



LanDB use cases

OpenSearch DataStreams, component templates

Marwan Khelif

IT-CS-CT

LanDB use cases

- **Access logs**
 - Ingested through Filebeat/Logstash

915+M docs
1.5Tb
- **Application logs**
 - Ingested through Filebeat/Logstash

900+M docs
1.3Tb
- **Live network scan data**
 - Ingested via Java client (legacy Elasticsearch)

21.5+B docs
1.7Tb
- **Call logs**
 - Ingested through Logstash

350+M docs
100Gb

Migration to DataStreams

- **Why?**
 - Operational burden of managing individual indices with `write alias`
 - Too much information in Kibana (time-based indices)
- **Create new DataStreams**
 - Review index policies from time based (daily/monthly) to size based
- **Minimal code change in the ingestion pipelines**
 - Remove time based indices
 - Change `op_type` to `create`
- **Reindex everything...**

Migration to DataStreams

Data streams Actions Create data stream

Search...

<input type="checkbox"/> Data stream name ↓	Status	Template	Backing indexes count	Total size
<input type="checkbox"/> production-netlive-wifi-user	● Green	netlive-wifi-user	11	711.8gb
<input type="checkbox"/> production-netlive-vrrp	● Green	netlive-vrrp	1	63.1kb
<input type="checkbox"/> production-netlive-topology	● Green	netlive-topology	1	416b
<input type="checkbox"/> production-netlive-system	● Green	netlive-system	1	3gb
<input type="checkbox"/> production-netlive-poe	● Green	netlive-poe	1	106.8kb
<input type="checkbox"/> production-netlive-ospf	● Green	production-netlive-ospf	1	416b
<input type="checkbox"/> production-netlive-mac	● Green	netlive-mac	6	344.9gb
<input type="checkbox"/> production-netlive-iftable	● Green	netlive-iftable	5	235.2gb
<input type="checkbox"/> production-netlive-dhcp-lease	● Green	netlive-dhcp-lease	1	111.9gb
<input type="checkbox"/> production-netlive-bgp	● Green	netlive-bgp	1	416b
<input type="checkbox"/> production-netlive-arp	● Green	netlive-arp	4	219.4gb
<input type="checkbox"/> production-filebeat	● Green	logging-filebeat	17	1.3tb
<input type="checkbox"/> production-access-logs	● Green	logging-access-logs	24	1.5tb

Rows per page: 20 < 1 >

State management policies (2) Delete Edit Create policy

Search

<input type="checkbox"/> Policy ↓	Description	Last updated time
<input type="checkbox"/> production-netlive-rollover	Policy to rollover NetLive datastreams	04/11/24 10:10 am
<input type="checkbox"/> production-logging	Policy for managing Logging infrastructure datastreams (access logs, filebeat)	04/02/24 12:44 pm

Rows per page: 20 < 1 >

Component templates

- **Take profit of the migration to review index templates**
- **Avoid configuration duplication**
- **Templates map to actual code**

Component templates

Templates

Index templates let you initialize new indexes or data streams with predefined mappings and settings. [Learn more](#)

Actions ▾ Create template

<input type="checkbox"/> Template name ▾	Template type	Index patterns	Priority	Associated component templates	Actions
<input type="checkbox"/> netlive-wifi-user-active	Indexes	production-netlive-wifi-user-active	0	4	∞ 🗑️
<input type="checkbox"/> netlive-wifi-user	Data streams	production-netlive-wifi-user	0	4	∞ 🗑️
<input type="checkbox"/> netlive-vrrp	Data streams	production-netlive-vrrp	0	1	∞ 🗑️
<input type="checkbox"/> netlive-topology	Data streams	production-netlive-topology	0	1	∞ 🗑️
<input type="checkbox"/> netlive-system	Data streams	production-netlive-system	0	1	∞ 🗑️
<input type="checkbox"/> netlive-poe	Data streams	production-netlive-poe	0	1	∞ 🗑️
<input type="checkbox"/> netlive-ospf-active	Indexes	production-netlive-ospf-active	0	4	∞ 🗑️
<input type="checkbox"/> netlive-mac-active	Indexes	production-netlive-mac-active	0	5	∞ 🗑️
<input type="checkbox"/> netlive-mac	Data streams	production-netlive-mac	0	5	∞ 🗑️
<input type="checkbox"/> netlive-bgp-active	Indexes	production-netlive-bgp-active	0	4	∞ 🗑️
<input type="checkbox"/> netlive-bgp	Data streams	production-netlive-bgp	0	4	∞ 🗑️
<input type="checkbox"/> netlive-arp-active	Indexes	production-netlive-arp-active	0	5	∞ 🗑️
<input type="checkbox"/> netlive-arp	Data streams	production-netlive-arp	0	5	∞ 🗑️

Rows per page: 20 ▾ < 1 >

Conclusion

- **Migration to DataStreams is easy**
- **Drastic improvement of operations**
- **Thanks to OpenSearch service team!**

Conclusion

- **Migration to DataStreams is easy**
- **Drastic improvement of operations**
- **Thanks to OpenSearch service team!**

Questions?