OPENNTF WEBINARS

November, 2022
Integrate Keycloak with Domino for Identity Management
Heiko Voigt, sIT GmbH
AGENDA

• Welcome
• Presentation – Heiko Voigt
• Q and A
THANKS TO THE OPENNTF SPONSORS

• HCL made a contribution to help our organization
  • Funds these webinars!
  • Contests like Hackathons
  • Running the organization

• Prominic donates all IT related services
  • Cloud Hosting for OpenNTF
  • Infrastructure management for HCL Domino and Atlassian Servers
  • System Administration for day-to-day operation
THIS IS OUR COMMUNITY

• Join us and get involved!
• We are all volunteers
• No effort is too small
• If your idea is bigger than you can do on your own, we can connect you to a team to work on it
• Test or help or modify an existing project
• Write guides or documentation
• Add reviews on projects / stars on Snippets
DECEMBER HAPPY HOUR

• Join us in December for a virtual Happy Hour!
  • Thursday 15th
  • APAC, Europe, North America
• Watch the web site for details
REPAIR CAFE

• Open chat room to bring your questions / problems / ideas
• Share your tips
• What topics do you want?
  • Use the Discord #suggestion-box

• January 12 – Development Topics
• January 25 – Admin Topics
ASKING QUESTIONS

• First Question – Will this be recorded?
  • Yes, view on YouTube!!!
  • https://www.youtube.com/user/OpenNTF

• Use the Questions Pane in GoToWebinar

• We will get to your questions at the end of the webinar

• The speakers will respond to your questions verbally
  • (not in the Questions pane)

• Please keep all questions related to the topics that our speakers are discussing!!!

• Unrelated Question => post at:
  • https://openntf.org/discord
Integrate Keycloak with Domino for identity management
Heiko Voigt
ABOUT HEIKO

- CEO of SIT GmbH in Germany and Harbour Light Software Development Ltd. in Canada
- Software Architect for 25+ years with N/D, Full-Stack Web Developer
- HCL Ambassador 2019-2022, IBM Champion 2019
- Core Team Member at C3UG and Board Member at OpenNTF
- Proud father of twins
- Sailor, Home brewer

https://www.sit.de
https://www.harbour-light.com
AGENDA

Few things to clear out:

OAUTH2 != Authentication, only Authorization

OpenID Connect = Identity + Authentication + Authorization

What we will cover:
• Keycloak and SAML/Web with Domino (Web + Notes SSO for DS <12.0.2 EA5)
• Keycloak and OIDC/OAUTH2 with AppDevPack and Domino REST APIs
• Keycloak and OIDC/OAUTH2 with Domino >= 12.0.2 EA3
• Keycloak and VERSE / Nomad Web /XPAGES
WHAT IS KEYCLOAK?

Core Concepts

Realm: master
- Roles
- Security Defenses

Identity Provider
- Users

OpenID Connect

SAML

Github, Twitter, Google, Facebook, etc

User Federation
- Roles
- Groups
- Events

UI (Themes)

Keycloak
WHY IS KEYCLOAK A GREAT MATCH FOR DOMINO SHOPS?

- **Reliable Solution**
  “Red Hat running on Red Hat products (Red Hat SSO)”: the entire authentication/authorization system is based on Red Hat SSO, which is the downstream version of upstream product keycloak. It is designed following the standard security protocols to provide a dynamic single sign-on solution to small/large scale industry.

- **Open Source (3C’s): Cost, Customizable / Contributions, Community**
  Apache License Version 2.0 with support of strong active open source community

- **Is it ready for production?**
  Yes, it can be used in production (Make sure to read documentation guide)

- **Standard Protocols (supported by keycloak)**
  - OpenID Connect
  - OAuth 2.0
  - SAML 2.0

- **Applications/Tools** that support integration with the above protocols can be plugged with Keycloak.
  E.g. MFA components, FIDO2 plugins, HW-Token Handling and much much more.
OUR BASE ARCHITECTURE CHART...

Keycloak

SPA / Web App

NGINX RP/LB

SPA

SAML/OIDC

DOMINO REST APIs

App Server (Express / Java / .NET Middleware)

OIDC

ADP/Proton

LDAP

HTTP

DSAPI / OIDC

NOMAD Web Server

Scope Mapping NSF

NSF

NSF

NSF

ADPConfig.nsf
DOMINO REST API/ADP OAUTH2/OIDC FLOW

Alice

React-App

Keycloak

can I see that resource?

Hey, can Alice see that page?

Hey Alice, Please enter your login credentials?

Hey Keycloak, authenticate me, here my credentials?

Alice can see this page!

Here you go enjoy?

Alice

React-App

Keycloak
NOTES/DOMINO SAML CONFIGURATION

- Create and configure IDP Catalog (idpcat.nsf)
- Create trust configuration
- Configure Domino HTTP Settings
- Setup User Security Policy
- If needed: configure ID Vault for federated Login (Notes Client)
- Test!
1) DOMINO WEB ACCESS SAML CONFIG – IDPCAT.NSF
1) DOMINO WEB ACCESS SAML CONFIGURATION

https://sitlux01.sit.de

- **Client ID**: https://sitlux01.sit.de
- **Name**: Login@ST GmbH
- **Description**: Login@ST GmbH
- **Enabled**: ON
- **Always Display in Console**: OFF
- **Consent Required**: OFF
- **Login Theme**: sit-theme
- **Client Protocol**: saml
- **Include AuthStatement**: ON
- **Include OneTimeUse Condition**: ON
- **Force Artifact Binding**: OFF
- **Sign Documents**: ON
- **Optimize REDIRECT signing**
## 2) DOMINO REST API KEYCLOAK CONFIG

### Clients

<table>
<thead>
<tr>
<th>Client ID</th>
<th>Enabled</th>
<th>Base URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domino_confidential_client</td>
<td>True</td>
<td>Not defined</td>
</tr>
<tr>
<td>account</td>
<td>True</td>
<td><a href="https://login.sit.de/auth/realms/DLR-Dashboard/account/">https://login.sit.de/auth/realms/DLR-Dashboard/account/</a></td>
</tr>
<tr>
<td>account-console</td>
<td>True</td>
<td><a href="https://login.sit.de/auth/realms/DLR-Dashboard/account/">https://login.sit.de/auth/realms/DLR-Dashboard/account/</a></td>
</tr>
<tr>
<td>admin-cli</td>
<td>True</td>
<td>Not defined</td>
</tr>
<tr>
<td>broker</td>
<td>True</td>
<td>Not defined</td>
</tr>
<tr>
<td>dir-abo-api</td>
<td>True</td>
<td><a href="https://dirprocess.sit.dehttps://dirprocess.sit.de">https://dirprocess.sit.dehttps://dirprocess.sit.de</a></td>
</tr>
<tr>
<td>dir-dashboard-app</td>
<td>True</td>
<td>Not defined</td>
</tr>
<tr>
<td>hcl-rest-api-test</td>
<td>True</td>
<td>Not defined</td>
</tr>
<tr>
<td><a href="https://dirprocess.sit.de">https://dirprocess.sit.de</a></td>
<td>True</td>
<td>Not defined</td>
</tr>
<tr>
<td><a href="https://sitfp1.sit.de">https://sitfp1.sit.de</a></td>
<td>True</td>
<td>Not defined</td>
</tr>
<tr>
<td><a href="https://sitlux01.sit.de">https://sitlux01.sit.de</a></td>
<td>True</td>
<td><a href="https://sitlux01.sit.dehttps://sitlux01.sit.de">https://sitlux01.sit.dehttps://sitlux01.sit.de</a></td>
</tr>
<tr>
<td><a href="https://sitlux02.sit.de">https://sitlux02.sit.de</a></td>
<td>True</td>
<td><a href="https://sitlux02.sit.dehttps://sitlux02.sit.de">https://sitlux02.sit.dehttps://sitlux02.sit.de</a></td>
</tr>
<tr>
<td>realm-management</td>
<td>True</td>
<td>Not defined</td>
</tr>
<tr>
<td>security-admin-console</td>
<td>True</td>
<td><a href="https://login.sit.de/auth/admin/DLR-Dashboard/console/">https://login.sit.de/auth/admin/DLR-Dashboard/console/</a></td>
</tr>
</tbody>
</table>
2) DOMINO REST API KEYCLOAK CONFIG

Client Scopes > Add client scope

Add client scope

Name: keep-common
Description: Shared claims expected by keep
Protocol: openid-connect
Display On Consent Screen: ON
Consent Screen Text: Hey Dude, is that alright
Include In Token Scope: OFF

Save Cancel
2) DOMINO REST API KEYCLOAK CONFIG
3) APPDEVPACK IAM REPLACEMENT

- Keycloak
- OIDC/OAUTH2 Additional Claims Config
- Node.js / Java/ C# Middleware App
- Language Bindings
- Proton Task
- Domino
- LDAP
- ADPConfig.nsf
- Act As User
- Additional Claims Config
- Act As User
- ADPConfig.nsf
### Proton_fnd

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>openId-connect</td>
</tr>
<tr>
<td>ID</td>
<td>4b8e5c2a-743e-4181-a3b1-8da79fbeb32c</td>
</tr>
<tr>
<td>Name</td>
<td>proton_fnd</td>
</tr>
<tr>
<td>Mapper Type</td>
<td>Hardcoded claim</td>
</tr>
<tr>
<td>Token Claim Name</td>
<td>proton_fnd</td>
</tr>
<tr>
<td>Claim value</td>
<td>CN=app4.0+ST GmbH,C=DE</td>
</tr>
<tr>
<td>Claim JSON Type</td>
<td>String</td>
</tr>
<tr>
<td>Add to ID token</td>
<td>OFF</td>
</tr>
<tr>
<td>Add to access token</td>
<td>ON</td>
</tr>
<tr>
<td>Add to userinfo</td>
<td>OFF</td>
</tr>
<tr>
<td>Multivalued</td>
<td>OFF</td>
</tr>
<tr>
<td>Aggregate attribute values</td>
<td>OFF</td>
</tr>
</tbody>
</table>
3) APPDEVPACK IAM REPLACEMENT - INTROSPECTION
4) APPDEVPACK DSAPI FILTER – OIDC/OAUTH

- IDP, e.g. Keycloak
- OIDC/OAUTH2
- Clients & Claims Config
- Granular access to apps additional to ACL in DB
- Node.JS / Java/ C# Middleware App
- Language Bindings

Dev and Prod Environments, Docker (Cluster)

Act As User

Proton Task

Domino

App & Claims Definitions

ADPConfig.nsf
5) DOMINO 12.0.2 – “DANUBE” & OAUTH/OIDC

DEV and Prod Environments, Docker (Cluster)

Web App / XPages(?)

IDP, e.g. Keycloak

OIDC/OAUTH2

KEEP

Domino
5) DOMINO 12.0.2 – “DANUBE” TLS IN CERTMGR

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Certificate Expiration</th>
<th>Type</th>
<th>CurveSize</th>
<th># SANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>* sli.de</td>
<td>13.11.2021 06:03:11</td>
<td>RSA</td>
<td>2048</td>
<td>1</td>
</tr>
</tbody>
</table>

- Discover
- Workspace
- Certificate Store - TLS Credentials
- Add TLS Credentials
- Edit Document
- Delete TLS Credentials

**TLS CREDENTIALS**
- By Host Name
- By Domino Server
- By Account Name
- Archive
- Jconsole

**CONFIGURATIONS**
- ACME Accounts
- Certificate Authorities
- DNS Providers
- DNS Configuration
- DNS Trace Logs
- Trusted Roots
- Password Store
5) DOMINO 12.0.2 – “DANUBE” OIDC PROVIDER CONFIG

**OIDC Provider Settings**

- **Host names or addresses mapped to this site:** sitns85.sit.de; 141.95.94.63
- **Provider name:** Keycloak
- **Base URL:** https://login.sit.de/auth/realms/DLR-Dashboard
- **Trusted roots:** ISRG Root X1/Internet Security Research Group/US
- **Logging level:** Verbose
DOMINO 12.0.2 “DANUBE” KEYCLOAK CONFIG

DOMINO_confidential_client

- **Client ID**: Domino_confidential_client
- **Name**: 
- **Description**: 
- **Enabled**: ON
- **Always Display in Console**: OFF
- **Consent Required**: OFF
- **Login Theme**: sit-theme
- **Client Protocol**: openid-connect
- **Access Type**: confidential
- **Standard Flow Enabled**: ON
- **Implicit Flow Enabled**: OFF
- **Direct Access Grants Enabled**: ON
Now includes Noamd Web Server Domino!
4TH APP – DOMINO 12.0.2 OIDC

Keycloak

SPA / Web App
NGINX RP/LB

SAML/OIDC

SPA

SAML/OIDC

SPA / Web App
NGINX RP/LB

SAML/OIDC

SPA

SAML/OIDC

App Server (Express / Java / .NET Middleware)

Domino REST APIs

LDAP

HTTP

DSAPI / OIDC

NOMAD Web Server

Scope Mapping NSF

NSF

NSF

NSF

ADP/Proton

ADPConfig.nsf

Domino Backend
const auth = async function (req, res) {

try {
    keycloakIssuer = await Issuer.discover(config.keycloak_issuer);
    client = new keycloakIssuer.Client(
        client_id: config.keycloak_client_id,
        client_secret: config.keycloak_client_secret,
        redirect_uri: config.keycloak_redirect_uri,
        response_types: config.keycloak_response_types,
    );

    const authorizationUri = client.authorizationUrl({
        scope: 'openid',
        resource: config.baseURL,
        code_challenge,
        code_challenge_method: 'S256',
    });
    console.log('in AUTH');
    const reacback = req.query.callback;
    req.session.react_callback = reacback;
    res.status(302).redirect(authorizationUri);
} catch (error) {
    console.error(error);
    res.status(500).send("Error", error);
}

};
const auth_callback = async function(req, res) {
    console.log('in Callback!');
    const reactback = req.session.react_callback;
    try {
        const params = client.callbackParams(req);
        const tokenSet = await client.callback('config.redirect_uri, params, { code_verifier });
        const access_token = tokenSet.access_token;
        const userinfo = await client.userinfo(access_token);
        req.session.tokenSet = tokenSet;
        req.session.userinfo = userinfo;

        // decode id token
        req.session.access_token = access_token;
        const token = req.session.id;
        const all_in = reactback+"/"+token;

        /*
        * Diese Passage müssen wir ändern - hier muss in Zukunft KEINE Prüfung mehr
        * rein sondern der DSAPI Filter muss die Prüfung des AccessTokens übernehmen
        * LTPA kann dann entfallen.
        */
        let ltpa_check = await forms.views_api.get_LTPA_Token_From_Access_Token(access_token);
        if(ltpa_check.result=="ERROR") {
            res.cookie('ltpa_check.cookie_name',ltpa_check.ltpatoken,{domain:'.sit.de',httpOnly: false,secure:false,path:"/
})
            res.cookie('ltpaCheck',ltpa_check.ltpatoken,{domain:'.sit.de',httpOnly: false,secure:false,path:"/
})
        }
        res.cookie('token',token,{ domain:'sit.de', expires: new Date(Date.now() + 900000), httpOnly: false});
        res.status(302).redirect(all_in);
    } catch(e) {
        console.error(e);
        res.status(403).redirect(reactback+"/ERROR");
    }
};
SSO between Connections, SameTime and Domino can be done via Keycloak. We can also include DX and even Commerce.

MFA & STEP-UP AUTHENTICATION IN KEYCLOAK

- Keycloak supports step up authentication
- TOTP Config per REALM & Users
- Supports Google Authenticator and FreeOTP

- Business Rules for Step Up Config
- Apps request the step up flow by sending ACR levels
- For APIs as well!

With step-up authentication, Web Applications or APIs that allow access to different types of resources can require users to authenticate with a stronger authentication mechanism to access sensitive resources.
WHAT IS IDENTITY BROKERING?

Identity Brokering

An Identity Broker is an intermediary service that connects multiple service providers with different identity providers. As an intermediary service, the identity broker is responsible for creating a trust relationship with an external identity provider in order to use its identities to access internal services exposed by service providers.

From a user perspective, an identity broker provides a user-centric and centralized way to manage identities across different security domains or realms. An existing account can be linked with one or more identities from different identity providers or even created based on the identity information obtained from them.

An identity provider is usually based on a specific protocol that is used to authenticate and communicate authentication and authorization information to their users. It can be a social provider such as Facebook, Google or Twitter. It can be a business partner whose users need to access your services. Or it can be a cloud-based identity service that you want to integrate with.
WHAT’S THE TAKE?

- Keycloak covers all SSO angles for the HCL Digital Solutions portfolio.
- Keycloak offers Identity Brokering capabilities for free
- Token mapping between SAML and OIDC is brilliant
- Open Source and Extensibility
- Cloud Hosting, SaaS and on-premises
- High availability scenarios available (on-prem and SaaS)
- Keycloak brings even more that we did not cover (WebAuthn, MFA ...)

Keycloak & HCL Domino - The perfect match for all things SSO.
Thank you!

Heiko Voigt
- heiko.voigt@harbour-light.com
- @HarbourLightcom
- https://github.com/heikovoigt

https://www.c3ug.ca/
QUESTIONS?

Use the GoToWebinar Questions Pane

Please keep all questions related to the topics that our speakers are discussing!!!

Unrelated Question => post at:

https://openntf.org/discord