LanDB use cases

OpenSearch DataStreams, component templates

Marwan Khelif

IT-CS-CT

LanDB use cases

- **Access logs** — 915+M docs, 1.5Tb
  - Ingested through Filebeat/Logstash
- **Application logs** — 900+M docs, 1.3Tb
  - Ingested through Filebeat/Logstash
- **Live network scan data** — 21.5+B docs, 1.7Tb
  - Ingested via Java client (legacy Elasticsearch)
- **Call logs** — 350+M docs, 100Gb
  - Ingested through Logstash

Migration to DataStreams

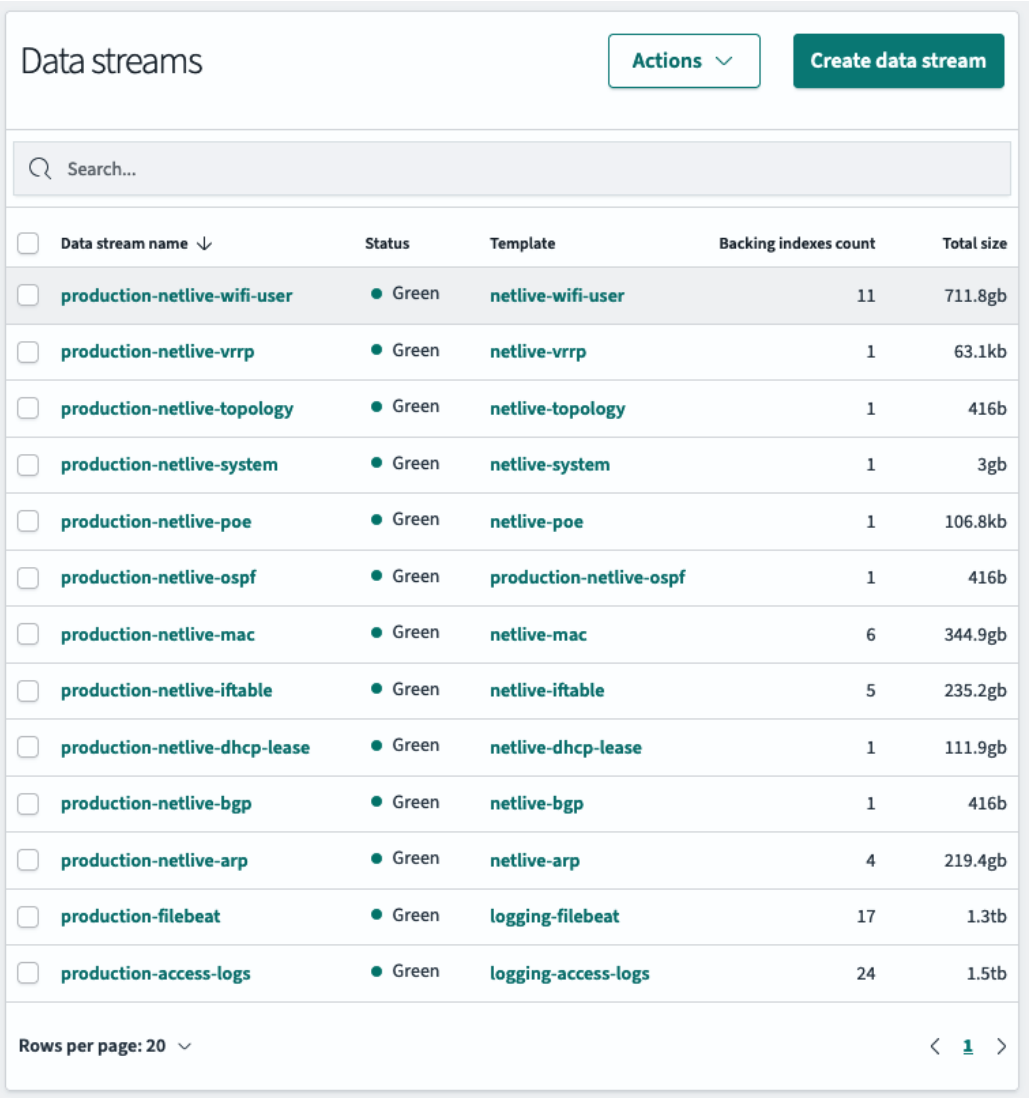
- **Why?**
  - Operational burden of managing individual indices with `write` alias
  - Too much information in Kibana (time-based indices)

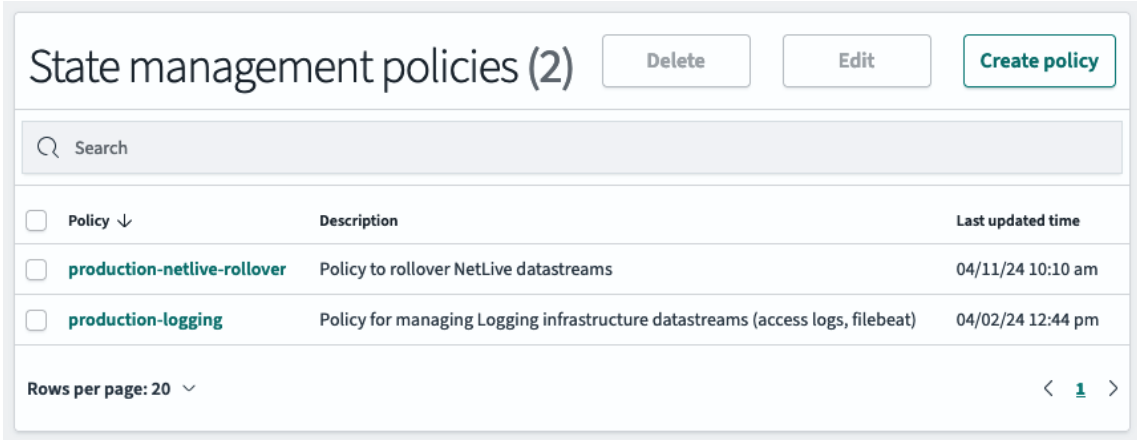
- **Create new DataStreams**
  - Review index policies from time based (daily/monthly) to size based

- **Minimal code change in the ingestion pipelines**
  - Remove time based indices
  - Change `op_type` to `create`

- **Reindex everything…**

Migration to DataStreams

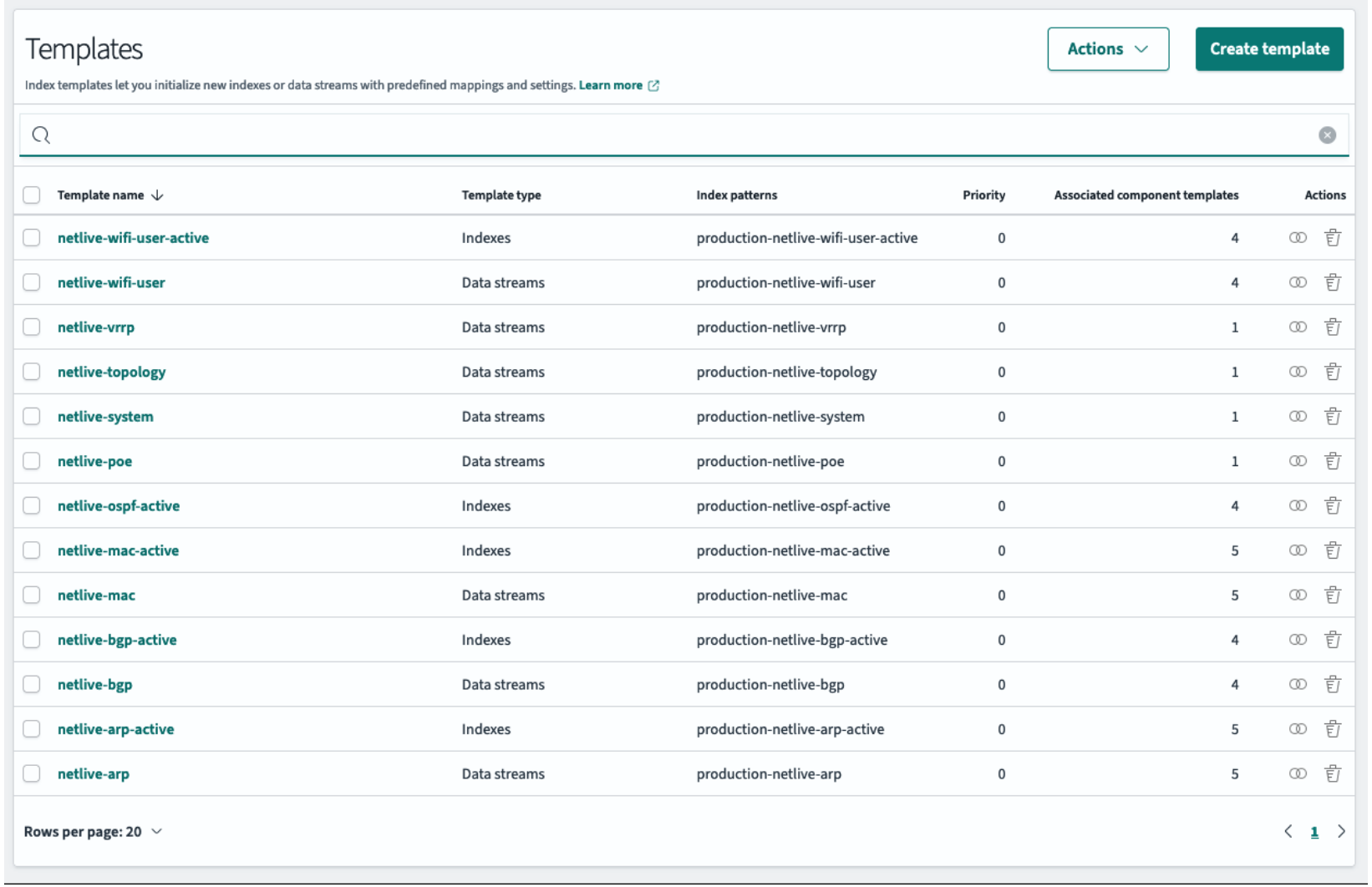




Component templates

- **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

Template name	Template type	Index patterns	Priority	Associated component templates	Actions
netlive-wifi-user-active	Indexes	production-netlive-wifi-user-active	0	4	
netlive-wifi-user	Data streams	production-netlive-wifi-user	0	4	
netlive-vrrp	Data streams	production-netlive-vrrp	0	1	
netlive-topology	Data streams	production-netlive-topology	0	1	
netlive-system	Data streams	production-netlive-system	0	1	
netlive-poe	Data streams	production-netlive-poe	0	1	
netlive-ospf-active	Indexes	production-netlive-ospf-active	0	4	
netlive-mac-active	Indexes	production-netlive-mac-active	0	5	
netlive-mac	Data streams	production-netlive-mac	0	5	
netlive-bgp-active	Indexes	production-netlive-bgp-active	0	4	
netlive-bgp	Data streams	production-netlive-bgp	0	4	
netlive-arp-active	Indexes	production-netlive-arp-active	0	5	
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?