

Single Sign-On für alle!

100 Years
MAN Truck and Bus



Tobias Stark – MAN Truck & Bus AG

Niels de Bruijn – MT AG

APEX Connect

Berlin, 27.04.2016



Agenda

100
100 Years
MAN Truck and Bus

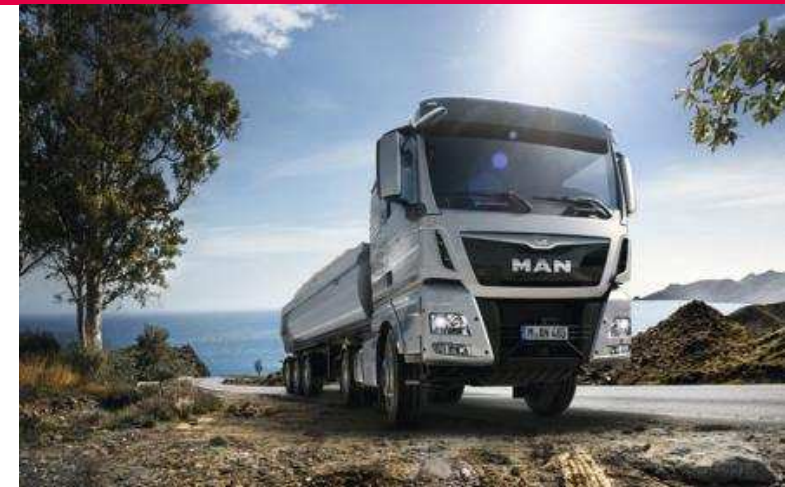


- 1 Vorstellung
- 2 Warum Single Sign-On?
- 3 Architektur
- 4 Vorgehensweise
- 5 APEX und Single Sign-On bei MAN
- 6 Q & A



MAN Truck & Bus ist das größte Unternehmen der MAN Gruppe und einer der führenden Anbieter von Nutzfahrzeugen und Transportlösungen.

- Lkw von 7,5 bis 44 t Gesamtgewicht
- Schwere Sonderfahrzeuge bis 250 t Zuggesamtgewicht
- Stadt-, Überland- und Reisebusse sowie Bus-Chassis der Marke MAN sowie Luxus-Reisebusse der Marke NEOPLAN
- Industrie-, Marine- sowie On- und Offroadmotoren
- Umfangreiche Dienstleistungen rund um Personenbeförderung und Gütertransport



Vorstellung

Tobias Stark




- Informatik-Betriebswirt (VWA)
- Datenbankentwickler
- 20 Jahre Erfahrung mit Oracle-Datenbanken (ab Version 7.3.x)
- 5 Jahre Mitarbeiter bei MAN Truck & Bus AG
- Tätigkeiten im Bereich „Business Intelligence“
 - Betreuung der „Information Warehouse“-Oracle Datenbanken
 - Aufbau und Betreuung neue APEX-Umgebung seit März 2015

Vorstellung

Niels de Bruijn



- Niels de Bruijn, Business Unit Manager APEX bei der  MT AG
- Beschäftigt sich seit 2004 mit APEX
- Federführend beim Vertrieb/Marketing/Delivery von APEX Projekten aller Art
 - <https://apex.mt-ag.com>
- Themenverantwortlicher für APEX bei der DOAG
- Initiator & Organisator von APEX Connect



[@nielsdb](https://twitter.com/nielsdb)



<https://blog.mt-ag.com/apex>



<https://linkedin.com/in/nielsdebruijn>



https://xing.com/profile/Niels_deBruijn



ORACLE
ACE Director

Agenda

100
100 Years
MAN Truck and Bus



1 Vorstellung

2 Warum Single Sign-On?

3 Architektur

4 Vorgehensweise

5 APEX und Single Sign-On bei MAN

6 Q & A

Warum Single Sign-On?



Aus Sicherheitsgründen


- Kontodaten werden nicht an die Datenbank weiter gereicht
- Das Kerberos-Protokoll ist sicher (wird durch Windows selbst verwendet)
- Konten werden zentral in z.B. Active Directory verwaltet
 - Passwort Policy ist somit auch zentral implementiert

Aus Produktivitätsgründen

- Die Endanwender lieben es 😊
 - Es kommt auch die Akzeptanz von der Anwendung zu Gute
- Die Entwickler können jetzt ohne eine erneute Anmeldung zwischen den Workspaces wechseln

TI-Monitoring - Overview x

Datei Bearbeiten Ansicht Favoriten Extras ?



MANTIAS MAN TI-AuswerteSystem

c6462

- Start
- Stammdaten der Aktion
- Arbeitsanweisung zur Aktion
- Betroffene Fahrzeuge zur Aktion
- Kundenstammdaten
- Berechtigungen

Start

- > Stammdaten der Aktion - Anlage und Pflege von Stammdaten zu Aktionen
- > Arbeitsanweisung zur Aktion - Anlage und Pflege von Arbeitsanweisungen zu Aktionen
- > Betroffene Fahrzeuge zur Aktion - Anlage und Pflege von Fahrzeugdaten zu Aktionen
- > Kundenstammdaten - Anlage und Pflege von Kundenstammdaten
- > Berechtigungen - Anlage und Pflege von Länderdaten und Zugriffsberechtigungen

Agenda

100
100 Years
MAN Truck and Bus



1 Vorstellung

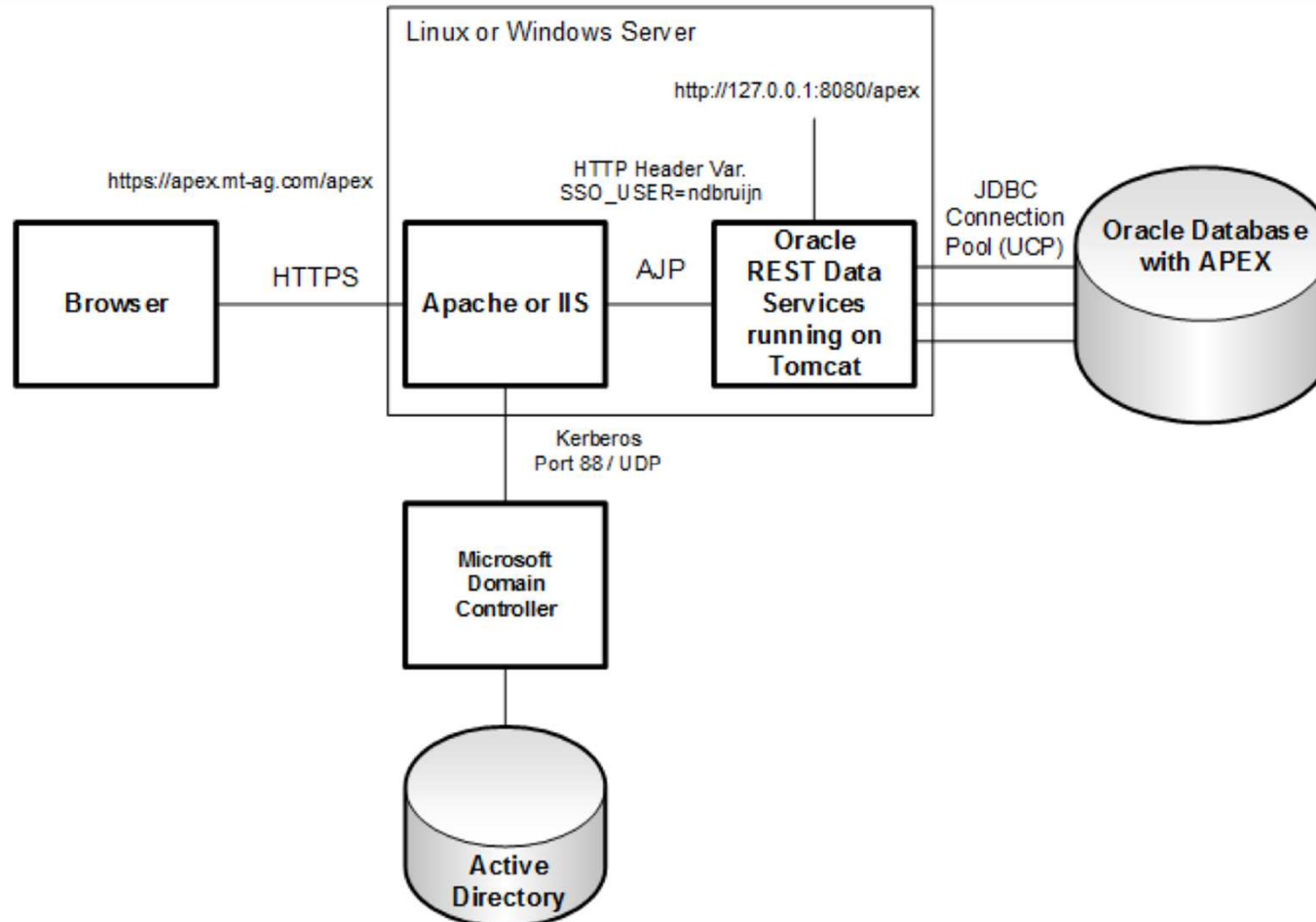
2 Warum Single Sign-On?

3 Architektur

4 Vorgehensweise

5 APEX und Single Sign-On bei MAN

6 Q & A



Agenda

100
100 Years
MAN Truck and Bus



1 Vorstellung

2 Warum Single Sign-On?

3 Architektur

4 Vorgehensweise

5 APEX und Single Sign-On bei MAN

6 Q & A

Installation der Software

- APEX: docs.oracleapex.com
- Apache & ORDS: www.opal-consulting.de/downloads/presentations/2015-11-DOAG-ORDS-Setup

Konfigurationsanleitung für Single Sign-On

<http://de.slideshare.net/nielsdb/mt-ag-howtosingle-signonforapexapplicationsusingkerberos-46435415>

- Linux als Web Gateway im Einsatz? Apache + mod_auth_kerb verwenden
- Windows als Web Gateway im Einsatz? IIS statt Apache verwenden

Agenda

100
100 Years
MAN Truck and Bus



- 1 Vorstellung
- 2 Warum Single Sign-On?
- 3 Architektur
- 4 Vorgehensweise
- 5 APEX und Single Sign-On bei MAN**
- 6 Q & A

8 Workspaces

19 APEX-Anwendungen

~ 1.100 Pages

~ 2.400 DB-Objekte

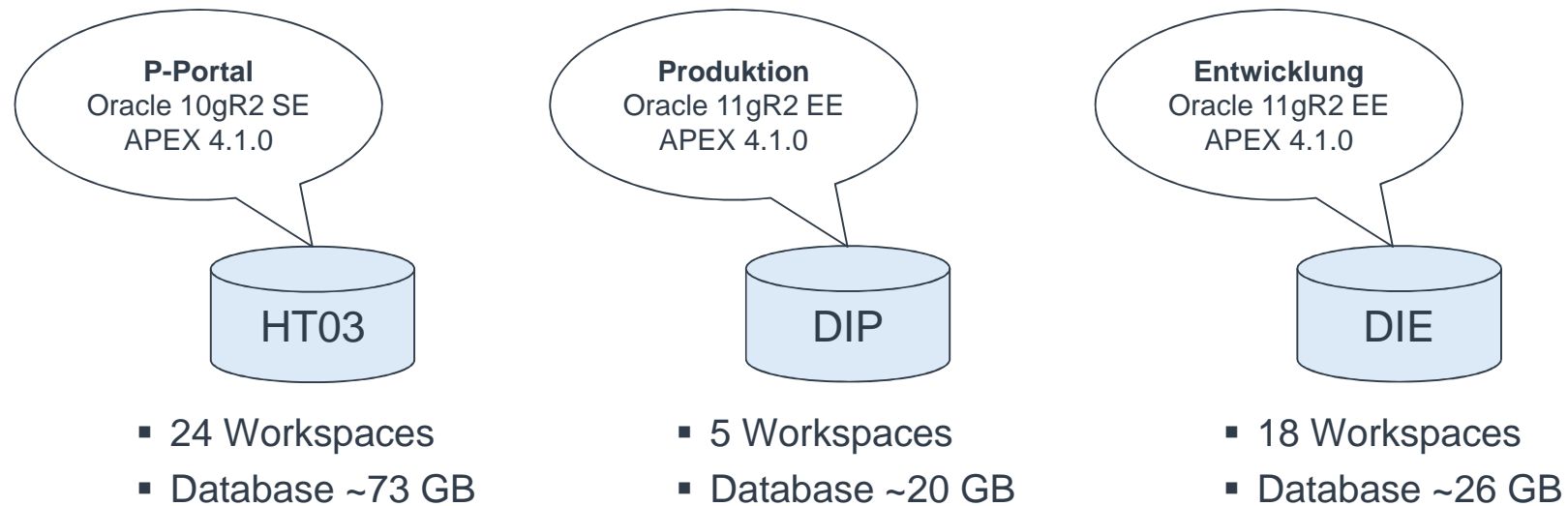
~1.000 aktive APEX User / 4 Wochen

~ 77 GB

~ 800.000 Page Views / 4 Wochen

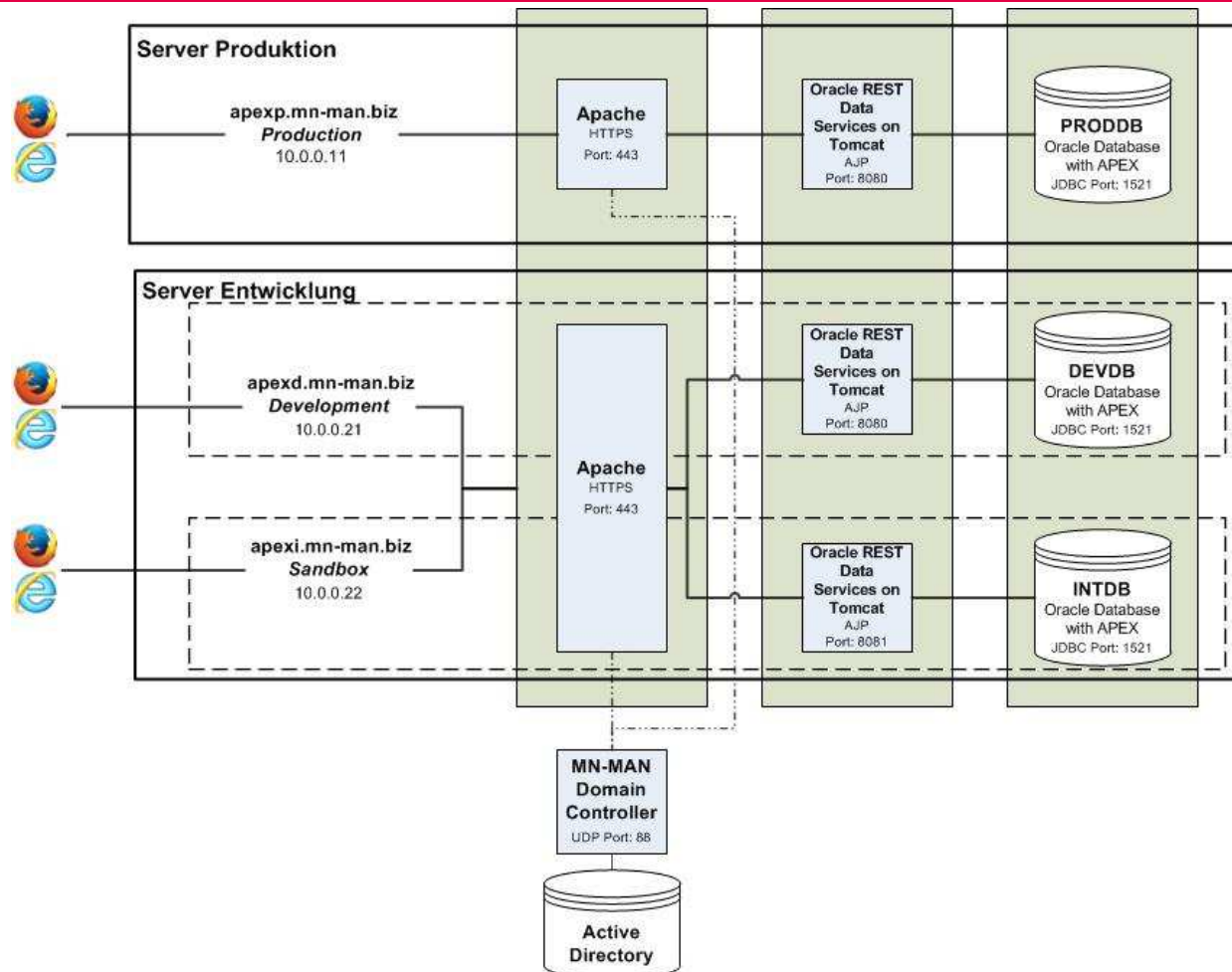
Ausgangssituation APEX@MTB

Überblick



Istzustand APEX@MTB

Überblick



Aufbau der Umgebung

Vorgehen



- Installation des geplanten Software-Stacks in VM mit CentOS 6.x
- Installation Oracle-Datenbanken
- Installation APEX in Oracle-Datenbanken
- Installation und Konfiguration Tomcat
- Installation und Konfiguration Oracle REST Data Services
- Installation und Konfiguration Apache
- Konfiguration Single Sign-On mit Apache und Kerberos
- Konfiguration APEX Instanzen

- Software von tomcat.apache.org
 - Aktualisierung der Tomcat-Software unabhängig von RHEL möglich
 - Parallelbetrieb unterschiedlicher Tomcat-Versionen möglich
- Einbindung der Tomcat-Instanzen als System-Dienst
 - Nutzung Tomcat 6 von RHEL zum Start von Tomcat 8-Instanzen
 - Automatisches starten und stoppen der Tomcat-Instanzen bei Neustart des Systems
- Berücksichtigung Security-Vorgaben von VW-IT
 - Aktivierung Java Security Manager
 - Löschung der Tomcat-Standard-Anwendungen
- Konfiguration zu weiten Teilen identisch zu Dokumentation von Niels de Bruijn

- Einstellungen server.xml

```
<Connector address="127.0.0.1"
            port="8080"
            protocol="AJP/1.3"
            packetSize="65536"
            URIEncoding="UTF-8"
/>
<Server port="9005" address="127.0.0.1" shutdown="SHUTDOWN">
```

- Einstellungen catalina.policy

```
grant codeBase "file:${catalina.base}/webapps/apex/-" {
    permission java.security.AllPermission;
};
```

Oracle REST Data Services

Konfiguration



- Einstellungen APEX_PUBLIC_USER (defaults.xml)

```
<entry key="jdbc.InitialLimit">20</entry>
```

```
<entry key="jdbc.MaxLimit">50</entry>
```

```
<entry key="jdbc.MinLimit">20</entry>
```

- Einstellungen APEX_LISTENER (apex_al.xml), ORDS_PUBLIC_USER (apex_pu.xml) und APEX_REST_PUBLIC_USER (apex_rt.xml)

```
<entry key="jdbc.InitialLimit">5</entry>
```

```
<entry key="jdbc.MaxLimit">20</entry>
```

```
<entry key="jdbc.MinLimit">5</entry>
```

- Aktivierung Debugging

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

```
<entry key="debug.printDebugToScreen">true</entry>
```

```
<VirtualHost 10.0.0.11:443>
```

```
LimitRequestFieldSize 65536
```

```
Alias /i/ "/u00/app/apache/docs/apex/apex/images/"
```

```
ProxyPass /apex/ ajp://127.0.0.1:8080/apex/ connectiontimeout=2100 timeout=2100
```

```
ProxyIOBufferSize 65536
```

```
ErrorDocument 503 /messages/msg_status_code_503.html
```

```
</VirtualHost>
```

SSO in APEX

Authorization Scheme

Authorization Scheme

Show All Name Subscription Authorization Scheme Evaluation Point Comments

Name

Application: 1000 MAN_APEX_USER_ADMINISTRATION

* Name AS APX APP ENABLED

Subscription

Reference Master Authorization Scheme From Refresh

This is the "master" copy of this authorization scheme.

No authorization schemes subscribe to this authorization scheme.

Authorization Scheme

* Scheme Type PL/SQL Function Returning Boolean

```
RETURN pkg_sec_apex_privs.fnc_chk_apex_app_enabled(i_app_id => :APP_ID,  
i_app_user => :APP_USER);
```

* PL/SQL Function Body

Application Builder > Application 1000 > Edit Security Attributes

Definition Security Globalization User Interface

Application 1000

Show All Authentication Authorization Database Schema Session Timeout Session State Protection

Authentication

Authentication is the process of establishing each user's identify before they can access your application. scheme is used when your application is run.

Application 1000

Public User APEX PUBLIC USER

Authentication Scheme HEADER_AUTH

Deep Linking Disabled

Authorization

Application authorization schemes control access to all pages within an application. Unauthorized access

Authorization Scheme AS APX APP ENABLED

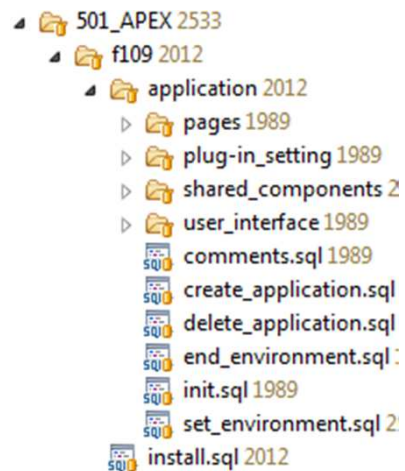
Run on Public Pages No

Versionierung

Quellcode



- Einsatz von Subversion zur Verwaltung des Quellcodes von DB-Objekten und APEX-Anwendungen
- Export der APEX-Anwendung als Datei in Dateisystem
- Split exportierter APEX-Anwendung mit „APEXExportSplitter“
- Versionierung nur der von „APEXExportSplitter“ erzeugten Dateien
- Einspielung der APEX-Anwendung in Produktion mit „install.sql“



Best Practices

Oracle Security



- APEX-Datenbanken arbeiten mit „encrypted“ Tablespaces
 - Ist in APEX-Konfiguration bei „Instance Settings/Storage“ für Nutzung bei Neuanlage von Workspaces zu aktivieren
- SQLNet encryption für Datenbankverbindungen aktiviert
- Einsatz von Oracle Database Vault
 - Keine Probleme im Zusammenspiel mit APEX
 - ORDS-Aktualisierungen erfordern wegen DB-Änderungen eine Downtime der Datenbank zur Deaktivierung

- Schrittweises Vorgehen mit Test abgeschlossener Teile zur frühzeitigen Erkennung von Problemen
- Nutzung von symbolischen Links
 - Installation der Software mit Version im Verzeichnisnamen
 - Symbolischer Link verweist auf aktuell aktive Software-Version
 - einfacher Fallback bei Problemen mit neuer Software-Version
 - einfache Vorbereitung von Software-Upgrades

```
[root@██████████ apexd]# ls -la
total 16
drwxr-x---. 4 tcuser tomcat 4096 Feb  4 10:33 .
drwxr-x---. 4 tcuser tomcat 4096 Jan 19 14:22 ..
drwxr-x---. 8 tcuser tomcat 4096 Jan 20 09:53 apache-tomcat-8.0.30
drwxr-x---. 4 tcuser tomcat 4096 Feb 16 07:51 etc
lrwxrwxrwx. 1 tcuser tomcat  20 Jan 20 09:53 tomcat -> apache-tomcat-8.0.30
[root@██████████ apexd]# █
```

Haben Sie noch Fragen?

100
100 Years
MAN Truck and Bus



Tobias Stark

Business Intelligence (FIUB)

MAN Truck & Bus AG

München

tobias.stark@man.eu

Niels de Bruijn

Business Unit Manager APEX

MT AG

Ratingen

niels.de.bruijn@mt-ag.com