Container Information

The table below notes information about the various containers available within Splunk. A container is both an object in the file system and a logical configuration used to classify contexts. These files are located in the lookups folder under the application location folders. For example, change to directory /opt/splunk/etc/apps/Splunk\_SA\_ExtremeSearch/lookups for some of the context files. The table is as follows:

| **Container Name** | **Context Name** | **App Location** | **Dynamic context search name** |
| --- | --- | --- | --- |
| authentication | failures\_by\_src\_count\_1h | SA-AccessProtection | Access – Authentication Failures By Source – Context Gen |
| failures\_by\_src\_count\_1d | Access – Authentication Failures By Source Per Day – Context Gen |
| count\_1d | Access – Authentication Volume Per Day – Context Gen |
| change\_analysis | change\_count\_by\_user\_by\_change\_type\_id | SA-EndpointProtection | Change – Total Change Count By User By Change Type Per Day – Context Gen |
| email | destinations\_by\_src\_1h | SA-EndpointProtection | Endpoint – Emails By Destination Count – Context Gen |
| recipients\_by\_src\_1h | Endpoint – Emails By Source – Context Gen |
| malware | count\_id | SA-NetworkProtection | Endpoint – Malware Daily Count – Context Gen |
| ids\_attacks | count\_by\_signature\_1h | SA-NetworkProtection | Network – Event Count By Signature Per Hour – Context Gen |
| network\_traffic | count\_by\_dest\_port\_1d | SA-NetworkProtection | Network – Port Activity By Destination Port – Context Gen |
| src\_count\_30m | Network – Traffic Source Count Per 30m – Context Gen |
| count\_30m | Network – Traffic Volume per 30m – Context Gen |
| web | count\_by\_http\_method\_by\_src\_1d | SA-NetworkProtection | Web – Web Event Count By Src By HTTP method per 1d – Context Gen |
| risk | Median\_object\_risk\_by\_object\_type\_1d | SA-ThreatIntelligence | Risk – Median Object Risk Per Day – Context Gen |
| total\_risk\_by\_object\_type\_1d | Risk – Total Risk By Object Type Per Day – Context Gen |
| default | percentile | SA-Utils | ESS – Percentile – Context Gen |
| default | height | Splunk\_SA\_ExtremeSearch | None |
| trendchange | None |
| compability | None |