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 ⇕ ✎
1 0 0 1	2025-12-02 13:22:58.5 03	kimj oe	sear ch	'typeahead prefix="index=botsv3 sourcetype=aws:s3:accesslogs buck" max_time="1" count="50" use_cache=1'
1 0 0 2	2025-12-02 13:22:58.4 92	kimj oe	sear ch	'typeahead prefix="index=botsv3 sourcetype=aws:s3:accesslogs bucket" max_time="1" count="50" use_cache=1'
1 0 0 3	2025-12-02 13:22:58.4 82	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket=* ht tp_method="PUT" http_status=200'

	_time ⬍	user ⬍ ✎	action ⬍ ✎	search ⬍ ✎
1 0 0 4	2025-12-02 13:22:30.9 74	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket=* ht tp_method="PUT" http_status=200'
1 0 0 5	2025-12-02 13:22:28.5 00	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode" http_method="PUT" http_status=200'
1 0 0 6	2025-12-02 13:22:28.4 86	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs http_method ="PUT" http_status=200'
1 0 0 7	2025-12-02 13:22:21.4 99	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode" http_method="PUT" http_status=200'
1 0 0 8	2025-12-02 13:22:08.7 94	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs http_method ="PUT" http_status=200'
1 0 0 9	2025-12-02 13:21:58.4 85	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs http_method ="PUT" | stats count by key, object | table key, object'

	_time ⇕	user ⇕ ✎	action ⇕ ✎	search ⇕ ✎
1 0 1 0	2025-12-02 13:21:52.4 38	kimj oe	sear ch	'typeahead prefix="index=botsv3 sourcetype=aws:s3:accesslogs http_method=\"PUT\"frothlywebcode" max_time="1" count="50" use_cache=1'
1 0 1 1	2025-12-02 13:21:47.1 67	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs http_method ="PUT" | stats count by key, object | table key, object'
1 0 1 2	2025-12-02 13:21:45.5 47	kimj oe	sear ch	'typeahead prefix="index=botsv3 sourcetype=aws:s3:accesslogs buck" max_time="1" count="50" use_cache=1'
1 0 1 3	2025-12-02 13:21:45.1 29	kimj oe	sear ch	'typeahead prefix="index=botsv3 sourcetype=aws:s3:accesslogs bucket" max_time="1" count="50" use_cache=1'
1 0 1 4	2025-12-02 13:21:28.5 33	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode" http_method="PUT" http_status=200 | stats count by key, object | table key, object'
1 0 1 5	2025-12-02 13:21:28.5 17	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode " http_method="PUT" http_status=200 | stats count by key, object | table key, object'

	_time ⬍	user ⬍ ✎	action ⬍ ✎	search ⬍ ✎
1 0 1 6	2025-12-02 13:21:28.5 01	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlyweblogs" http_method="PUT" http_status=200 | stats count by key, object | table key, object'
1 0 1 7	2025-12-02 13:21:28.4 87	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="[BU CKET_NAME]" http_method="PUT" http_status=200 | stats count b y key, object | table key, object'
1 0 1 8	2025-12-02 13:21:26.2 03	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode" http_method="PUT" http_status=200 | stats count by key, object | table key, object'
1 0 1 9	2025-12-02 13:21:24.7 05	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode " http_method="PUT" http_status=200 | stats count by key, object | table key, object'
1 0 2 0	2025-12-02 13:21:14.2 53	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlyweblogs" http_method="PUT" http_status=200 | stats count by key, object | table key, object'
1 0 2 1	2025-12-02 13:20:59.7 21	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="[BU CKET_NAME]" http_method="PUT" http_status=200 | stats count b y key, object | table key, object'

	_time ⬍	user ⬍ 🖊	action ⬍ 🖊	search ⬍ 🖊
1 0 2 2	2025-12-02 13:20:28.5 03	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats cou nt by bucket, http_method, http_status'
1 0 2 3	2025-12-02 13:20:28.4 77	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket=* | stats count by bucket, http_method, http_status'
1 0 2 4	2025-12-02 13:20:08.4 81	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats cou nt by bucket, http_method, http_status'
1 0 2 5	2025-12-02 13:20:02.3 58	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket=* | stats count by bucket, http_method, http_status'
1 0 2 6	2025-12-02 13:19:58.5 02	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats cou nt by bucket, http_method, http_status'
1 0 2 7	2025-12-02 13:19:50.5 66	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats cou nt by bucket, http_method, http_status'

	_time ⇕	user ⇕ ✎	action ⇕ ✎	search ⇕ ✎
1 0 2 8	2025-12-02 13:19:28.5 43	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_statu s'
1 0 2 9	2025-12-02 13:19:28.5 26	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs http_method ="PUT" http_status=200 | search "*.txt" | rex field=object " (?<filename>[^/]+\.txt$)" | where isnotnull(filename) | table filename'
1 0 3 0	2025-12-02 13:19:11.9 99	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_statu s'
1 0 3 1	2025-12-02 13:19:00.8 81	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs http_method ="PUT" http_status=200 | search "*.txt" | rex field=object " (?<filename>[^/]+\.txt$)" | where isnotnull(filename) | table filename'
1 0 3 2	2025-12-02 13:18:58.4 94	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlyweblogs"'
1 0 3 3	2025-12-02 13:18:34.7 88	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlyweblogs"'

	_time ⭥	user ⭥ ✎	action ⭥ ✎	search ⭥ ✎
1 0 3 4	2025-12-02 13:18:28.5 88	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode"'
1 0 3 5	2025-12-02 13:18:28.5 74	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode" http_method="PUT" http_status=200 | table _time, bucket, key, http_method, http_status'
1 0 3 6	2025-12-02 13:18:25.8 14	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode"'
1 0 3 7	2025-12-02 13:18:01.3 87	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode" http_method="PUT" http_status=200 | table _time, bucket, key, http_method, http_status'
1 0 3 8	2025-12-02 13:17:58.4 79	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_statu s'
1 0 3 9	2025-12-02 13:17:28.9 71	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_statu s'

_time ⬍	user ⬍ ✎	action ⬍ ✎	search ⬍ ✎
1 0 4 0	2025-12-02 13:17:28.4 99	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlyweblogs" | stats count by bucket, http_method, http_statu s'
1 0 4 1	2025-12-02 13:17:20.5 96	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlyweblogs" | stats count by bucket, http_method, http_statu s'
1 0 4 2	2025-12-02 13:16:58.4 74	kimj oe	sear ch	'typeahead prefix="index=botsv3 sourcetype=aws:s3:accesslogs" max_time="1" count="50" use_cache=1'
1 0 4 3	2025-12-02 13:16:28.4 79	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table *'
1 0 4 4	2025-12-02 13:15:59.5 62	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table *'
1 0 4 5	2025-12-02 13:15:58.5 30	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table'

	user ⬍ ✎	actio n ⬍ ✎	
_time ⬍			search ⬍ ✎
1 0 4 6	2025-12-02 13:15:58.5 18	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_statu s'
1 0 4 7	2025-12-02 13:15:58.5 02	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats cou nt by bucket, http_method, http_status'
1 0 4 8	2025-12-02 13:15:50.1 44	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table'
1 0 4 9	2025-12-02 13:15:42.5 33	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_statu s'
1 0 5 0	2025-12-02 13:15:29.5 48	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | stats cou nt by bucket, http_method, http_status'
1 0 5 1	2025-12-02 13:15:29.0 51	kimj oe	sear ch	'typeahead prefix="index=botsv3 sourcetype=aws:s3:accesslogs" max_time="1" count="50" use_cache=1'

_time ⇕	user ⇕ 🖋	action ⇕ 🖋	search ⇕ 🖋
1 0 5 2	2025-12-02 13:15:28.4 76	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode" | stats count by bucket, http_method, http_statu s'
1 0 5 3	2025-12-02 13:15:18.1 72	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="fro thlywebcode" | stats count by bucket, http_method, http_statu s'
1 0 5 4	2025-12-02 13:14:58.4 72	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_statu s'
1 0 5 5	2025-12-02 13:14:29.1 42	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, operation, key, http_method, http_statu s'
1 0 5 6	2025-12-02 13:13:58.4 77	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="[BU CKET_NAME]" http_method="PUT" http_status=200 | search object ="*.txt" OR key="*.txt" | table _time, bucket, object, key, h ttp_method, http_status'
1 0 5 7	2025-12-02 13:13:53.6 22	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs bucket="[BU CKET_NAME]" http_method="PUT" http_status=200 | search object ="*.txt" OR key="*.txt" | table _time, bucket, object, key, h ttp_method, http_status'

_time ⇕	user ⇕ ✎	action ⇕ ✎	search ⇕ ✎
1 0 5 8	2025-12-02 13:13:28.4 69	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 10 | table _time, bucket, operation, http_method, http_status, obj ect, key'
1 0 5 9	2025-12-02 13:13:25.9 64	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 10 | table _time, bucket, operation, http_method, http_status, obj ect, key'
1 0 6 0	2025-12-02 13:09:58.4 73	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | table eventID, userIdentity.userName, requestPar ameters.bucketName'
1 0 6 1	2025-12-02 13:09:35.5 93	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | table eventID, userIdentity.userName, requestPar ameters.bucketName'
1 0 6 2	2025-12-02 13:09:28.4 94	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | search requestParameters.acl="public-read" | tab le eventID, userIdentity.userName, requestParameters.bucketNa me'
1 0 6 3	2025-12-02 13:09:28.4 81	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | table eventID, _time, requestParameters.bucketNa me, requestParameters.acl'

	_time ⇕	user ⇕ ✎	action ⇕ ✎	search ⇕ ✎
1 0 6 4	2025-12-02 13:09:28.4 66	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="btaylor" | table eventID, _ time, requestParameters.bucketName, requestParameters.acl'
1 0 6 5	2025-12-02 13:09:27.5 81	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | search requestParameters.acl="public-read" | tab le eventID, userIdentity.userName, requestParameters.bucketNa me'
1 0 6 6	2025-12-02 13:09:09.2 55	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | table eventID, _time, requestParameters.bucketNa me, requestParameters.acl'
1 0 6 7	2025-12-02 13:09:00.1 02	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="btaylor" | table eventID, _ time, requestParameters.bucketName, requestParameters.acl'
1 0 6 8	2025-12-02 13:08:58.4 87	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | fieldsummary | search field="*acl*" OR field="*A CL*"'
1 0 6 9	2025-12-02 13:08:46.3 94	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | fieldsummary | search field="*acl*" OR field="*A CL*"'

	_time ⇕	user ⇕ ✎	action ⇕ ✎	search ⇕ ✎
1 0 7 0	2025-12-02 13:08:28.5 24	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | stats count by _time, eventID, userIdentity.user Name | sort -_time'
1 0 7 1	2025-12-02 13:08:28.5 10	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail | stats values (eventName) as events | search events=*Bucket*'
1 0 7 2	2025-12-02 13:08:15.2 49	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | stats count by _time, eventID, userIdentity.user Name | sort -_time'
1 0 7 3	2025-12-02 13:08:02.4 17	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail | stats values (eventName) as events | search events=*Bucket*'
1 0 7 4	2025-12-02 12:59:28.5 06	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | where (requestParameters.acl="public-read" OR re questParameters.acl="public-read-write" OR requestParameters. acl="authenticated-read") OR requestParameters.grantList LIKE "%AllUsers%" | table eventID, userIdentity.userName, requestP arameters.bucketName, requestParameters.acl'
1 0 7 5	2025-12-02 12:59:28.4 88	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | search requestPar ameters.grantList=*AllUsers* | table eventID'

	_time ⬍	user ⬍ ✎	actio n ⬍ ✎	search ⬍ ✎
1 0 7 6	2025-12-02 12:59:10.6 56	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | where (requestParameters.acl="public-read" OR re questParameters.acl="public-read-write" OR requestParameters. acl="authenticated-read") OR requestParameters.grantList LIKE "%AllUsers%" | table eventID, userIdentity.userName, requestP arameters.bucketName, requestParameters.acl'
1 0 7 7	2025-12-02 12:58:58.4 63	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | search requestPar ameters.acl=*public* OR requestParameters.grantList=*AllUsers * | table eventID'
1 0 7 8	2025-12-02 12:58:58.3 15	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | search requestPar ameters.grantList=*AllUsers* | table eventID'
1 0 7 9	2025-12-02 12:58:46.1 75	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | search requestPar ameters.acl=*public* OR requestParameters.grantList=*AllUsers * | table eventID'
1 0 8 0	2025-12-02 12:56:28.4 86	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | table eventID, re questParameters.bucketName, requestParameters.acl, requestPar ameters.grantList'
1 0 8 1	2025-12-02 12:56:28.4 66	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | table eventID, re questParameters.bucketName, requestParameters.acl, requestPar ameters.grantList | head 1'

	_time ⇕	user ⇕ ↗	action ⇕ ↗	search ⇕ ↗
1 0 8 2	2025-12-02 12:56:23.5 95	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | table eventID, re questParameters.bucketName, requestParameters.acl, requestPar ameters.grantList'
1 0 8 3	2025-12-02 12:56:18.4 46	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | table eventID, re questParameters.bucketName, requestParameters.acl, requestPar ameters.grantList | head 1'
1 0 8 4	2025-12-02 12:55:28.4 79	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | table _time, eventID, userIdentity.userName, req uestParameters.bucketName'
1 0 8 5	2025-12-02 12:55:28.4 64	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="btaylor" | table eventID, r equestParameters.bucketName, requestParameters.acl, requestPa rameters.grantList | head 1'
1 0 8 6	2025-12-02 12:55:18.6 96	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | table _time, eventID, userIdentity.userName, req uestParameters.bucketName'
1 0 8 7	2025-12-02 12:55:02.2 96	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="btaylor" | table eventID, r equestParameters.bucketName, requestParameters.acl, requestPa rameters.grantList | head 1'

	_time ⬍	user ⬍ ✎	action ⬍ ✎	search ⬍ ✎
1 0 8 8	2025-12-02 12:43:28.5 25	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab456 89d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
1 0 8 9	2025-12-02 12:43:01.5 62	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab456 89d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
1 0 9 0	2025-12-02 12:42:58.5 40	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventID="9a33d 8df-1e16-4d58-b36d-8e80ce68f8a3" | spath | table *'
1 0 9 1	2025-12-02 12:42:36.7 43	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventID="9a33d 8df-1e16-4d58-b36d-8e80ce68f8a3" | spath | table *'
1 0 9 2	2025-12-02 12:41:58.5 75	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | stats count by _time, eventID, userIdentity.user Name | sort -_time'
1 0 9 3	2025-12-02 12:41:58.5 60	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail | stats values (eventName) as events | search events=*Bucket*'

	_time ⇕	user ⇕ ✎	actio n ⇕ ✎	search ⇕ ✎
1 0 9 4	2025-12-02 12:41:51.7 18	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" | stats count by _time, eventID, userIdentity.user Name | sort -_time'
1 0 9 5	2025-12-02 12:41:39.7 90	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail | stats values (eventName) as events | search events=*Bucket*'
1 0 9 6	2025-12-02 12:41:28.5 11	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | search requestPar ameters.acl=*public* | table eventID'
1 0 9 7	2025-12-02 12:41:17.8 00	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | search requestPar ameters.acl=*public* | table eventID'
1 0 9 8	2025-12-02 12:40:58.4 84	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | search requestPar ameters.acl=*public* OR requestParameters.grantList=*AllUsers * | table eventID'
1 0 9 9	2025-12-02 12:40:48.4 10	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | search requestPar ameters.acl=*public* OR requestParameters.grantList=*AllUsers * | table eventID'

	_time	user	action	search
1 1 0 0	2025-12-02 12:40:28.4 96	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Put BucketAcl" userIdentity.userName="bstoll" | table eventID, _t ime, requestParameters.bucketName, requestParameters.acl'