



User Authentication in Distributed Applications

Denis Mekhanikov

Team Lead @ GridGain Cloud Team

Alexander Kozhenkov

Software Engineer @ GridGain Cloud Team

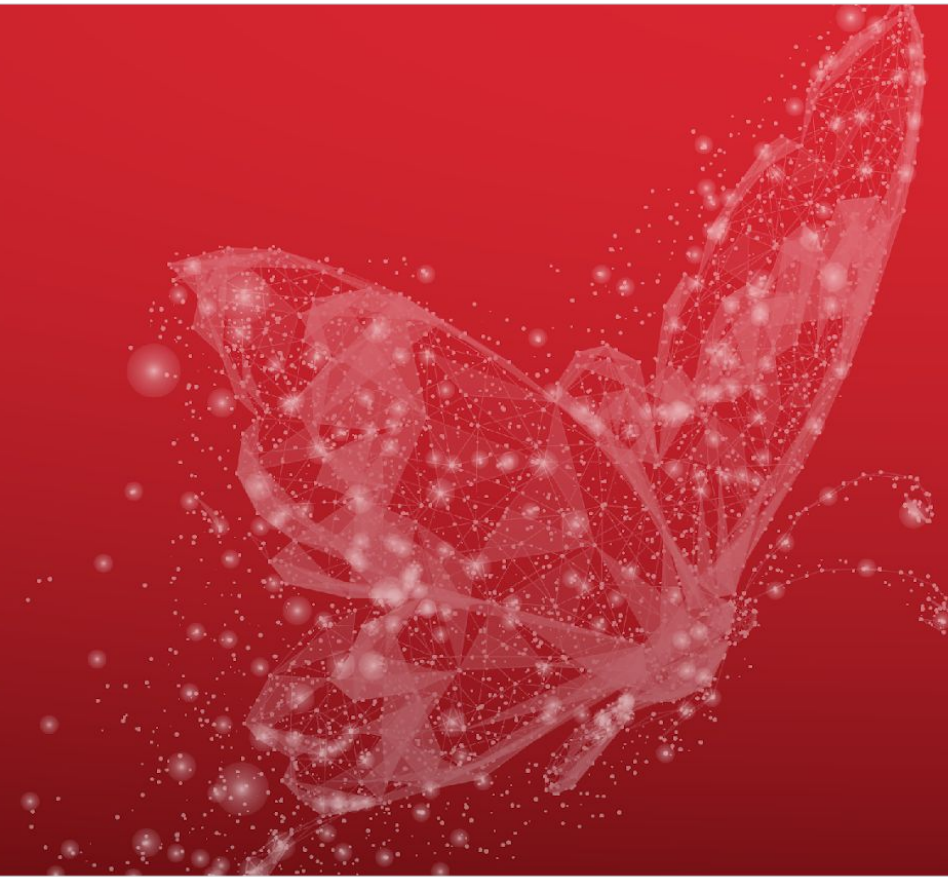


Agenda



- Authentication models
- Single Sign On
- Example
 - GridGain and Control Center
- Demo
 - Integration of OpenID Connect with Control Center
 - SSO with secured cluster
 - Implementation of a custom Authenticator

Authentication models

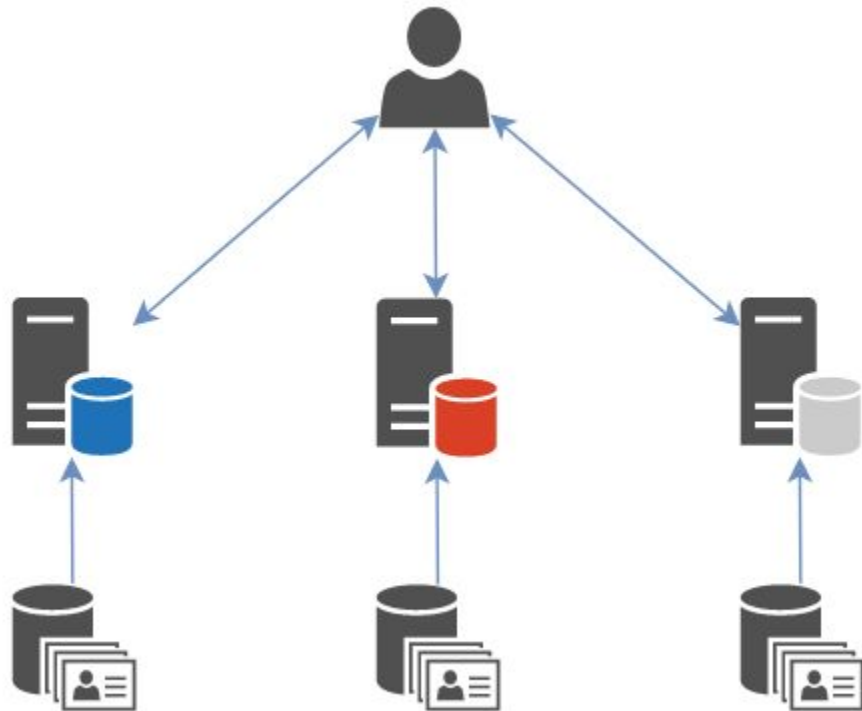


Model #1: Database of users inside application



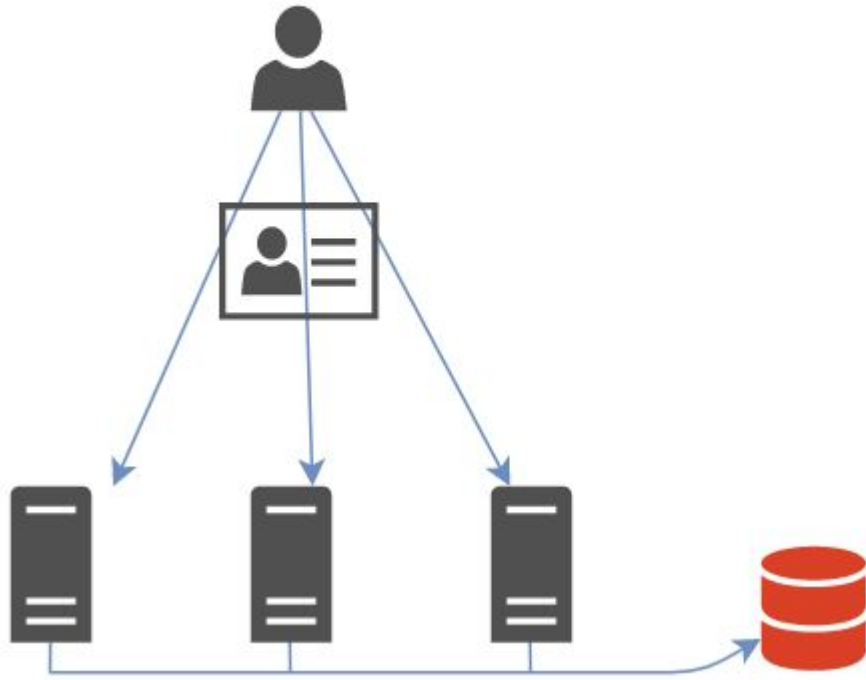
- No need for special interaction protocols
- An existing database can be used

Model #1: Database of users inside application



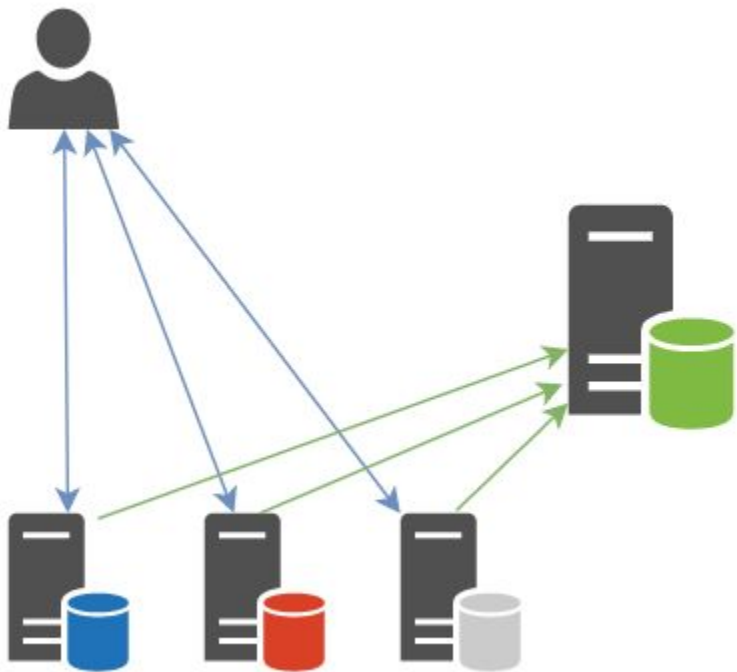
- ! Synchronization issues between several applications
- ! Global user sessions are not supported

Model #2: Shared database of users



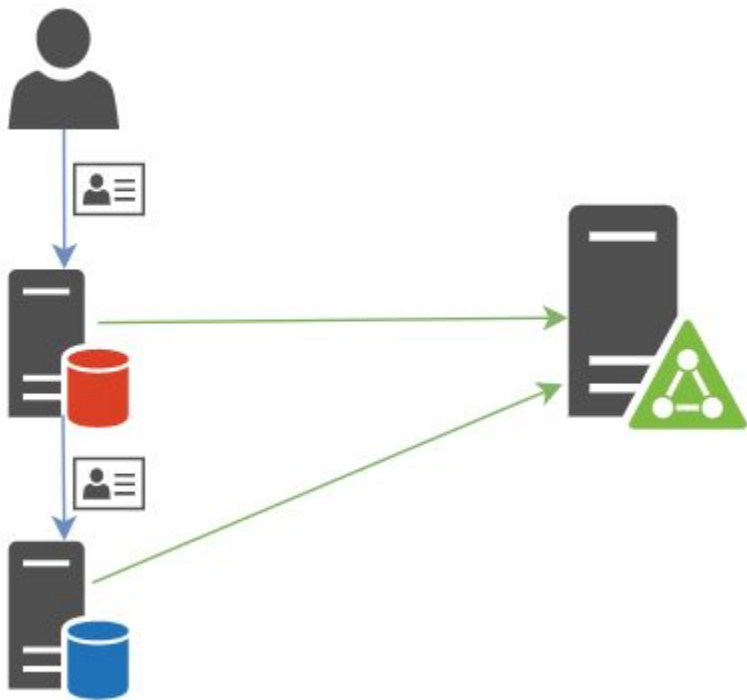
- No need for synchronization
- Global sessions can be stored
- ! Duplication of logic
- ! Problematic to make schema changes
- ! Only trusted applications can access the database

Model #3: Separate authentication service



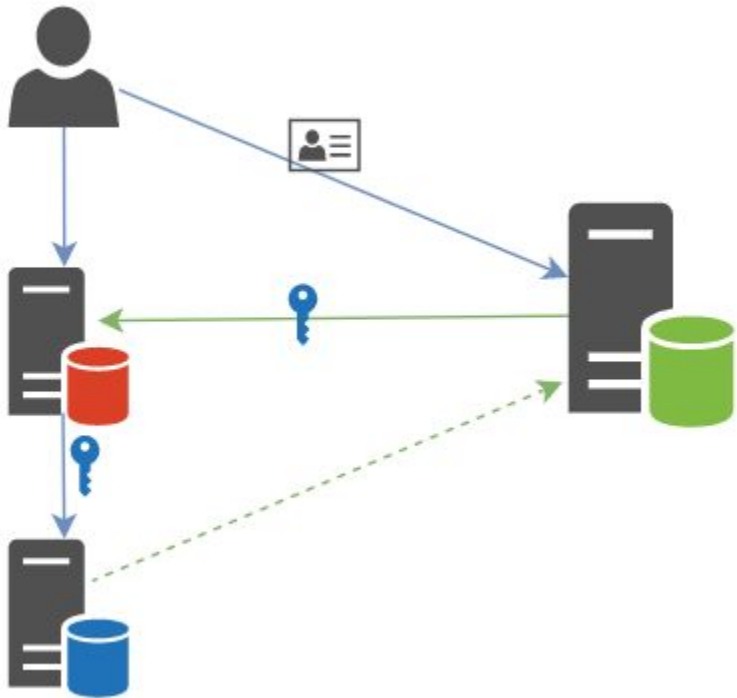
- Centralized database of users
- ! Need a special authentication protocol
- ! Overhead on an additional external request

Model #3: Separate authentication service



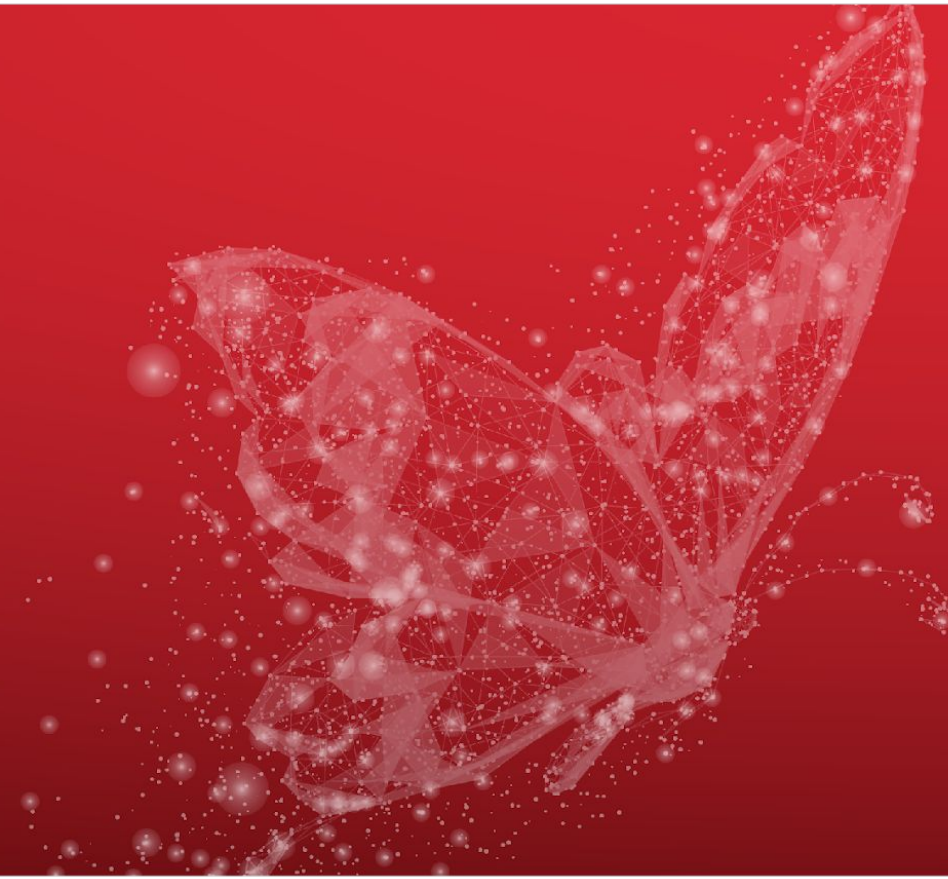
- ! Request to a new system – new authentication
- ! Propagation of users credentials between subsystems

Model #4: Single sign on



- Centralized database of users
- Single session for multiple applications
- Temporary token instead of a password

Single Sign On



OAuth 2.0



OAuth 2.0 flows



- Authorization code
- Implicit
- Client credentials
- Resource owner password
- Authorization code with proof key for code exchange



OAuth 2.0 flows



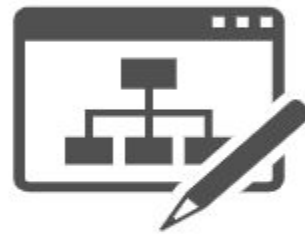
- Authorization code
- Implicit
- Client credentials
- Resource owner password
- Authorization code with proof key for code exchange



OAuth 2.0. Authorization code



PhotoEditor Frontend



PhotoEditor Backend

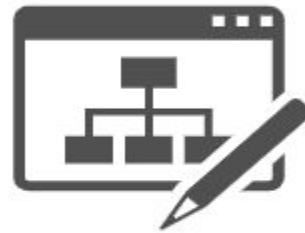


Facebook

OAuth 2.0. Authorization code



PhotoEditor Frontend

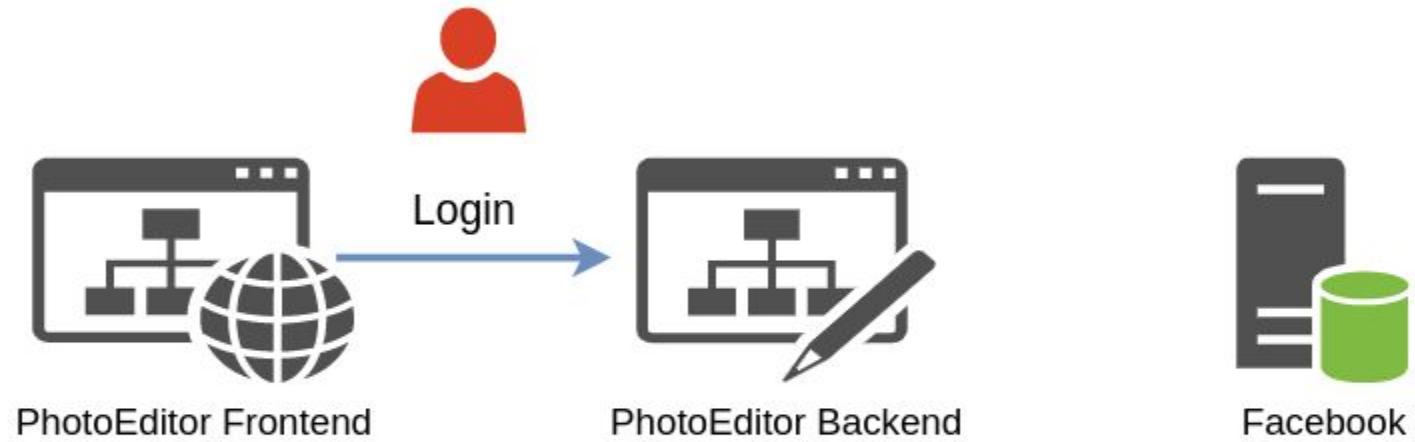


PhotoEditor Backend

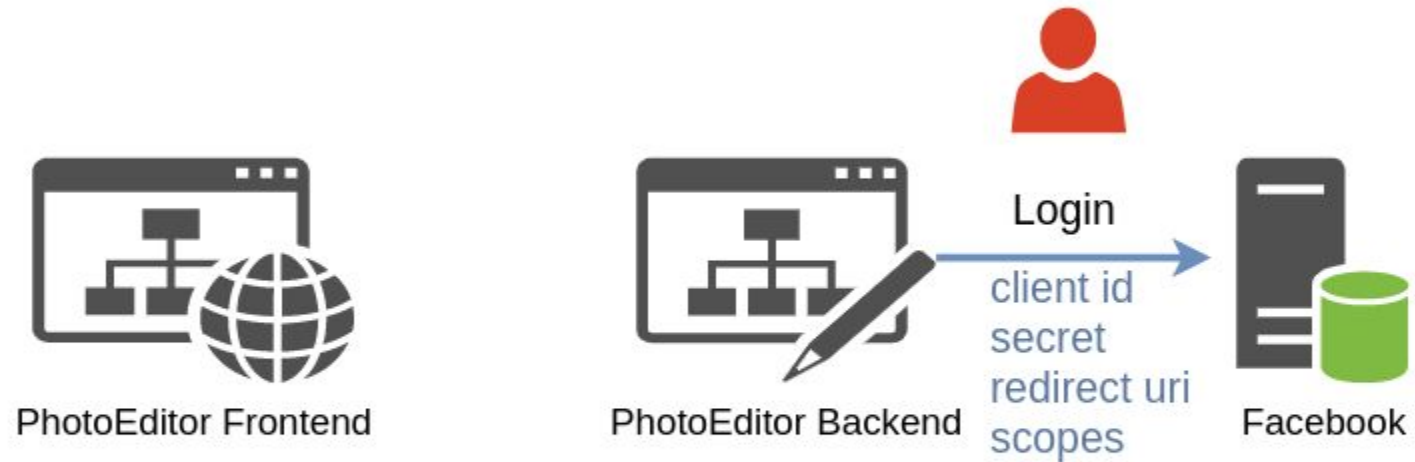


Facebook

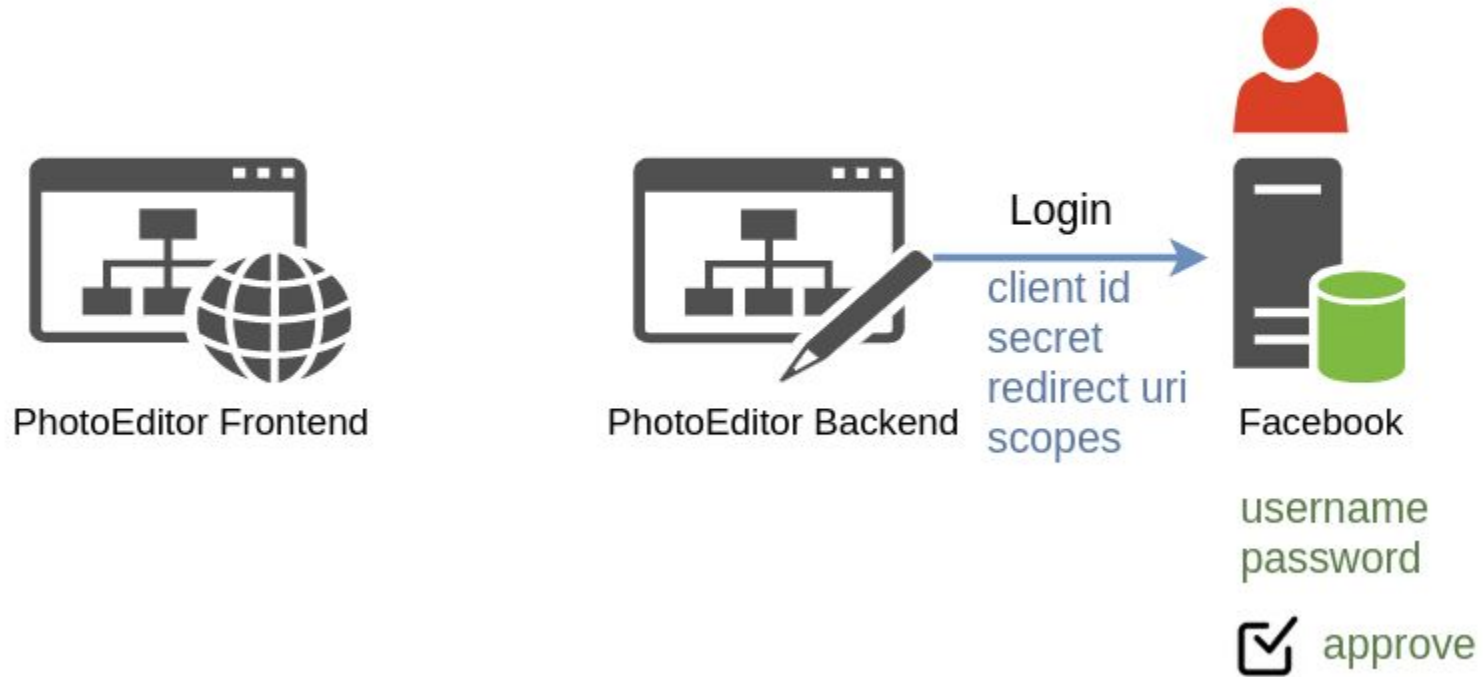
OAuth 2.0. Authorization code



OAuth 2.0. Authorization code



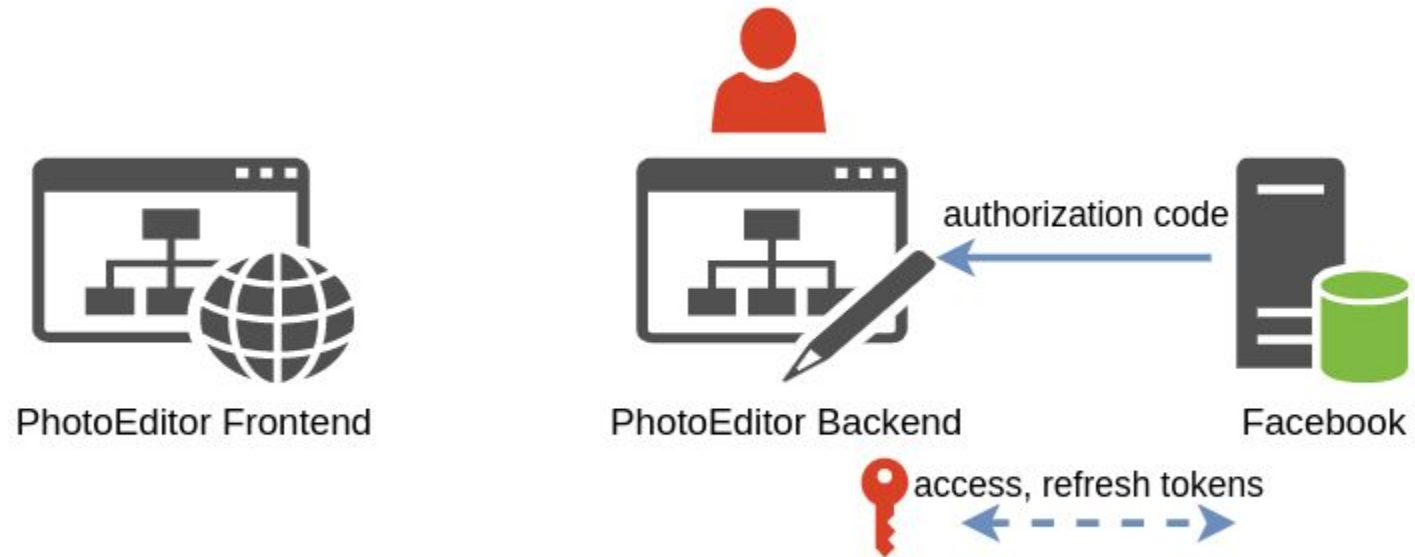
OAuth 2.0. Authorization code



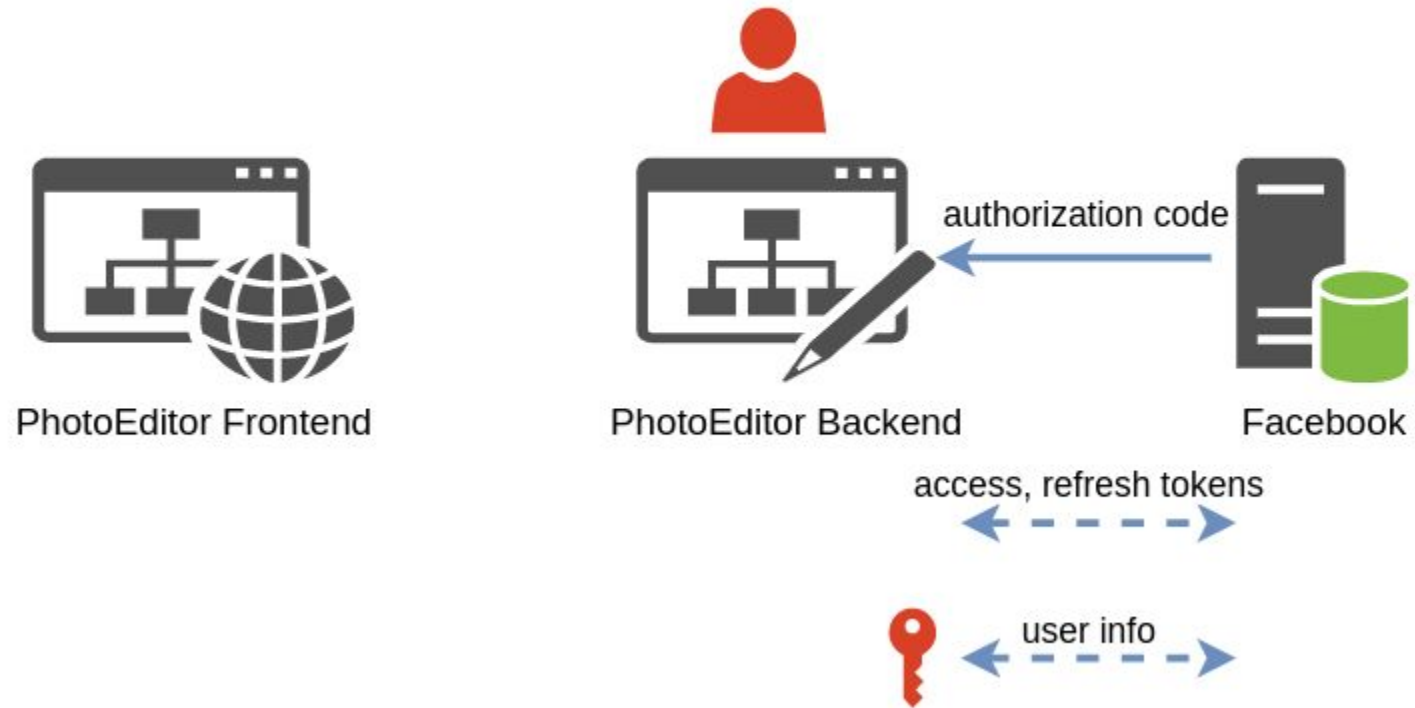
OAuth 2.0. Authorization code



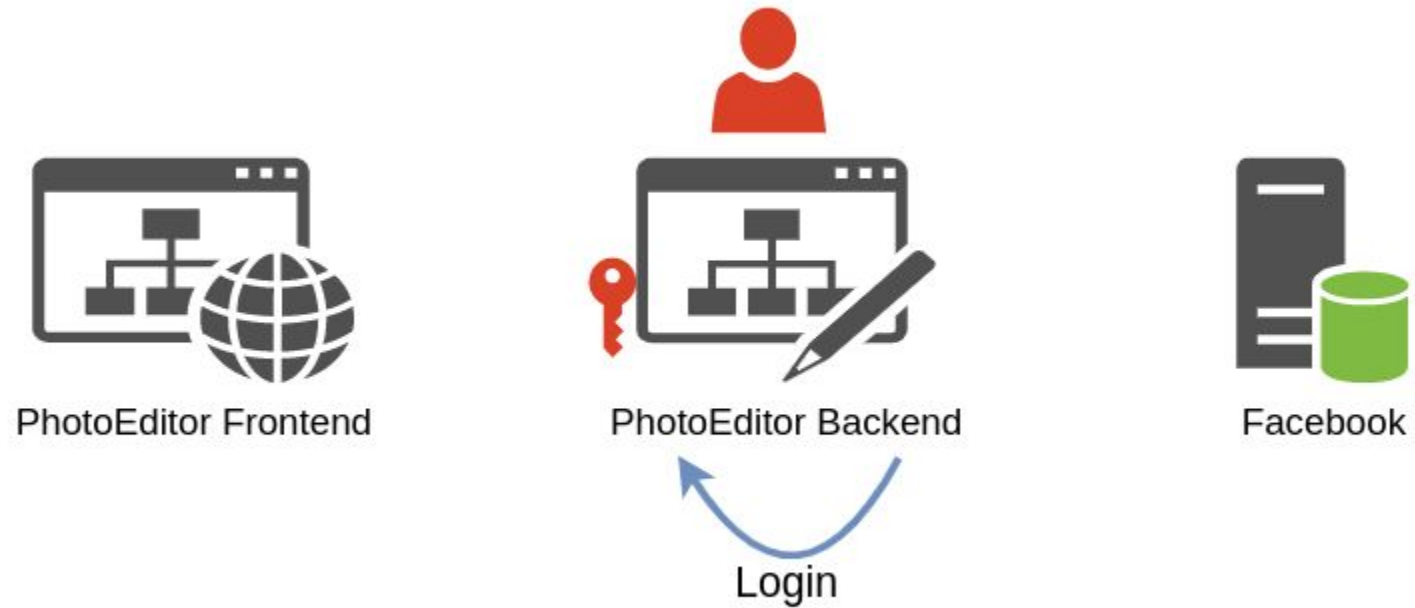
OAuth 2.0. Authorization code



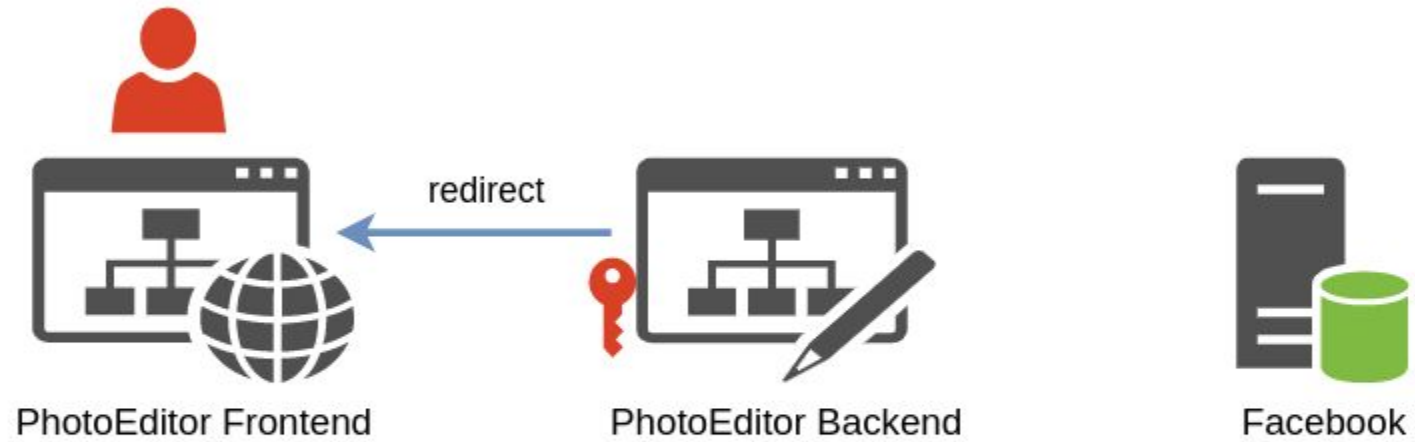
OAuth 2.0. Authorization code



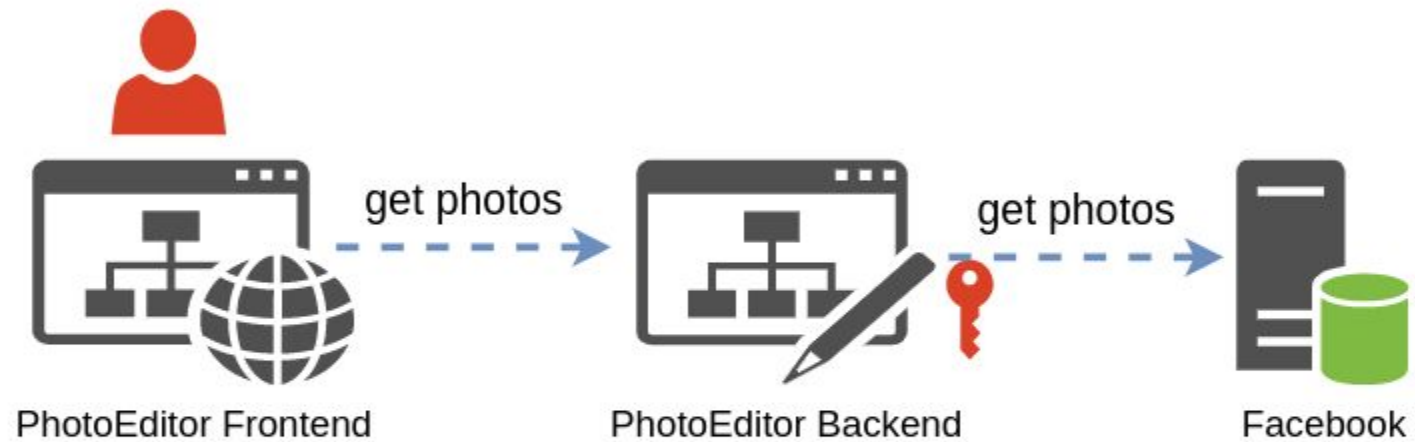
OAuth 2.0. Authorization code



OAuth 2.0. Authorization code



OAuth 2.0. Authorization code



OpenID Connect



OpenID Connect



- Extension of OAuth2.0



OpenID Connect



- Extension of OAuth2.0
- Authentication and authorization



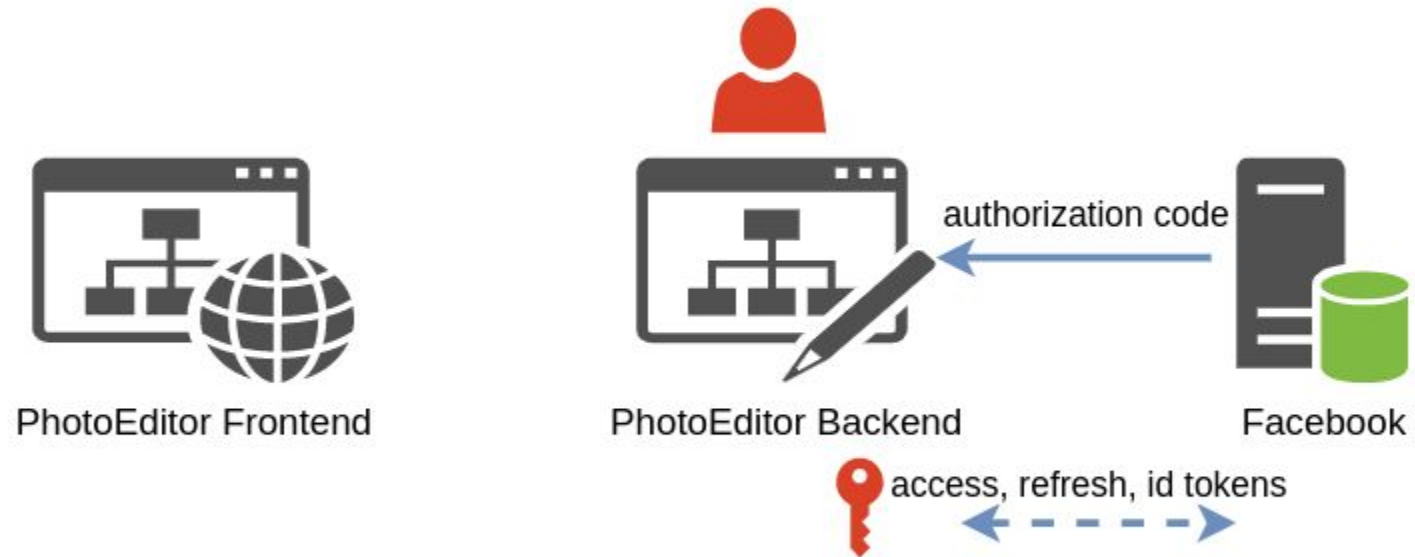
OpenID Connect



- Extension of OAuth2.0
- Authentication and authorization
- The specification is more strict



OpenID Connect



OpenID Connect ID token



```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache

{
  "access_token": "S1AV32hkKG",
  "token_type": "Bearer",
  "refresh_token": "8xL0xBtZp8",
  "expires_in": 3600,
  "id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjFlOWdkazcifQ.ewogImlzc
yI6ICJodHRwOi8vc2VydmVyLmV4YW1wbGUuY29tIiwiaWF0IjoiYiMjQ4Mjg5
NzYxMDAxIiwiaWF0IjoiYiMjQ4Mjg5NzYxMDAxIiwiaWF0IjoiYiMjQ4Mjg5
fV3pBMk1qIiwiaWF0IjoiYiMjQ4Mjg5NzYxMDAxIiwiaWF0IjoiYiMjQ4Mjg5
AKfQ.ggW8hZ1EuVLuxNuuIJKX_V8a_OMXzR0EHR9R6jgdqr00F4daGU96Sr_P6q
Jp6IcmD3HP990bi1PRs-cwh3L0-p146waJ8IhehcwL7F09JdijmBqkvPeB2T9CJ
NqeGpe-gccMg4vfKjkm8FcGvnzZUN4_KSP0aAp1t0J1zZwgjxqGByKHi0tX7Tpd
QyHE5lcMiKPXfEIQILVq0pc_E2DzL7emopWoaoZTF_m0_N0YzFC6g6EJb0EoRoS
K5hoDa1rcvRYLSrQAZZKf1yuVCyixEoV9GfnQC3_osjzw2PAithfubEEBLuVvk4
XUVrWOLrLl0nx7RkKU8NXNHq-rvKMzqg"
}
```

OpenID Connect ID token



HTTP/1.1 200 OK

Content-Type: application/json

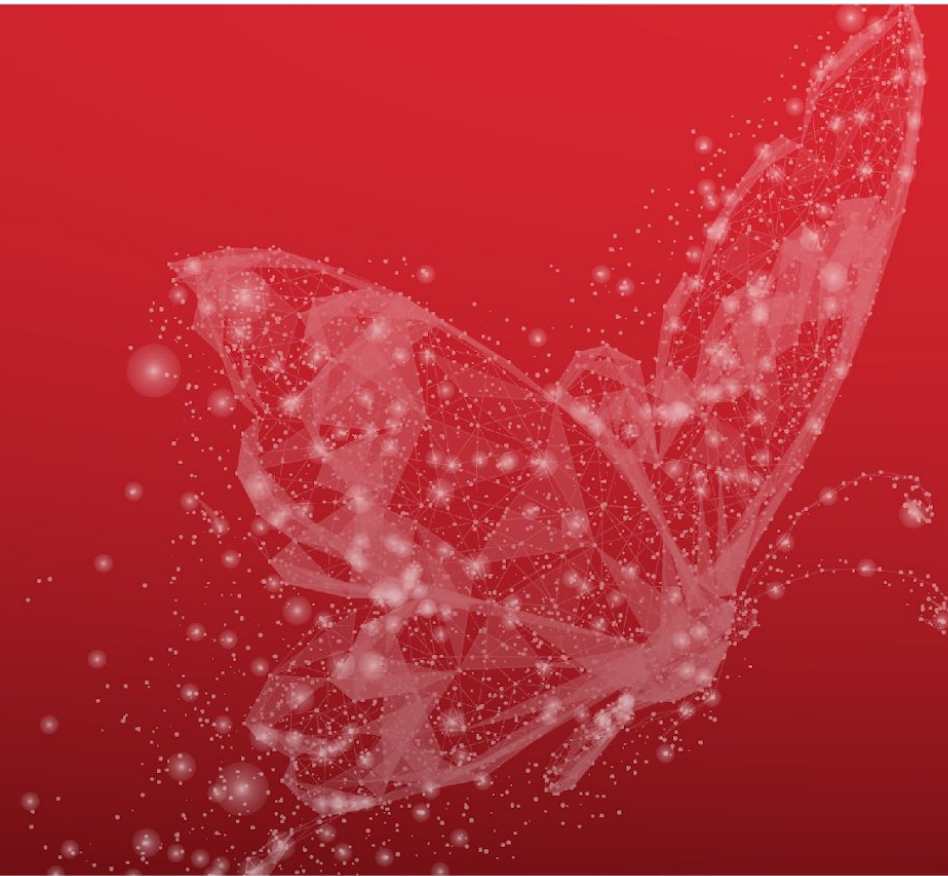
Cache-Control: no-store

Pragma: no-cache

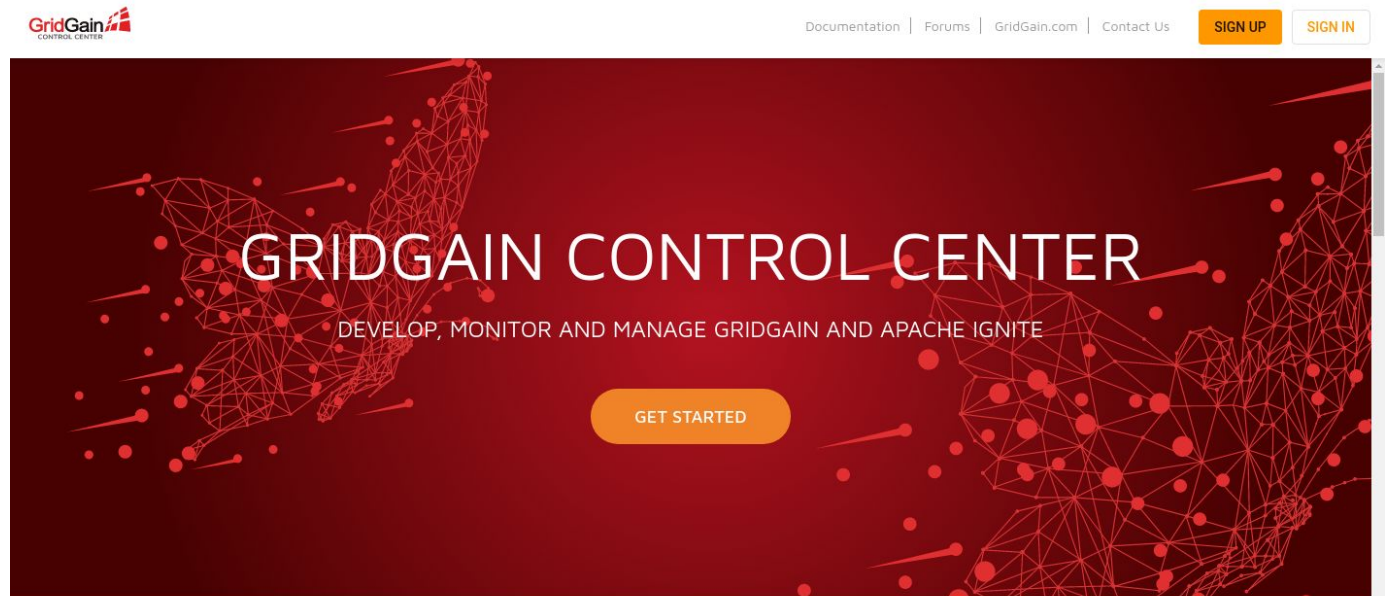
```
{
  "access_token": "S1AV32hkKG",
  "token_type": "Bearer",
  "refresh_token": "8xL0xBtZp8",
  "expires_in": 3600,
  "id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjFlOWdkazcifQ.ewogImlzc
yI6ICJodHRwOi8vc2VydmVyLmV4YW1wbGUuY29tIiwKICJzdWIiOiAiMjQ4Mjg5
NzYxMDAxIiwKICJhdWQiOiAic2ZCaGRSa3F0MyIsCiAibm9uY2UiOiAibi0wUzZ
fV3pBMk1qIiwKICJleHAiOiAxeMzExMjg5OTcwLAogImlhdCI6IDEzMTI4MTI4
AKfQ.ggW8hZ1EuVLuxNuuIJKX_V8a_OMXzR0EHR9R6jgdqr00F4daGU96Sr_P6q
Jp6IcmD3HP990bi1PRs-cwh3L0-p146waJ8IhehcwL7F09JdijmBqkvPeB2T9CJ
NqeGpe-gccMg4vfkjkm8FcGvnzZUN4_KSP0aAp1t0J1zZwgjxqGByKHi0tX7Tpd
QyHE5lcMiKPXfEIQILVq0pc_E2DzL7emopWoaoZTF_m0_N0YzFC6g6EJb0EoRoS
K5hoDa1rcvRYLSrQAZZKf1yuVCyixEoV9GfNQC3_osjzw2PAithfubEEBLuVvk4
XUVrWOLrLl0nx7RkKU8NXNHq-rvKMzqg"
}
```

```
{
  "iss": "http://server.example.com",
  "sub": "248289761001",
  "aud": "s6BhdRkqt3",
  "nonce": "n-0S6_WzA2Mj",
  "exp": 1311281970,
  "iat": 1311280970,
  "name": "Jane Doe",
  "given_name": "Jane",
  "family_name": "Doe",
  "gender": "female",
  "birthdate": "0000-10-31",
  "email": "janedoe@example.com",
  "picture": "http://example.com/me.jpg"
}
```

Control Center



Control Center overview

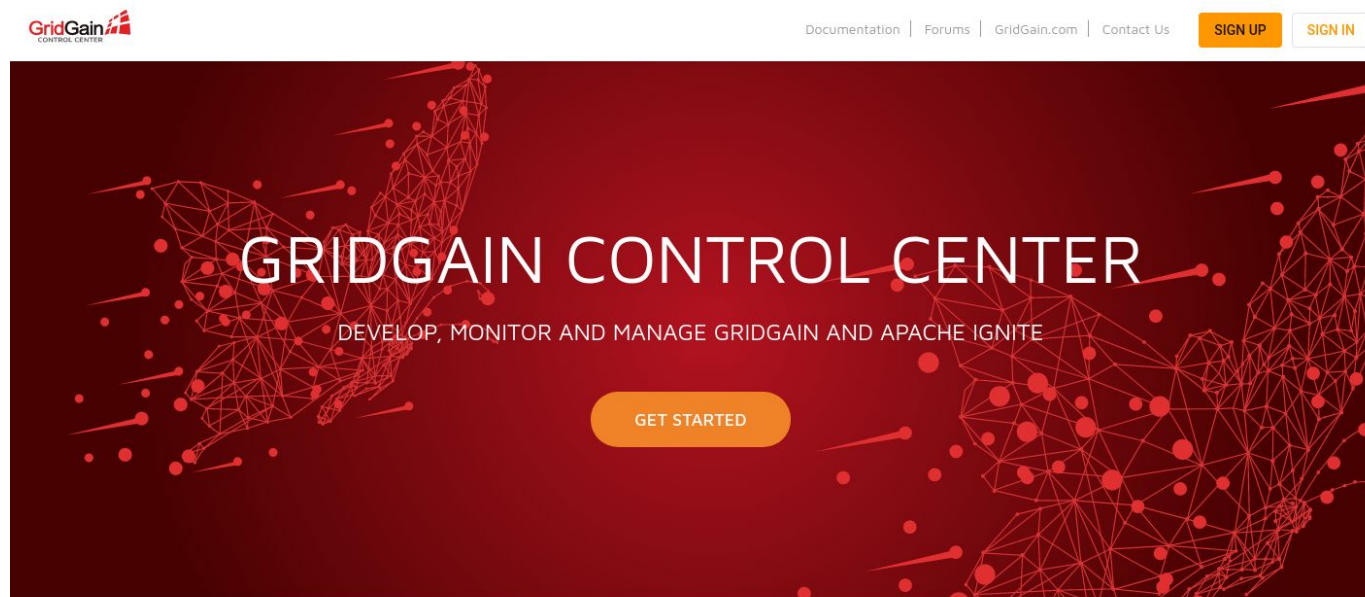


GridGain Control Center is a comprehensive, customizable cluster management and developer tool for GridGain® 8.7.23+ and Apache Ignite® 2.8.1+.

<https://control.gridgain.com>

Control Center overview

- Monitoring and management

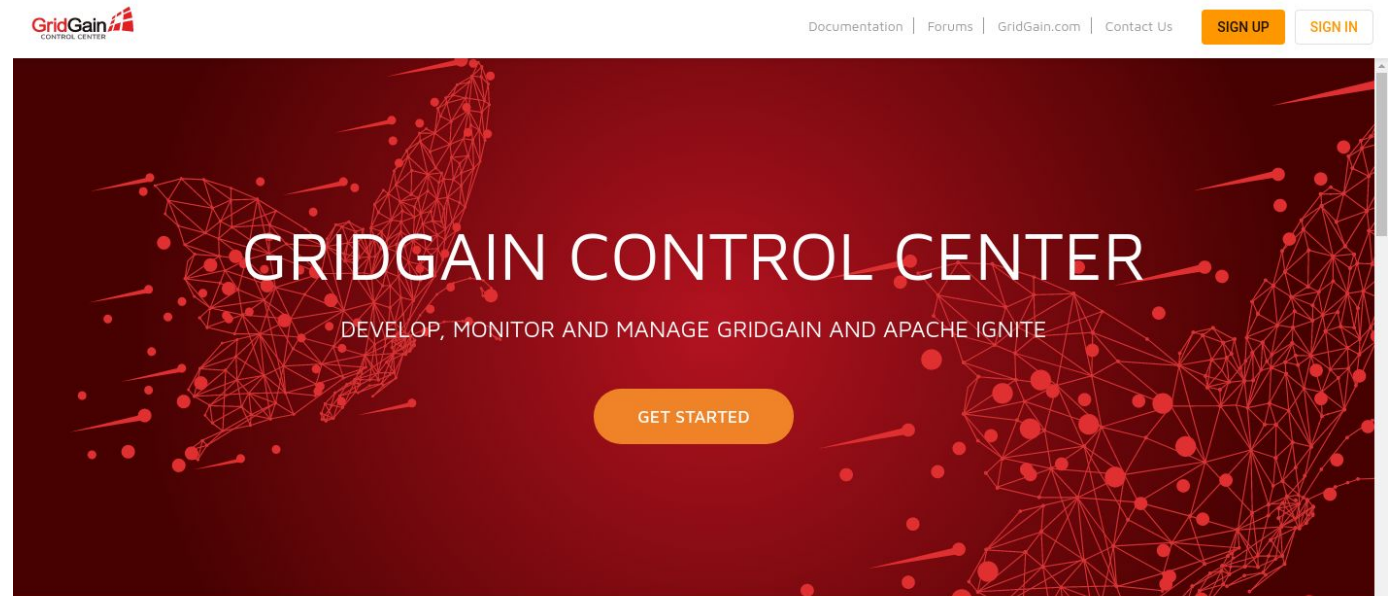


GridGain Control Center is a comprehensive, customizable cluster management and developer tool for GridGain® 8.7.23+ and Apache Ignite® 2.8.1+.

<https://control.gridgain.com>

Control Center overview

- Monitoring and management
- Hosted, on-premise

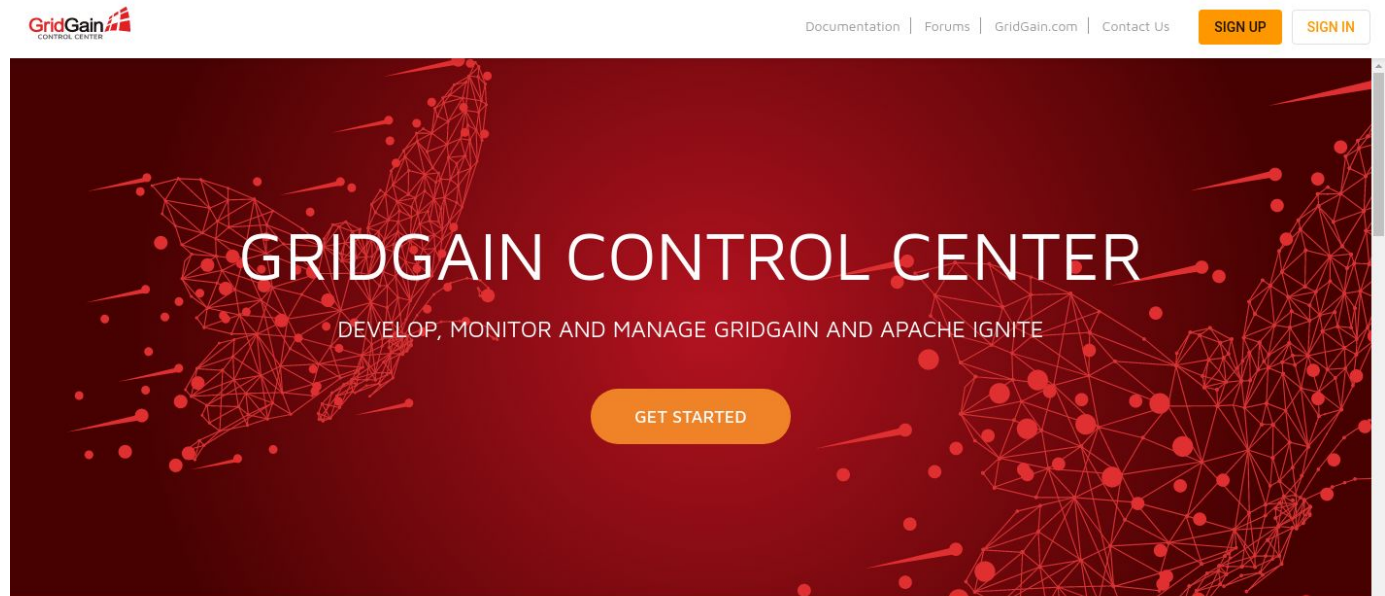


GridGain Control Center is a comprehensive, customizable cluster management and developer tool for GridGain® 8.7.23+ and Apache Ignite® 2.8.1+.

<https://control.gridgain.com>

Control Center overview

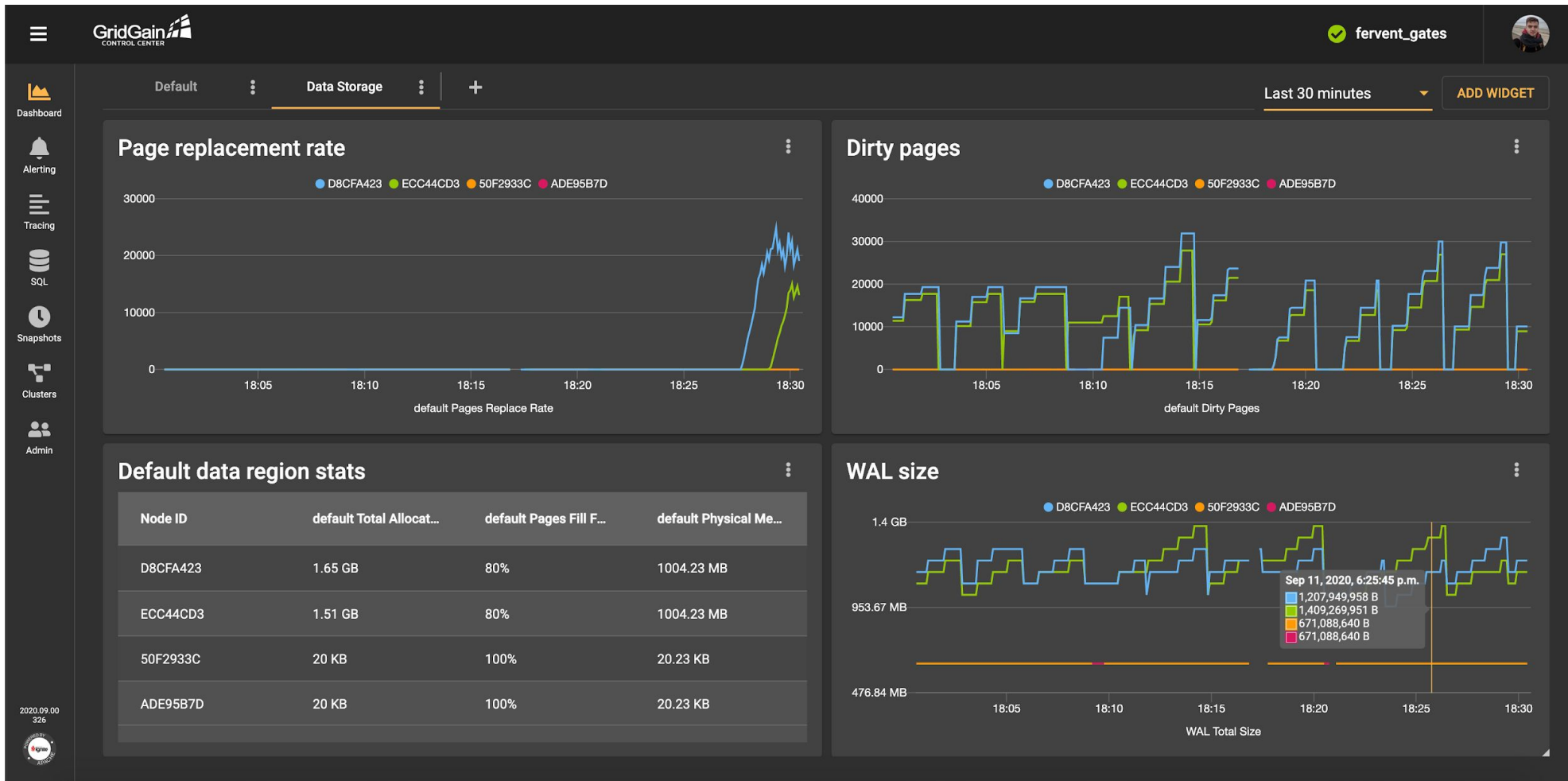
- Monitoring and management
- Hosted, on-premise
- Successor of Web Console



GridGain Control Center is a comprehensive, customizable cluster management and developer tool for GridGain® 8.7.23+ and Apache Ignite® 2.8.1+.

<https://control.gridgain.com>

Control Center overview



Control Center overview



Tracing

[CONFIGURE TRACING](#)

Name	Start Time ↓	Duration	Total Spans	Details
discovery.node.join.request	Sep 8, 15:11:53.920	94 ms	9	
discovery.custom.event	Sep 8, 13:43:52.399	2 ms	3	Message Class: FinishSnapshotOperationAckDiscoveryMe...
discovery.custom.event	Sep 8, 13:43:51.965	4 ms	3	Message Class: FinishSnapshotOperationAckDiscoveryMe...

discovery.node.join.request

Trace Start September 8, 2020 at 15:11:53.920 GMT+3 Duration 94 ms Depth 4 Total Spans 40

Filters

Span Name _____

Roots only

Event Node ID _____

Node Consistent ID _____

Start Time

From _____

To _____

Control Center overview



The screenshot displays the Control Center interface with three tabs: "QUERIES LIST", "RUNNING QUERIES", and "QUERY STATISTICS". The "QUERIES LIST" tab is active, showing a tree view on the left with "angry_wilson" expanded to show "Schemas", "Caches", and "Nodes". The main area is titled "Query" and "Explain query". It contains a text area with the following SQL query:

```
1 EXPLAIN SELECT country.name, city.name, MAX(city.population) as max_pop FROM country
2 JOIN city ON city.countrycode = country.code
3 WHERE country.code IN ('USA', 'RUS', 'CHN')
4 GROUP BY country.name, city.name ORDER BY max_pop DESC LIMIT 3
```

Below the query is an "EXECUTE" button and a settings icon. The execution plan is displayed below, showing the "Map" and "Reduce" stages:

EXPLAIN SELECT country.name, city.name, MAX(city.population) as max_pop FROM country JOIN city ON city.countrycode = country.code WHERE country.code IN ('USA','RUS','CHN') GROUP BY country.name, city.name ORDER BY max_pop DESC LIMIT 3

Map

```
1 SELECT
2   "__Z0"."NAME" AS "__C0_0",
3   "__Z1"."NAME" AS "__C0_1",
4   MAX("__Z1"."POPULATION") AS "__C0_2"
5 FROM "PUBLIC"."COUNTRY" "__Z0"
6 /* PUBLIC._key_PK_proxy: CODE IN('USA', 'RUS', 'CHN')
7 /* WHERE __Z0.CODE IN('USA', 'RUS', 'CHN')
8 */
```

Reduce

```
1 SELECT
2   "__C0_0" AS "NAME",
3   "__C0_1",
4   CAST(CAST(MAX("__C0_2") AS INTEGER) AS INTEGER) AS "max_pop"
5 FROM "PUBLIC"."__T0"
6 /* PUBLIC.merge_scan */
7 GROUP BY "__C0_0", "__C0_1"
8 ORDER BY 3 DESC
```

Control Center overview



SNAPSHOTS ADD SNAPSHOT

Start Time ↓	Type	ID	Mode	Status	Caches	
Sep 11, 19:08	INCREMENTAL	1599840500602	MANUAL	✓ OK	2	⋮
Sep 11, 19:07	FULL	1599840454829	MANUAL	✓ OK	2	⋮
Sep 9, 17:05	FULL	1599660319690	MANUAL	✓ OK	3	⋮
Sep 8, 15:15	FULL	1599567347617	MANUAL	✓ OK	2	⋮
Sep 8, 13:43	FULL	1599561828534	MANUAL	✓ OK	1	⋮

Filters

Snapshot Type ▼

Schedule Name ▼

Mode ▼

Cache Name ▼

Snapshot ID ▼

Show related snapshots

Period

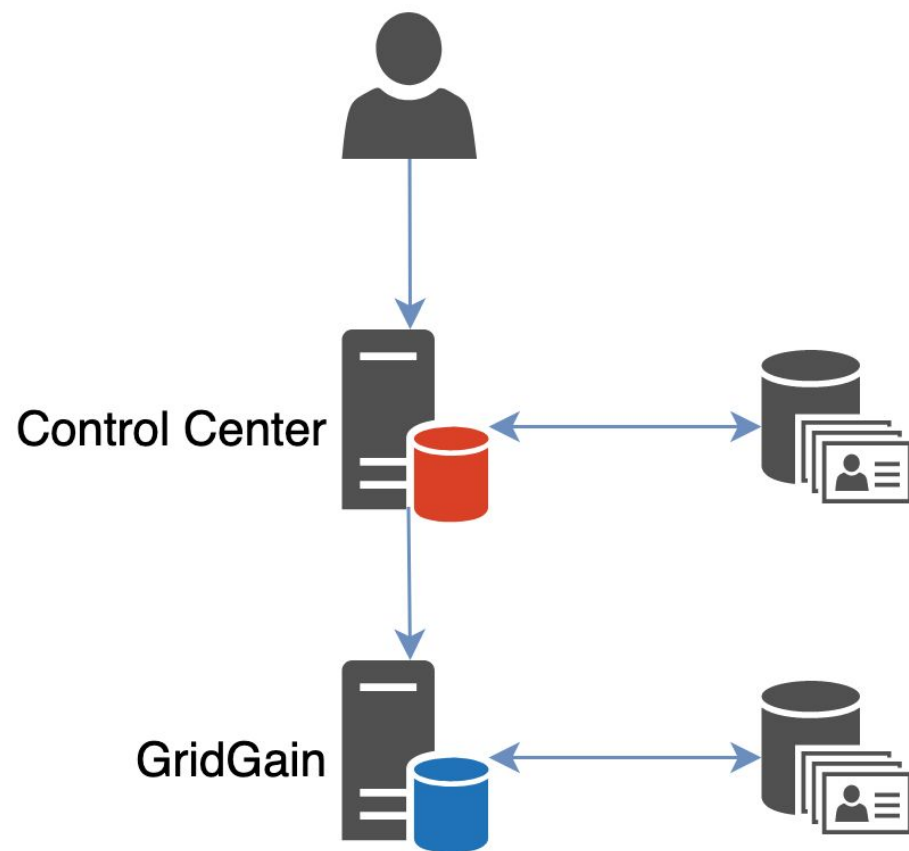
From 📅

To 📅

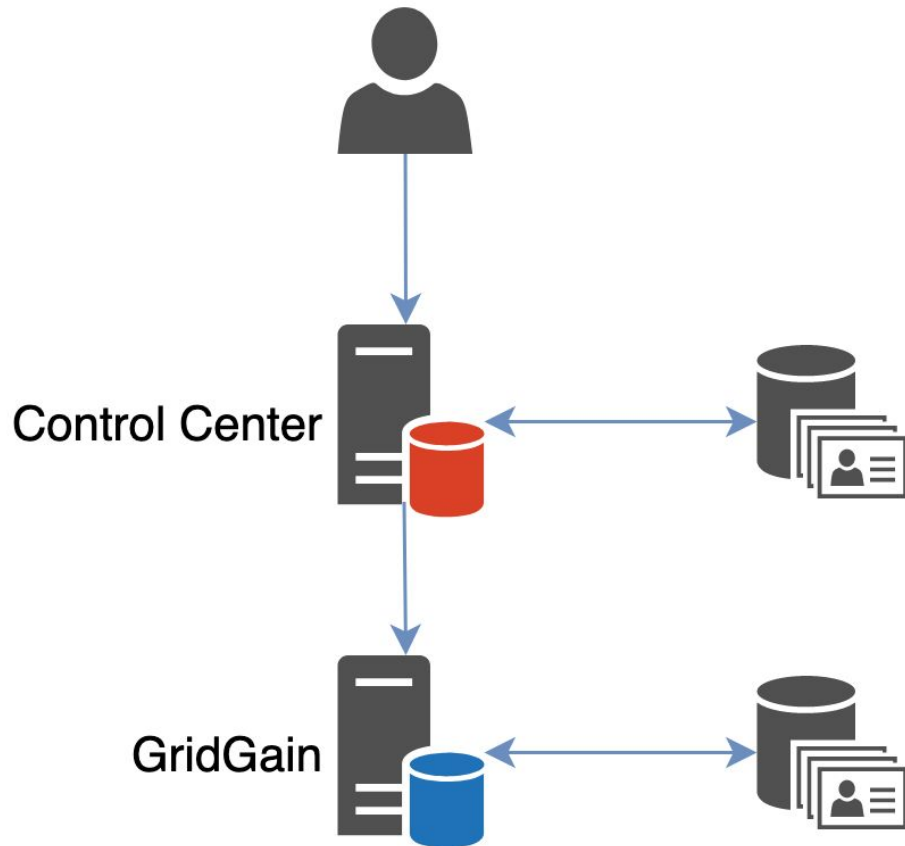
Demo. Control Center



Demo #1: Separate users storage

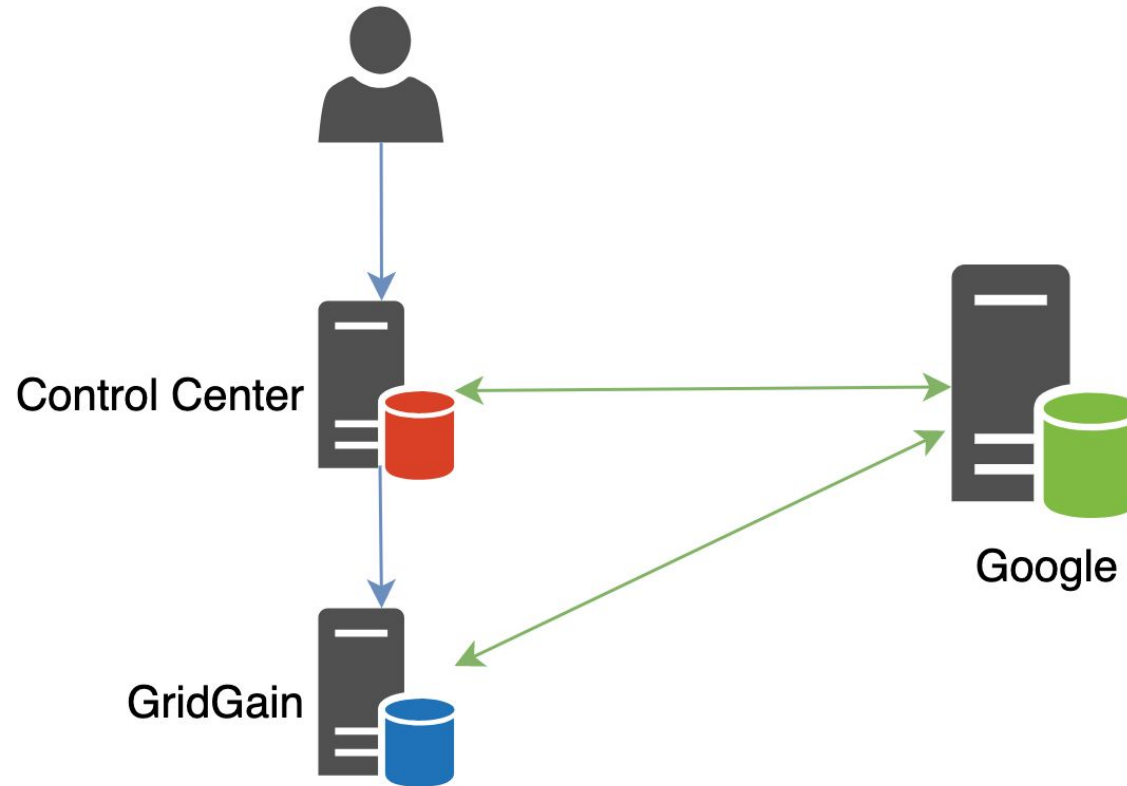


Demo #1: Separate users storage

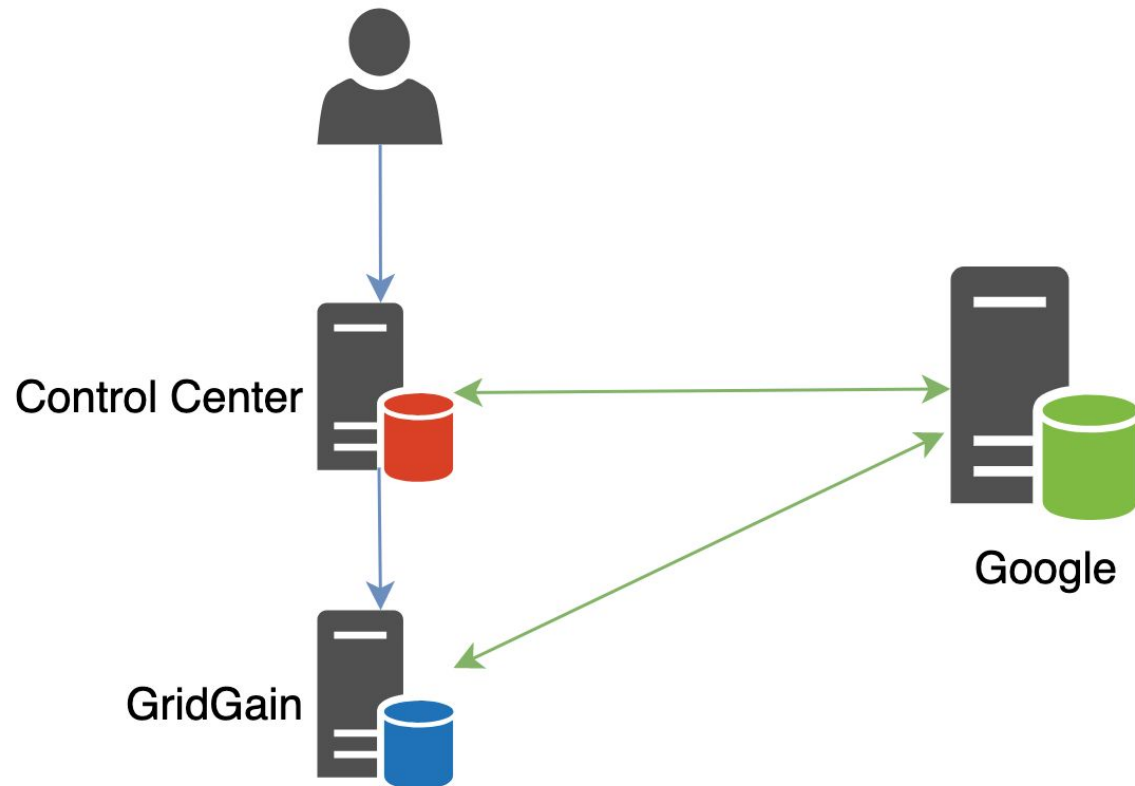


- ! Control Center and GridGain have different sets of users
- ! Repetitive password requests

Demo #2: Centralized users storage

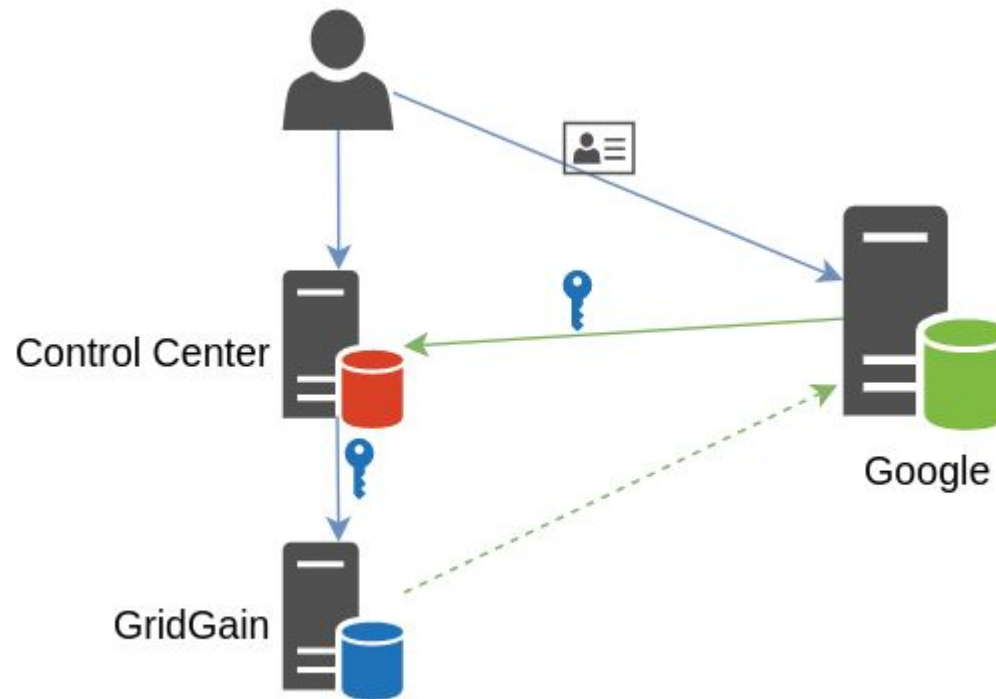


Demo #2: Centralized users storage

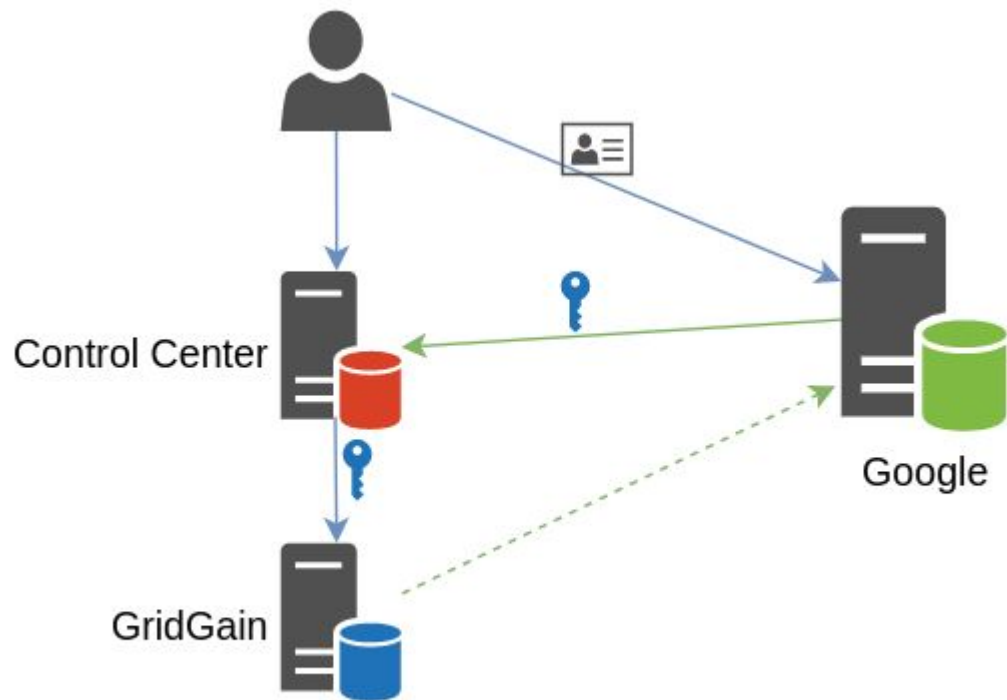


- The same set of users in both systems
- ! Repetitive password requests

Demo #3: Single sign on

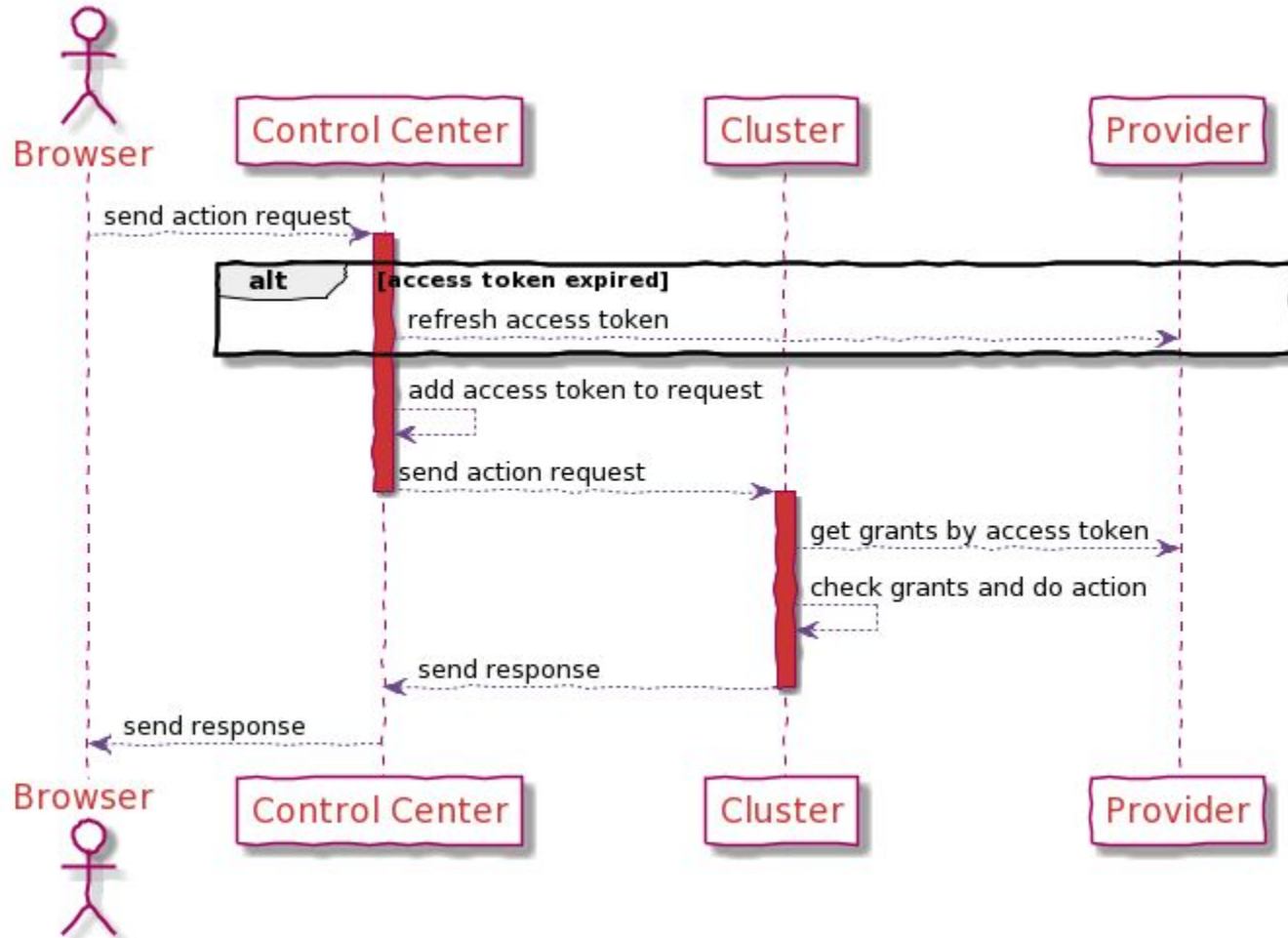


Demo #3: Single sign on

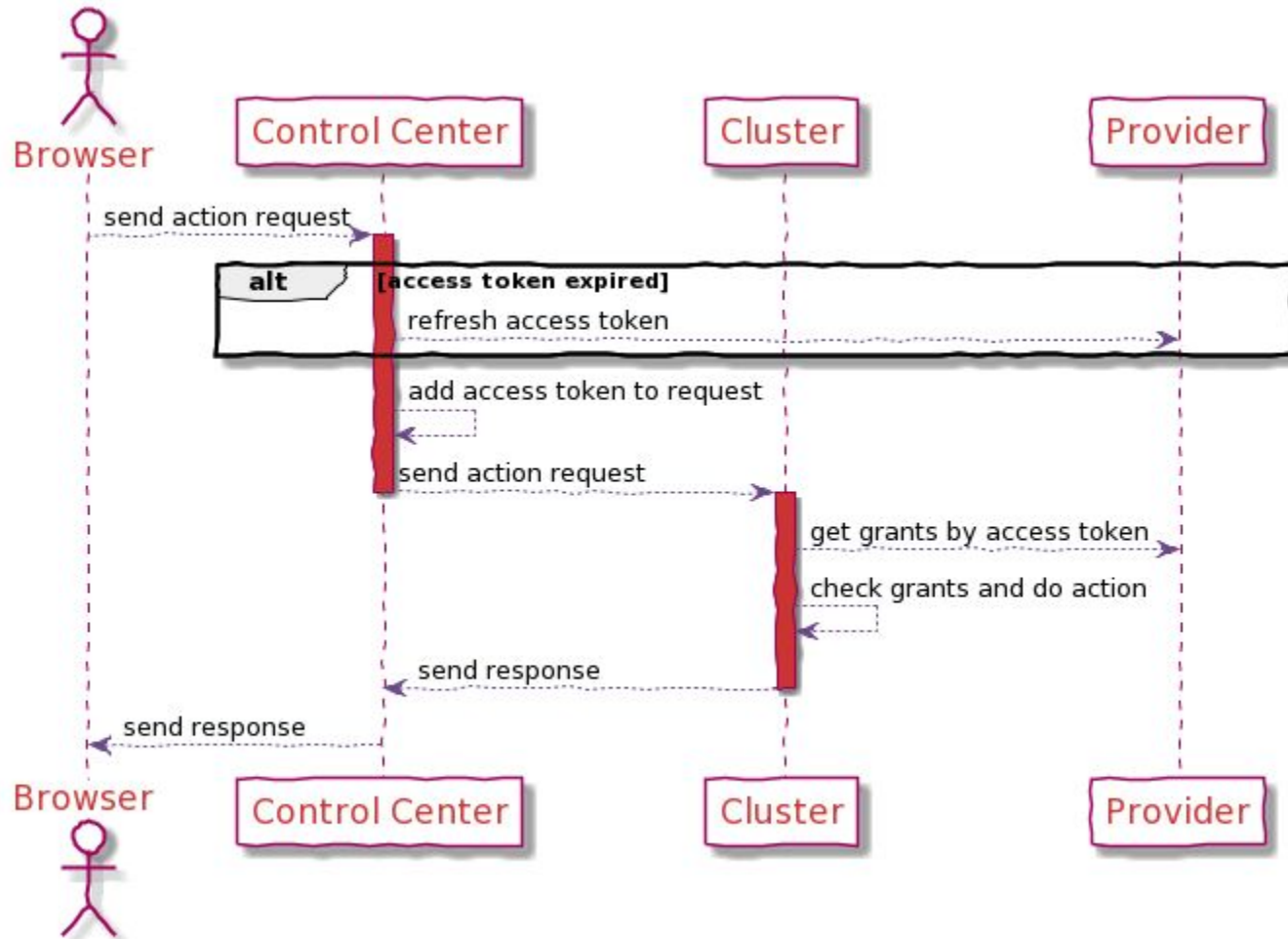


- The same set of users in both systems
- No need to type sign in multiple times

Single sign on flow

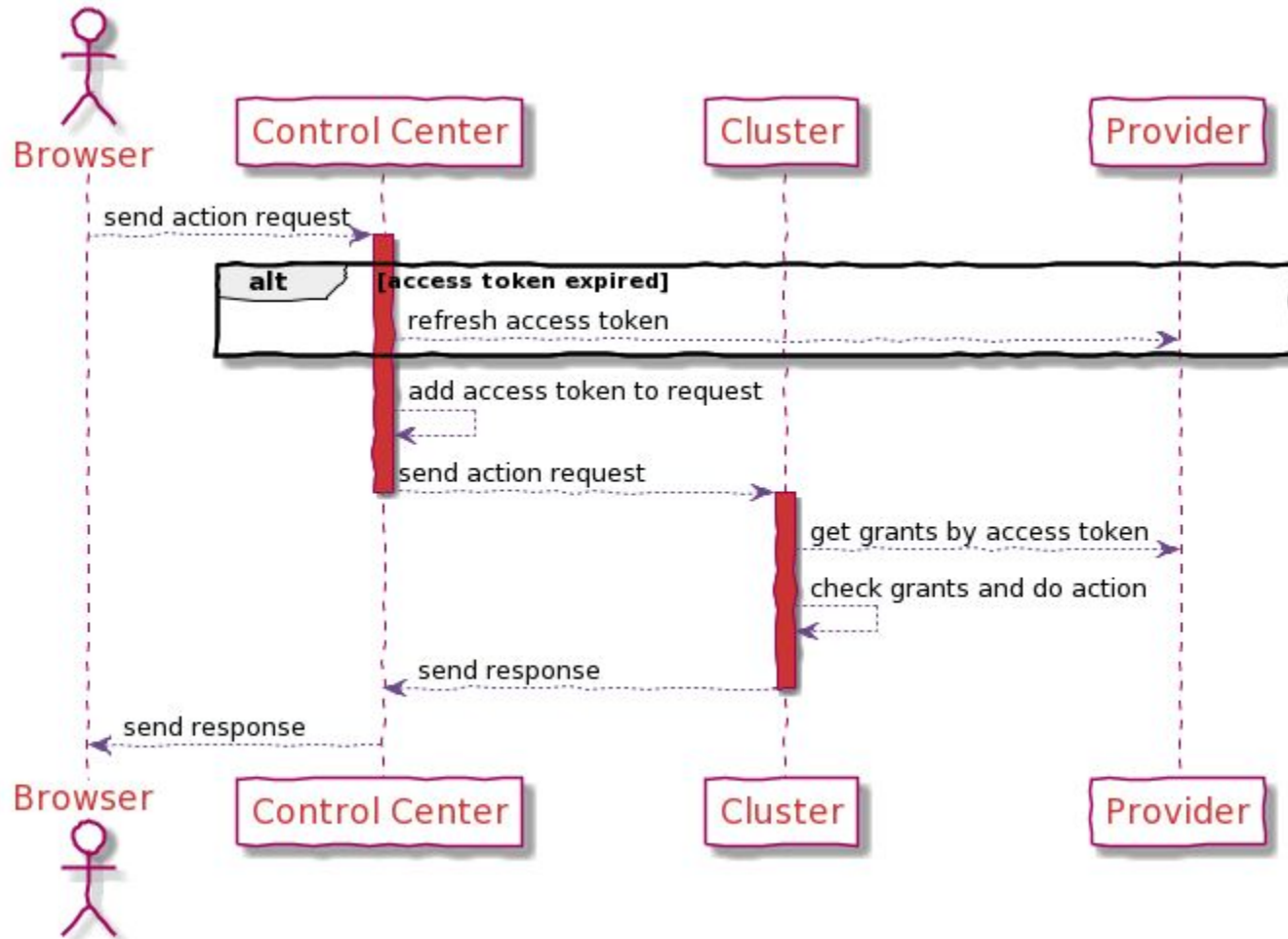


Single sign on flow



```
{
  "login": "firstuser",
  "password": "m5faSDf3",
  "userObject": null
}
```

Single sign on flow



```
{
  "login": null,
  "password": null,
  "userObject": {
    "tokenType": "Bearer",
    "accessToken": "S1AV32hkKG"
  }
}
```

GridGain Authenticator



- Responsible for users authentication in the cluster
- Possible to extend to support authorization
- Available in GridGain Enterprise+

<https://github.com/GridGain-Demos/gridgain-oauth2-authenticator-example/>

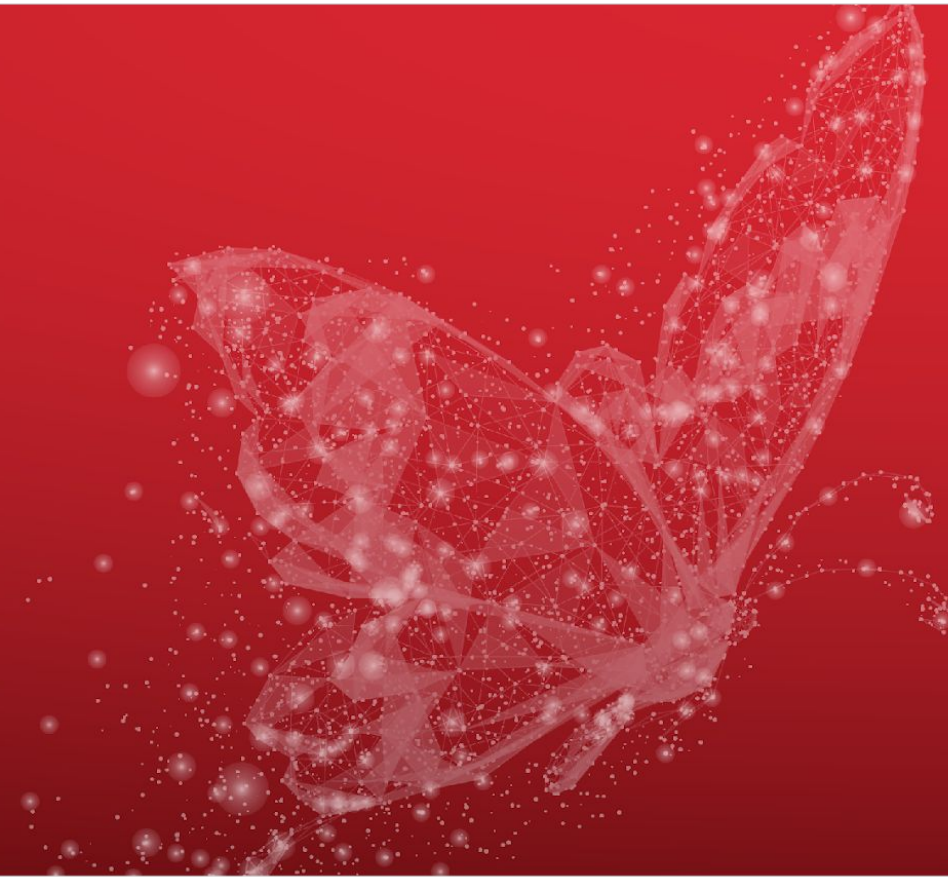
OpenID Connect. Required steps.



- Register your application at the provider
 - Specify the redirect URL
- Specify the properties:
 - Client id
 - Client secret
 - Authorization URI
 - Token URI
 - JWK set URI

Demo

Adding another provider



Single sign on



! The setup is trickier

- Users management is more convenient
- The same credentials for the cluster and Control Center
- No repetitive identity checks
- Sessions are stored on the provider's side

Control Center plans



- OAuth2 Authenticator
- More providers
- LDAP



Thank you!

Denis Mekhanikov

Team Lead @ GridGain Cloud Team
dmekhanikov@gridgain.com

Alexander Kozhenkov

Software Engineer @ GridGain Cloud Team
akozhenkov@gridgain.com

