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	2025-12-02 02:36:42.099	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 5 | table _time, eventName, additionalEventData.*'
2	2025-12-02 02:35:09.374	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search *MFA* | fieldsummary | search field="*MFA*"'
3	2025-12-02 02:34:47.131	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search *MFA* | fieldsummary | search field="*MFA*"'

	_time	user	action	search
1	2025-12-02 02:32:39.462	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users)'
1	2025-12-02 02:32:32.084	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users)'
1	2025-12-02 02:32:09.364	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1	2025-12-02 02:31:57.115	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1	2025-12-02 02:23:09.446	kimjoe	search	'| search (index=botsv3 sourcetype=aws:cloudtrail "userIdentity.type"="IAMUser") | stats values(userIdentity.userName) as usernames | eval usernames=mvdedup(usernames) | eval usernames=mvsort(usernames) | eval answer=mvjoin(usernames,",")'
1	2025-12-02 02:23:09.440	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvsort(usernames) | eval answer = mvjoin(usernames,",")] | table unique_users, answer'

	_time	user	action	search
1	2025-12-02 02:22:39.451	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvsort(usernames) | eval answer = mvjoin(usernames,",")] | table unique_users, answer'
2	2025-12-02 02:22:39.427	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats count by userIdentity.type'
3	2025-12-02 02:22:16.958	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats count by userIdentity.type'
4	2025-12-02 02:20:39.348	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
5	2025-12-02 02:20:18.689	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'

	_time	user	action	search
1	2025-12-02 02:20:09.402	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
2	2025-12-02 02:19:44.721	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
3	2025-12-02 02:19:09.378	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
4	2025-12-02 02:18:55.069	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
5	2025-12-02 02:18:09.388	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | head 5 | table _time, eventName, userIdentity.userName, userIdentity.type'

	_time	user	action	search
1	2025-12-02 02:18:09.375	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
2	2025-12-02 02:18:00.265	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | head 5 | table _time, eventName, userIdentity.userName, userIdentity.type'
3	2025-12-02 02:17:49.057	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
4	2025-12-02 02:17:39.354	kimjoe	search	'| search (index=botsv3 sourcetype=aws:cloudtrail "userIdentity.type"="IAMUser") | stats values(userIdentity.userName) as usernames | eval usernames=mvdedup(usernames) | eval usernames=mvsort(usernames) | eval answer=mvjoin(usernames,",")'
5	2025-12-02 02:17:39.346	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvsort(usernames) | eval answer = mvjoin(usernames,",")] | table unique_users, answer'

	_time	user	action	search
1	2025-12-02 02:17:18.117	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvsort(usernames) | eval answer = mvjoin(usernames, ",")] | table unique_users, answer'
2	2025-12-02 02:17:09.394	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
3	2025-12-02 02:17:09.379	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
4	2025-12-02 02:16:59.512	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
5	2025-12-02 02:16:45.733	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'

	_time	user	action	search
1	2025-12-02 02:16:39.387	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
1	2025-12-02 02:16:11.664	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
1	2025-12-02 02:16:09.369	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1	2025-12-02 02:16:09.355	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | head 5 | table _time, eventName, userIdentity.userName, userIdentity.type'
1	2025-12-02 02:15:54.739	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1	2025-12-02 02:15:39.704	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | head 5 | table _time, eventName, userIdentity.userName, userIdentity.type'

	_time	user	action	search
1	2025-12-02 02:15:39.340	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
2	2025-12-02 02:15:39.325	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
3	2025-12-02 02:15:22.890	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
4	2025-12-02 02:15:15.917	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
5	2025-12-02 02:13:39.368	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
6	2025-12-02 02:13:39.356	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'

	_time	user	action	search
1	2025-12-02 02:13:39.343	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
2				
1	2025-12-02 02:13:37.981	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
3				
1	2025-12-02 02:13:29.601	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
4				
1	2025-12-02 02:13:10.731	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
5				
1	2025-12-02 02:13:09.425	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
6				
1	2025-12-02 02:13:09.411	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
7				

	_time	user	action	search
1	2025-12-02 02:13:09.398	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
2	2025-12-02 02:13:09.386	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
3	2025-12-02 02:13:09.375	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
4	2025-12-02 02:13:09.362	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
5	2025-12-02 02:13:06.490	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
6	2025-12-02 02:13:00.619	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'

	_time	user	action	search
1	2025-12-02 02:12:57.683	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
2	2025-12-02 02:12:44.319	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
3	2025-12-02 02:12:42.392	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
4	2025-12-02 02:12:40.900	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
5	2025-12-02 02:12:39.378	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
6	2025-12-02 02:12:39.364	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'

	_time	user	action	search
1	2025-12-02 02:12:39.350	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
2	2025-12-02 02:12:39.335	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
3	2025-12-02 02:12:31.657	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'
4	2025-12-02 02:12:19.262	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
5	2025-12-02 02:12:17.438	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'

	_time	user	action	search
1	2025-12-02 02:12:15.338	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
2	2025-12-02 02:10:09.391	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
3	2025-12-02 02:10:09.374	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
4	2025-12-02 02:10:09.355	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
5	2025-12-02 02:10:09.339	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'

	_time	user	action	search
1	2025-12-02 02:09:54.768	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
1	2025-12-02 02:09:49.553	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
1	2025-12-02 02:09:41.551	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
1	2025-12-02 02:09:39.824	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
1	2025-12-02 02:09:39.406	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'

	_time	user	action	search
1	2025-12-02 02:09:39.394	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
2	2025-12-02 02:09:39.380	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
3	2025-12-02 02:09:39.367	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
4	2025-12-02 02:09:38.431	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'

	_time	user	action	search
1	2025-12-02 02:09:36.914	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
2	2025-12-02 02:09:33.395	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
3	2025-12-02 02:09:25.554	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
4	2025-12-02 02:06:39.352	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
5	2025-12-02 02:06:39.338	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'

	_time	user	action	search
1	2025-12-02 02:06:35.054	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
2	2025-12-02 02:06:33.596	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
3	2025-12-02 02:04:39.345	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
4	2025-12-02 02:04:14.801	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
5	2025-12-02 02:04:09.379	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
6	2025-12-02 02:04:09.366	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'

	_time	user	action	search
1	2025-12-02 02:04:09.353	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
2	2025-12-02 02:04:08.568	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
3	2025-12-02 02:03:59.523	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
4	2025-12-02 02:03:56.003	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
5	2025-12-02 02:01:09.356	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | head 5 | table _time, eventName, userIdentity.*'
6	2025-12-02 02:00:40.806	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | head 5 | table _time, eventName, userIdentity.*'

	_time	user	action	search
1	2025-12-02 02:00:39.322	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | head 5 | table _time, eventName, userIdentity.*'
2	2025-12-02 02:00:17.179	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | head 5 | table _time, eventName, userIdentity.*'
3	2025-12-02 02:00:09.381	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail"'
4	2025-12-02 02:00:09.366	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | head 5 | table _time, eventName, userIdentity.*'
5	2025-12-02 02:00:06.672	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail"'