

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)

	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
1501	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.*'
1502	2025-12-02 02:35:09.374	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail search *MFA* fieldsummary search field="*MFA*"'
1503	2025-12-02 02:34:47.131	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail search *MFA* fieldsummary search field="*MFA*"'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1504	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)'
1505	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)'
1506	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"'
1507	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"'
1508	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,",")'
1509	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'

	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
1510	2025-12-02 02:22:39.4	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'
1511	2025-12-02 02:22:39.4	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail stats count by userIdentity.type'
1512	2025-12-02 02:22:16.9	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail stats count by userIdentity.type'
1513	2025-12-02 02:20:39.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1514	2025-12-02 02:20:18.6	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1515	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'
1521	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'
1578	2025-12-02 02:19:09.378	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
1569	2025-12-02 02:18:55.069	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
1588	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'

	<div><div>_time ↕</div></div>	<div><div>user ↕</div></div>	<div><div>action ↕</div></div>	<div><div>search ↕</div></div>
1520	2025-12-02 02:18:09.375	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail head 5 table _time, eventName, userIdentity.*'
1521	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'
1522	2025-12-02 02:17:49.057	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail head 5 table _time, eventName, userIdentity.*'
1523	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,",")'
1524	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'

	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
1 5 2 5	2025-12-02 02:17:18.1 17	kimj oe	sear ch	'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'
1 5 2 6	2025-12-02 02:17:09.3 94	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1 5 2 7	2025-12-02 02:17:09.3 79	kimj oe	sear ch	'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 5 2 8	2025-12-02 02:16:59.5 12	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1 5 2 9	2025-12-02 02:16:45.7 33	kimj oe	sear ch	'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'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1530	2025-12-02 02:16:39.387	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
1531	2025-12-02 02:16:11.664	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
1532	2025-12-02 02:16:09.369	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail head 5 table _time, eventName, userIdentity.*'
1533	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'
1534	2025-12-02 02:15:54.739	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail head 5 table _time, eventName, userIdentity.*'
1535	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'

	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
1536	2025-12-02 02:15:39.340	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1537	2025-12-02 02:15:39.325	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1538	2025-12-02 02:15:22.890	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1539	2025-12-02 02:15:15.917	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1540	2025-12-02 02:13:39.368	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1541	2025-12-02 02:13:39.356	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'

	<div><div>_time ↕</div></div>	<div><div>user ↕</div></div>	<div><div>action ↕</div></div>	<div><div>search ↕</div></div>
154	2025-12-02 02:13:39.342	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
153	2025-12-02 02:13:37.943	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
152	2025-12-02 02:13:29.604	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
151	2025-12-02 02:13:10.735	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
150	2025-12-02 02:13:09.426	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
149	2025-12-02 02:13:09.411	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'






	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
1548	2025-12-02 02:13:09.398	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1549	2025-12-02 02:13:09.386	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1550	2025-12-02 02:13:09.375	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1551	2025-12-02 02:13:09.362	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1552	2025-12-02 02:13:06.490	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1553	2025-12-02 02:13:00.619	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1554	2025-12-02 02:12:57.683	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1555	2025-12-02 02:12:44.319	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1556	2025-12-02 02:12:42.392	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1557	2025-12-02 02:12:40.900	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1558	2025-12-02 02:12:39.378	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1559	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'

	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
1	2025-12-02 02:12:39.3	kimj	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	50	oe		
6				
0				
1	2025-12-02 02:12:39.3	kimj	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	35	oe		
6				
1				
1	2025-12-02 02:12:31.6	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	57	oe		
6				
2				
1	2025-12-02 02:12:19.2	kimj	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	62	oe		
6				
3				
1	2025-12-02 02:12:17.4	kimj	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	38	oe		
6				
4				

	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
1 5 6 5	2025-12-02 02:12:15.38	kimj oe	sear ch	'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 5 6 6	2025-12-02 02:10:09.391	kimj oe	sear ch	'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 5 6 7	2025-12-02 02:10:09.374	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
1 5 6 8	2025-12-02 02:10:09.355	kimj oe	sear ch	'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 5 6 9	2025-12-02 02:10:09.339	kimj oe	sear ch	'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'

	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
1 5 7 0	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 5 7 1	2025-12-02 02:09:49.553	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
1 5 7 2	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 5 7 3	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 5 7 4	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 02:09:39.3	kimj	sear	'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	94	oe	ch		
7					
5					
1	2025-12-02 02:09:39.3	kimj	sear	'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	80	oe	ch		
7					
6					
1	2025-12-02 02:09:39.3	kimj	sear	'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	67	oe	ch		
7					
7					
1	2025-12-02 02:09:38.4	kimj	sear	'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	31	oe	ch		
7					
8					

	<div><div></div><div>_time</div><div></div></div>	<div><div></div><div>user</div><div></div></div>	<div><div></div><div>action</div><div></div></div>	<div><div></div><div>search</div><div></div></div>
1 5 7 9	2025-12-02 02:09:36.9 14	kimj oe	sear ch	'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 5 8 0	2025-12-02 02:09:33.3 95	kimj oe	sear ch	'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 5 8 1	2025-12-02 02:09:25.5 54	kimj oe	sear ch	'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 5 8 2	2025-12-02 02:06:39.3 52	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
1 5 8 3	2025-12-02 02:06:39.3 38	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1584	2025-12-02 02:06:35.054	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
1585	2025-12-02 02:06:33.596	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
1586	2025-12-02 02:04:39.345	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
1587	2025-12-02 02:04:14.801	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
1588	2025-12-02 02:04:09.379	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
1589	2025-12-02 02:04:09.366	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'

	<div><div>_time ↕</div></div>	<div><div>user ↕</div></div>	<div><div>action ↕</div></div>	<div><div>search ↕</div></div>
1590	2025-12-02 02:04:09.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
1591	2025-12-02 02:04:08.5	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
1592	2025-12-02 02:03:59.5	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
1593	2025-12-02 02:03:56.0	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
1594	2025-12-02 02:01:09.3	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" head 5 table _time, eventName, userIdentity.*'
1595	2025-12-02 02:00:40.8	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" head 5 table _time, eventName, userIdentity.*'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>	<div><div></div><div></div></div>
1596	2025-12-02 02:00:39.322	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" head 5 table _time, eventName, userIdentity.*'	
1597	2025-12-02 02:00:17.179	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" head 5 table _time, eventName, userIdentity.*'	
1598	2025-12-02 02:00:09.381	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail"'	
1599	2025-12-02 02:00:09.366	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" head 5 table _time, eventName, userIdentity.*'	
1600	2025-12-02 02:00:06.672	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail"'	