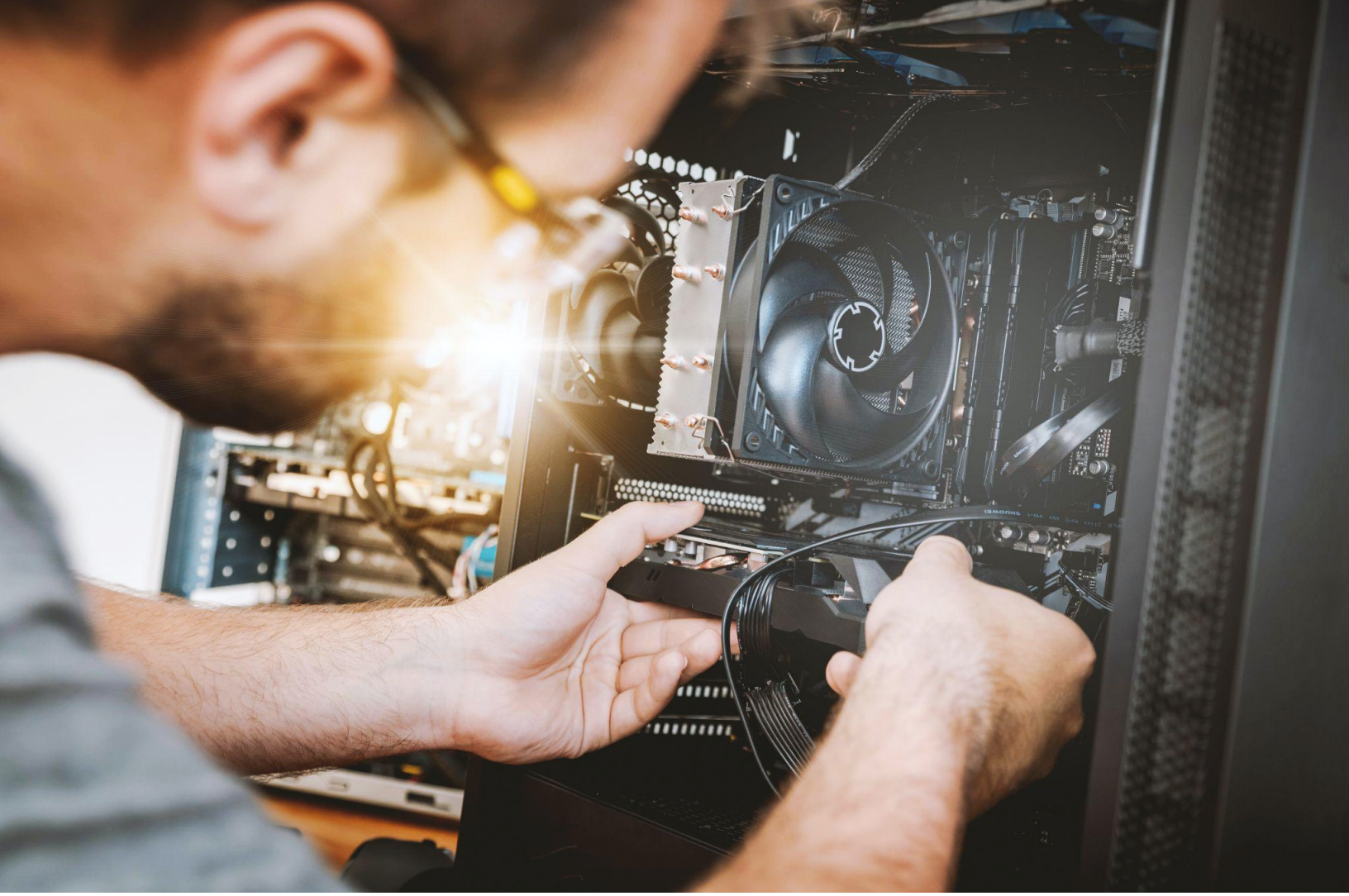

Splunk Enterprise Admin Troubleshooting Use Cases (Part-1)

Soft Mania

Version 1

Date: 2023-June-02

Table of Contents

Data Replication Issues

Issue-1: Indexed data present only on 1 indexer, not replicated across peers/indexers

Root Cause: Index definition was not having the “repFactor” property value defined

Solution: Add “repFactor=auto” under all of the indexes, which requires replication

Step-1: In Cluster Master node, open “**/opt/splunk/etc/master-apps/_cluster/local/indexes.conf**” file & add the property as shown below.

Step-2: Deploy the bundle to Peers using CLI or GUI

Step-3: Check the replication status for each index to make sure changes are reflecting.

```
[web_logs_idx]
repFactor=auto

[db_crashlogs_idx]
repFactor=auto

[ui_debuglogs_idx]
repFactor=auto
```

Issue-2: Data is getting indexed to default index, instead of custom index

Root Cause: Index definition was not present in the Cluster, as it was removed in previous deployment

Solution: Add the index name in the Cluster master & deploy the bundle or Change the index name in inputs.conf for the respective sources.

Data Forwarding Issues

Issue-3: Forwarder is not sending data

Scenario-1: No logs are sent by forwarder, even internal logs

Root Cause: Forwarder is stopped due to source server restart done by the Application team

Solution: Enable boot start for forwarder, this will make sure the Forwarder is also started, after the source server restarted.

In Linux:

```
/opt/splunkforwarder/bin/splunk enable boot-start -user splunk
```

Scenario-2: Forwarder is running & was sending data earlier, all the accesses are there

Root Cause: Forwarder had indexer IP in outputs.conf, the corresponding indexer was down

Solution: Bring up the Indexer (or) Enable Indexer Discovery

In the manager node's server.conf

```
[indexer_discovery]
pass4SymmKey = my_secret
indexerWeightByDiskCapacity = true
```

In each forwarder's outputs.conf:

```
[indexer_discovery:manager1]
pass4SymmKey = my_secret
manager_uri = https://10.152.31.202:8089

[tcpout:group1]
autoLBFrequency = 30
forceTimebasedAutoLB = true
indexerDiscovery = manager1
useACK=true

[tcpout]
defaultGroup = group1
```

Scenario-3: None of the logs are available in Indexer for last few hours, even Indexer's internal logs

Root Cause: The Indexer **Disk size** was full.

Solution: Increase the Indexer Disk/Storage size or remove unwanted data from the Indexer, Like test index logs

Scenario-4: Intermittent data flow - though the source is producing the data live

Root Cause: Sudden burst of incoming data, leads to stall the forwarder queue.

Solution: This is expected in few scenarios where the data sources are too many. One way to reduce this issue is to enable inputs one by one.

Scenario-5: Forwarder error logs say, Indexers are not reachable

Root Cause: Security Groups were not having inbound & outbound rules set for 9997 port.

Solution: Enable 9997 port in the outbound of the Forwarder instance & inbound of Indexer instance.

Scenario-6: Except 1 source other sources are sending logs from same forwarder

Root Cause: Data input was disabled during previous deployment.

Solution: Enable the data input & check if the data starts flowing for the respective source.

Timestamp Issues

Issue-4: Event timestamp & _time field is not matching

Scenario-1: All events are showing same Timestamp (current timestamp)

Root Cause: Event timestamp is not in the standard format.

Solution: Configure your custom timestamp format in the sourcetype, as shown below in props.conf file

```
[yoursourcetype]
TIME_PREFIX = Valid_Until=
TIME_FORMAT = %a %b %d %H:%M:%S %Z%:z %Y
```

Scenario-2: Event timestamp & _time field are having a difference, which is same for all events

Root Cause: Data is coming from a different time zone, but the Forwarder is configured with UTC timezone. So that difference in the timezones reflecting during the search

Solution: **Configure Time zone property "TZ" in the sourcetype,** as shown below in props.conf file

```
[host::nyc*]
TZ = US/Eastern

[host::ind*]
TZ = Asia/Kolkata

[host::canad*]
TZ = America/Glace_Bay
```

Event Truncation Issues

Issue-5: Json Data - Events are truncated, only half of the event is indexed

Root Cause: Event size is too big - more than 10,000 bytes.

Solution: **Configure "TRUNCATE" property in the sourcetype,** as shown below in props.conf

```
[yoursourcetype]
TRUNCATE = 0
```

App Deployment Issues

Issue-6: Dashboard changes are not reflecting in all the Search heads

Root Cause: Previous changes of the dashboard were available in the local folder of all the search heads.

Solution: Remove the local folder copy from all the search heads & do a debug refresh. Then disable edit access for all the users, so that nobody can edit the dashboards.

Issue-7: Latest entries in lookups were not detected by queries

Root Cause: Lookup with the same name present in another app.

Solution: Remove the local folder copy from all the search heads & do a debug refresh. Then disable edit access for all the users, so that nobody can edit the dashboards.

Retention Policy Issues

Issue-8: Indexed data (more than 35 days) is removed even before the retention period (90 days)

Root Cause: The max size of an index **(maxTotalSizeMB) is reached** before the retention period in seconds **(frozenTimePeriodInSecs)**.

Solution: Increase the maxTotalSizeMB to a big number, say 100 GB, based on the size of 90 days data. In indexes.conf.

SAML Issues

Issue-9: Users were on boarded to security groups, but not able to login to Splunk.

Root Cause: The new security group was not configured/mapped with none of the roles in Splunk.

Solution: Configure the security group & map it with the correct security group.

Happy Splunking…!!

*Any help/support required on the Splunk, please contact the **Splunk Mania Team** using any one of the methods mentioned at the end of this document.*

References:

1. Splunk Documentation - https://docs.splunk.com/Documentation/Splunk
2. Cover page photo by JESHOOTS.COM on Unsplash

Contact

WhatsApp: https://wa.me/918317349618

Email: info@softmania.in

LinkedIn: https://www.linkedin.com/company/softmania-tech

Website: Soft Mania