

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 02:36:42.0	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin" search *MFA* head 5 table _time, eventName, additionalEventData.*'
5	99			
0		oe	ch	
1				
1	2025-12-02 02:35:09.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail search *MFA* fieldsummary search field="*MFA*"'
5	74			
0		oe	ch	
2				
1	2025-12-02 02:34:47.1	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail search *MFA* fieldsummary search field="*MFA*"'
5	31			
0		oe	ch	
3				

		user	action	
	_time	user	action	search
1	2025-12-02 02:32:39.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) AS IAM_Users eval IAM_Users = mvdedup(IAM_Users)'
5	62	oe	search	
0				
4				
1	2025-12-02 02:32:32.0	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) AS IAM_Users eval IAM_Users = mvdedup(IAM_Users)'
5	84	oe	search	
0				
5				
1	2025-12-02 02:32:09.3	kimj	search	'search index="botsv3" sourcetype="aws:cloudtrail" stats count by userIdentity.userName rename userIdentity.userName AS "IAM_User"'
5	64	oe	search	
0				
6				
1	2025-12-02 02:31:57.1	kimj	search	'search index="botsv3" sourcetype="aws:cloudtrail" stats count by userIdentity.userName rename userIdentity.userName AS "IAM_User"'
5	15	oe	search	
0				
7				
1	2025-12-02 02:23:09.4	kimj	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	46	oe	search	
0				
8				
1	2025-12-02 02:23:09.4	kimj	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'
5	40	oe	search	
0				
9				

		user	action	
	_time	♦	♦	search ♦
1	2025-12-02 02:22:39.4	kimj	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'
5	51	oe	search	'search index=botsv3 sourcetype=aws:cloudtrail stats count by userIdentity.type'
1				
1	2025-12-02 02:22:16.9	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail stats count by userIdentity.type'
5	58	oe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1				
2				
1	2025-12-02 02:20:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	48	oe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1				
3				
1	2025-12-02 02:20:18.6	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	89	oe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
1				
4				

		user	action	search
_time	✓	✓	✓	✓
1	2025-12-02 02:20:09.4	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	02	oe	ch	
1				
5				
1	2025-12-02 02:19:44.7	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames eval usernames = mvdedup(usernames) eval usernames = mvmmap(usernames, lower(usernames)) eval sorted_usernames = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
5	21	oe	ch	
1				
6				
1	2025-12-02 02:19:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
5	78	oe	ch	
1				
7				
1	2025-12-02 02:18:55.0	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
5	69	oe	ch	
1				
8				
1	2025-12-02 02:18:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" head 5 table _time, eventName, userIdentity.userName, userIdentity.type'
5	88	oe	ch	
1				
9				

		user	action	
	_time	↓	↑	search ↓
1	2025-12-02 02:18:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail head 5 table _time, eventName, userIdentity.*'
5	75	oe	ch	
0				
1	2025-12-02 02:18:00.2	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" head 5 table _time, eventName, userIdentity.userName, userIdentity.type'
5	65	oe	ch	
2				
1	2025-12-02 02:17:49.0	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail head 5 table _time, eventName, userIdentity.*'
5	57	oe	ch	
2				
1	2025-12-02 02:17:39.3	kimj	search	' search (index=botsv3 sourcetype=aws:cloudtrail "userIdentity.type"="IAMUser") stats values(userIdentity.userName) as usernames eval usernames=mvdedup(usernames) eval usernames=mvsort(usernames) eval answer=mvjoin(usernames, ",")'
5	54	oe	ch	
2				
3				
1	2025-12-02 02:17:39.3	kimj	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'
5	46	oe	ch	
2				
4				

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

		user	action	search
_time	♦	↙	↙	search ♦
1	2025-12-02 02:16:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
5	87	oe	ch	
3				
0				
1	2025-12-02 02:16:11.6	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
5	64	oe	ch	
3				
1				
1	2025-12-02 02:16:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail head 5 table _time, eventName, userIdentity.*'
5	69	oe	ch	
3				
2				
1	2025-12-02 02:16:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" head 5 table _time, eventName, userIdentity.userName, userIdentity.type'
5	55	oe	ch	
3				
3				
1	2025-12-02 02:15:54.7	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail head 5 table _time, eventName, userIdentity.*'
5	39	oe	ch	
3				
4				
1	2025-12-02 02:15:39.7	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" head 5 table _time, eventName, userIdentity.userName, userIdentity.type'
5	04	oe	ch	
3				
5				

		user	action	search
1	2025-12-02 02:15:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	40	oe	search	
3				
6				
1	2025-12-02 02:15:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	25	oe	search	
3				
7				
1	2025-12-02 02:15:22.8	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	90	oe	search	
3				
8				
1	2025-12-02 02:15:15.9	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	17	oe	search	
3				
9				
1	2025-12-02 02:13:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	68	oe	search	
4				
0				
1	2025-12-02 02:13:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	56	oe	search	
4				
1				

		user	action	search
_time	◆	◆	◆	◆
1	2025-12-02 02:13:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	43	oe	ch	
4				
2				
1	2025-12-02 02:13:37.9	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	81	oe	ch	
4				
3				
1	2025-12-02 02:13:29.6	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	01	oe	ch	
4				
4				
1	2025-12-02 02:13:10.7	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	31	oe	ch	
4				
5				
1	2025-12-02 02:13:09.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	25	oe	ch	
4				
6				
1	2025-12-02 02:13:09.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	11	oe	ch	
4				
7				

		user	action	search
1	2025-12-02 02:13:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	98	oe	ch	
4				
8				
1	2025-12-02 02:13:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	86	oe	ch	
4				
9				
1	2025-12-02 02:13:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	75	oe	ch	
5				
0				
1	2025-12-02 02:13:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	62	oe	ch	
5				
1				
1	2025-12-02 02:13:06.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	90	oe	ch	
5				
2				
1	2025-12-02 02:13:00.6	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5	19	oe	ch	
5				
3				

_time	user	action	search
1 2025-12-02 02:12:57.6	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5 83	oe	ch	
5			
4			
1 2025-12-02 02:12:44.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5 19	oe	ch	
5			
5			
1 2025-12-02 02:12:42.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5 92	oe	ch	
5			
6			
1 2025-12-02 02:12:40.9	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5 00	oe	ch	
5			
7			
1 2025-12-02 02:12:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" dedup userIdentity.userName table userIdentity.userName'
5 78	oe	ch	
5			
8			
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 64	oe	ch	
5			
9			

		user	action	search
_time		↓	↑	↓
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	ch	
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 = mvmmap(usernames, lower(usernames)) eval sorted_usernames = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
5	35	oe	ch	
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	ch	
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 = mvmmap(usernames, lower(usernames)) eval sorted_usernames = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
5	62	oe	ch	
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 = mvmmap(usernames, lower(usernames)) eval sorted_usernames = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
5	38	oe	ch	
6				
4				

		user	action	search
_time		↓	↑	↓
1	2025-12-02 02:12:15.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames eval usernames = mvdedup(usernames) eval usernames = mvmay(usernames, lower(usernames)) eval sorted_usernames = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
5	38	oe	ch	
6				
5				
1	2025-12-02 02:10:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames eval usernames = mvdedup(usernames) eval usernames = mvmay(usernames, lower(usernames)) eval sorted_usernames = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
5	91	oe	ch	
6				
6				
1	2025-12-02 02:10:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
5	74	oe	ch	
6				
7				
1	2025-12-02 02:10:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames eval usernames = mvdedup(usernames) eval usernames = mvmay(usernames, lower(usernames)) eval sorted_usernames = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
5	55	oe	ch	
6				
8				
1	2025-12-02 02:10:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames eval usernames = mvdedup(usernames) eval usernames = mvmay(usernames, lower(usernames)) eval sorted_usernames = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
5	39	oe	ch	
6				
9				

		user	action	search
_time		↓ ↴	↑ ↴	↓ ↴
1	2025-12-02 02:09:54.7	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	68	oe	ch	
7				
0				
1	2025-12-02 02:09:49.5	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
5	53	oe	ch	
7				
1				
1	2025-12-02 02:09:41.5	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	51	oe	ch	
7				
2				
1	2025-12-02 02:09:39.8	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	24	oe	ch	
7				
3				
1	2025-12-02 02:09:39.4	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	06	oe	ch	
7				
4				

		user	action	search
_time		♦	♦	♦
1	2025-12-02 02:09:39.3	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	94	oe	ch	
7				
5				
1	2025-12-02 02:09:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames eval usernames = mvdedup(usernames) eval usernames = mvmmap(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	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames eval usernames = mvdedup(usernames) eval usernames = mvmmap(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	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames eval usernames = mvdedup(usernames) eval usernames = mvmmap(usernames, lower(usernames)) eval sorted_usernames = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
5	31	oe	ch	
7				
8				

		user	action	search
	_time	↓	↑	↓
1	2025-12-02 02:09:36.9	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	14	oe	ch	
7				
9				
1	2025-12-02 02:09:33.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames eval usernames = mvdedup(usernames) eval usernames = mvmmap(usernames, lower(usernames)) eval sorted_usernames = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
5	95	oe	ch	
8				
0				
1	2025-12-02 02:09:25.5	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames eval usernames = mvdedup(usernames) eval usernames = mvmmap(usernames, lower(usernames)) eval sorted_usernames = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
5	54	oe	ch	
8				
1				
1	2025-12-02 02:06:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
5	52	oe	ch	
8				
2				
1	2025-12-02 02:06:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
5	38	oe	ch	
8				
3				

		user	action	search
1	2025-12-02 02:06:35.0	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser'"
5	54	oe	ch	
8				
4				
1	2025-12-02 02:06:33.5	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser'"
5	96	oe	ch	
8				
5				
1	2025-12-02 02:04:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as username'
5	45	oe	ch	
8				
6				
1	2025-12-02 02:04:14.8	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as username'
5	01	oe	ch	
8				
7				
1	2025-12-02 02:04:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser'"
5	79	oe	ch	
8				
8				
1	2025-12-02 02:04:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as username'
5	66	oe	ch	
8				
9				

		user	action	search
_time	◆	◆	◆	◆
1	2025-12-02 02:04:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as username'
5	53	oe	ch	
9				
0				
1	2025-12-02 02:04:08.5	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"'
5	68	oe	ch	
9				
1				
1	2025-12-02 02:03:59.5	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as username'
5	23	oe	ch	
9				
2				
1	2025-12-02 02:03:56.0	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as username'
5	03	oe	ch	
9				
3				
1	2025-12-02 02:01:09.3	kimj	search	'search index="botsv3" sourcetype="aws:cloudtrail" head 5 table _time, eventName, userIdentity.*'
5	56	oe	ch	
9				
4				
1	2025-12-02 02:00:40.8	kimj	search	'search index="botsv3" sourcetype="aws:cloudtrail" head 5 table _time, eventName, userIdentity.*'
5	06	oe	ch	
9				
5				

		user	action	
		♦	♦	search ♦
1	2025-12-02 02:00:39.3	kimj	search	'search index="botsv3" sourcetype="aws:cloudtrail" head 5 table _time, eventName, userIdentity.*'
5	22	oe	ch	
9				
6				
1	2025-12-02 02:00:17.1	kimj	search	'search index="botsv3" sourcetype="aws:cloudtrail" head 5 table _time, eventName, userIdentity.*'
5	79	oe	ch	
9				
7				
1	2025-12-02 02:00:09.3	kimj	search	'search index="botsv3" sourcetype="aws:cloudtrail"'
5	81	oe	ch	
9				
8				
1	2025-12-02 02:00:09.3	kimj	search	'search index="botsv3" sourcetype="aws:cloudtrail" head 5 table _time, eventName, userIdentity.*'
5	66	oe	ch	
9				
9				
1	2025-12-02 02:00:06.6	kimj	search	'search index="botsv3" sourcetype="aws:cloudtrail"'
6	72	oe	ch	
0				
0				