

## New Search

```
index=* (failed OR failure OR error)
| stats count by host, source, sourcetype
| where count > 50
| sort -count
```





Time range: All time





✓ **89,372 events** (before 27/12/2025 00:54:47.000) No Event Sampling





### Statistics (193)





host	source	sourcetype	count
Redwan	WinEventLog:Microsoft-Windows-Store/Operational	WinEventLog	21018
splunk3	C:\Program Files\Splunk\etc\apps\sample_app\logs\maillog.1	syslog	4490
splunk3	C:\Program Files\Splunk\etc\apps\sample_app\logs\maillog	syslog	2207
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\winerror.py	winerror	1984
Webserve rX	C:\Program Files\Splunk\etc\system\default\messages.conf	conf	1868
Redwan	WinEventLog:Microsoft-Windows-WMI-Activity/Operational	WinEventLog	1089
Webserve rX	C:\Users\parth\Local Settings\Google\Chrome\User Data\Default\Extensions\gighmmpiobklfepjocnamgkbiglidom\6.33.2.1_0\abp-background.js	knockout	1053
Webserve rX	C:\Users\parth\Local Settings\Google\Chrome\User Data\Profile 1\Extensions\cfhdojbkjhnklbpkdaibdccddilifddb\4.32.2.1_0\background.js	knockout	961
Webserve rX	C:\Program Files (x86)\Google\GoogleUpdater\updater.log	updater	901
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\ec2\2016-11-15\service-2.json	unknown-4	859
Redwan	WinEventLog:Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	WinEventLog	802
Webserve rX	C:\Windows\WinSxS\amd64_netfx4-cfx_extended_sql_files_b03f5f7f11d50a3a_4.0.15912.0_none_7867cadf720b6302\Tracking_Logic.sql	sql	788
Redwan	WinEventLog:Microsoft-Windows-AppXDeploymentServer/Operational	WinEventLog	749
Redwan	WinEventLog:Microsoft-Windows-LiveId/Operational	WinEventLog	732
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\pinpoint\2016-12-01\service-2.json	json	698

host ↕	source ↕	sourcetype ↕	count ↕
Webserve rX	C:\Program Files\Splunk\var\lib\splunk\_introspection\db\hot_v1_7\Strings.data	data	592
Webserve rX	C:\Program Files\Splunk\var\lib\splunk\_introspection\db\db_1766522350_1766269995_0\Strings.data	data	591
Webserve rX	C:\Windows\WinSxS\amd64_netfx4-aspnet_perf_ini_b03f5f7f11d50a3a_4.0.15920.100_none_173cb45ee8546f5a\aspnet_perf.ini	ini	576
Webserve rX	C:\Windows\WinSxS\amd64_netfx4-aspnet_perf_ini_b03f5f7f11d50a3a_4.0.15920.100_none_173cb45ee8546f5a\aspnet_perf2.ini	ini	576
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-w..d-line-utility-base_31bf3856ad364e35_10.0.26100.2314_none_a999255e735f454f\cliegaliases.mof	breakable_text	545
Redwan	WinEventLog:Microsoft-Windows-CloudStore/Operational	WinEventLog	527
Redwan	WinEventLog:Microsoft-Windows-UserSettingsBackup-EarlyDownloader/Operational	WinEventLog	498
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botcore\data\macie2\2020-01-01\service-2.json	json-8	455
Webserve rX	C:\Users\parth\Local Settings\Google\Chrome\User Data\Profile 1\Cache\Cache_Data\af_000363	unknown	454
Webserve rX	C:\Program Files\Splunk\etc\apps\splunk_instrumentation\appserver\static\build\pages\inst.js	jsConsole	446
Webserve rX	C:\Windows\Logs\DISM\dism.log	dism	436
Redwan	WinEventLog:Microsoft-Windows-Known Folders API Service	WinEventLog	426
Webserve rX	C:\ProgramData\Microsoft\Windows Defender\Support\MPLog-20251218-040618.log	MPLog	388
Redwan	WinEventLog:Microsoft-Windows-Shell-Core/Operational	WinEventLog	379
Redwan	WinEventLog:Microsoft-Windows-Diagnosis-PCW/Operational	WinEventLog	349
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-a..nt-server.resources_31bf3856ad364e35_10.0.26100.7309_en-us_1d3bee687b38a021\AppXDeploymentServer.dll.mui	mui	317
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-help-credits.resources_31bf3856ad364e35_10.0.26100.7309_en-us_4a38ae80942229dc\credits.txt	NOTICE	304
Webserve rX	C:\Windows\INF\setupapi.offline.20240401_072605.log	setupapi.offline-2	294
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-ie-f12script_31bf3856ad364e35_11.0.26100.1_none_425802b7115a0adb\F12Script.dll	dll	281

host 	source 	sourcetype 	count 
Webserve rX	C:\Windows\WinSxS\x86_microsoft-windows-ie-f12script_31bf3856ad364e35_11.0.26100.1_none_e639673358fc99a5\F12Script.dll	dll	281
Redwan	WinEventLog:Microsoft-Windows-Crypto-NCrypt/Operational	WinEventLog	264
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\medialive\2017-10-14\service-2.json	json-8	245
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\rds\2014-09-01\service-2.json	json-8	244
Webserve rX	C:\Program Files\Splunk\etc\apps\Splunk_TA_windows\lookups\xmlsecurity_eventcode_errorcode_action.csv	csv	236
Webserve rX	C:\Windows\Logs\CBS\CbsPersist_20251223052642.log	CbsPersist	228
Redwan	WinEventLog:Microsoft-Windows-SMBServer/Operational	WinEventLog	227
Webserve rX	C:\Program Files\Splunk\etc\apps\Splunk_TA_windows\lookups\windows_reason_status_substatus_910.csv	csv	222
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-s..gementwmi.resources_31bf3856ad364e35_10.0.26100.1_en-us_769af521b18ff477\storage_wmi.mfl	mfl	220
Webserve rX	C:\Windows\Panther\setupact.log	setupact-2	218
Webserve rX	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25110.6-0\Microsoft-Windows-Windows Defender.man	man	211
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\elasticsearch\2014-09-30\service-2.json	json-8	207
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\cloudfront\2015-04-17\service-2.json	json-8	205
Webserve rX	C:\Users\parth\Local Settings\Google\Chrome\User Data\Profile 1\Extensions\cfhdojbkjhnlbpkdaibdcddilifddb\4.32.2.1_0\desktop-options.js	desktop-options	202
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\cloudfront\2014-10-21\service-2.json	json-8	199
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\cloudfront\2014-11-06\service-2.json	json-8	199
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\cloudfront\2014-05-31\service-2.json	json-8	197
Webserve rX	C:\Program Files\Splunk\share\splunk\search_mrsparkle\exposed\build\pages\admin-user-xp\federated_search_new_asl_providers	federated_search_new_asl_provider	194
Webserve rX	C:\Program Files\Splunk\etc\apps\Splunk_TA_windows\lookups\xmlsecurity_eventcode_action_multiinput.csv	csv	188

host 	source 	sourcetype 	count 
Webserve rX	C:\Program Files\Splunk\etc\system\default\sourcetypes.conf	conf	182
Redwan	WinEventLog:Microsoft-Windows-Bits-Client/Operational	WinEventLog	176
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\s3\2006-03-01\endpoint-rule-set-1.json	oobeprovisioningprogress-vm	173
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-wsp-spaces_31bf3856ad364e35_10.0.26100.7309_none_0204efba5d8a5ee1\mispace.mof	mof	172
DESKTOP- TK09M51	WinEventLog:Microsoft-Windows-Crypto-NCrypt/Operational	WinEventLog	161
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\win32inetcon.py	win32inetcon	160
Webserve rX	C:\Program Files\Splunk\etc\apps\splunk-dashboard-studio\appserver\static\build\chunks\chunk-NK3PM7J5.js	recover-padding-286	158
Webserve rX	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.log	ngen	152
Redwan	WinEventLog:System	WinEventLog	149
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\lxml\xmlerror.pxi	pxi	149
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\_pydecimal.py	_pydecimal	139
Redwan	WinEventLog:Microsoft-Windows-Kernel-Cache/Operational	WinEventLog	135
Redwan	WinEventLog:Microsoft-Windows-WebAuthN/Operational	WinEventLog	134
127.0.0. 1	alert:High Failure Event Volume	generic_single_line	131
Webserve rX	C:\Program Files\WindowsApps\MSTeams_25306.804.4102.7193_x64__8wekyb3d8bbwe\desktop-assets\hashed-assets\calling-webcv-9b863b97103cbdd8.js.gz	calling-webcv-9b863b97103cbdd-too_small	130
Webserve rX	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	ngen	129
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-p...rastructureconsumer_31bf3856ad364e35_10.0.26100.7309_none_4fa87c27e0718422\Rules.System.Configuration.xml	xml	129
Redwan	WinEventLog:Microsoft-Windows-Storage-ClassPnP/Operational	WinEventLog	121
Webserve rX	C:\Program Files\WindowsApps\MSTeams_25306.804.4102.7193_x64__8wekyb3d8bbwe\desktop-assets\hashed-assets\precompiled-shared-worker-f016b39f36b1d15d.js.gz	precompiled-shared-worker-f016b39f36b1d15d-too_small	121
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\quicksight\2018-04-01\service-2.json	json-8	120

host 	source 	sourcetype 	count 
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\cloudsearch\2011-02-01\service-2.json	json-8	116
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\amplifybackend\2020-08-11\service-2.json	json-8	114
Webserve rX	C:\Program Files\Splunk\var\log\spotlight\spotlight_metrics.js on	jsConsole	114
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\cloudformation\2010-05-15\service-2.json	unknown-4	110
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\stepfunctions\2016-11-23\service-2.json	json-8	110
Webserve rX	C:\Users\parth\Local Settings\Packages\MicrosoftWindows.Clients.CBS_cw5n1h2txyewy\LocalState\EBWebView\Default\Service Worker\ScriptCache\67a473248953641b_0	67a473248953641b	108
Webserve rX	C:\Users\parth\Local Settings\Packages\MicrosoftWindows.Clients.CBS_cw5n1h2txyewy\LocalState\EBWebView\Default\Service Worker\ScriptCache\ba23d8ecda68de77_0	ba23d8ecda68de	108
Webserve rX	C:\Program Files\Splunk\etc\apps\learned\local\sourcetypes.conf	jsConsole	106
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-a..bility-mathcat-main_31bf3856ad364e35_10.0.26100.7309_none_03aed51b145a74de\NOTICE.txt	NOTICE	105
Webserve rX	C:\Program Files\Splunk\quarantined_files\share\splunk\search_mrsparkle\exposed\js\contrib\jg_library.js	jg_library	104
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-s..tup-tool-powershell_31bf3856ad364e35_10.0.26100.1_none_43117bb40fcc215c\BitLocker.psm1	psm	104
Webserve rX	C:\Windows\WinSxS\amd64_dual_netathr10x.inf_31bf3856ad364e35_10.0.26100.1_none_4b60dfaa057a7db6\Data61x4_2_2.msc	msc-6	103
Webserve rX	C:\Windows\WinSxS\amd64_dual_netathr10x.inf_31bf3856ad364e35_10.0.26100.1_none_4b60dfaa057a7db6\Data9377_2_0.msc	msc-6	103
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\iotsitewise\2019-12-02\service-2.json	json-8	102
Webserve rX	C:\Users\parth\Local Settings\Google\Chrome\User Data\Default\Extensions\gighmmpiobk1fepjocnamgkbiglidom\6.33.2.1_0\global-s-front.js	globals-front	101
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-s..ementwmi-powershell_31bf3856ad364e35_10.0.26100.6725_none_84ecf77637d1c267\Storage.types.ps1xml	ps1xml	101
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\forecast\2018-06-26\service-2.json	json	100

host 	source 	sourcetype 	count 
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\kafka\2018-11-14\service-2.json	json-8	100
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-management-oobe_31bf3856ad364e35_10.0.26100.5074_none_0e19b812fcf157c9\autopilotDevicePreparation-vm.js	autopilotDevicePreparation-vm	100
Webserve rX	C:\Program Files\Splunk\etc\apps\splunk_secure_gateway\appserver\static\pages\administration.3.9.13.js	administration	99
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\cloudfront\2017-10-30\service-2.json	autopilotDevicePreparation-vm	98
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\botocore\data\cloudfront\2018-06-18\service-2.json	json-8	98
Webserve rX	C:\Windows\SystemResources\azroles.dll.mun	mun	98
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\future\backports\urllib\request.py	request	97
Webserve rX	C:\Program Files\Splunk\Python-3.9\Lib\site-packages\splunk\appserver\mrsparkle\locale\messages.pot	pot	96
Webserve rX	C:\Program Files\Splunk\etc\apps\splunk-visual-exporter\bin\native\windows\x86_64\chromium\legacy.js	jsConsole	94
Webserve rX	C:\Windows\WinSxS\amd64_microsoft-windows-e..gine-isam.resources_31bf3856ad364e35_10.0.26100.1_en-us_68cd365bddb88cf9\ESSENT.dll.mui	mui-3	93