:04:28 db1 sshd(pam_unix)[15979]: session opened for user root by (uid=0)
linux_secure	Red Hat, Debian, and equivalent distributions Linux authentication log	Aug 18 16:19:27 db1 sshd[29330]: Accepted publickey for root from ::ffff:10.2.1.5 port 40892 ssh2
log4j	Log4j standard output produced by any J2EE server using log4j	2022-03-07 16:44:03,110 53223013 [PoolThread-0] INFO [STDOUT] got some property...
mysqld_error	Standard MySQL error log	050818 16:19:29 InnoDB: Started; log sequence number 0 43644 /usr/libexec/mysqld: ready for connections. Version: '4.1.10a-log' socket: '/var/lib/mysql/mysql.sock' port: 3306 Source distribution
mysqld	Standard MySQL query log that also matches the MySQL binary log following conversion to text	53 Query SELECT xar_dd_itemid, xar_dd_propid, xar_dd_value FROM xar_dynamic_data WHERE xar_dd_propid IN (27) AND xar_dd_itemid = 2
postfix_syslog	Standard Postfix MTA log reported through the *nix syslog facility	Mar 1 00:01:43 avas postfix/smtpd[1822]: 0141A61A83: client=host76-117.pool80180.interbusiness.it[80.180.117.76]
sendmail_syslog	Standard Sendmail MTA log reported through the *nix syslog facility	Aug 6 04:03:32 nmrjl00 sendmail[5200]: q64F01Vr001110: to=root, ctladdr=root (0/0), delay=00:00:01, xdelay=00:00:00, mailer=relay, min=00026, relay=[101.0.0.1] [101.0.0.1], dsn=2.0.0, stat=Sent (v00F3HmX004301 Message accepted for delivery)
sugarcrm_log4php	Standard Sugarcrm activity log reported using the log4php utility	Fri Aug 5 12:39:55 2022,244 [28666] FATAL layout_utils - Unable to load the application list language file for the selected language(en_us) or the default language(en_us)
weblogic_stdout	Weblogic server log in the standard native BEA format	####<Sep 26, 2022 7:27:24 PM MDT> <Warning> <WebLogicServer> <bea03> <asiAdminServer> <ListenThread.Default> <<WLS Kernel>> <> <BEA-000372> <HostName: 0.0.0.0, maps to multiple IP addresses:169.254.25.129,169.254.193.219>
websphere_activity	Websphere activity log, also often referred to as the service log	-------------------------------------- ComponentId: Application Server ProcessId: 2580 ThreadId: 0000001c ThreadName: Non-deferrable Alarm : 3 SourceId: com.ibm.ws.channel.framework.impl. WSChannelFrameworkImpl ClassName: MethodName: Manufacturer: IBM Product: WebSphere Version: Platform 6.0 [BASE 6.0.1.0 o0510.18] ServerName: nd6Cell01\was1Node01\TradeServer1 TimeStamp: 2022-07-01

Source type	Origin	Examples
		13:04:55.187000000 UnitOfWork: Severity: 3 Category: AUDIT PrimaryMessage: CHFW0020I: The Transport Channel Service has stopped th Chain labeled SOAPAcceptorChain2 ExtendedMessage: ---
websphere_core	Core file export from Websphere	NULL--- 0SECTION TITLE subcomponent dump routine NULL=================================== 1TISIGINF signal 0 received 1TIDATETIME Date: 2022/08/02 at 10:19:24 1TIFILENAME Javacore filename: /kmbcc/javacore95014.1122945564.txt NULL --- 0SECTION XHPI subcomponent dump routine NULL ============================== 1XHTIME Tue Aug 2 10:19:24 20221XHSIGRECV SIGNONE received at 0x0 in <unknown>. Processing terminated. 1XHFULLVERSION J2RE 1.3.1 IBM AIX build ca131-20031105 NULL
websphere_trlog_syserr	Standard Websphere system error log in the IBM native trlog format	[7/1/05 13:41:00:516 PDT] 000003ae SystemErr R at com.ibm.ws.http.channel. inbound.impl.HttpICLReadCallback.complete (HttpICLReadCallback.java(Compiled Code)) (truncated)
websphere_trlog_sysout	Standard Websphere system out log in the IBM native trlog format. Similar to the log4j server log for Resin and Jboss. Sample format as the system error log but contains lower severity and informational events.	[7/1/05 13:44:28:172 PDT] 0000082d SystemOut O Fri Jul 01 13:44:28 PDT 2022 TradeStreamerMDB: 100 Trade stock prices updated: Current Statistics Total update Quote Price message count = 4400 Time to receiv stock update alerts messages (in seconds): min: -0.013 max: 527.347 avg 1.0365270454545454 The current price update is: Update Stock price for s:393 old price = 15.47 new price = 21.50
windows_snare_syslog	Standard windows event log reported through a third-party Intersect Alliance Snare agent to remote syslog on a *nix server	0050818050818 Sep 14 10:49:46 stage-test.splunk.com Windows_Host MSWinEventLog 0 Security 3030 Day Aug 24 00:16:29 2022 560 Security admin4 User Success Audit Test_Host Object Open: Object Server: Securit Object Type: File Object Name: C:\Directory\secrets1.doc New Handle ID: 1220 Operation ID: {0,117792} Process ID: 924 Primary User Name: admin4 Primary Domain: FLAME Primary Logon ID: (0x0,0x8F9F) Client User Name: Client Domain: - Client Logon ID: - Accesses SYNCHRONIZE ReadData (or ListDirectory) Privileges -Sep

Special source types

The following table shows the special source types:

Source type	Origin	Examples
known_binary	The file name matches a pattern generally known as that of a binary file, not a log file	MP3 files, images, .rdf files, .dat files, and other obvious non-text files

Pretrained source types

These following table shows pretrained source types, including both those that are automatically recognized and those that are not:

Category	Source types
Application servers	log4j, log4php, weblogic_stdout, websphere_activity, websphere_core, websphere_trlog, catalina, ruby_on_rails
Databases	db2_diag, mysqld, mysqld_error, mysqld_bin, mysql_slow
E-mail	exim_main, exim_reject, postfix_syslog, sendmail_syslog, procmail

Category	Source types
Operating systems	linux_messages_syslog, linux_secure, linux_audit, linux_bootlog, anaconda, anaconda_syslog, osx_asl, osx_crashreporter, osx_crash_log, osx_install, osx_secure, osx_daily, osx_weekly, osx_monthly, osx_window_server, windows_snare_syslog, dmesg, ftp, ssl_error, syslog, sar, rpmpkgs
Metrics	collectd_http, metrics_csv, statsd
Network	novell_groupwise, tcp
Printers	cups_access, cups_error, spooler
Routers and firewalls	cisco_cdr, cisco:asa, cisco_syslog, clavister
VoIP	asterisk_cdr, asterisk_event, asterisk_messages, asterisk_queue
Web servers	access_combined, access_combined_wcookie, access_common, apache_error, iis*
Splunk software	splunk_com_php_error, splunkd, splunkd_crash_log, splunkd_misc, splunkd_stderr, splunk-blocksignature, splunk_directory_monitor, splunk_directory_monitor_misc, splunk_search_history, splunkd_remote_searches, splunkd_access, splunkd_ui_access, splunk_web_access, splunk_web_service, splunkd_conf*, django_access, splunk_help, mongod
Non-log files	csv*, psv*, tsv*, _json*, json_no_timestamp, fs_notification, exchange*, generic_single_line
Miscellaneous	snort, splunk_disk_objects*, splunk_resource_usage*, kvstore*

The source types marked with an asterisk (*) use the INDEXED_EXTRACTIONS attribute, which sets other attributes in props.conf to specific defaults and requires special handling to forward to another Splunk platform instance. See Forward fields extracted from structured data files.

Learn a source type configuration

To find out what configuration information the Splunk platform uses to index a given source type, you can use the `btool` utility to show the properties on your forwarder. If you use Splunk Enterprise, you can do this on your Splunk Enterprise instance.

For more information on using `btool`, refer to Use btool to troubleshoot configurations in the *Troubleshooting Manual*.

The following example shows how to list out the configuration for the `tcp` source type:

```
$ ./splunk btool props list tcp
[tcp]
BREAK_ONLY_BEFORE = (=\+)+
BREAK_ONLY_BEFORE_DATE = True
CHARSET = UTF-8
DATETIME_CONFIG = /etc/datetime.xml
KV_MODE = none
LEARN_SOURCETYPE = true
MAX_DAYS_AGO = 2000
MAX_DAYS_HENCE = 2
MAX_DIFF_SECS_AGO = 3600
MAX_DIFF_SECS_HENCE = 604800
MAX_EVENTS = 256
MAX_TIMESTAMP_LOOKAHEAD = 128
MUST_BREAK_AFTER =
MUST_NOT_BREAK_AFTER =
MUST_NOT_BREAK_BEFORE =
REPORT-tcp = tcpdump-endpoints, colon-kv
```

```
SEGMENTATION = inner
SEGMENTATION-all = full
SEGMENTATION-inner = inner
SEGMENTATION-outer = foo
SEGMENTATION-raw = none
SEGMENTATION-standard = standard
SHOULD_LINEMERGE = True
TRANSFORMS =
TRANSFORMS-baindex = banner-index
TRANSFORMS-dlindex = download-index
TRUNCATE = 10000
maxDist = 100
pulldown_type = true
```