Installation Guide

DS.IAM Installation

Inhalt

[Konfiguration der OUD Instanzen 1](#_Toc136525405)

[Roadmap 1](#_Toc136525406)

[Prüfen der Ports 1](#_Toc136525407)

[Erzeugen der Kennwortdatei 1](#_Toc136525408)

[Setup der Instanz 2](#_Toc136525409)

[Vorgabe 2](#_Toc136525410)

[Durchführung 2](#_Toc136525411)

[Prüfen der Instanz 4](#_Toc136525412)

## Konfiguration der OUD Instanzen

|  | **Wichtig** |
| --- | --- |
| Das in der Kommandozeile verwendete Kennwort *wmkah1mdkh@nuhr* ist nur ein Beispiel und muss durch das aus dem Passwort Safe zu beziehende Kennwort ersetzt werden. |

| D:\tt\icon-note-16.png | **Note** |
| --- | --- |
| Als Argument für den Hostnamen ist der jeweilige Knoten zu verwenden |

### Roadmap

Die Konfiguration der Instanz erfolgt auf jedem Knoten nach dem folgenden Ablauf:

* Prüfen der Ports
* Erzeugen der Kennwortdatei
* Setup der Instanz
* Prüfen der Instanz

### Prüfen der Ports

Die im nachfolgendem Verfahren zu spezifizierenden Ports dürfen durch anderweitige Dienste nicht bereits verwendet werden. Um dies sicherzustellen wird mit folgender Kommandozeile verifiziert, ob diese Voraussetzung eingehalten wird:

|  | **Kommando** |
| --- | --- |
| netstat -an | grep "7389"  netstat -an | grep "7636"  netstat -an | grep "7441" |

| D:\tt\icon-warning-16.png | **Warnung** |
| --- | --- |
| Sollte einer dieser Befehle eine Ausgabe zur Folge haben kann die Konfiguration in der hier beschriebenen Art und Weise **nicht** fortgesetzt werden |

### Erzeugen der Kennwortdatei

Die Verzeichnisdienste benötigt für jeglichen administrativen Zugriff eine Authentisierung mit Benutzerkonto und Kennwort. Hierfür wird eine Kennwortdatei erzeugt und entsprechend geschützt, die als Argument den im weiteren auszuführenden Befehlszeilen übergeben wird.

Diese Datei wird mit folgenden Kommando angelegt:

|  | **Kommando** |
| --- | --- |
| mkdir -p ~/.secrets/credential  touch ~/.secrets/credential/directory  chmod 600 ~/.secrets/credential/directory  cat >> ~/.secrets/credential/directory << EOF  wmkah1mdkh@nuhr  EOF |

### Setup der Instanz

|  | **Wichtig** |
| --- | --- |
| Die nachfolgend aufgeführten Abläufe sind auf jedem Knoten die den Verbund des Verzeichnisdienstes bilden zu wiederholen. |

#### Vorgabe

| **Vorgaben** | **Verwendung** |
| --- | --- |
| **Instance Name** | bka.bund.de |
| **Instance Home** | /opt/Anwendungen/instances/oud/bka.bund.de |

#### Durchführung

Der Basis-Kontext wird mit folgender Kommandozeile erzeugt:

|  | **Kommando** |
| --- | --- |
| export JAVA\_HOME=/usr/java/jdk1.8.0\_131  export INSTANCE\_NAME=../../../../../../opt/Anwendungen/instances/oud/bka.bund.de  export INSTANCE\_HOME=/opt/Anwendungen/instances/oud/bka.bund.de  cd *<ORACLE\_BASE>*/fmw/12.2.1/oud  ./oud-setup -i -h <binding-host-name> --adminConnectorPort 7441 -p 7389 -Z 7636 --generateSelfSignedCertificate -a --baseDN dc=bka,dc=bund,dc=de --baseDN dc=fim,dc=bund,dc=de --rootUserDN cn=Directory\ Manager --noPropertiesFile |

Dieses Kommando startet ein Questionaire, das in folgender Art und Weise beantwortet wird:

##### Do you want to enable the HTTP administration port?

| **Optionen** | **Antwort** |
| --- | --- |
| **(yes / no)** | no |

##### Please provide the password to use for the initial root user:

| **Optionen** | **Antwort** |
| --- | --- |
| **n.a.** | siehe Passwort Safe |

##### Do you want to enable Start TLS on LDAP Port '7389'??

| **Optionen** | **Antwort** |
| --- | --- |
| **(yes / no)** | no |

##### Do you want to enable HTTP?

| **Optionen** | **Antwort** |
| --- | --- |
| **(yes / no)** | no |

##### Do you want to enable HTTPS?

| **Optionen** | **Antwort** |
| --- | --- |
| **(yes / no)** | no |

##### Specify the Oracle components with which the server integrates:

| **Optionen** | | **Antwort** |
| --- | --- | --- |
| **1** | No Integration | 1 |
| **2** | DIP (Directory Integration Platform) |  |
| **3** | Generic: Database Net Services, EBS and DIP |  |
| **4** | EUS (Enterprise User Security), Database Net Services, EBS and DIP |  |

##### How do you want the OUD server to be tuned?

| **Optionen** | | **Antwort** |
| --- | --- | --- |
| **1** | Use specific Java Virtual Machine arguments | 1 |
| **2** | Use the default Java Virtual Machine settings |  |
| **3** | Provide the Java heap size to be used by the server |  |
| **4** | Provide the percentage of system memory to be used by the serve |  |
| **5** | Provide the size of system memory to be used by the server |  |

##### Java Virtual Machine arguments

| **Optionen** | **Antwort** |
| --- | --- |
| **-Xms3540m -Xmx3540m -d64 -XX:+UseCompressedOops -server -Xmn512m -XX:MaxTenuringThreshold=1 -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=55** | -d64 -server -Xms2048m -Xmx2048m -Xmn512m -XX:+UseCompressedOops -XX:MaxTenuringThreshold=1 -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=60 |

##### How do you want the off-line tools (import-ldif, export-ldif, verify-index and rebuild-index) to be tuned?

| **Optionen** | | **Antwort** |
| --- | --- | --- |
| **1** | Use specific Java Virtual Machine arguments | 1 |
| **2** | Use the default Java Virtual Machine settings |  |
| **3** | Automatic Tuning |  |
| **4** | Provide the Java heap size to be used by the off-line tools |  |

##### Java Virtual Machine arguments

| **Optionen** | **Antwort** |
| --- | --- |
| **-Xms3540m -Xmx3540m -d64 -XX:+UseCompressedOops -server -Xmn512m -XX:+UseParallelGC -XX:+UseNUMA** | -d64 -server -Xms1024m -Xmx1024m -Xmn512m -XX:+UseCompressedOops -XX:+UseParallelGC -XX:+UseNUMA |

##### Do you want to start the server when the configuration is completed?

| **Optionen** | **Antwort** |
| --- | --- |
| **(yes / no)** | yes |

##### Setup Summary

| **Optionen** | | **Antwort** |
| --- | --- | --- |
| **1** | Set up the server with the parameters above | 1 |
| **2** | Provide the setup parameters again |  |
| **3** | Print equivalent non-interactive command-line |  |
| **4** | Cancel and exit |  |

### Prüfen der Instanz

Nach der erfolgreichen Erzeugung der Instanz empfiehlt sich die die Prüfung dieser Instanz

|  | **Kommando** |
| --- | --- |
| . ods.env  cd ${INSTANCE\_HOME}/OUD/bin  ./ldapsearch -h <hostname>.zds.bka.bund.de -p 7389 -D cn=Directory\ Manager -j ~/.secrets/credential/directory -b "" "(objectClass=\*)" |

Wurde die Instanz des Verzeichnisdienstes korrekt erzeugt sind in der Ausgabe des obigen Kommandos die Liste der unterstützten Controls aufgeführt.

## Konfiguration Administration REST API

Oracle Unified Directory ermöglicht Benutzern die Verwaltung und Konfiguration über REST-APIs. Admin-REST-APIs werden über den HTTP Administration Connector bereitgestellt. Sie können grundlegende Vorgänge mit den HTTP-Methoden GET, POST, PATCH oder DELETE durchführen.

| D:\tt\icon-warning-16.png | **Warnung** |
| --- | --- |
| Der Zugriff auf das REST API ist nicht Bestandteil der regulären Konfiguration der Instanz des Verzeichnisdienstes. Aus diesem Grund setzen die nachfolgenden Schritte eine lauffähige Instanz des Verzeichnisdienstes voraus. |

### Prüfen der Ports

Die im nachfolgendem Verfahren zu spezifizierenden Ports dürfen durch anderweitige Dienste nicht bereits verwendet werden. Um dies sicherzustellen wird mit folgender Kommandozeile verifiziert, ob diese Voraussetzung eingehalten wird:

|  | **Kommando** |
| --- | --- |
| netstat -an | grep "8444" |

| D:\tt\icon-warning-16.png | **Warnung** |
| --- | --- |
| Sollte einer dieser Befehle eine Ausgabe zur Folge haben kann die Konfiguration in der hier beschriebenen Art und Weise **nicht** fortgesetzt werden |

### Prüfen der Konfiguration

Führen Sie das Programm dsconfig mit dem Befehl get-administration-connector-prop aus, um eine vorhandene Konfiguration des HTTP Administration Connector in Erfahrung zu bringen.

|  | **Kommando** |
| --- | --- |
| . ods.env  dsconfig -X -n get-administration-connector-prop \  --hostname <hostname>.zds.bka.bund.de \  --port 7441 \  --bindDN cn=Directory\ Manager \  --bindPasswordFile ~/.secrets/credential/directory \  --connector-name HTTP |

Der HTTP Administration Connector ist normalerweise entsprechend vor konfiguriertaber unter Umständen nicht aktiviert:

|  | **Ausgabe** |
| --- | --- |
| Property : Value(s)  -----------------------:---------------  enabled : false  key-manager-provider : Administration  listen-address : 0.0.0.0  listen-port : 8444  ssl-cert-nickname : admin-cert  ssl-cipher-suite : -  ssl-protocol : -  trust-manager-provider : Administration |

### Konfiguration

Aktivierung HTTP Konnektor

Führen Sie das Programm dsconfig mit dem Befehl set-administration-connector-prop aus, um eine vorhandene Konfiguration des HTTP Administration Connector anzupassen.

|  | **Kommando** |
| --- | --- |
| . ods.env  dsconfig -X -n set-administration-connector-prop \  --hostname <hostname>.zds.bka.bund.de \  --port 7441 \  --bindDN cn=Directory\ Manager \  --bindPasswordFile ~/.secrets/credential/directory \  --connector-name HTTP \  --set listen-port:8444 \  --set enabled:true |

Ist der HTTP Administration Connector erfolgreich konfiguriert erfolgt keine weitere Ausgabe.

Der Erfolg des obigen Kommandos kann durch Wiederholdung des Kommandos in überprüft werden.

|  | **Ausgabe** |
| --- | --- |
| Property : Value(s)  -----------------------:---------------  enabled : true  key-manager-provider : Administration  listen-address : 0.0.0.0  listen-port : 8444  ssl-cert-nickname : admin-cert  ssl-cipher-suite : -  ssl-protocol : -  trust-manager-provider : Administration |

Aktivierung des Token Endpoint

Führen Sie das Programm dsconfig mit dem Befehl set-end-point-prop aus, um Token Endpoint zu aktivieren.

|  | **Kommando** |
| --- | --- |
| . ods.env  dsconfig -X -n set-end-point-prop \  --hostname <hostname>.zds.bka.bund.de \  --port 7441 \  --portProtocol LDAP \  --bindDN cn=Directory\ Manager \  --bindPasswordFile ~/.secrets/credential/directory \  --point-name 'Token Generator' \  --set enabled:true |

Ist der Token Endpoint erfolgreich aktiviert erfolgt keine weitere Ausgabe.

Aktivierung des REST Endpoint Extension

Führen Sie das Programm dsconfig mit dem Befehl set-extension-prop aus, um REST Endpoint zu aktivieren.

|  | **Kommando** |
| --- | --- |
| . ods.env  dsconfig -X -n set-extension-prop \  --hostname <hostname>.zds.bka.bund.de \  --port 7441 \  --portProtocol LDAP \  --bindDN cn=Directory\ Manager \  --bindPasswordFile ~/.secrets/credential/directory \  --extension-name 'REST Server' \  --set enabled:true |

Ist der REST Endpoint erfolgreich aktiviert erfolgt keine weitere Ausgabe.

Aktivierung des DirectoryT Endpoint Extension

Führen Sie das Programm dsconfig mit dem Befehl set-directory-end-point-prop aus, um REST Endpoint zu aktivieren.

|  | **Kommando** |
| --- | --- |
| . ods.env  dsconfig -X -n set-directory-end-point-prop \  --hostname oliver.cinnamonstar.net \  --port 7441 \  --portProtocol LDAP \  --bindDN cn=Directory\ Manager \  --bindPasswordFile ~/.secrets/credential/directory \  --set enabled:true |

|  | **Wichtig** |
| --- | --- |
| Der Verzeichnisdienst ist nach diesen Operationen neu zu starten. |