oVirt

oVirt SSO

Artur Socha
Senior Software Engineer
@ Red Hat

09/2020

Agenda

- Authentication, Authorization and Accounting (AAA)
  - Authentication
  - Authorization
  - Accounting / Federated Identity Management
  - JSON Web Token (JWT)
- Single Sign-On (SSO)
  - OAuth 2.0
  - Kerberos + LDAP
  - External OpenID Connect Identity Provider (IDP)
- Keycloak & oVirt Engine from scratch - live session

AAA - oVirt engine

AAA - oVirt engine

AAA: **Authentication** provides the answer for the question:

- ***“who you are”***

AAA - oVirt engine

AAA: **Authentication** provides the answer for the question:

- ***“who you are”***

Some of (web) authentication methods:

- HTTP basic (*plain-ish* username/passwd)
- HTTP digest (hash from credentials)
- Bearer authentication (token authentication)
- X.509 certificates
- Custom (biometrics, hybrid, multiple factor authentication … sky is the limit)

AAA - oVirt engine

AAA: **Authentication** provides the answer for the question:

- *“who you are”*

AAA: **Authorization** provides the answer for the question:

- *“what you are allowed to do”*

AAA - oVirt engine

AAA: **Authentication** provides the answer for the question:

- *“who you are”*

Fine grained permission management not a part of this session

AAA: ~~**Authorization** provides the answer for the question:~~

- ~~*“what you are allowed to do”*~~

AAA - oVirt engine

AAA: **Authentication** provides the answer for the question:

- *"who you are"*

Fine grained permission management not a part of this session

AAA: ~~**Authorization** provides the answer for the question:~~

- ~~*"what you are allowed to do"*~~

… but I will cover "**what parts of oVirt Engine you are allowed to access**"

AAA - oVirt engine

AA**A**: Accounting ~ Federated Identity Management for oVirt Manager

- DB (JDBC) `ovirt-aaa-jdbc-tool`

AAA - oVirt engine

AA**A**: Accounting ~ Federated Identity Management for oVirt Manager

- DB (JDBC) `ovirt-aaa-jdbc-tool`
- Directory Servers
  - https://www.ovirt.org/documentation/administration_guide/#Introduction_to_Directory_Servers

AAA - oVirt engine

AA**A**: Accounting ~ Federated Identity Management for oVirt Manager

- DB (JDBC) `ovirt-aaa-jdbc-tool`
- Directory Servers
  - https://www.ovirt.org/documentation/administration_guide/#Introduction_to_Directory_Servers

```
Available LDAP implementations:
 1 - 389ds
 2 - 389ds RFC-2307 Schema
 3 - Active Directory
 4 - IBM Security Directory Server
 5 - IBM Security Directory Server RFC-2307
Schema
 6 - IPA
 7 - Novell eDirectory RFC-2307 Schema
 8 - OpenLDAP RFC-2307 Schema
 9 - OpenLDAP Standard Schema
10 - Oracle Unified Directory RFC-2307 Schema
11 - RFC-2307 Schema (Generic)
12 - RHDS
13 - RHDS RFC-2307 Schema
14 - iPlanet
```

AAA - oVirt engine

AA**A**: Accounting ~ Federated Identity Management for oVirt Manager

- DB (JDBC) `ovirt-aaa-jdbc-tool`
- Directory Servers
  - https://www.ovirt.org/documentation/administration_guide/#Introduction_to_Directory_Servers
- External OpenID Connect Identity Provider (IDP)

```
Available LDAP implementations:
 1 - 389ds
 2 - 389ds RFC-2307 Schema
 3 - Active Directory
 4 - IBM Security Directory Server
 5 - IBM Security Directory Server RFC-2307
Schema
 6 - IPA
 7 - Novell eDirectory RFC-2307 Schema
 8 - OpenLDAP RFC-2307 Schema
 9 - OpenLDAP Standard Schema
10 - Oracle Unified Directory RFC-2307 Schema
11 - RFC-2307 Schema (Generic)
12 - RHDS
13 - RHDS RFC-2307 Schema
14 - iPlanet
```

AAA - oVirt engine

AAA: Authentication & Authorization

Some of (web) authentication methods:

- Bearer authentication (token authentication) https://tools.ietf.org/html/rfc6750
  - JSON Web Token (JWT, https://tools.ietf.org/html/rfc7519)

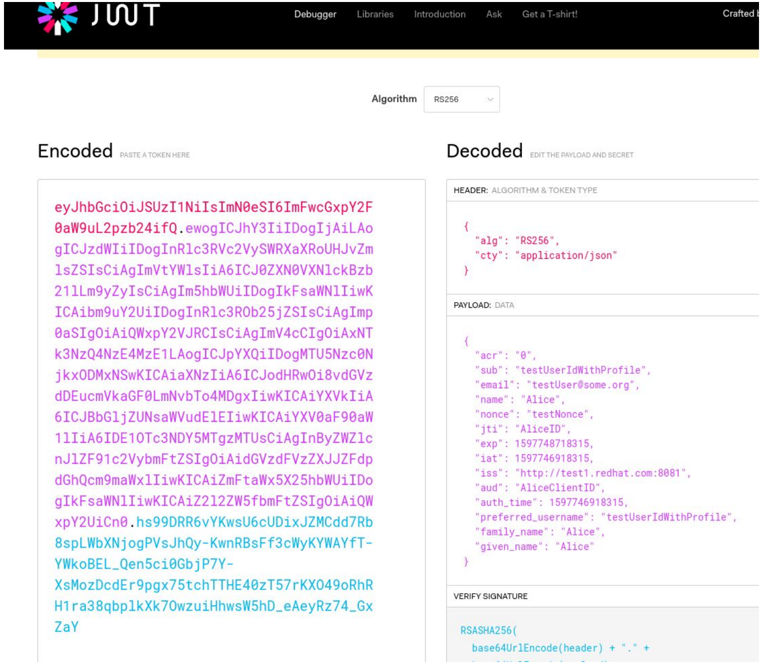
```
(...)is a compact, URL-safe means of representing
   claims to be transferred between two parties.  The claims in a JWT
   are encoded as a JSON object that is used as the payload of a JSON
   Web Signature (JWS) structure or as the plaintext of a JSON Web
   Encryption (JWE) structure, enabling the claims to be digitally
   signed or integrity protected with a Message Authentication Code
   (MAC) and/or encrypted
```

AAA - oVirt engine

AAA: Authentication & Authorization

Some of (web) authentication methods:

- Bearer authentication (token authentication)
  - JSON Web Token (JWT, https://tools.ietf.org/html/rfc7519)



Algorithm RS256

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsImN0eSI6ImFwcGxpY2F
0aW9uL2pzb24ifQ.ewogICJhY3IiIDogIjAiLAo
gICJzdWIiIDogInRlc3RVc2VySWRXaXRoUHJvZm
lsZSIsCiAgImVtYWlsIiA6ICJ0ZXN0VXNlckBzb
21lLm9yZyIsCiAgIm5hbWUiIDogIkFsaWNlIiwK
ICAibm9uY2UiIDogInRlc3ROb25jZSIsCiAgImp
0aSIgOiAiQWxpY2VJRCIsCiAgImV4cCIgOiAxNT
k3NzQ4NzE4MzE1LAogICJpYXQiIDogMTU5Nzc0N
jkxODMxNSwKICAiaXNzIiA6ICJodHRwOi8vdGVz
dDEucmVkaGF0LmNvbTo4MDgxIiwKICAiYXVkIiA
6ICJBbGljZUNsaWVudElEIiwKICAiYXV0aF90aW
1lIiA6IDE1OTc3NDY5MTgzMTUsCiAgInByZWZlc
nJlZF91c2VybmFtZSIgOiAidGVzdFVzZXJJZFdp
dGhQcm9maWxlIiwKICAiZmFtaWx5X25hbWUiIDo
gIkFsaWNlIiwKICAiZ2l2ZW5fbmFtZSIgOiAiQW
xpY2UiCn0.hs99DRR6vYKwsU6cUDixJZMCdd7Rb
8spLWbXNjogPVsJhQy-KwnRBsFf3cWyKYWAYfT-
YWkoBEL_Qen5ci0GbjP7Y-
XsMozDcdEr9pgx75tchTTHE40zT57rKXO49oRhR
H1ra38qbplkXk7OwzuiHhwsW5hD_eAeyRz74_Gx
ZaY
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS256",
  "cty": "application/json"
}
```

PAYLOAD: DATA

```
{
  "acr": "0",
  "sub": "testUserIdWithProfile",
  "email": "testUser@some.org",
  "name": "Alice",
  "nonce": "testNonce",
  "jti": "AliceID",
  "exp": 1597748718315,
  "iat": 1597746918315,
  "iss": "http://test1.redhat.com:8081",
  "aud": "AliceClientID",
  "auth_time": 1597746918315,
  "preferred_username": "testUserIdWithProfile",
  "family_name": "Alice",
  "given_name": "Alice"
}
```

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
```

Single Sign-On (SSO)

SSO

https://en.wikipedia.org/wiki/Single_sign-on

“(...) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.”

SSO - OAUTH 2.0

https://oauth.net/2/

“(...) authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.”

SSO - OAUTH 2.0

oVirt engine as OAuth 2.0 provider

- Minimal Viable ~~Product~~ Support
- Refresh tokens https://tools.ietf.org/html/rfc6749#section-1.5
- Revoke tokens https://tools.ietf.org/html/rfc7009
- Supports UI and Restful API http://ovirt.github.io/ovirt-engine-api-model/master/#_authentication
  - Rest API Clients: Java, Python, Ruby, Curl

SSO - Kerberos + LDAP

https://www.ovirt.org/documentation/administration_guide/#Configuring_LDAP_and_Kerberos_for_Single_Sign-on

- ovirt-engine-extension-aaa-ldap
- Apache modules
  - mod_auth_gssapi
  - mod_session

SSO - external IDP

IDP: OpenID Connect Identity Provider (IDP)

Configurable via extension API:

- `ovirt-engine-extension-aaa-misc`
- `mod_auth_openidc`

Documentation needs improvement, but there is:

- Ongoing work
- Ravi’s blog post: https://blogs.ovirt.org/2019/01/federate-ovirt-engine-authentication-to-openid-connect-infrastructure/
    - Valid for 4.3, in 4.4 some config changes required
    - Based on Keycloak version <= 9, >10 currently not supported

SSO - external IDP

Keycloak https://www.keycloak.org/about.html

“Keycloak is an open source Identity and Access Management solution aimed at modern applications and services.”

- **SSO**
- **Identity brokering** and social login
- User Federation (ver 9.x **LDAP, Kerberos**), others can be implemented
- **OpenID Connect**, SAML
- **GUI admin console**, Rest API

Live session

Live session

- Topology & setup
  - Ovirt engine host:
    - `enginedemo.workstation.dom`
  - Keycloak host:
    - `sso.workstation.dom`
    - `Https endpoint on 8443`
    - `Http endpoint on 8080`
  - Poor man’s DNS aka. `/etc/hosts`
- Configuration sources
  - `https://github.com/arso/conferences/tree/master/ovirt.org/2020/ovirt_sso`

oVirt

Thank you!

https://ovirt.org/

users@ovirt.org

@ovirt