OpenAM OpenDJ Questions and Answers

OpenAM OpenDJ Questions and Answers Iteration 1

Custom User Class

Acme wants to use their own custom class rather than the default User object.

1. What is the opinion on this?
2. Is 2Keys doing this?
3. What are the minimal attributes required by OpenAm.

> It is strongly recommended to use the default User object and extend by adding custom attributes. This is an established schema in information security and will provide maximum future compatibility and sensibility. In regards to concerns raised by the Acme,
>
> - Extra data muddling the view.
>   - Almost all LDAP browsers including the OpenDJ Control Panel default to hide extra information - "Only Show Attributes with Values".
> - Performance
>   - By design, there would not be any impact to performance. This is proven in Production environments as the default User object is used by large FI's and Governments.
>
> 2Keys Ottawa uses the standard User object and adds custom object class to hold their own specific attributes. 2Keys Toronto, also uses the following techniques for PKI systems with our FI clients.
>
> If taking this approach, Acme should account for extra development and consider becoming familiar with OpenAM source code.
>
> The minimal attributes required is problematic if it will be used to create a new custom class. 2Keys can recommend certain fields being disabled but can not guarantee that they will not be used in the future by OpenAM. If Acme takes this approach, it is recommended to also scan the source code of OpenAM and OpenDJ at when upgrading to new release to ensure the fields are not being used.

User States

Acme wants a two step registration process. Sign up (where user name and password set) and then actual activation where the user verifies the provided email is valid via a url.

Usage scenario, user only signed up, but did not activate. User goes to website and puts credentials. User should see "please check your email and click on the activate link".

What is the recommended approach to dealing with the user in these states and additional states like disabled with OpenAM? What attributes should be used? Can OpenAM be used to direct the user to the appropriate page. Is this all configurable on OpenAM and if so where is this configured

> Acme can use the Post-Authentication Plug-In and there might already be one available for two step registration that can be dropped in.
>
> Also, consider the the OTP (One Time Password) approach. See the article OpenSSO One Time Password Authentication is the One That I Want for more details.

OpenAM Dynamic Rules to Protect Content

Acme will have some articles initially put forth as free content for x days. When expired, the content should only be available to Premium paid

customers. Can this be achieved with OpenAM and controlled from OpenAM via configuration files (not hard coded)?

> Options undergoing discussion.

SSO Cookie Not Being Set

Acme has observed that in their Dev there is no iplanet SSO cookie being set. Acme observed that their generic vanilla does create the SSO cookie.

> The iplanet SSO cookie defined in **com.iplanet.am.cookie.name=iPlanetDirectoryPro** stored in **/opt/openam-agents/j2ee_agents/tomcat_v6_agent/Agent_001/config/OpenSSOAgentConfiguration.properties**.
>
> 2Keys confirms that our own implementations do generate the iPlanetDirectoryPro cookie for example,
>
> acme.com (site being protected)
>
> 1. AMAuthCookie
> 2. amlbcookie
> 3. iPlanetDirectoryPro
>
> openam.2keys.com (login site)
>
> 1. JSESSIONID
>
> Recently (2021-03-30 ~ 10am) tested the Acme dev environment and the iPlanetDirectoryPro cookie is showing. Closing this case.

How Does Caching Work with OpenAM

Acme is planning on using Akamai and/or Varnish to cache their content. How will OpenAM work with these caching solutions? Does 2Keys or the Government sites being protected use caching?

> Currently even with load, 2Keys systems do not require caching. If they did, 2Keys would take the approach of placing the cached content behind OpenAM. This would require
>
> 1. Using OpenAm compatible caching technology
> 2. Working with ForgeRock to certify a mutually selected caching technology

Using Cassandra in Place of OpenDJ

Acme currently uses Cassandra a NOSQL database as their preferred data store.

Acme would like to know if there are any real world examples of using Cassandra or equivalent in place of OpenDJ.

Please also provide opinions and recommendations about this approach.

> 2Keys has not encountered any real world examples of Cassandra as a directory. 2Keys has also not encountered any companies successfully converting a non-directory based database into a LDAP directory.
>
> In regards to opinions, specifically with OpenAM and Cassandra it is technically feasible to write a custom authentication module. Customization would also be required for OpenAM as we believe it only has consideration for directories and traditional relational databases.
>
> First if taking this route, it is recommended to keep the authentication data from the customer data logically and if possible physically.
>
> A true LDAP directory has the following core features that make it compelling and still used today for authentication,
>
> 1. Fast Queries
> 2. Replication
> 3. Partition-able
> 4. LDAP Protocal
>
> 2Keys recommends that Acme ensure that Casssandra can match the first 3 requirements. Also, if possible consider adding LDAP functionality to Cassandra to increase compatibility as many systems use LDAP for authentication.
>
> As a side-note, even most SQL databases do not meet this criteria and changing the backend database is not officially supported. An OpenDJ engineer provides his reasoning here.

Log Auth and Related OpenAM Activity to External File

Acme would like to record most importantly authentication events into a database. Acme research shows that a plug-in needs to be used,

1. Is this the best way?
2. Can we supply an example of how to write (can be to our own file), test and deploy?

> Acme can configure OpenAM to log to a database. 2Keys will check whether it is a global setting for all logs or per log group.
>
> 2Keys can also provide code samples for a post authentication plugin.

Delays When Changing User Properties

Acme has experience delays where changes (adding user to a group, adding a new user) does not happen right away. In some cases, a manual intervention is required using the OpenAM console to force a refresh. Has the 2Keys team experienced this behaviour? Any ideas on what could cause this?

Acme, has mentioned that this was not experienced this with a vanilla install.

> There should not be any delay. 2Keys will need details on how the system is configured. Because the system is still at an early stage, it is recommended to rebuild the environment and add customization one at a time. 2Keys can also provide some oversight to verify the environment build and the customization applied.

Session Fail Over

Acme is looking for lessons learned and any material we have on setting up fail over.

1. Can 2Keys provide enhanced setup instructions (OpenAM documentation experience has not been positive)
2. Instructions on handling fail over scenarios (for example, Is it automatic? Do we need to specify a new master?)

> Yes 2Keys can provide enhanced setup instructions and the architecture used at 2Keys.
>
> With OpenAM the fail over scenario is automatic. However, with OpenDJ there are some steps that will need to be taken during setup to define the architecture. 2Keys has 5 subject matter expert staff (3 in Toronto, 3 in Ottawa) for directories and as such do not have the process documented non security experts. However, we can put together the documentation for the Acme.

Confirm OpenAM Use Back Channel for Authentication?

Can we confirm that OpenAM uses a back channel for authentication?

> Based on the Oracle Using a Single Policy Agent article, 2Keys believes that OpenAM does use back channel for agent based authentication.
>
> 2Keys Ottawa requires a followup discussion with Toronto for more details on how other authentication models are being used.

Is OpenAM Non-Sticky

Acme would like to confirm that OpenAM is non-sticky by default and if not,

- Can OpenAM manage non-sticky?
- Can a session login from two locations?
- Running from a different machine, will the SSO token be the same or different? Acme assumes different but wants to be sure. This question is related to the case of expired articles that move from public to premium locations on different devices

> Overall the model is for most implementation and yes a session can log in from two different locations.
>
> Different machines are different sessions. It is configurable to allow concurrent logins, how many allowed and what happens when the limit is reached.
>
> More details will summarized by the team next week.

Add User to Group

When the REST API is used to add a user to the group list, it resets the group list to just the one user. Ticket RPU-317174 was opened up by the Acme on this topic. ForgeRock's response was this is not part of LDAP and you can't even do this in LDIF.

The response from Rockforge as follows,

Click here to expand...

> Hi Dmitry, I know the task seems to be simple at first site, but 'update' could also mean assign the member to this group only.

Looking at how this would be done in LDAP is similar, if you just replace the uniquemember attribute of the static group all others would be removed.

'LDIF' for this ...

dn:

changetype: modfiy
replace: uniquemember
uniquemember:

The Acme has to take care that the uniquemember is 'added'.

'LDIF' for this ...

dn:

changetype: modfiy
add: uniquemember
uniquemember:

Currently there's no operation to provide the latter functionality and again you are some kind 'abusing' OpenAM as a 'provisioning tool'.

OpenAM is not an LDAP gateway... it abstracts from the data store.

This will only work correctly if you have only one data store.

Furthermore what would happen if you use a JDBC data store?

I would higly recommend to use the means of the data store to manipulate the identity data and let OpenAM consume this information.

Regards,

Bernhard

2Keys agrees with Acme's assessment and request. 2Keys own experience with groups on other technologies and LDAP does allow appending. 2Keys will raise the issue with the ForgeRock.