ambassador

Running and Extending Keycloak for Your Identity Needs

Alex Gervais, ConFoo 2022

Alex Gervais

Principal Software Developer

@alex_gervais on Twitter

github.com/alexgervais

ambassador

EMISSARY INGRESS

TELEPRESENCE

Ambassador Labs

Developer Control Plane

Computer Science is half-remembering something and googling the rest
CHANGE MY MIND
LOUDER CROWDER
LOUDER CROWDER

Keycloak in a Nutshell

Single Sign-On

Multiple realms and clients

Identity and Access Management (IAM)

Brokering with Identity Providers

Social Logins

Google, GitHub, GitLab, etc.

OpenID Connect, OAuth 2.0 and SAML 2.0

+ LDAP, Active Directory, 2FA

Apache License 2.0

Commercial Use

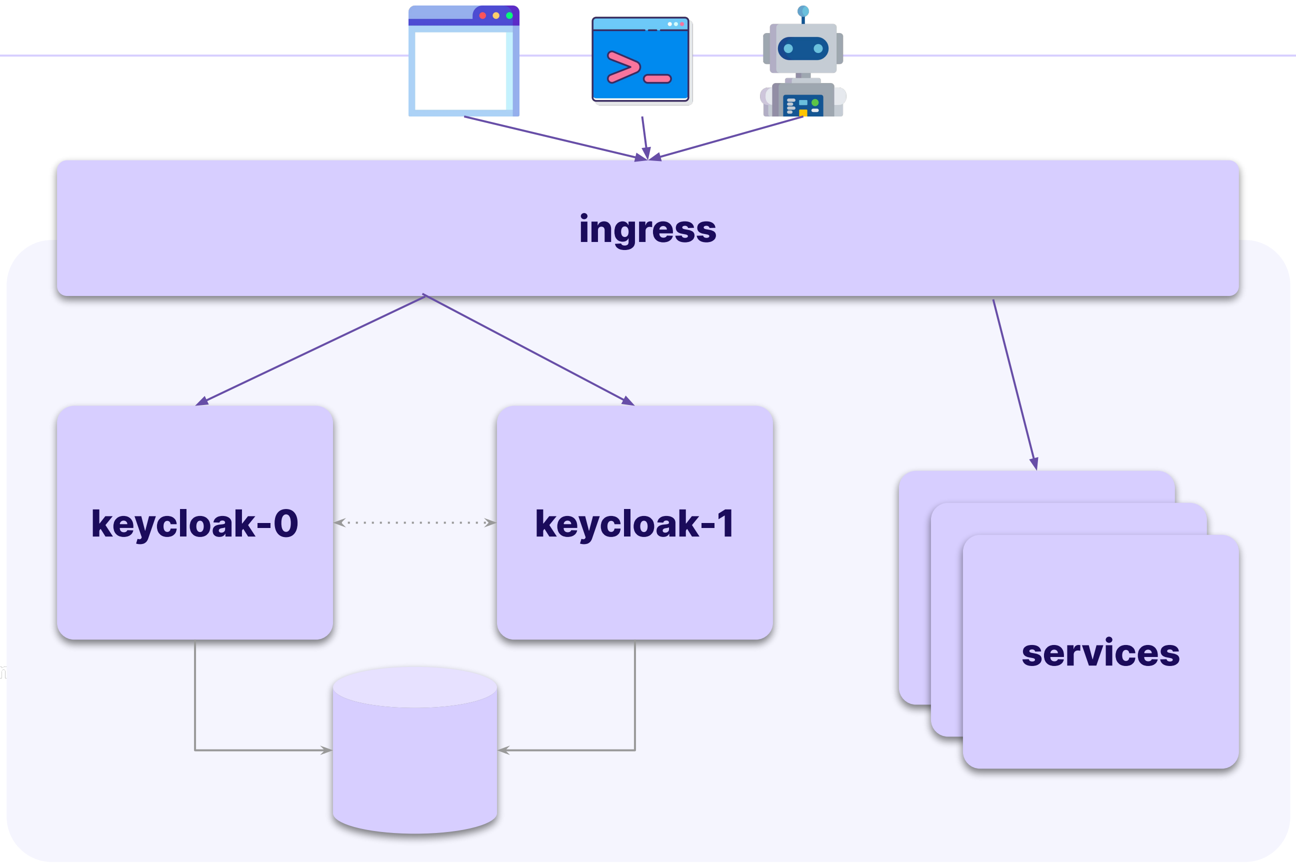
Modify

Distribute

Use Patent Claims

https://tldrlegal.com/license/apache-license-2.0-%28apache-2.0%29

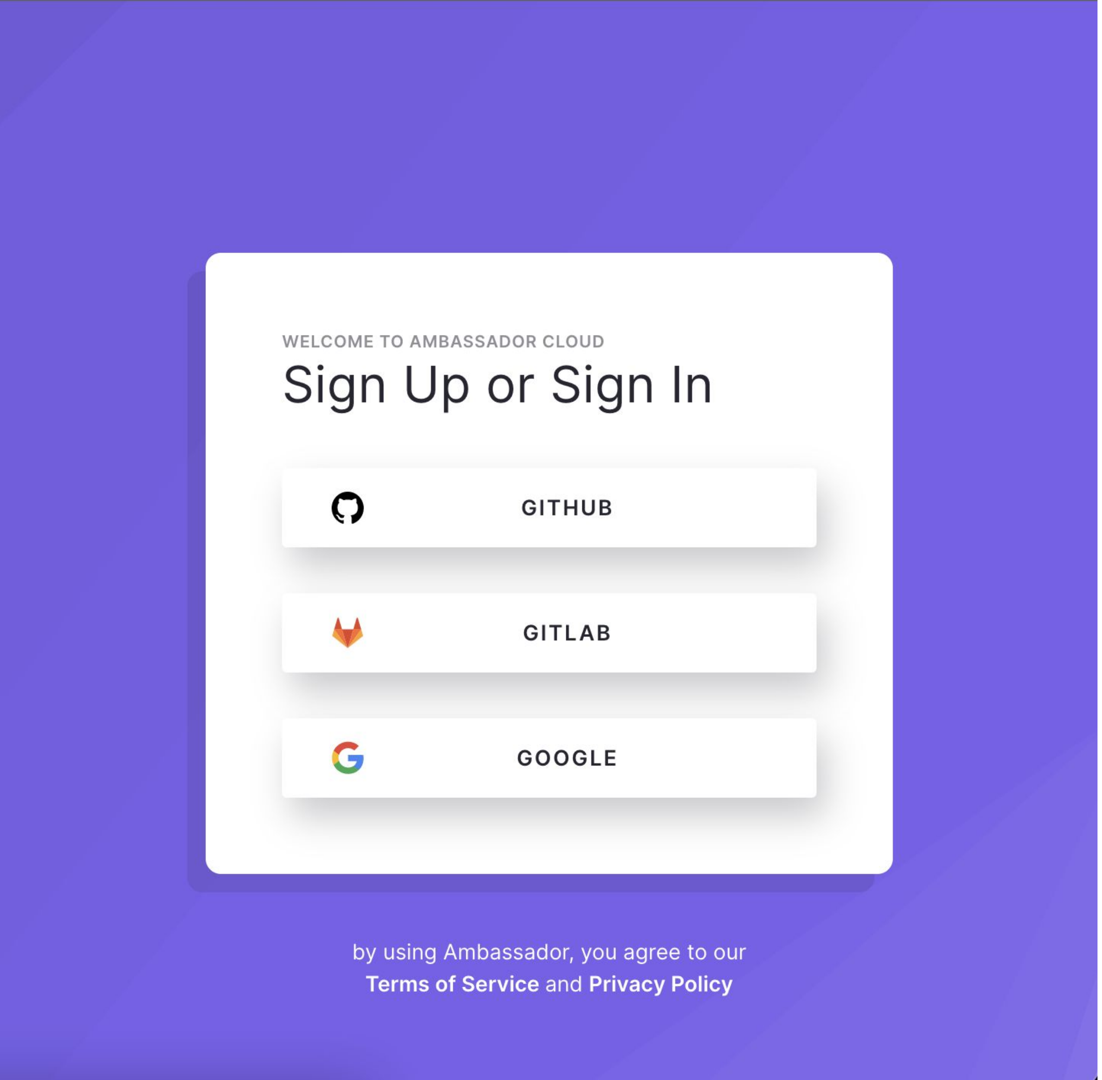
A Bit of Architecture



Java application,
WildFly distribution

Relational database

Infinispan



WELCOME TO AMBASSADOR CLOUD

Sign Up or Sign In

GITHUB

GITLAB

GOOGLE

by using Ambassador, you agree to our
Terms of Service and **Privacy Policy**

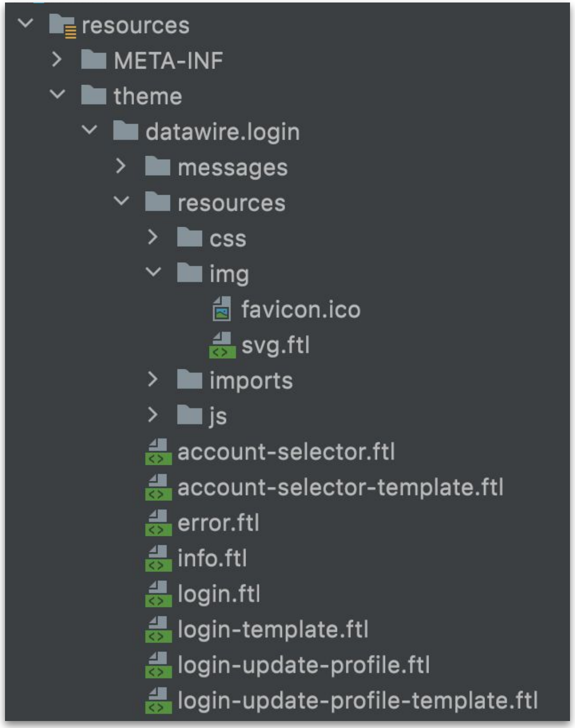
Ambassador Labs' Usage

app.getambassador.io

Customizations

1. Themes
2. Resources & APIs
3. Events

ambassador



```
resources
  META-INF
  theme
    datawire.login
      messages
      resources
        css
        img
          favicon.ico
          svg.ftl
        imports
        js
      account-selector.ftl
      account-selector-template.ftl
      error.ftl
      info.ftl
      login.ftl
      login-template.ftl
      login-update-profile.ftl
      login-update-profile-template.ftl
```

Themes

```
<#import "template.ftl" as layout>
<#import "resources/img/svg.ftl" as svg>
<@layout.registrationLayout displayMessage=false; section>
  <#if section = "form">
    <section class="login-wrapper">
      <div class="login-message-wrapper">
        <div class="login-message-content">
          <h1>
            <@svg.logoAmbassador />
            <ins>Ambassador Labs</ins>
          </h1>
          <div id="kc-info-message" class="login-message">
            [...]
          </div>
        </div>
      </div>
      <div class="messages-background-pattern">
        <@svg.backgroundPattern />
      </div>
    </section>
  </#if>
</@layout.registrationLayout>
```

https://github.com/keycloak/keycloak/tree/main/themes/src/main/resources/theme

Resources & APIs

```
import java.util.Collections;
import java.util.List;
import org.keycloak.connections.jpa.entityprovider.JpaEntityProvider;

public class TeamJpaEntityProvider implements JpaEntityProvider {
  @Override
  public List<Class<?>> getEntities() {
    return Collections.<Class<?>>singletonList(TeamEntity.class);
  }

  @Override
  public String getChangelogLocation() {
    return "META-INF/teams-changelog-master.xml";
  }

  @Override
  public String getFactoryId() {
    return TeamJpaEntityProviderFactory.ID;
  }

  @Override
  public void close() {}
}
```

Resources & APIs

```
import org.keycloak.models.KeycloakSession;
import org.keycloak.services.resource.RealmResourceProvider;
import org.keycloak.utils.MediaType;

public class TeamRestApi implements RealmResourceProvider {
  private final KeycloakSession session;
  private final TeamService teamService;

  public TeamRestApi(KeycloakSession session, TeamService teamService) {
    this.session = session;
    this.teamService = teamService;
  }

  public Object getResource() {
    return this;
  }

  @GET
  @Path("teams")
  @Produces({MediaType.APPLICATION_JSON})
  public List<TeamRepresentation> listTeams() {
    hasRealmRole(RealmRoles.VIEW_TEAMS);
    return teamService.listTeams(session.getContext().getRealm().getId()).stream()
      .map(this::toTeamRepresentation)
      .collect(Collectors.toList());
  }
}
```

Events

```java
import org.keycloak.events.Event;
import org.keycloak.events.EventListenerProvider;
import org.keycloak.events.EventType;
import org.keycloak.events.admin.AdminEvent;

public class UserRegistrationEventListenerProvider implements EventListenerProvider {
  private static final Logger log = Logger.getLogger(UserRegistrationEventListenerProvider.class);
  private final KeycloakSession session;

  public UserRegistrationEventListenerProvider(KeycloakSession session) {
    this.session = session;
  }

  @Override
  public void onEvent(Event event) {
    if (EventType.REGISTER.equals(event.getType())) {
      RealmModel realm = session.realms().getRealm(event.getRealmId());
      UserModel user = session.users().getUserById(event.getUserId(), realm);
      if (user != null && user.getEmail() != null) {
        log.info("Let's greet our new user!");
      }
    }
  }

  @Override
  public void onEvent(AdminEvent event, boolean includeRepresentation) {}
}
```

Operations

1. Packaging
2. Configuration & Deployment
3. Monitoring

ambassador

Docker Packaging

`ambassador-labs/keycloak`

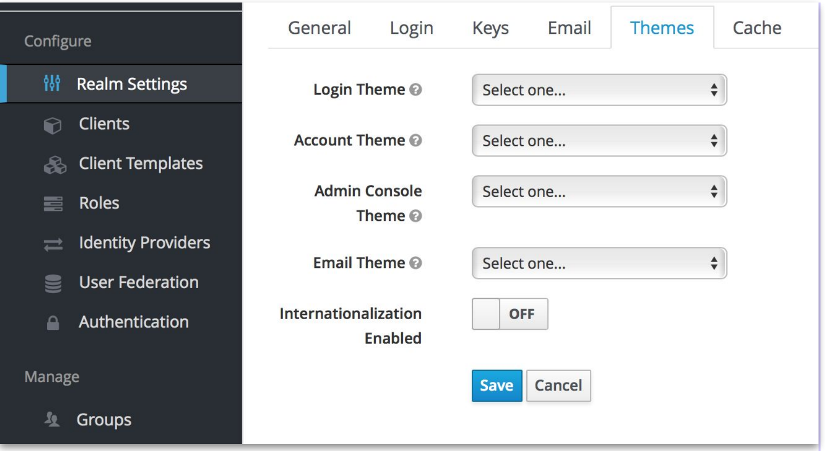
KEYCLOAK

```
FROM quay.io/keycloak/keycloak
```

Kubernetes Helm Installation

```
image:
  repository: ambassador-labs/keycloak
  tag: latest

replicas: 2

extraEnv: |
  - name: FORMAT_MESSAGES_PATTERN_DISABLE_LOOKUPS
    value: "true"
  - name: PROXY_ADDRESS_FORWARDING
    value: "true"
  - name: JGROUPS_DISCOVERY_PROTOCOL
    value: kubernetes.KUBE_PING
  - name: KUBERNETES_NAMESPACE
    valueFrom:
      fieldRef:
        apiVersion: v1
        fieldPath: metadata.namespace
  - name: CACHE_OWNERS_COUNT
    value: "2"
  - name: CACHE_OWNERS_AUTH_SESSIONS_COUNT
    value: "2"
```

https://github.com/codecentric/helm-charts/tree/master/charts/keycloak



Login Theme: Select one...

Account Theme: Select one...

Admin Console Theme: Select one...

Email Theme: Select one...

Internationalization Enabled: OFF

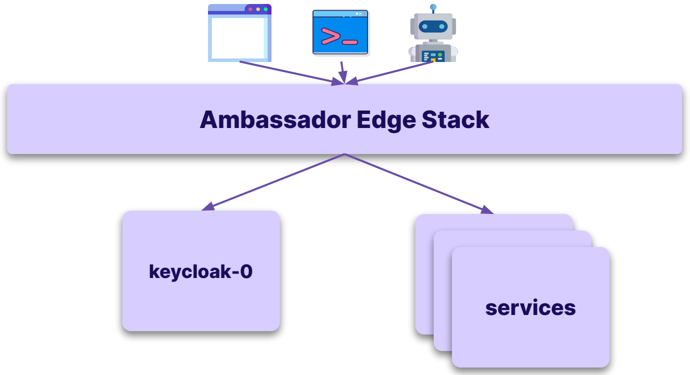
Configuration as Code!

```
terraform {
  required_providers {
    keycloak = {
      source  = "mrparkers/keycloak"
      version = "= 2.2.2"
    }
  }
}

provider "keycloak" {
}

data "keycloak_realm" "realm" {
  realm = var.realm_name
}

resource "keycloak_realm_events" "events" {
  realm_id        = data.keycloak_realm.realm.id
  events_enabled = true
  events_listeners = [
    "UserRegistrationEventListenerProvider",
    "jboss-logging",
  ]
}
```

https://github.com/mrparkers/terraform-provider-keycloak

API Gateway Filters

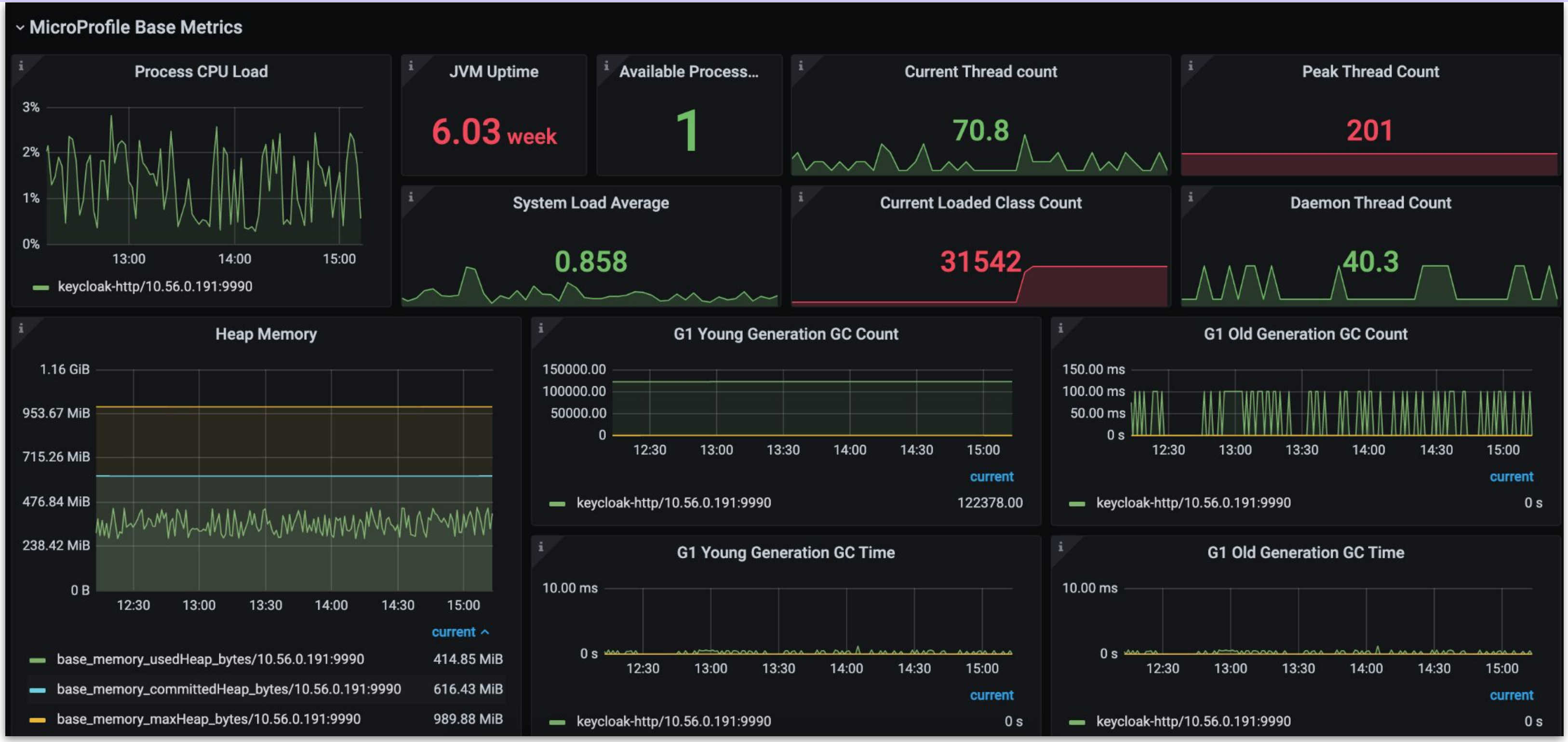
```
apiVersion: getambassador.io/v2
kind: Filter
metadata:
  name: keycloak-jwt
spec:
  JWT:
    injectRequestHeaders:
      - name: Authorization
        value: Bearer {{ .token.Raw }}
    issuer: https://app.getambassador.io/auth/realms/p
    jwksURI:
https://app.getambassador.io/auth/realms/p/protocol/openid-connect/certs
---
apiVersion: getambassador.io/v2
kind: Filter
metadata:
  name: keycloak-oauth2
spec:
  OAuth2:
    accessTokenJWTFilter:
      name: keycloak-jwt
    audience: ambassador
    authorizationURL: https://app.getambassador.io/auth/realms/p
    clientID: ambassador
    protectedOrigins:
      - origin: https://app.getambassador.io
    secretName: keycloak-ambassador-client-secret
```



```
apiVersion: getambassador.io/v2
kind: FilterPolicy
metadata:
  name: keycloak
spec:
  rules:
    - filters:
        - name: keycloak-oauth2
          arguments:
            scopes: [email, profile]
      host: app.getambassador.io
      path: /cloud/*
```

https://www.getambassador.io/docs/edge-stack/latest/topics/using/filters/

Monitoring


MicroProfile Base Metrics
Process CPU Load
3%
2%
1%
0%
13:00
14:00
15:00
keycloak-http/10.56.0.191:9990
JVM Uptime
6.03 week
Available Process...
1
Current Thread count
70.8
Peak Thread Count
201
System Load Average
0.858
Current Loaded Class Count
31542
Daemon Thread Count
40.3
Heap Memory
1.16 GiB
953.67 MiB
715.26 MiB
476.84 MiB
238.42 MiB
0 B
12:30
13:00
13:30
14:00
14:30
15:00
current
base_memory_usedHeap_bytes/10.56.0.191:9990 414.85 MiB
base_memory_committedHeap_bytes/10.56.0.191:9990 616.43 MiB
base_memory_maxHeap_bytes/10.56.0.191:9990 989.88 MiB
G1 Young Generation GC Count
150000.00
100000.00
50000.00
0
current
keycloak-http/10.56.0.191:9990 122378.00
G1 Old Generation GC Count
150.00 ms
100.00 ms
50.00 ms
0 s
current
keycloak-http/10.56.0.191:9990 0 s
G1 Young Generation GC Time
10.00 ms
0 s
current
keycloak-http/10.56.0.191:9990 0 s
G1 Old Generation GC Time
10.00 ms
0 s
current
keycloak-http/10.56.0.191:9990 0 s

ambassador @alex_gervais

https://grafana.com/grafana/dashboards/13489

Other Considerations

1. Inner Dev-Loop
2. Testing

ambassador

Local Dev Loop

1

docker build

2

docker run --debug

3

terraform apply

Testing

End-to-End

with Cypress

Integration

Standalone volatile process
with reproducible configurations

⏪

SSO

Protected endpoints with social logins and multiple clients

Customizations

Branding - Teams - Greeting

Operations

Locally, and at scale with Keycloak

Thanks!

We're hiring!

@alex_gervais on Twitter

github.com/alexgervais

a8r.io/Slack

ambassador