MT AG

Ultimate Technical Guide: SSO for your APEX apps

Niels de Bruijn

January 23th, 2020

Facts & Figures

Independent Technology House with Cross-Industry Expertise

Headquarter Ratingen (North Rhine – Westphalia)

280 employed

MT AG

Oracle Platinum Partner

Privately-Owned Corporation

28 Mio. Euro Revenue

Founded 1994

Top Company for Trainees & Students

kununu TOP COMPANY www.kununu.com VON MITARBEITERN EMPFOHLEN!

Branches in Frankfurt and Cologne

About me

- **Niels de Bruijn, Business Unit Manager Low-Code / APEX**
- Born in 1977, married, three daughters, living in Ratingen
- Working for MT AG since DEC-2003
- Responsible for the APEX practise
- Presenting at various conferences

ORACLE ACE Director

- Involvement in Oracle User Groups
  - DOAG e.V. – Board Member & Conference Chair of APEX Connect (apex.doag.org)
  - ODTUG - Part of APEX Content Committee for Kscope

Agenda

- Why Single Sign-On?
- How does the magic work?
- Caveats
- I want more
- Questions I get
- More information

Why Single Sign-On?

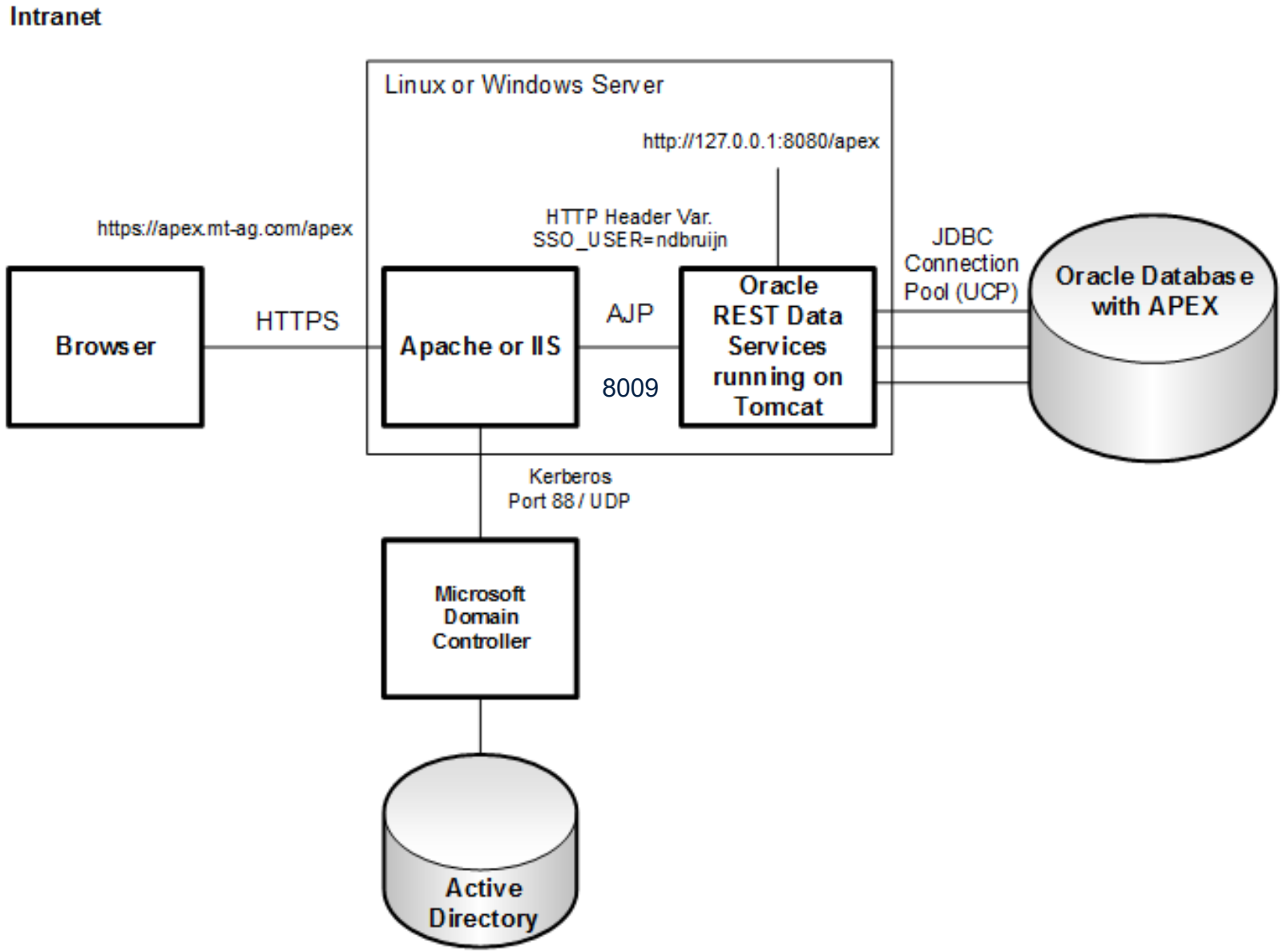
For the sake of security

- Credentials are not passed to the database
- Kerberos is secure (as used by Windows itself)
- Central user store in Active Directory
- No corporate password policy needed within APEX

For the sake of productivity

- End users love it
- Developers can now switch between workspaces without logging in again

How does the magic work?



How does the magic work?

Start here: http://knowledgebase.mt-ag.com/q/kerberos (Viewed over 11.000 times!)

Overview

- Install RDBMS & APEX
- Install JDK, Tomcat & Apache/IIS
- Configure ORDS & deploy
- Configure Apache or IIS for SSO incl. SSL certificate

General installation steps of Apache & ORDS can be found here:

http://www.opal-consulting.de/downloads/presentations/2015-11-DOAG-ORDS-Setup

Caveats

- Local user in table != Active Directory user?
  - Use “post-authentication procedure” in authentication scheme:

```
APEX_UTIL.SET_USERNAME
( p_userid     => APEX_UTIL.GET_USER_ID('ADMIN’)
, p_username   => 'NDBRUIJN’
);
```

- When using mod_auth_kerb and AD user is member of too many AD groups
  - Have a look here: http://blogs.technet.com/b/surama/archive/2009/04/06/kerberos-authentication-problem-with-active-directory.aspx

- Once enabled, you can’t change the identity without changing the OS user
  - Prepare your end users
  - Testing with other credentials: just switch the authentication scheme to “open door” in the dev environment

I want more

- Can I use multiple authentication schemes?
  - Yes, see: http://www.grassroots-oracle.com/2019/01/apex-authentication-switch-in-session.html
- What about devices like MacBooks or Smartphones that are not part of the Windows domain?
  - Fallback Authentication using Basic Authentication over HTTPS
    - Tipp: don't use Digest Authentication (doesn't work with Firefox)
  - Don't want to enter username/password? Client certificates will help you out.
- What about the Cloud?
  - Users in Azure Active Directory? Use mod_auth_mellon (for Apache Webserver): http://knowledgebase.mt-ag.com/q/saml
  - Users in Facebook/Google? Use Social Login: http://dgielis.blogspot.com/2018/06/facebook-google-and-custom.html

Questions I get

- "Should we still specify the same cookie name for all apps in our workspace?"
  - Yes, this prevents multiple APEX session cookies being created
  - It also makes it possible to share application items between apps (aka. "global" app items)

- "We already have LDAP authentication utilized in our APEX app"
  - Are you sure you want to pass your AD credentials to the database? Security risk!

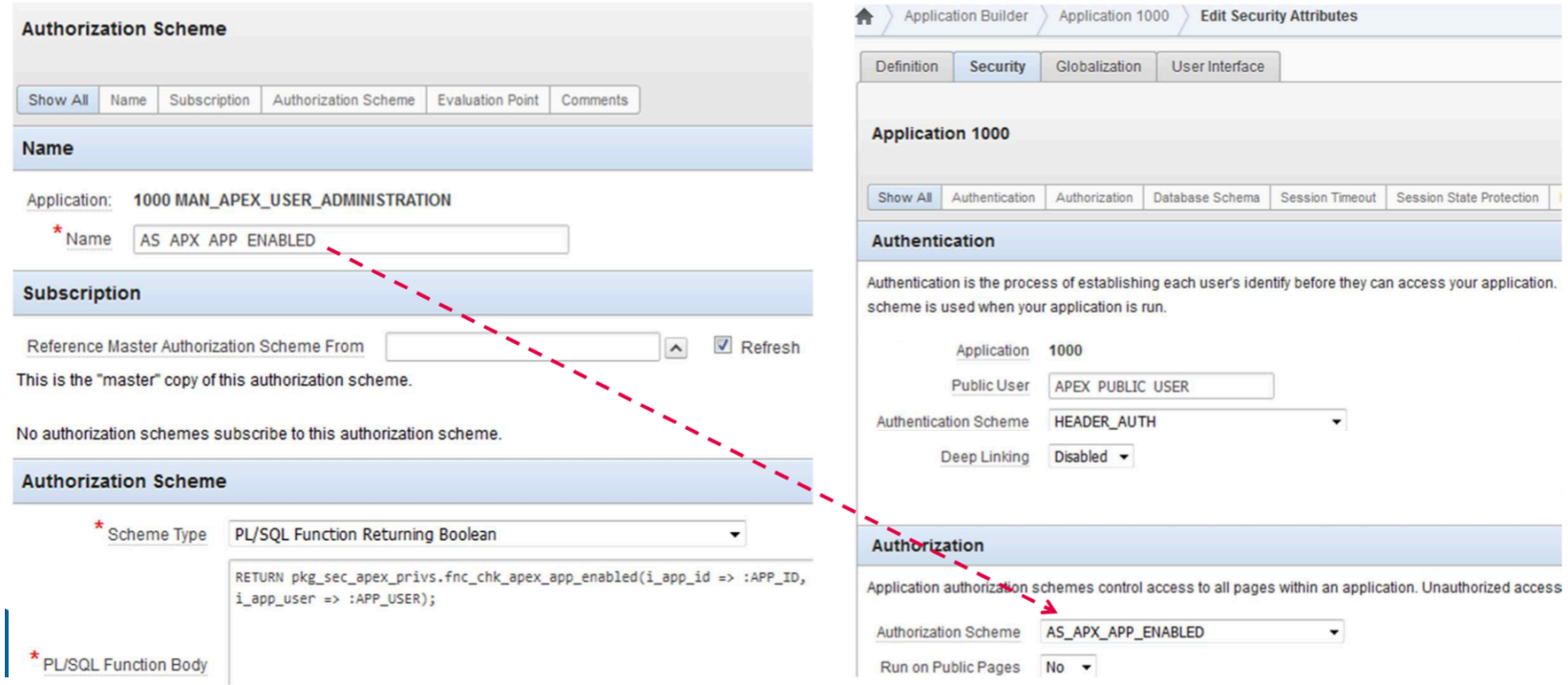
- "What about the rights in my app?"
  - We are talking about authentication here, the authorization is normally determined by the app
  - You could use dbms_ldap or apex_ldap.is_member to get privs
  - Apache already supports methods to check user groups
  - Also have a look at the low-code approach built-in: https://blogs.oracle.com/apex/custom-authentication-and-authorization-using-built-in-apex-access-control-a-how-to

- "Any concerns about the session timeout setting in APEX?"
  - Set it to 0 (= indefinitely) as session timeout is now delegated to Kerberos

Questions I get

- "The logout link in my app doesn't work anymore"
  - Just delete it, you don't need it anymore

- "How can I check in APEX if the user may access the app?"
  - Use an authorization scheme with your own PL/SQL function



More information

- General installation steps of Apache & ORDS can be found here:

http://www.opal-consulting.de/downloads/presentations/2015-11-DOAG-ORDS-Setup

- About Kerberos

http://www.roguelynn.com/words/explain-like-im-5-kerberos

- About mod_auth_kerb

http://blog.hallowelt.biz/wp-content/uploads/SSO_mit_mod_auth_kerb_v3.pdf

- More SSO options

http://wphilltech.com/options-for-windows-native-authentication-with-apex

MT AG

@nielsdb

http://blog.mt-ag.com/apex

http://de.linkedin.com/in/nielsdebruijn

XING

www.xing.com/profile/Niels_deBruijn