

# 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 03:00:28.2	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName 4 = "ConsoleLogin"   search *MFA*   head 5   table _time, event 0 Name, additionalEventData.*'	
1	2025-12-02 03:00:09.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   search *MFA 4 *   fieldsummary   search field="*MFA*"'	
0	2025-12-02 02:59:59.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   search *MFA 4 *   fieldsummary   search field="*MFA*"'	
3					

		user	action	search
1	2025-12-02 02:54:09.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"'
4	14	e	h	
0				
4				
1	2025-12-02 02:54:04.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"'
4	13	e	h	
0				
5				
1	2025-12-02 02:53:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where additionalEventData.MFAUsed="yes"   head 3   table _time, eventName, additionalEventData.MFAUse d'
4	64	e	h	
0				
6				
1	2025-12-02 02:52:51.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where additionalEventData.MFAUsed="yes"   head 3   table _time, eventName, additionalEventData.MFAUse d'
4	77	e	h	
0				
7				
1	2025-12-02 02:52:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where additionalEventData.MFAUsed="No"   h ead 3   table _time, eventName, additionalEventData.MFAUsed'
4	22	e	h	
0				
8				
1	2025-12-02 02:52:32.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where additionalEventData.MFAUsed="No"   h ead 3   table _time, eventName, additionalEventData.MFAUsed'
4	07	e	h	
0				
9				

		user	action	search
_time	◆	◆	◆	◆
1	2025-12-02 02:52:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsum mary   search field="*MFA*"   table field, count'
4	60	e	h	
1				
0				
1	2025-12-02 02:51:43.9	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsum mary   search field="*MFA*"   table field, count'
4	91	e	h	
1				
1	2025-12-02 02:51:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsum mary   search field="*MFA* OR *mfa*"   table field, count'
4	83	e	h	
1				
2				
1	2025-12-02 02:51:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsum mary   search field="*MFA*"   table field, count'
4	70	e	h	
1				
3				
1	2025-12-02 02:51:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 5   fieldsumm ary   search field="*MFA*"   table field, count'
4	55	e	h	
1				
4				
1	2025-12-02 02:51:36.9	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsum mary   search field="*MFA* OR *mfa*"   table field, count'
4	24	e	h	
1				
5				

	_time	user	action	search
1	2025-12-02 02:51:16.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsum mary   search field="*MFA*"   table field, count'
4	01	e	h	
1				
6				
1	2025-12-02 02:51:10.0	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 5   fieldsumm ary   search field="*MFA*"   table field, count'
4	14	e	h	
1				
7				
1	2025-12-02 02:51:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 2   fieldsumm ary   search field="*MFA*"   table field, count'
4	74	e	h	
1				
8				
1	2025-12-02 02:51:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 1   fieldsumm ary   search field="*MFA*"   table field, count'
4	57	e	h	
1				
9				
1	2025-12-02 02:51:03.2	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 2   fieldsumm ary   search field="*MFA*"   table field, count'
4	16	e	h	
2				
0				
1	2025-12-02 02:50:54.2	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA* OR *mfa*   head 1   fieldsumm ary   search field="*MFA*"   table field, count'
4	12	e	h	
2				
1				

	_time	user	action	search
1	2025-12-02 02:50:39.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea
4	63	e	h	rch field="*MFA*"   table field, count'
2				
1	2025-12-02 02:50:39.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA* or *mfa*   head 1   fieldsumm
4	51	e	h	ary   search field="*MFA*"   table field, count'
2				
3				
1	2025-12-02 02:50:39.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA* or   head 1   fieldsummary
4	39	e	h	search field="*MFA*"   table field, count'
2				
4				
1	2025-12-02 02:50:38.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea
4	63	e	h	rch field="*MFA*"   table field, count'
2				
5				
1	2025-12-02 02:50:28.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA* or *mfa*   head 1   fieldsumm
4	41	e	h	ary   search field="*MFA*"   table field, count'
2				
6				
1	2025-12-02 02:50:17.9	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA* or   head 1   fieldsummary
4	20	e	h	search field="*MFA*"   table field, count'
2				
7				

	_time	user	action	search
1	2025-12-02 02:50:09.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea
4	31	e	h	rch field="*MFA*"   table field, count'
2				
8				
1	2025-12-02 02:50:09.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
4	16	e	h	
2				
9				
1	2025-12-02 02:50:07.0	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea
4	47	e	h	rch field="*MFA*"   table field, count'
3				
0				
1	2025-12-02 02:49:55.1	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
4	91	e	h	
3				
1				
1	2025-12-02 02:49:09.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   stats value
4	19	e	h	s(additionalEventData.MFAUsed) AS MFAUsed, values(userIdentifi
3				ty.sessionContext.attributes.mfaAuthenticated) AS mfaAuthent
2				icated'
1	2025-12-02 02:49:06.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   stats value
4	65	e	h	s(additionalEventData.MFAUsed) AS MFAUsed, values(userIdentifi
3				ty.sessionContext.attributes.mfaAuthenticated) AS mfaAuthent
3				icated'

	_time	user	action	search
1	2025-12-02 02:48:39.3	kimjo	search	'search index=botsv3 sourcetype=aws:cloudtrail   fieldsummary   search field="*mfa*" OR field="*MFA*"   table field, count'
4	86	e	h	
3				
4				
1	2025-12-02 02:48:27.6	kimjo	search	'search index=botsv3 sourcetype=aws:cloudtrail   fieldsummary   search field="*mfa*" OR field="*MFA*"   table field, count'
4	85	e	h	
3				
5				
1	2025-12-02 02:48:09.3	kimjo	search	'search index=botsv3 sourcetype=aws:cloudtrail   search "MFA Used"   head 5   table _time, eventName, additionalEventData.MFAUsed'
4	82	e	h	
3				
6				
1	2025-12-02 02:48:09.3	kimjo	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated)   stats count by userIdentity.sessionContext.attributes.mfaAuthenticated'
4	68	e	h	
3				
7				
1	2025-12-02 02:48:04.5	kimjo	search	'search index=botsv3 sourcetype=aws:cloudtrail   search "MFA Used"   head 5   table _time, eventName, additionalEventData.MFAUsed'
4	46	e	h	
3				
8				
1	2025-12-02 02:47:43.3	kimjo	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated)   stats count by userIdentity.sessionContext.attributes.mfaAuthenticated'
4	35	e	h	
3				
9				

		user	action	search
_time	✓	✓	✓	✓
1	2025-12-02 02:47:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
4	75	e	h	
4				
0				
1	2025-12-02 02:47:11.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
4	89	e	h	
4				
1				
1	2025-12-02 02:47:09.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
4	06	e	h	
4				
2				
1	2025-12-02 02:46:46.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
4	50	e	h	
4				
3				
1	2025-12-02 02:46:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'
4	58	e	h	
4				
4				
1	2025-12-02 02:45:40.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'
4	26	e	h	
4				
5				

		user	action	search
_time	sort	sort	sort	sort
1	2025-12-02 02:45:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName =\"ConsoleLogin\"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values=\"No\"   head 10'
4	76	e	h	
4				
6				
1	2025-12-02 02:45:09.1	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName =\"ConsoleLogin\"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values=\"No\"   head 10'
4	58	e	h	
4				
7				
1	2025-12-02 02:42:39.5	kimjo	searc	'typeahead prefix=\"index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" a\" max_time=\"1\" count=\"50\" use_cache=1'
4	12	e	h	
4				
8				
1	2025-12-02 02:42:39.5	kimjo	searc	'typeahead prefix=\"index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" addi\" max_time=\"1\" count=\"50\" use_cache=1'
4	01	e	h	
4				
9				
1	2025-12-02 02:42:39.4	kimjo	searc	'typeahead prefix=\"index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" additionalEventData\" max_time =\"1\" count=\"50\" use_cache=1'
4	88	e	h	
5				
0				
1	2025-12-02 02:42:39.4	kimjo	searc	'typeahead prefix=\"index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" additionalEventData.MFAUsed\" ma_x_time=\"1\" count=\"50\" use_cache=1'
4	79	e	h	
5				
1				

	_time	user	action	search
1	2025-12-02 02:42:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea rch field="*MFA*"   table field, count'
4	69	e	h	
5				
2				
1	2025-12-02 02:42:18.7	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea rch field="*MFA*"   table field, count'
4	67	e	h	
5				
3				
1	2025-12-02 02:42:09.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   foreach * [eval <>FIELD>_exists = if(isnotnull('
4	17	e	h	
5				
4				
1	2025-12-02 02:42:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" additionalEventData.MFAUsed=*   stats count by additionalEventData.MFAUsed'
4	61	e	h	
5				
5				
1	2025-12-02 02:42:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" additionalEventData.MFAUsed=*'
4	49	e	h	
5				
6				
1	2025-12-02 02:41:55.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   foreach * [eval <>FIELD>_exists = if(isnotnull('
4	22	e	h	
5				
7				

		user	action	search
_time	◆	◆	◆	◆
1	2025-12-02 02:41:44.0	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" additionalEventData.MFAUsed=*   stats count by additionalEventData.MFAUsed'
4	65	e	h	
5				
8				
1	2025-12-02 02:41:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" additionalEventData.MFAUsed=*'
4	54	e	h	
5				
9				
1	2025-12-02 02:41:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"'
4	35	e	h	
6				
0				
1	2025-12-02 02:41:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" additionalEventData.MFAUsed=*'
4	64	e	h	
6				
1				
1	2025-12-02 02:41:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" additionalEventData.MFAUsed=*'
4	63	e	h	
6				
2				
1	2025-12-02 02:41:37.2	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" additionalEventData.MFAUsed=*'
4	53	e	h	
6				
3				

	_time	user	action	search
1	2025-12-02 02:41:23.7	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"'
4	36	e	h	
6				
4				
1	2025-12-02 02:41:22.7	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO T eventName=\\"ConsoleLogin\\" a" max_time="1" count="50" use_ cache=1'
4	75	e	h	
6				
5				
1	2025-12-02 02:41:22.3	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO T eventName=\\"ConsoleLogin\\" addi" max_time="1" count="50" u se_cache=1'
4	42	e	h	
6				
6				
1	2025-12-02 02:41:21.8	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO T eventName=\\"ConsoleLogin\\" additionalEventData" max_time ="1" count="50" use_cache=1'
4	74	e	h	
6				
7				
1	2025-12-02 02:41:21.4	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO T eventName=\\"ConsoleLogin\\" additionalEventData.MFAUsed" ma x_time="1" count="50" use_cache=1'
4	32	e	h	
6				
8				
1	2025-12-02 02:41:15.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" additionalEventData.MFAUsed=*
4	69	e	h	
6				
9				

		user	action	
_time	sort	user	action	search
1	2025-12-02 02:41:09.3	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" m
4	32	e	h	ax_time="1" count="50" use_cache=1'
7				
0				
1	2025-12-02 02:40:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	89	e	h	= "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)
7				
1				
1	2025-12-02 02:40:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	77	e	h	= "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
7				
2				
1	2025-12-02 02:40:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	64	e	h	= "ConsoleLogin"'
7				
3				
1	2025-12-02 02:40:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	95	e	h	= "ConsoleLogin"'
7				
4				
1	2025-12-02 02:40:37.7	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	65	e	h	= "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)
7				
5				

		user	action	search
_time	◆	◆	◆	◆
1	2025-12-02 02:40:31.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName 4    ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse 7       d)   stats count by additionalEventData.MFAUsed'
4	37	e	h	
7				
1	2025-12-02 02:40:26.7	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName 4    ="ConsoleLogin"'
4	48	e	h	
7				
1	2025-12-02 02:40:17.2	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName 4    ="ConsoleLogin"'
4	48	e	h	
7				
1	2025-12-02 02:40:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName 4    ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse 7       d)   stats count by additionalEventData.MFAUsed'
4	19	e	h	
7				
1	2025-12-02 02:40:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Co 4    nsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   8       stats count by additionalEventData.MFAUsed'
0				
1	2025-12-02 02:40:04.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName 4    ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse 8       d)   stats count by additionalEventData.MFAUsed'
56		e	h	
1				

		user	action	search
_time	◆	◆	◆	◆
1	2025-12-02 02:39:40.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Co
4	23	e	h	nsoleLogin"   where isnotnull(additionalEventData.MFAUsed)
8				stats count by additionalEventData.MFAUsed'
2				
1	2025-12-02 02:39:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	97	e	h	="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse
8				d)   stats count by additionalEventData.MFAUsed'
3				
1	2025-12-02 02:39:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	81	e	h	="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse
8				d)   stats count by additionalEventData.MFAUsed'
4				
1	2025-12-02 02:39:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	68	e	h	="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse
8				d)   stats count by additionalEventData.MFAUsed'
5				
1	2025-12-02 02:39:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	56	e	h	="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse
8				d)   stats count by additionalEventData.MFAUsed'
6				
1	2025-12-02 02:39:39.2	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" m
4	88	e	h	ax_time="1" count="50" use_cache=1'
8				
7				

		user	action	search
_time	◆	◆	◆	◆
1	2025-12-02 02:39:21.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse d)   stats count by additionalEventData.MFAUsed'
4	58	e	h	
8				
1	2025-12-02 02:39:19.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse d)   stats count by additionalEventData.MFAUsed'
4	57	e	h	
8				
1	2025-12-02 02:39:17.2	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse d)   stats count by additionalEventData.MFAUsed'
4	36	e	h	
9				
0				
1	2025-12-02 02:39:14.0	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse d)   stats count by additionalEventData.MFAUsed'
4	93	e	h	
9				
1				
1	2025-12-02 02:39:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse d)   stats count by additionalEventData.MFAUsed'
4	31	e	h	
9				
2				
1	2025-12-02 02:39:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" additionalEventData.MFAUsed=*   stats count by additionalEventData.MFAUsed'
4	20	e	h	
9				
3				

	_time	user	action	search
1	2025-12-02 02:39:07.6	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse d)   stats count by additionalEventData.MFAUsed'
4	54	e	h	
9				
4				
1	2025-12-02 02:38:46.9	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" additionalEventData.MFAUsed=*   stats count by additionalEventData.MFAUsed'
4	29	e	h	
9				
5				
1	2025-12-02 02:38:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse d)   stats count by additionalEventData.MFAUsed'
4	25	e	h	
9				
6				
1	2025-12-02 02:38:20.6	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse d)   stats count by additionalEventData.MFAUsed'
4	26	e	h	
9				
7				
1	2025-12-02 02:38:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse d)   stats count by additionalEventData.MFAUsed'
4	25	e	h	
9				
8				
1	2025-12-02 02:38:03.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   where isnotnull(additionalEventData.MFAUse d)   stats count by additionalEventData.MFAUsed'
4	57	e	h	
9				
9				

		user	action	
	_time	▼ ↗	▼ ↗	search ▼ ↗
1	2025-12-02 02:37:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA*   head 5   table _time, event Name, additionalEventData.*'
5	03	e	h	
0				
0				