Index Pattern/Policy Guide

Forward: In this guide I will outline how to create index patterns and policies for Logstash and Winlogbeat indices. We decided to create this guide after our initial patterns were disrupted and we realized that reestablishing the patterns were quite difficult. Therefore this is the process we took to get our patterns back.

Daily Logstash Index Pattern:

Step 1 – Stop the Logstash pipeline.

- Run this in the ELK VM: `systemctl stop logstash`

Step 2 – Delete any existing Logstash indices in Kibana.

- This is to remove any overlapping aliases and whatnot.

Step 3 – If not created, create the Index Lifecycle Policy (ILM).

- Our current policy (logstash-policy) specifies rollover and a deletion phase after 25 hours.
- We also already had a legacy index template for the logstash-* which is linked to logstash-policy so nothing more had to be done regarding index templates.

Step 4 – Create the index pattern chain.

- Run this API command in Dev Tools:

```
PUT /%3Clogstash-%7Bnow%2Fd%7D-000001%3E
{
    "aliases": {
        "logstash": {
            "is_write_index": true
         }
    }
}
```

Step 5 – Start the Logstash pipeline again.

- Run this in the ELK VM: `systemctl restart logstash`

For future reference or use, here is the logstash-policy ILM request:

```
PUT _ilm/policy/logstash-policy
{
  "policy": {
```

```
    "phases": {
      "hot": {
        "min_age": "0ms",
        "actions": {
          "rollover": {
            "max_size": "50gb",
            "max_age": "1d"
          }
        }
      },
      "delete": {
        "min_age": "25h",
        "actions": {
          "delete": {
            "delete_searchable_snapshot": true
          }
        }
      }
    }
  }
}
```

Daily Winlogbeat Index Pattern:

Step 1 – Stop the Logstash pipeline.

- Run this in the ELK VM: `systemctl stop logstash`

Step 2 – Delete any existing Winlogbeat indices in Kibana.

- This is to remove any overlapping aliases and whatnot.

Step 3 – If not created, create the Index Lifecycle Policy (ILM).

- Our current policy (winlogbeat) specifies deletion phase after 25 hours.
- We are skipping a rollover because our Winlogbeat indices do not need to rollover since we are generating them daily through our Logstash output, which

automatically designates the newest index as the write index. Adding a rollover could complicate things.

- This is the Winlogbeat output in the /etc/logstash/conf.d/logstash-syslog.conf:

```
if [type]=="winlogbeat" {
                elasticsearch {
                hosts => ["localhost:9200"]
                index => "winlogbeat-%{+yyyy.MM.dd}"
                }
```

What is the reason why we use different methods for Logstash and Winlogbeat indices? I initially tried to create the daily indices through the logstash-syslog.conf output. However only the winlogbeat index had the date. It seems that the winlogbeat logs provide a usable date, while the syslog logs do not. There may be a workaround for getting the date for the syslog but as of now I am just using two different methods.

Step 4 – Create the index template for winlogbeat-*.

- The index template is necessary for the Winlogbeat indices because it automatically assigns the generated indices to the ILM policy. Without the template, this would not be possible.
- It is easiest to create the index template in Kibana in Stack Management > Index Management > Index Templates.
- Just be sure that the index template follows the winlogbeat-* index pattern.
- Also be sure that the Settings and Mappings are correct. I cloned these over from the winlogbeat-7.10.0-* pattern that we already had. If you don't clone these over you will run into problems with the reporting and ElastAlert.

Step 5 – Start the Logstash pipeline again.

- Run this in the ELK VM: `systemctl restart logstash`

For future reference or use, here is the logstash-policy ILM request:

```
PUT _ilm/policy/winlogbeat
{
  "policy": {
    "phases": {
      "hot": {
        "min_age": "0ms",
        "actions": {}
      },
      "delete": {
        "min_age": "25h",
        "actions": {
          "delete": {
            "delete_searchable_snapshot": true
```

```
            }
          }
        }
      }
    }
  }
```