New Search

```
index=_audit action="search" user="kimjoe" "botsv3"
| table _time user action search
| sort - _time
```

Time range: All time

✓ **1,848 events** (before 15/12/2025 09:58:33.000) No Event Sampling

Statistics (1,848)

	_time	user	action	search
90	2025-12-02 14:33:58.477	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_method="PUT" http_status=200 | table _time, bucket, object, http_method, http_status'
91	2025-12-02 14:33:49.608	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search "*.txt" | table _time, bucket, key, object, http_method, http_status'
92	2025-12-02 14:33:41.860	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_method="PUT" http_status=200 | table _time, bucket, object, http_method, http_status'
93	2025-12-02 14:33:28.477	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" | stats count by bucket, http_method, http_status'
94				

	_time	user	action	search
90	2025-12-02 14:32:59.869	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" | stats count by bucket, http_method, http_status'
90	2025-12-02 14:32:58.472	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, key, http_method, http_status'
90	2025-12-02 14:32:52.155	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, key, http_method, http_status'
90	2025-12-02 14:31:28.479	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_status'
90	2025-12-02 14:31:28.459	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="[BUCKET_NAME]" | stats count by bucket, http_method, http_status'
90	2025-12-02 14:31:22.668	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_status'
90	2025-12-02 14:31:09.073	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="[BUCKET_NAME]" | stats count by bucket, http_method, http_status'
90	2025-12-02 14:30:58.460	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_status'

	_time	user	action	search
91	2025-12-02 14:30:52.793	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_status'
91	2025-12-02 14:27:58.474	kimjoe	search	'search
91	2025-12-02 14:27:58.461	kimjoe	search	'search
91	2025-12-02 14:27:52.997	kimjoe	search	'search
91	2025-12-02 14:27:41.650	kimjoe	search	'search
91	2025-12-02 14:27:28.496	kimjoe	search	'search
91	2025-12-02 14:27:28.478	kimjoe	search	'search
92	2025-12-02 14:27:27.184	kimjoe	search	'search

	_time	user	action	search
921	2025-12-02 14:27:01.722	kimjoe	search	'search
922	2025-12-02 13:45:58.514	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | search sourcetype="*s3*"'
923	2025-12-02 13:45:56.178	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | search sourcetype="*s3*"'
924	2025-12-02 13:45:28.489	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'
925	2025-12-02 13:45:23.878	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'
926	2025-12-02 13:43:28.505	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | fieldsummary | table field'
927	2025-12-02 13:43:28.493	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'
928	2025-12-02 13:43:20.494	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | fieldsummary | table field'

	_time	user	action	search
992	2025-12-02 13:43:15.598	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'
993	2025-12-02 13:42:58.489	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search "PUT" AND "200" | table _time, *'
991	2025-12-02 13:42:56.825	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search "PUT" AND "200" | table _time, *'
993	2025-12-02 13:42:28.476	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'
993	2025-12-02 13:42:25.377	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'
993	2025-12-02 13:41:58.479	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | search sourcetype="*s3*"'
993	2025-12-02 13:41:51.856	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | search sourcetype="*s3*"'
993	2025-12-02 13:40:58.502	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search "PUT" AND "200" | table _time, *'

	_time	user	action	search
93737	2025-12-02 13:40:40.462	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search "PUT" AND "200" | table _time, *'
93738	2025-12-02 13:40:28.504	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'
93739	2025-12-02 13:40:28.494	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | where _time >= strptime("2018-08-20 21:01:46", "%Y-%m-%d %H:%M:%S") | search http_method="PUT" http_status=200 | rex field=key "(?<filename>[^/]+\.txt)$" | where isnotnull(filename) | table _time, bucket, filename'
93740	2025-12-02 13:40:28.482	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | rex field=key "(?<filename>[^/]+\.\w+)$" | where isnotnull(filename) | stats count by bucket, filename'
93741	2025-12-02 13:40:17.762	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'
93742	2025-12-02 13:40:04.582	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | where _time >= strptime("2018-08-20 21:01:46", "%Y-%m-%d %H:%M:%S") | search http_method="PUT" http_status=200 | rex field=key "(?<filename>[^/]+\.txt)$" | where isnotnull(filename) | table _time, bucket, filename'
93743	2025-12-02 13:39:58.492	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search "frothly" OR "webcode" | table _time, bucket, key, object, http_method, http_status'

	_time	user	action	search
94	2025-12-02 13:39:58.475	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothly" http_status=200 (http_method="PUT" OR http_method="POST") | table _time, bucket, key, object, http_method, http_status'
94	2025-12-02 13:39:58.276	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | rex field=key "(?<filename>[^/]+\.\w+)$" | where isnotnull(filename) | stats count by bucket, filename'
94	2025-12-02 13:39:38.785	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search "frothly" OR "webcode" | table _time, bucket, key, object, http_method, http_status'
94	2025-12-02 13:39:28.286	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothly" http_status=200 (http_method="PUT" OR http_method="POST") | table _time, bucket, key, object, http_method, http_status'
94	2025-12-02 13:38:28.519	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search "frothly" OR "webcode" | table _time, bucket, key, object, http_method, http_status'
94	2025-12-02 13:38:28.505	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlyweblogs" http_status=200 (http_method="PUT" OR http_method="POST") | table _time, bucket, key, object, http_method, http_status'
95	2025-12-02 13:38:28.487	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_status=200 (http_method="PUT" OR http_method="POST") | table _time, bucket, key, object, http_method, http_status'

	_time	user	action	search
95691	2025-12-02 13:38:18.8	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search "frothly" OR "webcode" | table _time, bucket, key, object, http_method, http_status'
95702	2025-12-02 13:38:07.9	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlyweblogs" http_status=200 (http_method="PUT" OR http_method="POST") | table _time, bucket, key, object, http_method, http_status'
95603	2025-12-02 13:37:59.7	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_status=200 (http_method="PUT" OR http_method="POST") | table _time, bucket, key, object, http_method, http_status'
95564	2025-12-02 13:37:28.5	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket | sort -count'
95527	2025-12-02 13:37:28.5	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket'
95601	2025-12-02 13:37:28.5	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket'
95747	2025-12-02 13:37:24.9	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket | sort -count'
95838	2025-12-02 13:37:08.5	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket'

	_time	user	action	search
95 19	2025-12-02 13:37:05.419	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket'
96 02	2025-12-02 13:36:58.502	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket | sort -count'
96 21	2025-12-02 13:36:36.221	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket | sort -count'
96 30	2025-12-02 13:36:28.530	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlyweblogs" http_method="PUT" http_status=200 | table _time, bucket, object, http_method, http_status'
96 13	2025-12-02 13:36:28.513	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlyweblogs" http_method="PUT" http_status=200 | table _time, bucket, key, http_method, http_status'
96 72	2025-12-02 13:36:17.272	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlyweblogs" http_method="PUT" http_status=200 | table _time, bucket, object, http_method, http_status'
96 01	2025-12-02 13:36:01.101	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlyweblogs" http_method="PUT" http_status=200 | table _time, bucket, key, http_method, http_status'
96 69	2025-12-02 13:35:58.469	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlyweblogs" | stats count by bucket, http_method, http_status'

	_time	user	action	search
96	2025-12-02 13:35:43.032	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlyweblogs" | stats count by bucket, http_method, http_status'
96	2025-12-02 13:35:28.535	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket | sort -count'
96	2025-12-02 13:35:28.492	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_method="PUT" http_status=200 | table _time, bucket, object, http_method, http_status'
97	2025-12-02 13:35:13.723	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket | sort -count'
97	2025-12-02 13:35:01.551	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_method="PUT" http_status=200 | table _time, bucket, object, http_method, http_status'
97	2025-12-02 13:34:58.490	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_method="PUT" http_status=200 | table _time, bucket, key, http_method, http_status'
97	2025-12-02 13:34:58.475	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" | stats count by bucket, http_method, http_status'
97	2025-12-02 13:34:51.565	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_method="PUT" http_status=200 | table _time, bucket, key, http_method, http_status'

	_time	user	action	search
97	2025-12-02 13:34:31.224	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" | stats count by bucket, http_method, http_status'
97	2025-12-02 13:34:28.479	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, key, http_method, http_status'
97	2025-12-02 13:34:09.325	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, key, http_method, http_status'
97	2025-12-02 13:28:28.513	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'
97	2025-12-02 13:28:15.689	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'
98	2025-12-02 13:26:58.504	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs http_method="PUT" http_status=200 | table _time, bucket, key, object'
98	2025-12-02 13:26:58.490	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs http_method="PUT" http_status=200 | search "*.txt" | table _time, bucket, key, object'
98	2025-12-02 13:26:41.227	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs http_method="PUT" http_status=200 | table _time, bucket, key, object'

	_time	user	action	search
98	2025-12-02 13:26:35.445	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs http_method="PUT" http_status=200 | search "*.txt" | table _time, bucket, key, object'
98	2025-12-02 13:26:28.494	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_status=200 | stats count by http_method'
98	2025-12-02 13:26:14.026	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_status=200 | stats count by http_method'
98	2025-12-02 13:25:58.570	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | search sourcetype="*s3*"'
98	2025-12-02 13:25:58.556	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket'
98	2025-12-02 13:25:45.415	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats count by bucket'
98	2025-12-02 13:25:34.187	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | search sourcetype="*s3*"'
99	2025-12-02 13:25:28.512	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" | rex field=key "(?<extension>\.[^\.]+$)" | stats count by extension'

	_time	user	action	search
99971	2025-12-02 13:25:28.497	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_method="PUT" http_status=200 | rex field=key "(?<extension>\.[^\.]+$)" | stats count by extension'
99910	2025-12-02 13:25:22.410	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" | rex field=key "(?<extension>\.[^\.]+$)" | stats count by extension'
99967	2025-12-02 13:25:11.167	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_method="PUT" http_status=200 | rex field=key "(?<extension>\.[^\.]+$)" | stats count by extension'
99864	2025-12-02 13:24:58.498	kimjoe	search	'| search (index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlyweblogs" http_method="PUT" http_status=200 key="*.txt") | table _time, as, upload_time, key'
99885	2025-12-02 13:24:58.488	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table _time as bucket_made_public_time | appendcols [search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlyweblogs" http_method="PUT" http_status=200 key="*.txt" | table _time as upload_time, key] | table bucket_made_public_time, upload_time, key'
99866	2025-12-02 13:24:38.530	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table _time as bucket_made_public_time | appendcols [search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlyweblogs" http_method="PUT" http_status=200 key="*.txt" | table _time as upload_time, key] | table bucket_made_public_time, upload_time, key'
99907	2025-12-02 13:23:58.507	kimjoe	search	'| search (index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_method="PUT" http_status=200 key="*.txt") | table _time, as, upload_time, key'

	_time	user	action	search
99	2025-12-02 13:23:58.499	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table _time as bucket_made_public_time | appendcols [search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_method="PUT" http_status=200 key="*.txt" | table _time as upload_time, key] | table bucket_made_public_time, upload_time, key'
99	2025-12-02 13:23:38.019	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table _time as bucket_made_public_time | appendcols [search index=botsv3 sourcetype=aws:s3:accesslogs bucket="frothlywebcode" http_method="PUT" http_status=200 key="*.txt" | table _time as upload_time, key] | table bucket_made_public_time, upload_time, key'
10	2025-12-02 13:22:58.516	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:s3:accesslogs http_method=\"PUT\"frothlywebcode" max_time="1" count="50" use_cache=1'