DCAP CENTRAL

jSONAR Simplifying Security

tech note

jSonar Add-On for **Splunk**

By: Max Douglas and Jonatas Melo

tech note

The jSonar Add-On for Splunk (JAOS) allows Splunk GUI users to search and query data that resides within jSonar platforms. While you can also use Splunk virtual indexes (originally packaged within Hunk) JAOS provides two benefits:

1. It is actively supported by jSonar
2. It integrates with jSonar's Data Level Security (DLS) and Schema Level Security (SLS) layers so that you can enforce granular access control and ensure that different users using the Splunk GUI can only see data subsets that they should have access to.

JAOS is available for Splunk 7.x and 6.6 and is available directly from jSonar or from the Splunkbase.

DEPENDENCIES

- Splunk 7.x, 6.6.x
- jSonar SonarG or DCAP Central or IBM Guardium Big Data Intelligence
- Linux

SETUP

- On the jSonar system:
  - Install Sonar-Splunk service using jSonar-provided rpm
- On Splunk:
  - Install Sonar Add-on for Splunk from the GUI using a jSonar supplied tgz file or by downloading from Splunkbase

CONFIGURATION

- On jSonar:
  - Define which Splunk user accounts may query using the Sonar-Splunk service, e.g. using the shell:

```
use lmrm__sonarg
db.splunk_users.insert({splunk_user: "my_splunk_user", sonar_user: "my_sonar_user"})
```

  - Start Sonar-Splunk service

- On Splunk:
  - Define index in local/indexes.conf or using Settings->Virtual Index in the GUI:
  - A provider, in order to connect to the Sonar-Splunk service
  - Virtual Indexes, in order to enable queries on Sonar collections from Splunk Web. Each Virtual Index enables queries on a single Sonar collection

Below is an example of an entry in the indexes.conf template to help setting the provider and virtual indexes:

```
[provider:sonar-splunk]
vix.family              = jsonar
vix.jsonar.address      = <Sonar-Splunk service network address>
vix.jsonar.port         = <Sonar-Splunk service port>
vix.jsonar.ssl          = <Enabled/Disabled>
# The following 3 fields are required only when SSL is enabled
vix.jsonar.ssl.CA       = <Path to Certificate Authority file>
vix.jsonar.ssl.certificate = <Path to certificate file>
vix.jsonar.ssl.privatekey  = <Path to private key file>
```

```
[<My index>]
vix.provider            = sonar-splunk
vix.jsonar.db           = <My database>
vix.jsonar.collection   = <My collection>
vix.jsonar.field.timestamp = <Date/time field on collection>

[<My other index>]
vix.provider            = sonar-splunk
vix.jsonar.db           = <My other database>
vix.jsonar.collection   = <My other collection>
vix.jsonar.field.timestamp = <Date/time field on other collection>
```

HOW TO SEARCH

Use a standard Search Processing Language (SPL) while filtering by some virtual index(es).

Examples:

- index="My index"
- index="My index" OR index="My other index"
- index="My other index" company=CASE(jSonar)
- index="My index" | spath company | search company=jsonar

ARCHITECTURE/INTERNALS

Figure 1: below shows what happens when a user performes a search using a Splunk virtual index configured to use the JAOS add-on. JAOS is a small python program that runs on the Splunk server and communicates with the Sonar-Splunk service running on the jSonar server.

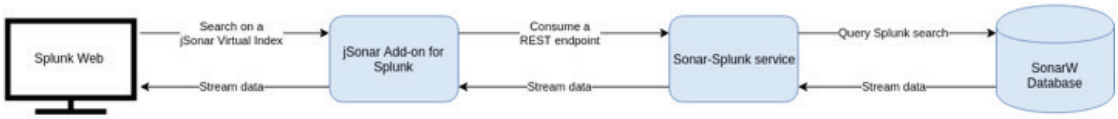

Figure 1: JAOS Architecture

The JAOS python add-on does almost no processing at all; the work in it's entirety is done on the jSonar service within the Sonar-Splunk service. JAOS is only responsible to make a secure REST call to the Sonar-Splunk service. Figure 2 shows the flow within the Sonar-Splunk service.

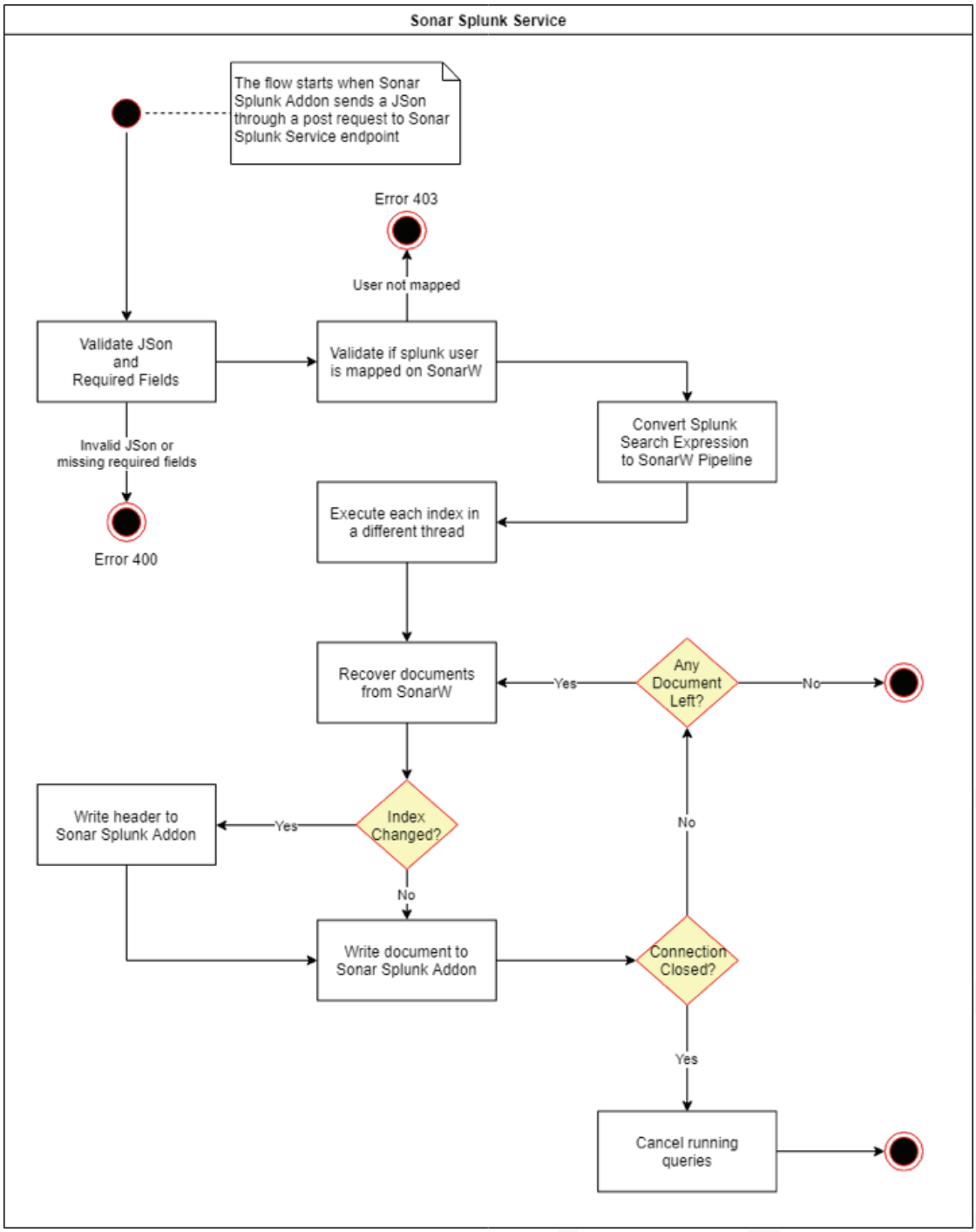

Figure 2: Sonar-Splunk Service Flow

TROUBLESHOOTING

If an error occurred, inspect the current job, open search.log and look for an ERROR message.
A few common error types are:

HTTP ERROR 111:
- Sonar-Splunk service is down

SOLUTION:
- Contact the jSonar admin to start/configure Sonar-Splunk service

HTTP ERROR 403:
- Your Splunk user is not allowed to access Sonar Database

SOLUTION:
- Contact the jSonar admin to enable access to your Splunk user

HTTP ERROR 404:
- Malformed URL to Sonar-Splunk service

SOLUTION:
- Contact the Splunk Admin.

POSSIBLE CAUSES:
- Issue in SSL configuration
- Wrong Endpoint in URL

EXCEPTION: Missing configuration:
Missing field in indexer or provider:
SOLUTION:
- Contact the Splunk Admin to find and configure the missing field

EXCEPTION: Incomplete input from Splunk:
HTTP ERROR 400:
HTTP ERROR 500:
OTHER ERRORS:
SOLUTION:
- Contact jSonar support and provide the ERROR messages found in "search.log" and some explanation on how it happened or how to reproduce it again

tech note