



Building Secure Rest Architectures With ORDS

Tech17

Luis Rodríguez Fernández

04/12/2017

Agenda

About your speaker

About CERN

ORDS. What?

ORDS@CERN

Do It Yourself!

ORDS Security

Basic authentication

OAUTH2-based Authentication

Conclusions



Agenda

About your speaker

About CERN

ORDS. What?

ORDS@CERN

Do It Yourself!

ORDS Security

Basic authentication

OAuth2-based Authentication

Conclusions



About your speaker

Asturias, Spain
Computing Engineer
Java & Middleware
CERN openlab staff (Oracle)
Public-private partnership
CERN IT-DB-IMS
Oracle Weblogic Applications
Java, APEX, ORDS, Forms
DB infrastructure support
Third party applications
Alfresco (CMS), Pentaho (BI)
Infor (EAM),...

| Service Availability Overview 29 Nov, 2017 10:15 | | | | | | | | | | | | |
|--|---------------------------------------|-----------------------------|-----------------------------------|--------------------------------------|--------------------------------|--------------------------|----------------------------|---------------------|-------------------|------------------|---------------------|----------------|
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| Accelerator Database | ACRON | Administration Database | AFS | AFS Web Hosting | Alerter | Backup and Restore | Batch | BOINC | Service Available | Service Degraded | Service Unavailable | No Information |
| Campus Network | CASTOR | CDS | Centralised Elasticsearch | Ceph | CERN Search | CERNbox | Certificate Authority | CIXP | Service Available | Service Degraded | Service Unavailable | No Information |
| Conference Rooms | Configuration Management | CVMFS | Database on Demand | Database Replication | Databases Applications | Datacenter Network | DFS | Drupal | Service Available | Service Degraded | Service Unavailable | No Information |
| E-Mail | Eduroam | Electronics Design Software | EOS | Experiment Database | E-Fax | File Transfer | FILER | Fixed Line Phone | Service Available | Service Degraded | Service Unavailable | No Information |
| General Purpose Database | Git | GRID Compute Element | GRID Development | GRID Information | GRID Infrastructure Monitoring | HADOOP | HPC | IIS Web Hosting | Service Available | Service Degraded | Service Unavailable | No Information |
| Indico Event Application Support | JIRA | Linux Operating System | Load Balancing | LXPLUS | Lync | Mathematics Software | Mechanical Design Software | Messaging | Service Available | Service Degraded | Service Unavailable | No Information |
| Monitoring | MultiMedia | MyProxy | Network Database and Registration | Network for Projects and Experiments | PaaS Web Application Hosting | Printing and Copying | Public Information Display | Server Provisioning | Service Available | Service Degraded | Service Unavailable | No Information |
| Sharepoint | Single Sign On and Account Management | SVN | Twiki | VOMS | Windows Desktop | Windows Terminal Servers | | | | | | |



Agenda

About your speaker

About CERN

ORDS. What?

ORDS@CERN

Do It Yourself!

ORDS Security

Basic authentication

OAUTH2-based Authentication

Conclusions



About CERN

Fundamental Research

What is the universe made of?

How did it start?

What matter is made of?

Tools

Accelerators

Detectors

Science for peace

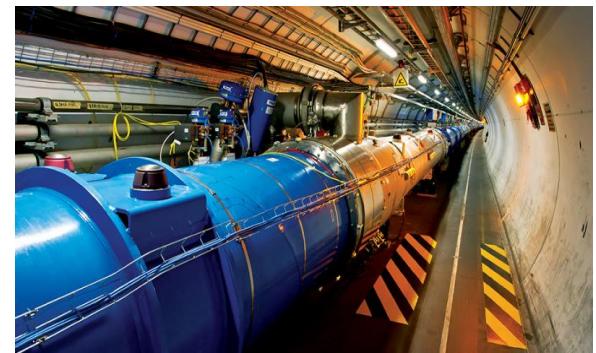
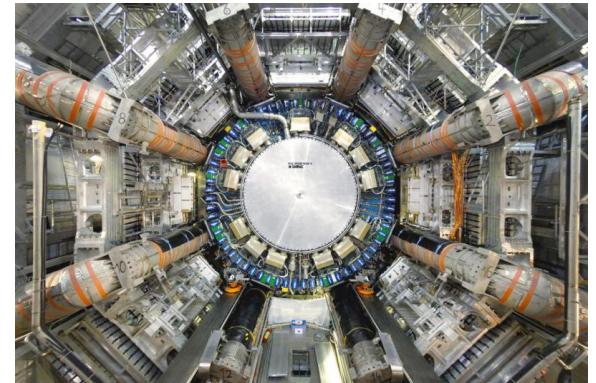
People from all over the world

Three pillars

Research

Innovation

Education



Agenda

About your speaker

About CERN

ORDS. What?

ORDS@CERN

Do It Yourself!

ORDS Security

Basic authentication

OAUTH2-based Authentication

Conclusions



ORDS. What ?

From oracle.com:

“Oracle REST Data Services (ORDS) makes it easy to develop modern REST interfaces for relational data in the Oracle Database, Oracle Database 12c JSON Document Store, and Oracle NoSQL Database. A mid-tier Java application, ORDS maps HTTP(S) verbs (GET, POST, PUT, DELETE, etc.) to database transactions and returns any results formatted using JSON.”

ORDS

GET /employee/64

```
POST /employee  
{  
  "name": "Luis"  
  "lastname": "Rodríguez"  
  .../  
}
```

DELETE /employee/32



Pros

Simple (autorest): automatically expose tables and views

Standalone & Application Server

Back-end APIs directly from PL/SQL

Nice integration with tools like SQLDeveloper

Different authentication methods: basic, OAUTH2



Agenda

About your speaker

About CERN

ORDS. What?

ORDS@CERN

Do It Yourself!

ORDS Security

Basic authentication

OAuth2-based Authentication

Conclusions



ORDS@CERN

15 deployments (dev + test + prod)

Automated configuration & deployment

Potential issue:

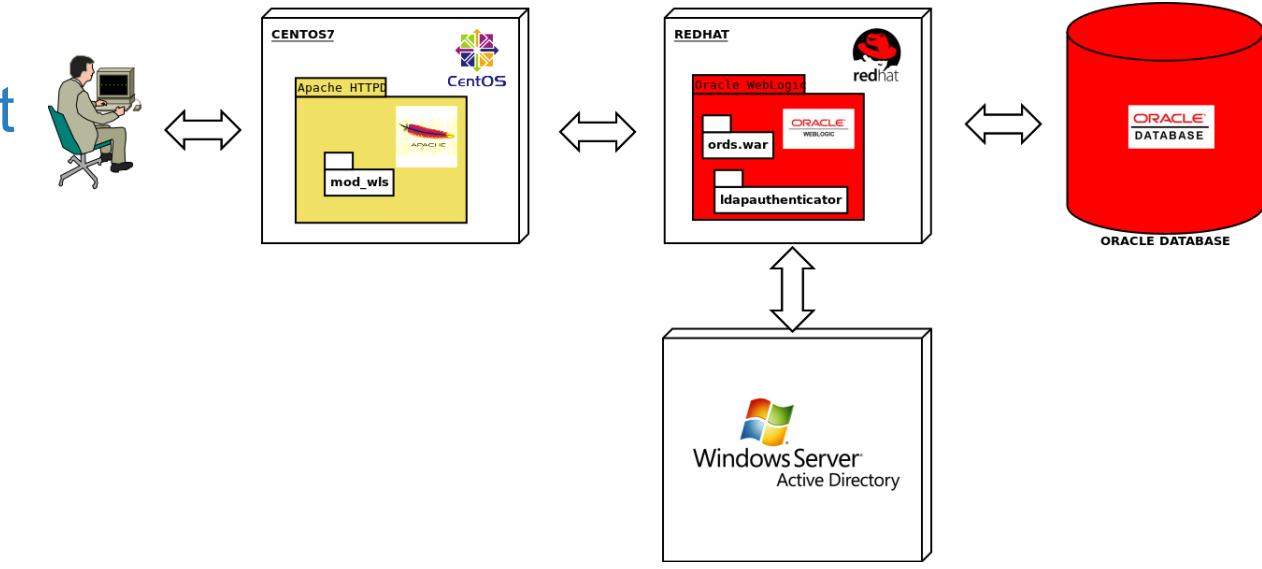
APEX, ORDS, PL/SQL are mixed

Open door to the database

APEX: auth & authz schemas

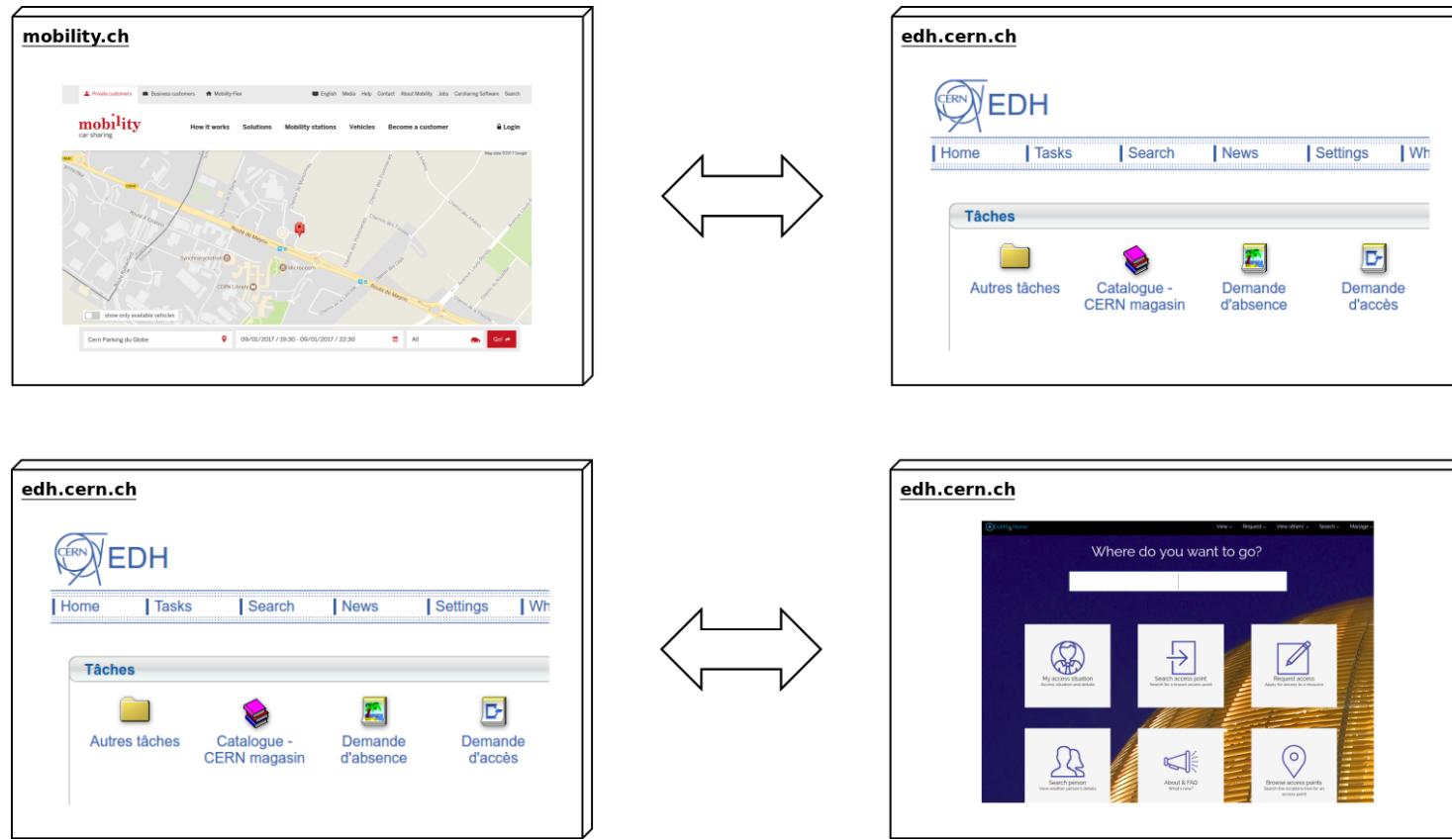
ORDS: basic auth & ORDS

PL/SQL: **custom developments**



ORDS@CERN

mobility.ch checks who can drive their vehicles at CERN (V permit)
edh.cern.ch uses adams.cern.ch services for approval/reject access



Agenda

About your speaker

About CERN

ORDS. What?

ORDS@CERN

Do It Yourself!

ORDS Security

Basic authentication

OAuth2-based Authentication

Conclusions

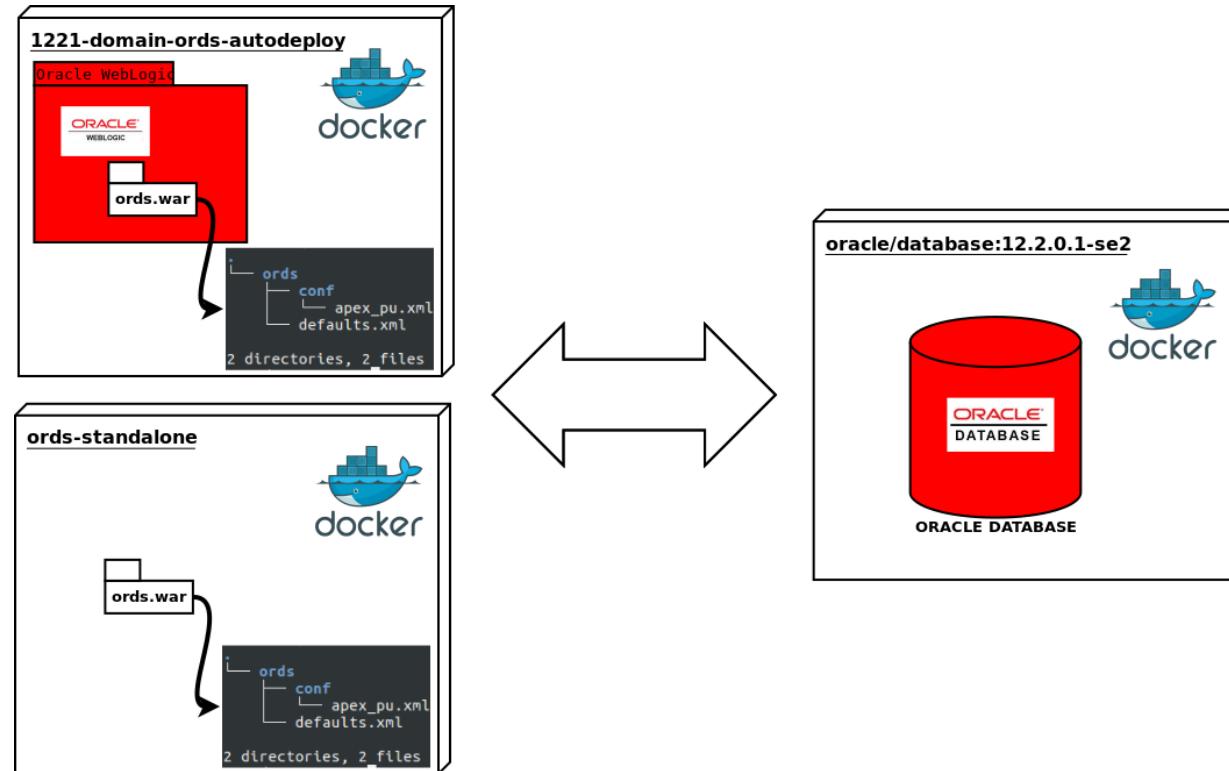


Do It Yourself !

Docker to the rescue!

Demo:

<https://github.com/cerndb/oracle-weblogic-1221-domain-ords-autodeploy>



Do It Yourself !

<entry key="debug.debugger">true</entry>

Tip: increase ORDS logging level
oracle.dbtools=FINEST

| | |
|--|---|
| Minimum severity to log: <input type="button" value="Trace"/> | The minimum severity of log messages going to all log destinations. More Info... |
| Logger severity properties: <input type="button" value="oracle.dbtools=FINEST"/> | The configuration of the different logger severities keyed by name. The values are one of the predefined Severity strings namely Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug, Trace. More Info... |
| Platform Logger Levels: oracle.dbtools=FINEST | Specifies the platform logger and the associated level names set through the WebLogic Server configuration. More Info... |

Agenda

About your speaker

About CERN

ORDS. What?

ORDS@CERN

Do It Yourself!

ORDS Security

Basic authentication

OAuth2-based Authentication

Conclusions



ORDS Security

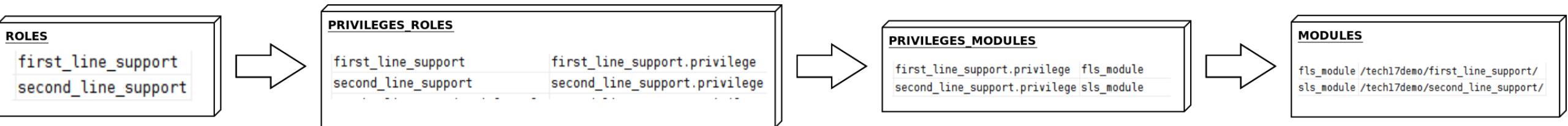
Key concepts:

Role: defines the user position/purpose in our application/system

Privilege: defines who (roles) can access what (urls)

Declared in the DB side

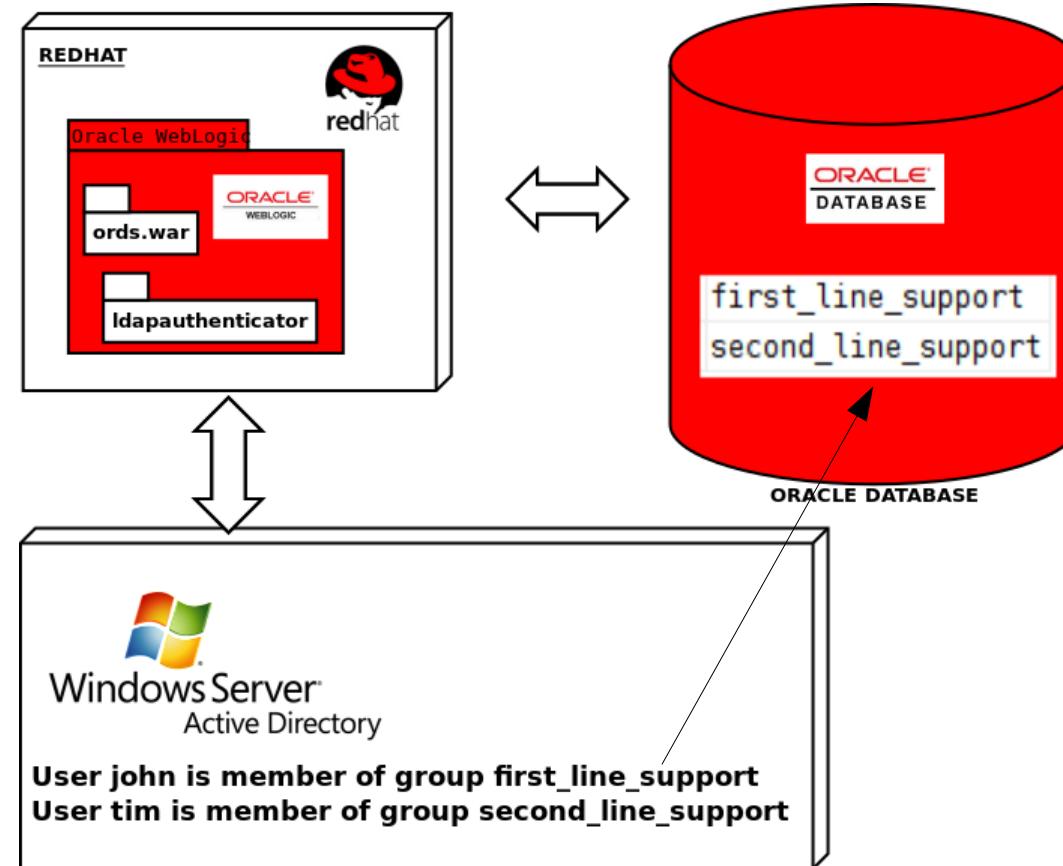
Module: way of grouping resources (urls)



ORDS Security

Users directory configured in the JAVA mid-tier

User's groups on mid-tier mapped to roles in the DB side



ORDS Security

Previous configuration says:

Members of ***first_line_support*** can access resources mapped against ***/tech17demo/first_line_support***

Members of ***second_line_support*** can access resources mapped against ***/tech17demo/second_line_support***

ORDS Security

TIP: show roles, privileges and mappings (url)

```
SELECT * FROM ORDS_METADATA.USER_ORDS_ROLES;
```

```
SELECT * FROM ORDS_METADATA.USER_ORDS_PRIVILEGES;
```

```
SELECT * FROM ORDS_METADATA.USER_ORDS_MODULES;
```

```
SELECT * FROM ORDS_METADATA.USER_ORDS_PRIVILEGE_ROLES;
```

```
SELECT * FROM ORDS_METADATA.USER_ORDS_PRIVILEGE_MODULES;
```

Agenda

About your speaker

About CERN

ORDS. What?

ORDS@CERN

Do It Yourself!

ORDS Security

Basic authentication

OAuth2-based Authentication

Conclusions



Basic Authentication

Non authenticated users are challenged for credentials

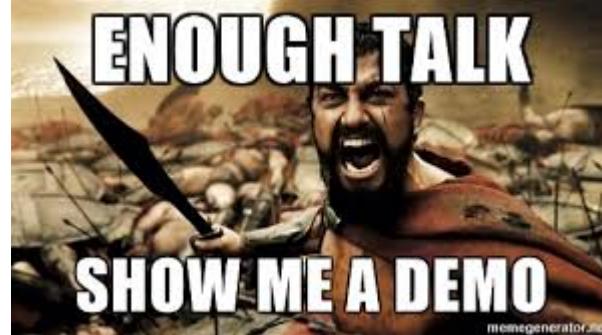
Default ORDS sign in form

Users Directory configured on the Java Mid-tier

ORDS checks user **principals** against **roles** in DB



Basic Authentication



Scenario

`first_line_support` users:

- Can read/update only the name and lastname of a customer

- Can not delete customers with `financial_statement_status` in RED

`second_line_support` users:

- Full access rights

Basic Authentication

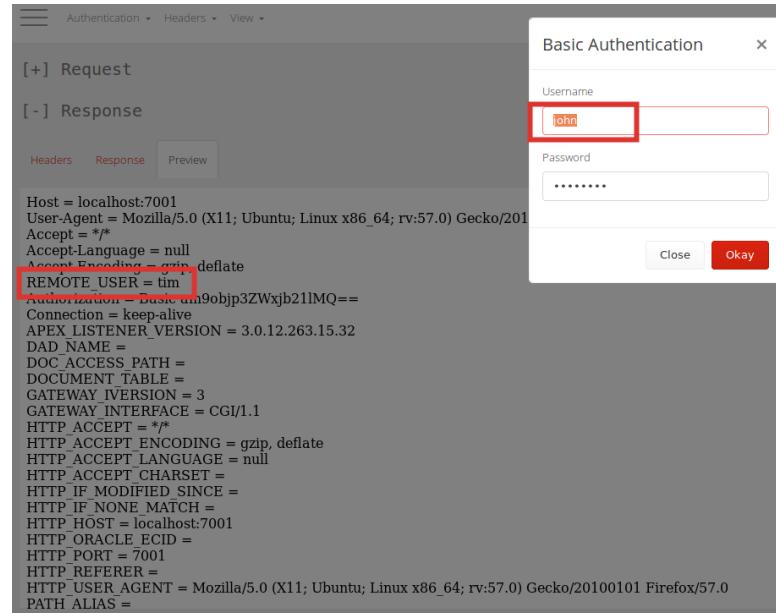
Question?

How to get user's principals on the DB side (PL/SQL)

```
SYS.OWA_UTIL.GET_CGI_ENV('REMOTE_USER');
```

Careful! It can be spoofed:

```
$curl -H "REMOTE_USER: tim"
```



Basic Authentication

Issue

User is member of ~300 groups

ORDS sign-in form throws an exception:

```
<Choosing: oracle.dbtools.http.dispatch.DispatchMetaData as current candidate with score: MetaDataScore  
[matchedMethod=      GET: protected void  
oracle.dbtools.signin.SignInForm.doGet(javax.servlet.http.HttpServletRequest,javax.servlet.http.HttpServletResponse) throws javax.servlet.ServletException,java.io.IOException
```

Agenda

About your speaker

About CERN

ORDS. What?

ORDS@CERN

Do It Yourself!

ORDS Security

Basic authentication

OAUTH2-based Authentication

Conclusions



OAUTH2-based Authentication

OAUTH2 in a nutshell

Security framework **Authorization**

Access Tokens + HTTPS

Actors:

Resource owner

Resource server (protected)

Client

Authorization Server



OAUTH2-based Authentication

OAUTH2. The Valet Parking Analogy

Car owner → Resource owner

Car owner → Authz server

Car → Protected resource

Parking Attendant → Client

Valet Key → Access token



OAUTH2-based Authentication

OAUTH2. The Valet Parking Analogy

Resource owner → ORDS

Authorization server → ORDS

Protected resource → Service

Client → User app

Valet Key → Access token

ORDS supports 3 different authorization grants

Client Credentials

Implicit

Authorization Code



ORACLE®

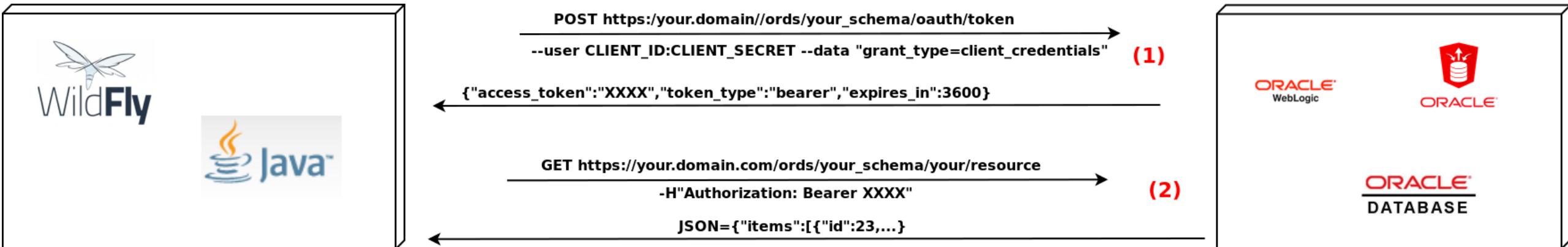
OAUT2-based Authentication

OAUT2. Client Credentials grant

Server side applications: e.g. servlet

Client secret can be stored by the application

No need for human interaction



OAUTH2-based Authentication

Client

Granted with the needed role



OAUTH2-based Authentication



Scenario

Servlet application wants to access a list of resources

Client credentials grant

<https://github.com/cerndb/oauth2-ords-client>

OAUT2-based Authentication

TIP: show client info, privileges and roles

```
SELECT * FROM ORDS_METADATA.USER_ORDS_CLIENTS;
```

```
SELECT * FROM ORDS_METADATA.USER_ORDS_CLIENT_PRIVILEGES;
```

```
SELECT * FROM ORDS_METADATA.USER_ORDS_CLIENT_ROLES;
```

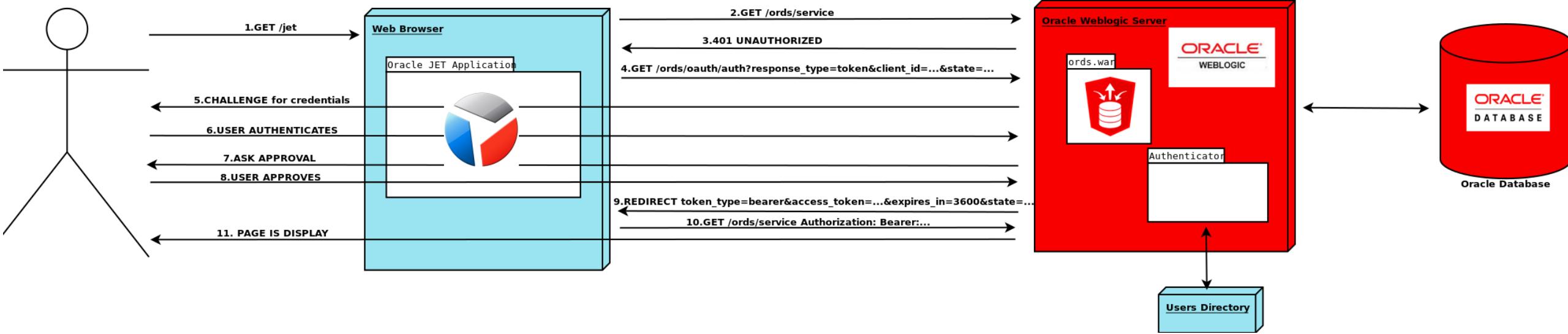
OAUTH2-based Authentication

OAUTH2. Implicit grant

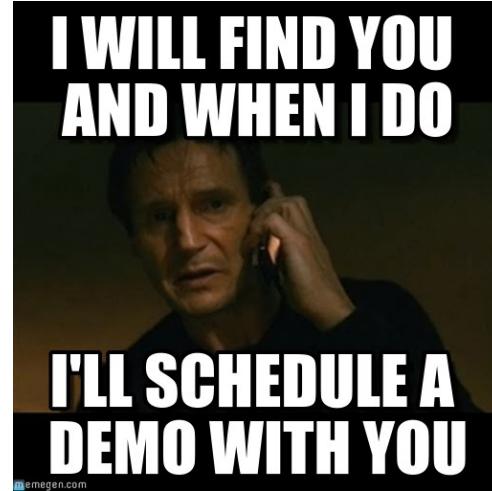
Client side applications: e.g. javascript, mobile

Client secret can not be stored by the application

User will be challenged for credentials



OAUTH2-based Authentication



Scenario

Oracle JET application wants to show a list of resources

<https://github.com/cerndb/jet-oauth2-ords>

Agenda

About your speaker

About CERN

ORDS. What?

ORDS@CERN

Do It Yourself!

ORDS Security

Basic authentication

OAuth2-based Authentication

Conclusions



Conclusions

It works!

- Easy and simple REST APIs
- “Slim down” middle tier
- Flexible
 - Standalone & Application Server
 - Different choices for authentication
- Easy to “containerized”

But...

- Sign in form issue
- Fine grained authorization?

Get principals on the PL/SQL? `sys.owa_util.get_cgi_env('REMOTE_USER');`

Warning! It can be override: `$curl -H "REMOTE_USER: BATMAN"...`

My TODO list:

- Investigate validation function



Acknowledgements

Damian Radoslaw Moskalik (CERN)

Use REST & ORDS. CERN IT-DB Database Tutorials

<https://indico.cern.ch/event/672720/contributions/2756384/attachments/1561072/2457613/ORDS.pdf>

Tim Hall (oracle-base.com)

Oracle REST Data Services (ORDS): Authentication

<https://oracle-base.com/articles/misc/oracle-rest-data-services-ords-authentication>

Gerald Venzl (Oracle)

Oracle Database on Docker

<https://github.com/oracle/docker-images/tree/master/OracleDatabase>

Monica Riccelli (Oracle)

Weblogic on Docker

<https://github.com/oracle/docker-images/tree/master/OracleWebLogic>

Martin Giffy D'Souza (talkapex.com)

Oracle REST Data Services on Docker

<https://github.com/oracle/docker-images/tree/master/OracleRestDataServices>



QUESTIONS?

luis.rodriguez.fernandez@cern.ch

CONTACTS

ALBERTO DI MEGLIO

CERN openlab Head

alberto.di.meglio@cern.ch

MARIA GIRONE

CERN openlab CTO

maria.girone@cern.ch

FONS RADEMAKERS

CERN openlab CRO

fons.rademakers@cern.ch

ANDREW PURCELL

CERN openlab Communications Officer

andrew.purcell@cern.ch

KRISTINA GUNNE

CERN openlab Administration/Finance Officer

kristina.gunne@cern.ch



www.cern.ch/openlab