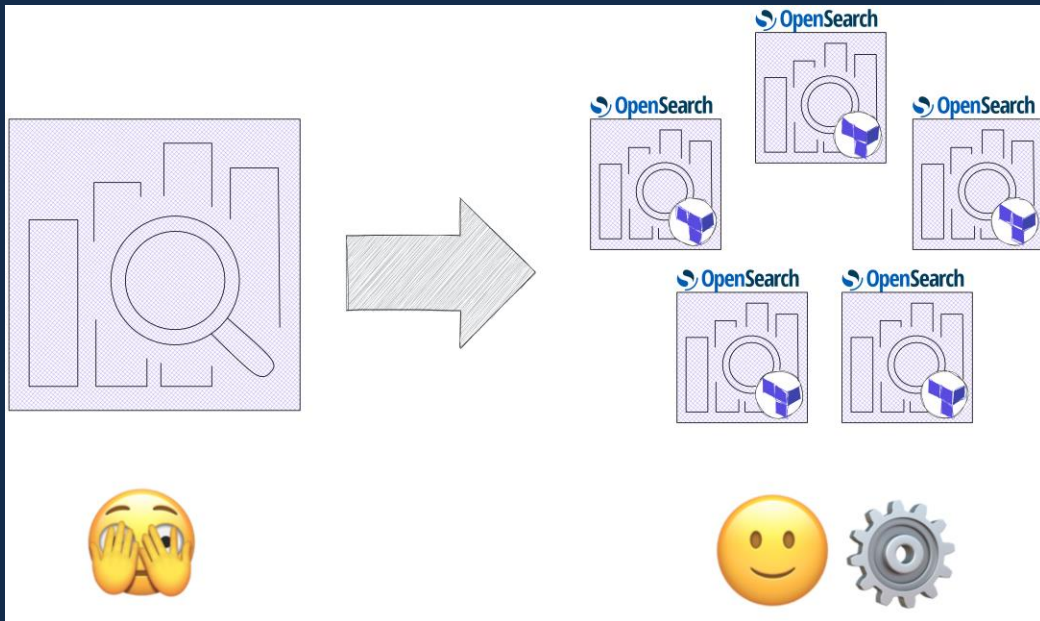# Delicacies of Observability:
AWS OpenSearch Cluster from 'rare' to 'well-done'

Eugene Tolbakov

WHAT'S ON MENU

Starter:
Introduction

Main Course:
From uber – cluster to 5 log-specific clusters
IaC approach & overview of OpenSearch settings

Dessert:
Key learnings, insights & tips

DISCLAIMER

ABOUT ME

Eugene Tolbakov
Platform Engineer within the Observability
Squad at Chase UK

```
1  GET london-o11y-engineering-meetup-speakers/_doc/4
2
3
```

```json
1  {
2    "_index": "london-o11y-engineering-meetup-speakers",
3    "_id": "4",
4    "_version": 1,
5    "_seq_no": 0,
6    "_primary_term": 1,
7    "found": true,
8    "_source": {
9      "name": "Eugene Tolbakov",
10     "organization": "Chase UK",
11     "position": "Platform Engineer",
12     "skills": [
13       "JVM-based languages (Clojure, Kotlin, Java)",
14       "Python",
15       "Rust"
16     ],
17     "interests": [
18       "Observability",
19       "Distributed Systems",
20       "Databases"
21     ],
22     "contacts": {
23       "LinkedIn": "Eugene Tolbakov",
24       "Twitter/X": "@evtolbakov",
25       "Telegram": "@evtolbakov"
26     }
27   }
28 }
```

Nutmeg. a J.P.Morgan company   CHASE

CHASE | AWARD-WINNING BANKING
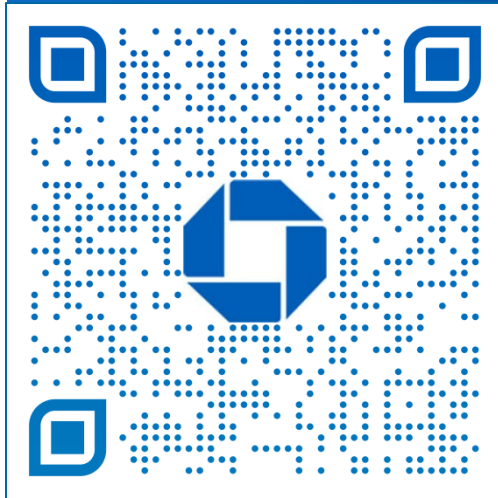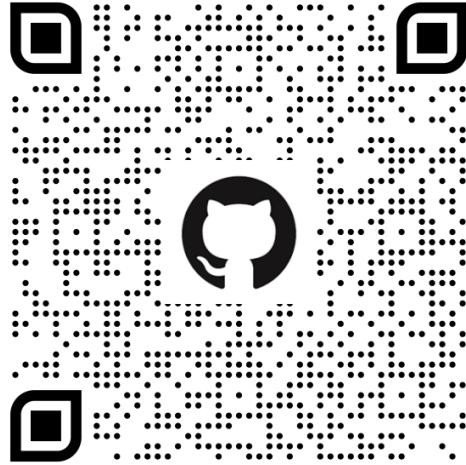
```
1  GET  british_banks/_doc/1
2
3
```

```json
1  {
2    "_index": "british_banks",
3    "_id": "1",
4    "_version": 1,
5    "_seq_no": 0,
6    "_primary_term": 1,
7    "found": true,
8    "_source": {
9      "name": "Chase UK",
10     "launch_date": "09/2021",
11     "number_of_customers": "2M",
12     "balance": "£20B",
13     "products": [
14       "current account",
15       "savings account",
16       "digital wealth & investments"
17     ],
18     "awards": {
19       "2023": [
20         "Best savings provider",
21         "Best current account provider"
22       ],
23       "2024": [
24         "Best British Bank",
25         "Best Current Account Provider"
26       ]
27     },
28     "ratings": {
29       "Trustpilot": 4.1,
30       "Google Play": 4.8,
31       "iOS App Store": 4.9
32     }
33   }
34 }
```

Nutmeg. a J.P.Morgan company   CHASE

TERRAFORM 101

- ***What?***
  🛠️ to define(declare) what your infrastructure looks like,
  instead of manually setting everything up (a.k.a. IaC)

- ***Why?***
  consistency, repeatability, collaboration

- ***How?***
  configuration files(HCL) that describes your infrastructure (VMs, storage, networking).
  Terraform figures out how to make those changes.

  - "**modules**" - reuse/avoid repetitive declarations
  - "**providers**" - interact with various APIs
    - ☁️ (AWS, etc)
    - ▯ (Mysql, Postrges)
    - 🤓 Spotify / Dominos
    - your_next_best_tool
    - **Elasticsearch** | **OpenSearch**

Nutmeg.
a J.P.Morgan company

CHASE ○
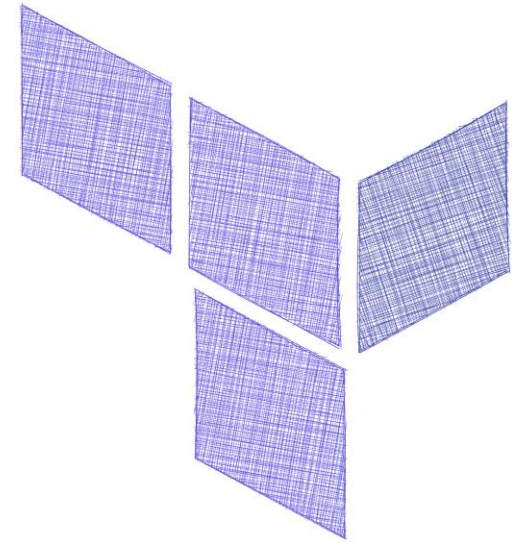
TERRAFORM 101 | AWS_OPENSEARCH_DOMAIN

```
1   locals {
2     cluster_params = {
3       cluster-x = {
4         engine_version       = "OpenSearch_2.13"
5         master_node_type     = "m6g.large.search"
6         master_node_number   = 3
7         data_node_type       = "r6g.2xlarge.search"
8         data_node_number     = 3
9       },
10      cluster-y = {
11
12      },
13      cluster-z = {
14
15      }
16    }
17  }
```
11.1

```
├── locals.tf
├── main.tf
└── module
    ├── iam.tf
    ├── logs.tf
    └── opensearch.tf
```
11.3

Terraform | Registry   Search all resources   Browse ∨   Publish ∨   Sign-in

Providers / hashicorp / aws / Version 5.50.0 ∨ | Latest Version |

aws 🔒   Overview

AWS DOCUMENTATION   **Resource: aws_opensearch_domain**

🔍 opensearch   Manages an Amazon OpenSearch Domain.

24 matching results   11.4

```
1   module "opensearch" {
2     source  = "./module/"
3     for_each             = local.cluster_params
4
5     cluster_name         = each.key
6     engine_version       = each.value["engine_version"]
7     master_node_type     = each.value["master_node_type"]
8     master_node_number   = each.value["master_node_number"]
9     data_node_type       = each.value["data_node_type"]
10    data_node_number     = each.value["data_node_number"]
11  }
```
11.2

11

Nutmeg.
a J.P.Morgan company   CHASE
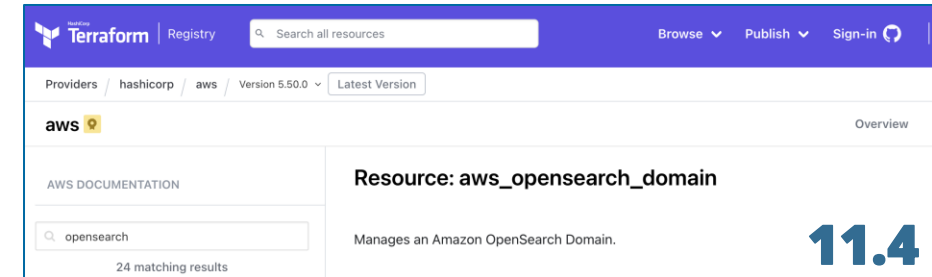
SMALLER CLUSTERS

- ✓ More stability
- ✓ Smaller cluster state
- ✓ Smaller blast radius
  - ✓ Migrations 😰 (2.13 improved 👏, Workaround)
  - ✓ Migrations are not "backward" 🙀

```
← → C ⌂    🌐 https://your-opensearch-domain/_dashboards/app/home#/

OpenSearch Dashboards server is not ready yet
```

14.1

```
resource "aws_opensearch_domain_saml_options" "example" {
  ......

  lifecycle {
    prevent_destroy = true
}
```
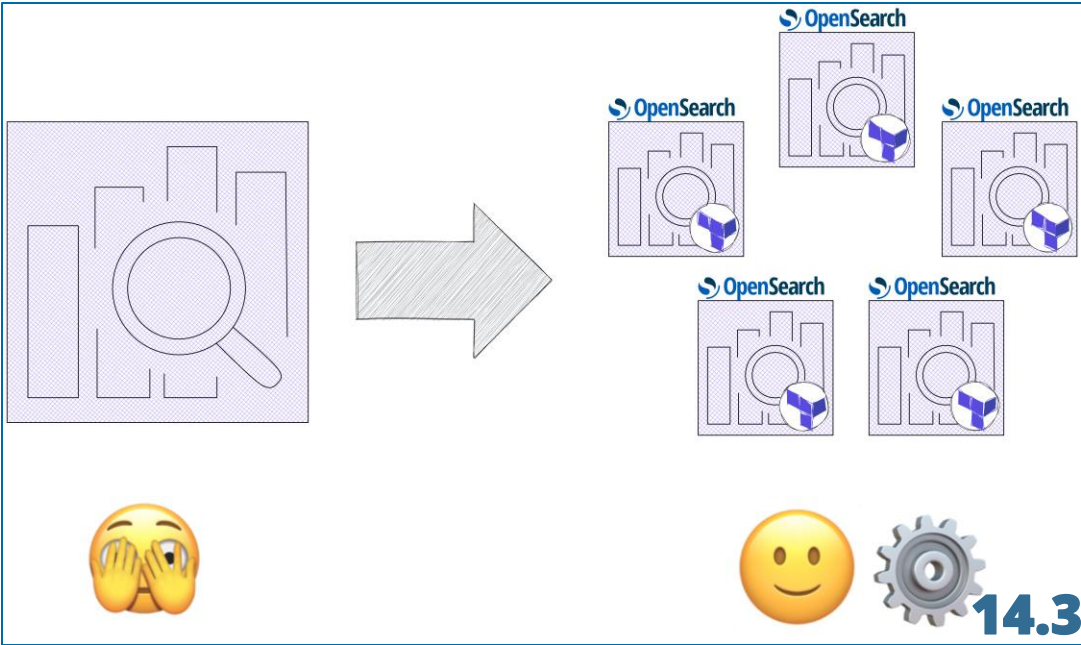
```
resource "aws_opensearch_domain_policy" "example" {
  ......

  lifecycle {
    prevent_destroy = true
}
```

```
resource "aws_opensearch_domain" "example" {
  ......

  lifecycle {
    prevent_destroy = true
}
```

14.2

14

14.3

OpenSearch cluster		
Cluster configuration	Data (_cat/allocation?v)	Environment
3 master nodes (r6g.xlarge.search) 24 data nodes (r6g.4xlarge.search)	120TB 70B docs 14k shards 300 indicies / 10 index templates 2.3 - 2.4 billion entries/day	Managed cluster Multi-AZ Engine version 2.11 Indexing Data Rate : 4k/12k (avg/peak) docs/second Average Search Latency: 10ms/500ms (avg/peak) **14.4**

Nutmeg.
a J.P.Morgan company

CHASE 🔷

TERRAFORM 101 | OPENSEARCH RESOURCE

- ✓ 2 providers
- ✓ .tftpl files
- ✓ terraform plan

```
1  - _id: "index-pattern:my-logs"
2    _source:
3      index-pattern:
4        timeFieldName: "@timestamp"
5        title: "${pass_from_terraform}my-logs*"
6        fieldFormatMap: "{\"payload_size\":{\"id\":\"bytes\"}}"
7      references: []
8      type: "index-pattern"
```
19.1

```
1   module "opensearch_resources" {
2     source = "./module"
3
4     index_pattern_files   = fileset(path.module, "../cluster-x-config/index-patterns/*.yml.tftpl")
5     index_template_files  = fileset(path.module, "../cluster-x-config/index-templates/*.yml.tftpl")
6     ism_policy_files      = fileset(path.module, "../cluster-x-config/ism-policies/*.yml.tftpl")
7     ingest_pipeline_files = fileset(path.module, "../cluster-x-config/ingest-pipelines/*.yml.tftpl")
8     role_files            = fileset(path.module, "../cluster-x-config/roles/*.yml.tftpl")
9     role_mapping_files    = fileset(path.module, "../cluster-x-config/role-mappings/*.yml.tftpl")
10  }
```
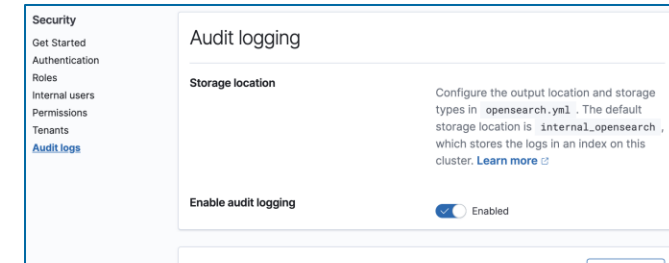**19.2**

```
1   locals {
2     index_templates = merge({
3       for filename in var.index_template_files :
4       replace(basename(filename), "/\\.yaml.tftpl$/", "")
5         => yamldecode(file(filename))
6     }, var.index_templates)
```
19.3

```
├── cluster-x-config
│   ├── index-patterns
│   │   └── example-pattern.yml.tftpl
│   ├── index-templates
│   │   └── example-template.yml.tftpl
│   ├── ingest-pipelines
│   │   └── example-pipeline.yaml.tftpl
│   ├── ism-policies
│   │   └── example-policy.yml.tftpl
│   ├── role-mappings
│   │   └── all_access.yml.tftpl
│   └── roles
│       └── write_access.yml.tftpl
├── cluster-y-config
├── cluster-z-config
├── main.tf
└── module
    ├── audit_config.tf
    ├── index_patterns.tf
    ├── index_templates.tf
    ├── ingest_pipeline.tf
    ├── ism_policy.tf
    ├── locals.tf
    ├── provider.tf
    ├── role_mappings.tf
    ├── roles.tf
    ├── variables.tf
    └── versions.tf
```
19.4

Security
Get Started
Authentication
Roles
Internal users
Permissions
Tenants
Audit logs

Audit logging

Storage location
Configure the output location and storage types in `opensearch.yml`. The default storage location is `internal_opensearch`, which stores the logs in an index on this cluster. Learn more

Enable audit logging   🔵 Enabled

```
resource "elasticsearch_opensearch_audit_config" "test" {
    provider = elasticsearch.audit_config
    enabled = true

  audit {
    enable_rest          = true
    disabled_rest_categories = ["GRANTED_PRIVILEGES", "AUTHENTICATED"]
```
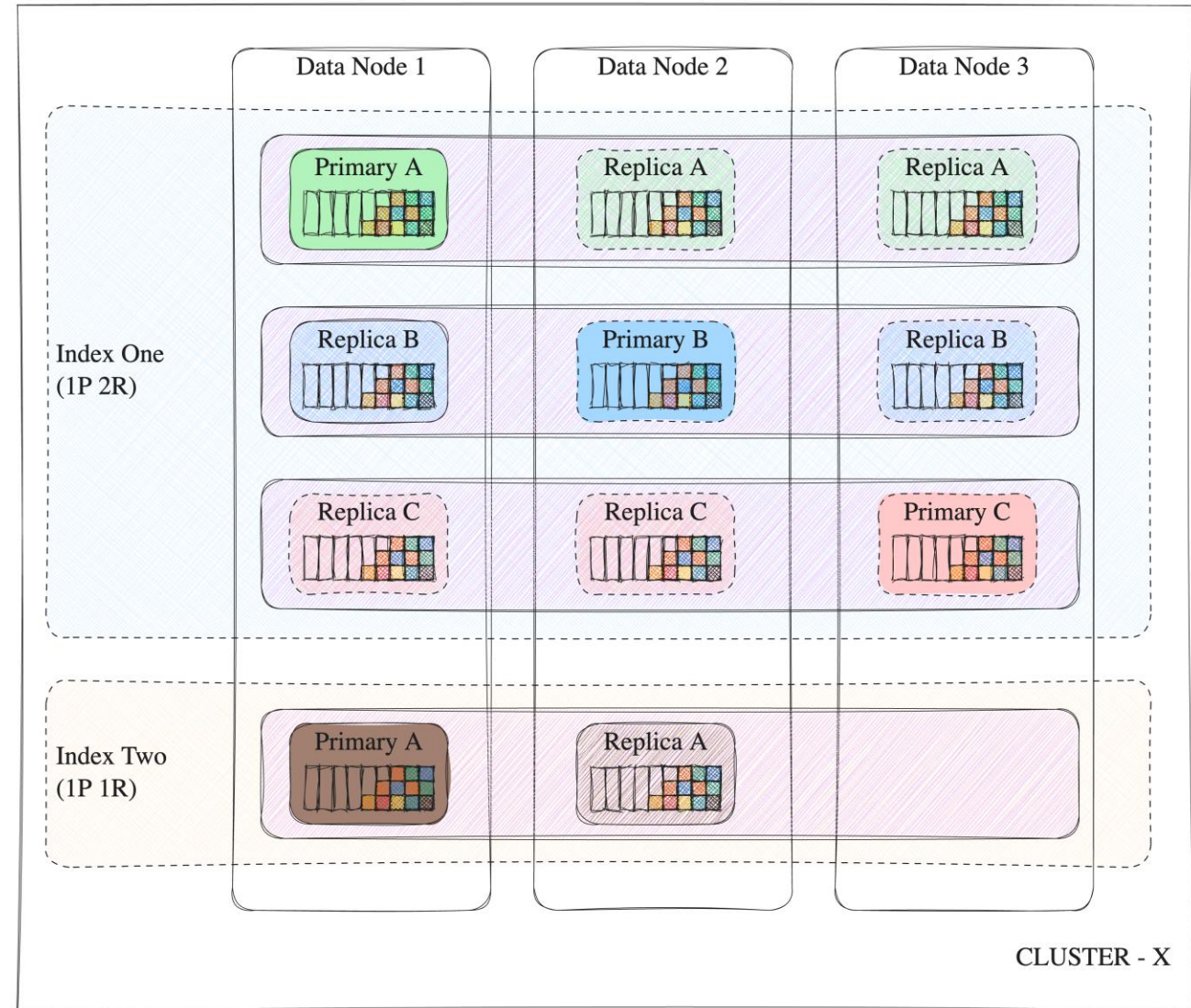**19.5**

```
1   provider "elasticsearch" {
2     url                 = local.cluster_endpoint
3     kibana_url          = "${local.cluster_endpoint}/_dashboards"
4     # ...
5     elasticsearch_version = "OpenSearch_2.11"
6   }
7
8   provider "elasticsearch" {
9     alias               = "audit_config"
10    url                 = local.cluster_endpoint
11    kibana_url          = "${local.cluster_endpoint}/_dashboards"
12    # ...
13    elasticsearch_version = "8.5"
14  }
```
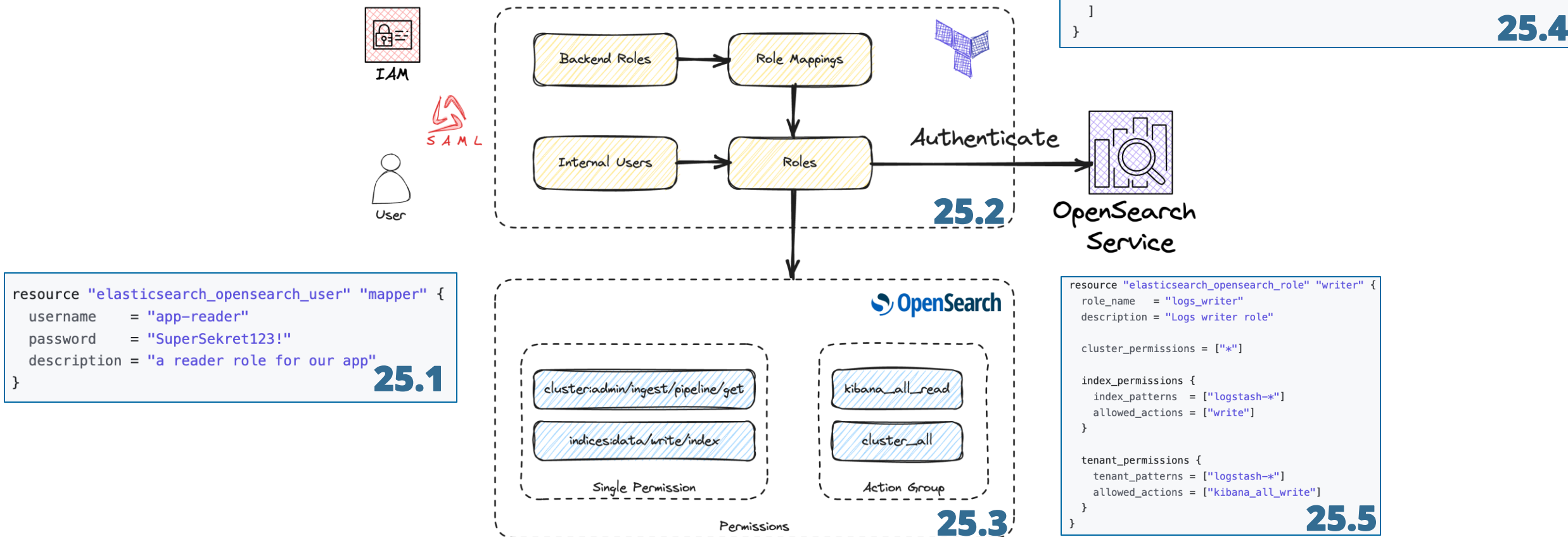**19.6**

OPENSEARCH 101

- ✓ Apache 2.0;
- ✓ 2021 Elasticsearch 🍴 (version 7.10.2)
- ✓ Workloads
  - ✓ search engine
  - ✓ logging

- ✓ Cluster
- ✓ Data node
- ✓ Index
- ✓ Shard
- ✓ Segment

- ✓ Index templates
- ✓ Index patterns
- ✓ ILM
- ✓ Roles
- ✓ Role-bindings

ROLES / ROLE-MAPPINGS


```
# Create a role mapping
resource "elasticsearch_opensearch_roles_mapping" "mapper" {
  role_name     = "logs_writer"
  description   = "Mapping AWS IAM roles to ES role"
  backend_roles = [
    "arn:aws:iam::123456789012:role/lambda-call-elasticsearch",
    "arn:aws:iam::123456789012:role/run-containers",
  ]
}
```
25.4

```
resource "elasticsearch_opensearch_user" "mapper" {
  username    = "app-reader"
  password    = "SuperSekret123!"
  description = "a reader role for our app"
}
```
25.1

25.2

25.3

```
resource "elasticsearch_opensearch_role" "writer" {
  role_name   = "logs_writer"
  description = "Logs writer role"

  cluster_permissions = ["*"]

  index_permissions {
    index_patterns  = ["logstash-*"]
    allowed_actions = ["write"]
  }

  tenant_permissions {
    tenant_patterns = ["logstash-*"]
    allowed_actions = ["kibana_all_write"]
  }
}
```
25.5

25

ROLES / ROLE-MAPPINGS Cont'd

✓ field-level security 🤓
✓ advanced settings granularity 😔
✓ 'security_manager' in terraform 😵‍💫
✓ debugging 🔍

Roles

Roles (1)

Roles are the core way of controlling access to your cluster. Roles contain any combination of cluster-wide permission, index-specific permissions, document- and field-level security, and tenants. Then you map users to these roles so that users gain those permissions.
Learn more ⧉

Actions ⌄   Create role

🔍 security ✕   Cluster permissions ⌄   Index permissions ⌄   Internal users ⌄   Backend roles ⌄   Tenants ⌄   Customization ⌄

☐	Role	Cluster permissions	Index permissions	Internal users	Backend roles	Tenants	Customization
☐	security_manager	—	—	—	arn:aws:iam::123456789012:your_role arn:aws:iam::123456789012:your_another_role ...	—	🔒 Reserved

Rows per page: 10 ⌄

26.1 ›

```
{
    "ok": false,
    "error": "[security_exception] no permissions for [indices:admin/delete] and User [name=opendistro_security_anonymous, backend_roles=[opendistro_security_anonymous_backendrole], requestedTenant=null]",
    "body": {
        "error": {
            "root_cause": [
                {
                    "type": "security_exception",
                    "reason": "no permissions for [indices:admin/delete] and User [name=opendistro_security_anonymous, backend_roles=[opendistro_security_anonymous_backendrole], requestedTenant=null]"
                }
            ],
            "type": "security_exception",
            "reason": "no permissions for [indices:admin/delete] and User [name=opendistro_security_anonymous, backend_roles=[opendistro_security_anonymous_backendrole], requestedTenant=null]"
        },
        "status": 403
    }
}
```

26.2

Nutmeg. a J.P.Morgan company   CHASE 🔷

INDEX TEMPLATES

- ### *What?*
  Blueprints for creating with predefined settings/mappings

- ### *How?*
  Index matches a template

- ### *Why?*
  Homogenous setting

composable / component

```
1   PUT _index_template/my_logs_template
2   {
3 >   "index_patterns": [
5     ],
6     "template": {
7 >     "aliases": {…
9       },
10 >    "settings": {…
13      },
14      "mappings": {
15 >      "properties": {…
23        }
24      }
25    }
26  }
```

```
3     "index_patterns": [
4       "my_logs-*"
5     ],
```

```
7     "aliases": {
8         "my_logs": {}
9     },
```

```
10    "settings": {
11        "number_of_shards": 2,
12        "number_of_replicas": 1
13    },
```

29.2

```
14    "mappings": {
15        "properties": {
16            "timestamp": {
17                "type": "date",
18                "format": "epoch_millis"
19            },
20            "value": {
21                "type": "double"
22            }
23        }
24    }
```

```
resource "elasticsearch_index_template" "template_1" {
  name = "template_1"
  body = <<EOF
{
  "template": "te*",
  "settings": {
    "number_of_shards": 1
  },
```
29.1

- ✓ link indices with UI

- ✓ reference to multiple indices

- ✓ refresh interval
- ✓ pipelines
- ✓ number of shards

- ✓ auto—generated IDs
- ✓ @timestamp and 'date_nanos'
- ✓ 'dynamic: false | true | runtime'
- ✓ 'type: flat_object '
- ✓ keyword 'doc_values'
- ✓ 'type: match_only_text' (stacktrace)
- ✓ '_size: enable=true' / painless

Nutmeg.   CHASE ◆

a J.P.Morgan company

INDEX PATTERNS

- ✓ '.kibana' index alias
- ✓ refresh
- ✓ Type: number / Format: Bytes

```
resource "elasticsearch_kibana_object" "index_pattern" {
  index = ".kibana"
  body = <<EOF
[
  {
```

31.3

Name	Type	Format	Searchable	Aggregatable
payload_size	number	Bytes	●	●

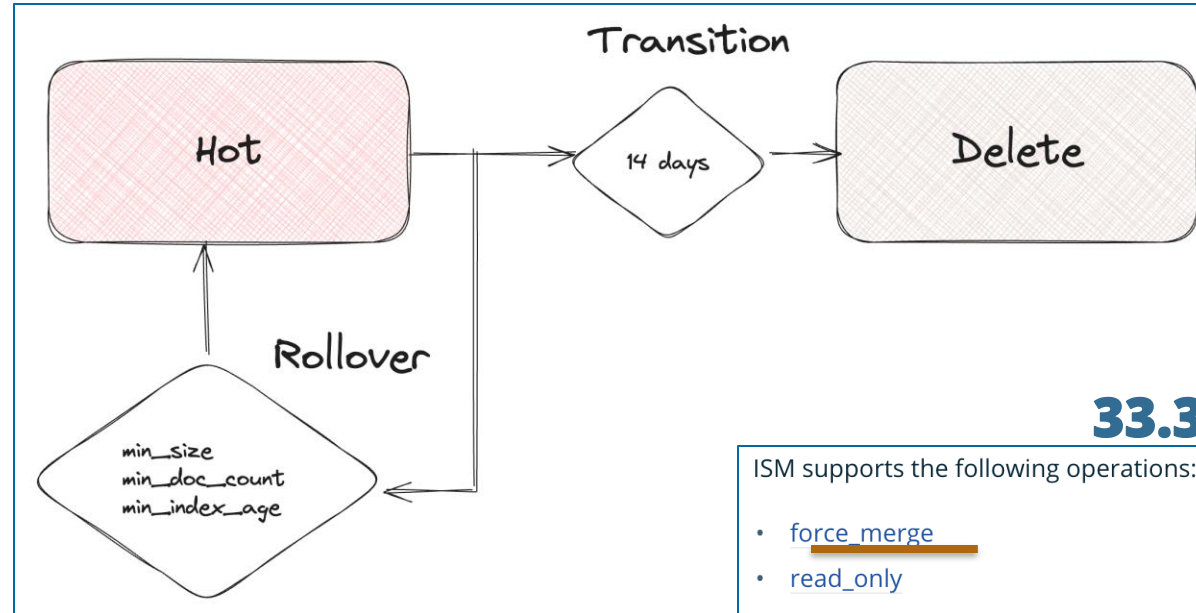**31.1**

```
1   ⌄ {
2       "_id": "index-pattern:my-logs",
3   ⌄    "_source": {
4   ⌄      "index-pattern": {
5           "timeFieldName": "@timestamp",
6           "title": "my-logs*",
7           "fieldFormatMap": "{\"payload_size\":{\"id\":\"bytes\"}}"
8         },
9         "references": [],
10        "type": "index-pattern"
11      }
12  }
```

31.2

31

Nutmeg.
a J.P.Morgan company   CHASE

ISM / ILM POLICIES

✓ Hot – fastest/costly (im4g/MRC-6g instances)
✓ UltraWarm (HDD)
✓ Cold (S3)
✓ Mixed Hot/Warm (OR1 instances*)

✓ Look after the rollover

33.3

```
PUT /my-index1
{
  "settings": {
    "index": {
      "replication.type": "SEGMENT"
    }
  }
}
```
33.1

Parameter
min_size
min_primary_shard_size
min_doc_count
min_index_age

33.2

ISM supports the following operations:

- force_merge
- read_only
- read_write
- replica_count
- shrink
- close
- open
- delete
- rollover
- notification
- snapshot
- index_priority
- allocation
- rollup

33.4

33

```json
{
  "default_state": "hot",
  "states": [
    {
      "name": "hot",
      "actions": [
        {
          "retry": {"count": 3...},
          "rollover": {
            "min_size": "100gb",
            "min_doc_count": 100000000,
            "min_index_age": "10d"
          }
        }
      ],
      "transitions": [
        {
          "state_name": "delete",
          "conditions": {
            "min_index_age": "14d"
          }
        }
      ]
    },
    {
      "name": "delete",
      "actions": [
        {
          "retry": {"count": 3...},
          "delete": {}
        }
      ],
      "transitions": []
    }
  ],
  "ism_template": [
    {
      "index_patterns": ["my-logs*"],
      "priority": 100
    }
  ]
}
```

33.5

INGEST PIPELINES

✓ Enrichment 💰

```
# Create a simple ingest pipeline
resource "elasticsearch_ingest_pipeline" "test" {
  name = "terraform-test"
  body = <<EOF
{

  "description" : "describe pipeline",           35.1
```

```
2  PUT _ingest/pipeline/my-pipeline
3 ▾ {
4 ▾   "processors": [
5 ▾     {
6 ▾       "set": {
7           "description": "Index the ingest timestamp as 'log_ingested'",
8           "field": "log_ingested",
9           "value": "{{{_ingest.timestamp}}}"
10 ▴      }
11 ▴    }
12 ▴  ]
13 ▴ }                                                          35.2
```

```
2  PUT _ingest/pipeline/my-second-pipeline
3 ▾ {
4     "description": "Set a human-understandable names for mobile device ",
5 ▾   "processors": [
6 ▾     {
7 ▾       "script": {
8           "lang": "painless",
9 ▾         "params" : {
10              "MAR-LX1A" : "HUAWEI P30 lite",
11              "SM-A137F" : "Galaxy A13"
12 ▴        },
13          "source": "ctx['mobile_device_name'] = params[ctx['mobile_device_code']]"
14 ▴      }
15 ▴    }
16 ▴  ]
17 ▴ }                                                          35.3
```

35

DESSERT | CHECKLIST | BEST PRACTICES

Managed clusters - best-practices mini-checklist
- Deploy, monitor, adjust
- use _bulk API
- use 3 Dedicated cluster manager nodes
- select 3 zones with Multi-AZ
- set a template and use 2 replicas

- Free storage `>= 25%`
- Shards:vCPU = `1:1.5`
- Shard size = 50GB(logs) / 30 for search
- Max shards per node = 25 * JVM heap size
- Total shard count < 30K

Nutmeg.
a J.P.Morgan company

CHASE

THANK YOU