Release H: Keycloak Quarkus distribution

Introduction

In Keycloak 17 and above the default distribution is now powered by Quarkus, while the legacy WildFly powered distribution will be phased out after June 2022.

The default path no longer contains the "auth" tag.

HTTPS

By default keycloak runs on https, you need to setup a keystore and and truststore for your certificates.

You can also enable http.

You can then start keycloak with the following arguements:

Keycloak args

```
args: [
        'start',
        '--https-key-store-file=/etc/x509/https/server.keystore',
        '--https-key-store-password=changeit',
        '--https-key-store-type=PKCS12',
        '--https-trust-store-file=/etc/x509/https/server.truststore',
        '--https-trust-store-password=changeit',
        '--https-trust-store-type=PKCS12',
        '--https-client-auth=request',
        '--http-enabled=true'
    ]
```

Client Authenticator

Keycloak clients support 4 authenticator types:

1. Client Secret
2. x509 certificate
3. JWT signed with certificate
4. JWT signed with secret

Client Secret

This is the default option, a secret is generated automatically when the client is created.

x509 Certificate

This requires setting up an authentication flow for the client and then setting the "Direct Grant Flow" to this new flow in the "Authentication flow overrides" section of the client configuration.
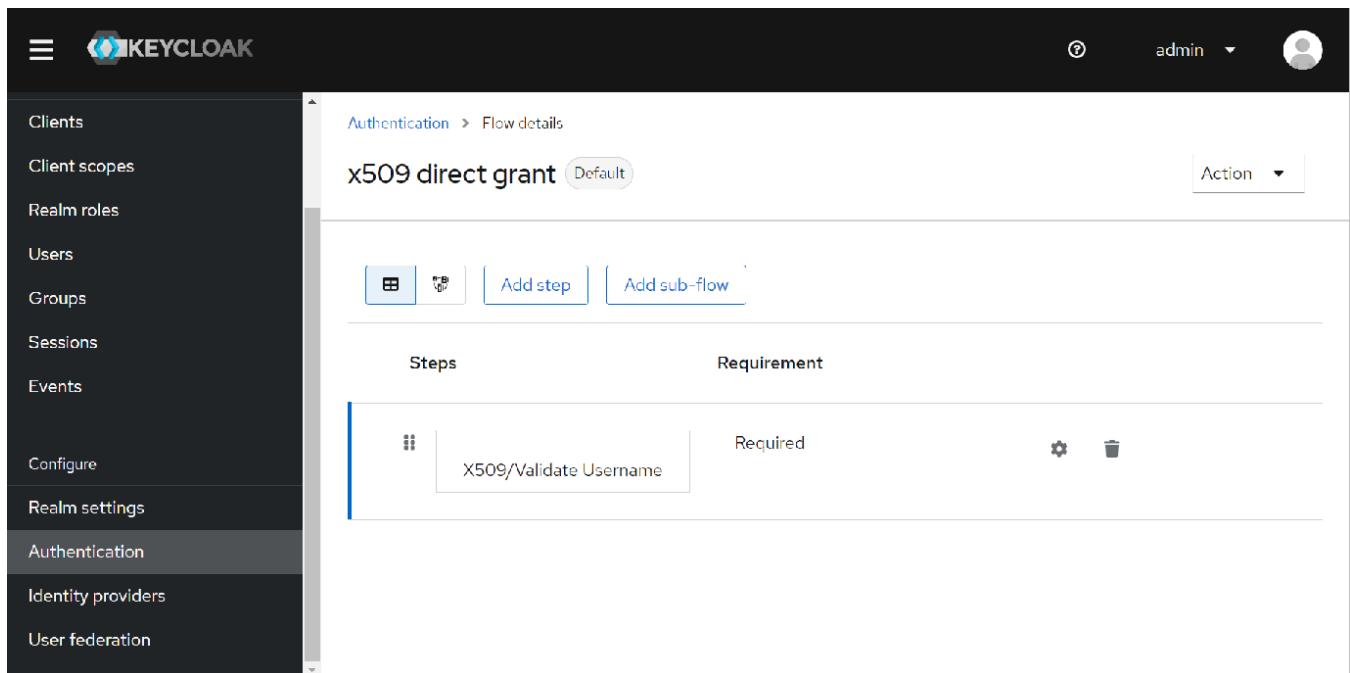
You can also enabled regexp pattern matching in the credentials section of the client if required.

When a token request is made with the x509 certificate, a part of the certificate like the subject's email is compared with the email from one of the users in the realm, if there is a match a token is issued.

See "Configuring X.509 client certificate authentication" in the keycloak documentation for more information.

JWT signed with certificate

A custom JWT is created and signed with a certificate.

The certificate is then compared with a JWK URI or a static JWKS (This can be created using the certificate and pubic key then imported into to keycloak).

If the signatures match, a token is issued.

JWT signed with secret

Similar to above except for JWT is signed with the client secret instead of a certificate.

Metrics

By including the following environment variable metrics will be available on the /metics endpoint

Keycloak ENV

```
    - name: KC_METRICS_ENABLED
      value: "true"
```

Prometheus

The metrics can then be scraped by Prometheus, just add an entry for it in the scrape_configs section:

Prometheus scrape_configs

```
scrape_configs:
- job_name: keycloak
  scrape_interval: 10s
  metrics_path: /metrics
  static_configs:
  - targets:
    - keycloak.default:8080
```

You can query all the keycloak metrics using: {instance="keycloak.default:8080", job="keycloak"}

Grafana

The metrics can then be viewed in Grafana:
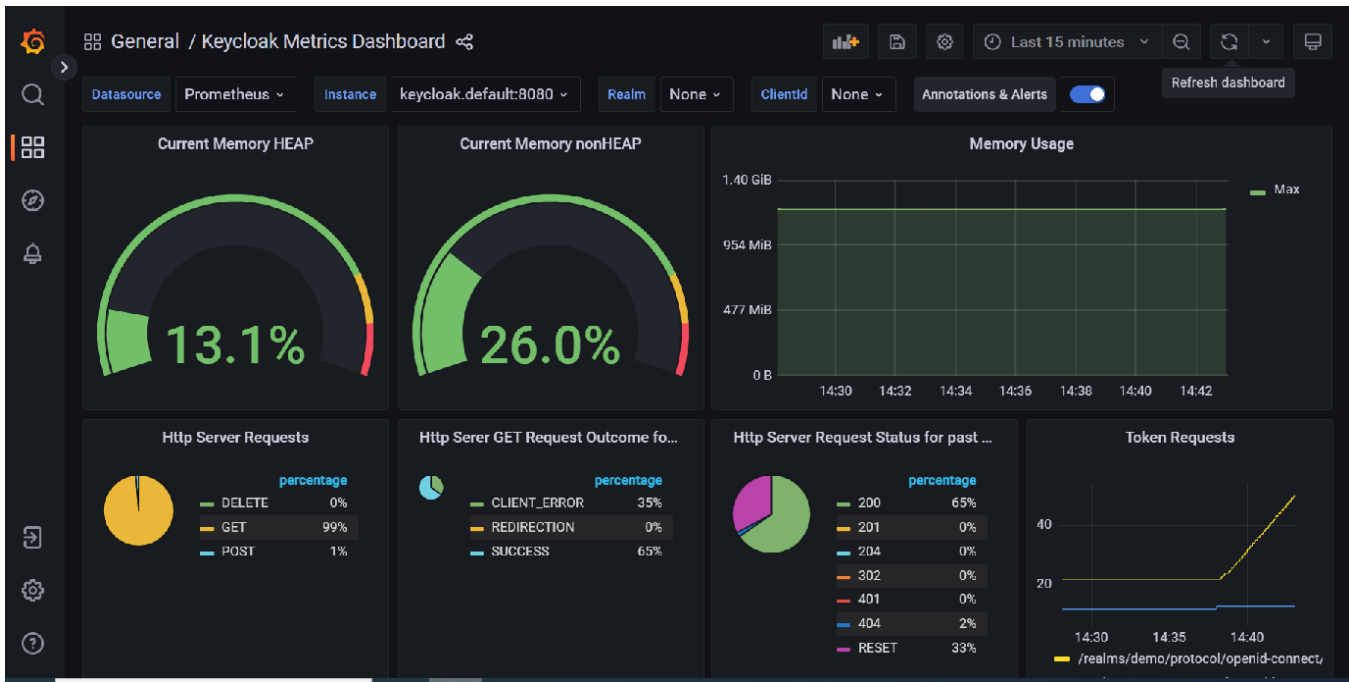
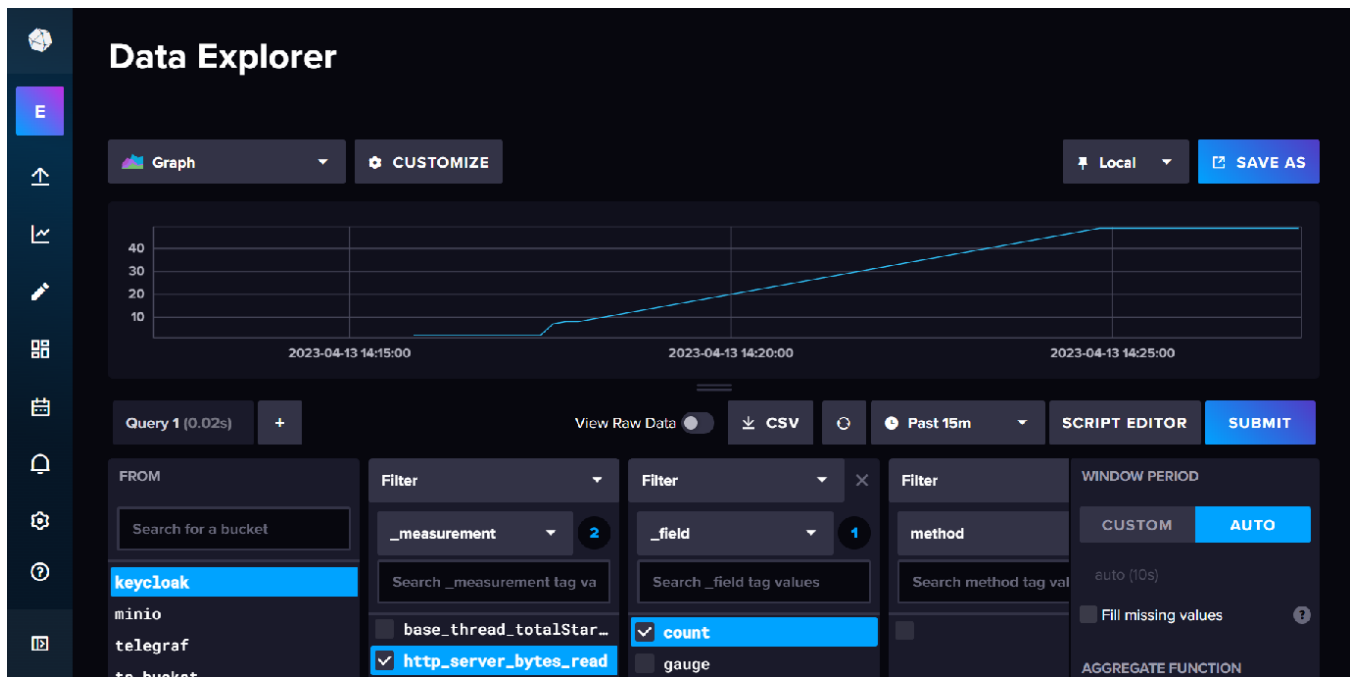This dashboard is available here: Keycloak Metrics Dashboard-1680702117153.json

InfluxDB

These metrics can also be made available in InfluxDB by setting up a metrics scraper and a bucket to store the metrics.

The metrics can then be viewed in data explorer.

LINKS

[Server Administration Guide](#)

[Keycloak Admin REST API](#)

[Configuring Keycloak](#)

[All configuration](#)

[Running Keycloak in a container](#)