# 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 |
|---|---|---|---|---|
| 201 | 2025-12-10 20:46:58.138 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" \| table _time, eventID, userIdentity.userName, requestParameters, requestParameters.acl, requestParameters.grantList' |
| 202 | 2025-12-10 20:44:53.168 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" \| table _time, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList' |
| 203 | 2025-12-10 20:44:53.149 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" \| table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList' |

| | _time | user | action | search |
|---|---|---|---|---|
| 204 | 2025-12-10 20:44:46.171 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" \| table _time, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList' |
| 205 | 2025-12-10 20:44:30.756 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" \| table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList' |
| 206 | 2025-12-10 20:44:23.235 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" \| table _time, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList' |
| 207 | 2025-12-10 20:43:58.309 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" \| table _time, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList' |
| 208 | 2025-12-10 20:43:53.151 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" \| table _time, eventID, userIdentity.userName, requestParameters.bucketName' |
| 209 | 2025-12-10 20:43:29.104 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" \| table _time, eventID, userIdentity.userName, requestParameters.bucketName' |
| 210 | 2025-12-10 20:41:23.043 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| stats dc(processor) as unique_processors, values(processor) as processor_models by host' |

| | _time | user | action | search |
|---|---|---|---|---|
| 211 | 2025-12-10 20:41:15.408 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| stats dc(processor) as unique_processors, values(processor) as processor_models by host' |
| 212 | 2025-12-10 20:40:53.027 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" \| table host, processor' |
| 213 | 2025-12-10 20:40:27.277 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" \| table host, processor' |
| 214 | 2025-12-10 20:40:23.159 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| stats dc(processor) as unique_processors, values(processor) as processor_models by host' |
| 215 | 2025-12-10 20:40:03.642 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| stats dc(processor) as unique_processors, values(processor) as processor_models by host' |
| 216 | 2025-12-10 20:39:53.037 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| search host="*web*" OR host="*www*" \| rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" \| table host, processor' |
| 217 | 2025-12-10 20:39:23.728 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| search host="*web*" OR host="*www*" \| rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" \| table host, processor' |
| 218 | 2025-12-10 20:38:53.054 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" \| table host, processor' |

| | _time | user | action | search |
|---|---|---|---|---|
| 219 | 2025-12-10 20:38:49.000 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" \| table host, processor' |
| 220 | 2025-12-10 20:38:23.034 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| head 10 \| table host, processor, os, category, type' |
| 221 | 2025-12-10 20:38:22.000 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| head 10 \| table host, processor, os, category, type' |
| 222 | 2025-12-10 20:34:53.344 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, values' |
| 223 | 2025-12-10 20:34:53.265 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, *' |
| 224 | 2025-12-10 20:34:45.194 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, values' |
| 225 | 2025-12-10 20:34:30.798 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, *' |
| 226 | 2025-12-10 20:34:23.299 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, value' |

| | _time | user | action | search |
|---|---|---|---|---|
| 227 | 2025-12-10 20:34:23.227 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, *' |
| 228 | 2025-12-10 20:34:16.430 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, value' |
| 229 | 2025-12-10 20:33:59.411 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, *' |
| 230 | 2025-12-10 20:33:53.083 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count' |
| 231 | 2025-12-10 20:33:27.545 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count' |
| 232 | 2025-12-10 20:30:23.106 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| foreach * [eval <<FIELD>>_exists = if(isnotnull(' |
| 233 | 2025-12-10 20:30:15.508 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| foreach * [eval <<FIELD>>_exists = if(isnotnull(' |
| 234 | 2025-12-10 20:29:53.087 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, item' |

| | _time | user | action | search |
|---|---|---|---|---|
| 235 | 2025-12-10 20:29:23.954 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, item' |
| 236 | 2025-12-10 20:27:23.087 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, "First Example Value"' |
| 237 | 2025-12-10 20:27:05.154 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, "First Example Value"' |
| 238 | 2025-12-10 20:26:23.105 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 239 | 2025-12-10 20:25:53.165 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 240 | 2025-12-10 20:25:51.530 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 241 | 2025-12-10 20:25:46.658 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |

| | _time | user | action | search |
|---|---|---|---|---|
| 242 | 2025-12-10 20:25:23.089 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 243 | 2025-12-10 20:25:09.658 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 244 | 2025-12-10 20:24:53.111 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 245 | 2025-12-10 20:24:53.094 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 246 | 2025-12-10 20:24:53.025 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 247 | 2025-12-10 20:24:52.151 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |

| | _time | user | action | search |
|---|---|---|---|---|
| 248 | 2025-12-10 20:24:44.269 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 249 | 2025-12-10 20:24:26.716 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 250 | 2025-12-10 20:24:23.040 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 251 | 2025-12-10 20:24:17.113 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 252 | 2025-12-10 20:23:23.222 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| stats count by additionalEventData.MFAUsed' |
| 253 | 2025-12-10 20:23:23.159 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where (additionalEventData.MFAUsed) \| stats count by additionalEventData.MFAUsed' |
| 254 | 2025-12-10 20:23:23.144 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(additionalEventData.MFAUsed) \| stats count by additionalEventData.MFAUsed' |

| | _time | user | action | search |
|---|---|---|---|---|
| 255 | 2025-12-10 20:23:19.354 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| stats count by additionalEventData.MFAUsed' |
| 256 | 2025-12-10 20:23:14.156 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where (additionalEventData.MFAUsed) \| stats count by additionalEventData.MFAUsed' |
| 257 | 2025-12-10 20:22:58.995 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(additionalEventData.MFAUsed) \| stats count by additionalEventData.MFAUsed' |
| 258 | 2025-12-10 20:22:53.072 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(additionalEventData.MFAUsed) \| stats count by additionalEventData.MFAUsed' |
| 259 | 2025-12-10 20:22:40.423 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(additionalEventData.MFAUsed) \| stats count by additionalEventData.MFAUsed' |
| 260 | 2025-12-10 20:20:53.195 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| stats count by userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 261 | 2025-12-10 20:20:53.135 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| stats count by userIdentity.sessionContext.attributes.mfaAuthenticated' |

| | _time | user | action | search |
|---|---|---|---|---|
| 262 | 2025-12-10 20:20:44.081 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| stats count by userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 263 | 2025-12-10 20:20:42.215 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| stats count by userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 264 | 2025-12-10 20:20:23.021 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| stats count by userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 265 | 2025-12-10 20:20:15.535 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| stats count by userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 266 | 2025-12-10 20:19:23.033 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 267 | 2025-12-10 20:19:20.392 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) \| table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated' |
| 268 | 2025-12-10 20:18:53.167 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| where isnotnull(additionalEventData.MFAUsed) \| table _time, eventName, additionalEventData.MFAUsed' |

| | _time | user | action | search |
|---|---|---|---|---|
| 269 | 2025-12-10 20:18:38.763 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| where isnotnull(additionalEventData.MFAUsed) \| table _time, eventName, additionalEventData.MFAUsed' |
| 270 | 2025-12-10 20:15:53.040 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(additionalEventData.MFAUsed) \| stats count by additionalEventData.MFAUsed' |
| 271 | 2025-12-10 20:15:40.264 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(additionalEventData.MFAUsed) \| stats count by additionalEventData.MFAUsed' |
| 272 | 2025-12-10 20:14:53.084 | kimjoe | search | 'typeahead prefix="index=botsv3 sourcetype=aws:" max_time="1" count="50" use_cache=1' |
| 273 | 2025-12-10 20:14:53.072 | kimjoe | search | 'typeahead prefix="index=botsv3 sourcetype=aws:cloudtra" max_time="1" count="50" use_cache=1' |
| 274 | 2025-12-10 20:14:53.061 | kimjoe | search | 'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1' |
| 275 | 2025-12-10 20:13:53.137 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| search *MFA* \| table _time, eventName, additionalEventData.MFAUsed' |
| 276 | 2025-12-10 20:13:53.057 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| search *MFA* \| where isnotnull(additionalEventData.MFAUsed) \| table _time, eventName, additionalEventData.MFAUsed' |

| | _time | user | action | search |
|---|---|---|---|---|
| 277 | 2025-12-10 20:13:44.197 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" \| search *MFA* \| table _time, eventName, additionalEventData.MFAUsed' |
| 278 | 2025-12-10 20:13:38.029 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" \| search *MFA* \| where isnotnull(additionalEventData.MFAUsed) \| table _time, eventName, additionalEventData.MFAUsed' |
| 279 | 2025-12-10 20:13:31.901 | kimjoe | search | 'typeahead prefix="index=botsv3 sourcetype=aws:" max_time="1" count="50" use_cache=1' |
| 280 | 2025-12-10 20:13:31.248 | kimjoe | search | 'typeahead prefix="index=botsv3 sourcetype=aws:cloudtra" max_time="1" count="50" use_cache=1' |
| 281 | 2025-12-10 20:13:30.727 | kimjoe | search | 'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1' |
| 282 | 2025-12-10 20:13:23.082 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| search *MFA* \| fieldsummary \| search field="*MFA*"' |
| 283 | 2025-12-10 20:13:16.525 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| search *MFA* \| fieldsummary \| search field="*MFA*"' |
| 284 | 2025-12-10 20:10:53.091 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| search *MFA* \| fieldsummary \| search field="*MFA*"' |

| | _time | user | action | search |
|---|---|---|---|---|
| 285 | 2025-12-10 20:10:26.301 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| search *MFA* \| fieldsummary \| search field="*MFA*"' |
| 286 | 2025-12-10 20:09:23.086 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count' |
| 287 | 2025-12-10 20:08:53.204 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count' |
| 288 | 2025-12-10 20:08:23.096 | kimjoe | search | 'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1' |
| 289 | 2025-12-10 20:08:23.088 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, "First Example Value"' |
| 290 | 2025-12-10 20:07:53.045 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| where isnotnull(additionalEventData.MFAUsed) \| table _time, eventName, additionalEventData.MFAUsed' |
| 291 | 2025-12-10 20:07:52.440 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count, "First Example Value"' |
| 292 | 2025-12-10 20:07:25.476 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| where isnotnull(additionalEventData.MFAUsed) \| table _time, eventName, additionalEventData.MFAUsed' |

| | _time | user | action | search |
|---|---|---|---|---|
| 293 | 2025-12-10 20:07:23.021 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" \| where isnotnull(additionalEventData.MFAUsed) \| table _time, eventName, additionalEventData.MFAUsed' |
| 294 | 2025-12-10 20:07:14.820 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" \| where isnotnull(additionalEventData.MFAUsed) \| table _time, eventName, additionalEventData.MFAUsed' |
| 295 | 2025-12-10 20:07:13.304 | kimjoe | search | 'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1' |
| 296 | 2025-12-10 20:06:53.034 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(additionalEventData.MFAUsed) \| table _time, eventName, additionalEventData.MFAUsed' |
| 297 | 2025-12-10 20:06:49.706 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" \| where isnotnull(additionalEventData.MFAUsed) \| table _time, eventName, additionalEventData.MFAUsed' |
| 298 | 2025-12-10 20:06:23.076 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| search *MFA* \| fieldsummary \| search field="*MFA*" \| table field, count' |
| 299 | 2025-12-10 20:06:16.783 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| search *MFA* \| fieldsummary \| search field="*MFA*" \| table field, count' |
| 300 | 2025-12-10 20:05:23.042 | 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,",")' |