Installation Guide

LB.IAM Installation

Autor: Dieter Steding  
 Sophie Strecke

Erstelldatum: 20-06-2019

Letzte Änderung: 17-12-2020

Kontrollnummer: OC\_DE/300516442/DO.081/0007

Version: 1.0

**Freigabe:**

|  |  |
| --- | --- |
| Bundeskriminalamt |  |
| Oracle Consulting |  |

logored Kopie-Nr. \_\_\_\_\_

## Dokumentenkontrolle

### Änderungshistorie

| Date | Autor | Version | | Änderungsreferenz |
| --- | --- | --- | --- | --- |
|  |  |  |  | |
| 20-06-19 | Dieter Steding | 1.0 | Kein vorheriges Dokument | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |

### Reviewer

| Name | Position |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Inhalt

[Dokumentenkontrolle ii](#_Toc59098756)

[Änderungshistorie ii](#_Toc59098757)

[Reviewer ii](#_Toc59098758)

[Einführung 1](#_Toc59098759)

[Leserkreis 1](#_Toc59098760)

[Bezugsdokumente 1](#_Toc59098761)

[Vertraulichkeit 1](#_Toc59098762)

[Typografische Konventionen 1](#_Toc59098763)

[Anforderungen 2](#_Toc59098764)

[Hardware und Software Zertifizierung 2](#_Toc59098765)

[Überprüfung der Anforderungen 2](#_Toc59098766)

[Erforderliche Komponentenversionen 2](#_Toc59098767)

[Erforderliche Patches 2](#_Toc59098768)

[Konventionen Verzeichnisvariablen 2](#_Toc59098769)

[Softwareinstallation 4](#_Toc59098770)

[Roadmap 4](#_Toc59098771)

[Java Development KIT (JDK) 4](#_Toc59098772)

[Festlegung der Lokation des Oracle Inventory 4](#_Toc59098773)

[Fusion Middleware 5](#_Toc59098774)

[Oracle HTTP Server 5](#_Toc59098775)

[Vorgabe 5](#_Toc59098776)

[Installation 5](#_Toc59098777)

[Patch 6](#_Toc59098778)

[Domain Konfiguration 7](#_Toc59098779)

[HTTP Service 7](#_Toc59098780)

[Verzeichnis 7](#_Toc59098781)

[Auswahl Template 7](#_Toc59098782)

[Konfiguration Datenbank 7](#_Toc59098783)

[Erweiterte Konfiguration 8](#_Toc59098784)

[System Components 8](#_Toc59098785)

[OHS Server 9](#_Toc59098786)

[Machines 10](#_Toc59098787)

[Assign Server To Maschines 10](#_Toc59098788)

[Summary 10](#_Toc59098789)

[Post Conditions 10](#_Toc59098790)

[Component Logging 11](#_Toc59098791)

[Error Log 11](#_Toc59098792)

[Access Log 11](#_Toc59098793)

[Ausrollen des Clusters 12](#_Toc59098794)

[Packen der Domain Konfiguration 12](#_Toc59098795)

[Entpacken der Domain Konfiguration 12](#_Toc59098796)

[Post Conditions 12](#_Toc59098797)

[Domain Verwaltung 13](#_Toc59098798)

## Einführung

### Leserkreis

Dieses Dokument wendet sich an Personen, die sich mit der Installation der Oracle Identity und Access Management Infrastruktur befassen.

Dieses Dokument beschreibt die Installation des Oracle® HTTP Server 12c Release 12.2.1.3.0.

### Bezugsdokumente

Informationen zur Installation und Verwendung von Oracle Identity und Access Management finden Sie auf der folgenden Oracle-Hilfeseite:

* <https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/index.html>
* <https://docs.oracle.com/en/middleware/lifecycle/12.2.1.3/imedg/>

### Vertraulichkeit

Das in dieser Dokumentation enthaltene Material enthält geschützte, vertrauliche Informationen zu Oracle-Produkten und –Methoden.

Der Leserkreis erklärt sich damit einverstanden, dass die Informationen in dieser Dokumentation nicht nach außerhalb weitergegeben und nicht für andere Zwecke als zur Bewertung dieses Verfahrens vervielfältigt, verwendet oder weitergegeben werden.

### Typografische Konventionen

Die folgenden typografischen Konventionen werden in diesem Dokument verwendet.

|  |  |
| --- | --- |
| **Konvention** | **Bedeutung** |
| **Fettdruck** | Fettdruck kennzeichnet Elemente der grafischen Benutzeroberfläche, die einer Aktion zugeordnet sind, oder Begriffe, die im Text oder im Glossar definiert sind. |
| *kursiv* | Kursivschrift kennzeichnet Buchtitel, Hervorhebungen oder Platzhalter, für die Sie bestimmte Werte angeben. |
| monospace | Monospace kennzeichnet in einem Absatz Befehle, URLs, Code-Beispiele, Text, der auf dem Bildschirm angezeigt wird, oder Text, den Sie eingeben. |

## Anforderungen

### Hardware und Software Zertifizierung

Die plattformspezifischen Anforderungen an Hardware und Software, die in diesem Dokument aufgeführt werden, sind gültig für den Zeitpunkt zu dem, dieses Dokument erstellt wurde. Da neue Plattformen und Betriebssysteme zertifiziert werden können, nachdem dieses Dokument veröffentlicht wurde, wird empfohlen die Zertifizierungsmatrix auf Oracle Technology Network heranzuziehen. Dort befinden sich die aktuellsten Aussagen zu zertifizierten Plattformen und Betriebssystemen.

Die jeweilige Zertifizierungsmatrix für Produkte der Oracle Identity und Access Management Suite sind unter folgenden URLs verfügbar:

[Oracle® Fusion Middleware 12c (12.2.1.3.0)](https://www.oracle.com/technetwork/middleware/fmw-122130-certmatrix-3867828.xlsx)

### Überprüfung der Anforderungen

#### Erforderliche Komponentenversionen

| **Komponente** | **Version** |
| --- | --- |
| **Oracle Java Development Kit** | JDK 1.8.0\_133 oder höher |
| **Oracle Infrastruktur** | Oracle® WebLogic 12c (12.2.1.3.0) |
| **Oracle HTTP Server** | Oracle® HTTP Server 12c Release 12.2.1.3.0 |

#### Erforderliche Patches

| **Komponente** | **Patch** |
| --- | --- |
| **Oracle HTTP Server** | 29307387 |
| **Oracle Access Management Webgate 12c (12.2.1.3.0)** | 29034045 |

### Konventionen Verzeichnisvariablen

|  |  |
| --- | --- |
| **Variable** | **Bedeutung** |
| *STAGE* | Das Basisverzeichnis, unter dem Oracle-Produkt Medien für die Installation aufzufinden sind. |
| *JAVA\_HOME* | Der Speicherort, an dem das unterstützte Java Development Kit (JDK) installiert wurde. |
| *ORACLE\_BASE* | Das Basisverzeichnis, unter dem Oracle-Produkte installiert sind. |
|  |  |
| *ORACLE\_HOME* | Der Speicherort für die Binärdateien eines Produkts. Für die Host-Computer der Anwendungsebene wird sie auf einer gemeinsam genutzten Festplatte gespeichert. |
| *ORACLE\_COMMON\_HOME* | Das Verzeichnis in dem gängige Dienstprogramme, Bibliotheken und andere notwendigen Oracle Fusion Middleware-Produkte gespeichert sind. |
| *ORACLE\_RUNTIME* | Dieses Verzeichnis enthält die Oracle-Laufzeitartefakte, z. B. die JMS-Protokolle und TLogs.  In der Regel stellen Sie dieses Verzeichnis als separates freigegebenes Dateisystem bereit, auf das alle Hosts in der Domäne zugreifen können. |
| *KEYSTORE\_HOME* | Der freigegebene Speicherort für benutzerdefinierte Zertifikate und Schlüssel. |

## Softwareinstallation

|  |  |
| --- | --- |
|  | Wichtig: |
| Der empfohlene Installationsmodus für Oracle® HTTP Server 12c Release 12.2.1.3.0 ist der kombinierte Modus. Für den kombinierten Modus müssen vor der Installation von Oracle® HTTP Server 12c Release 12.2.1.3.0 einige abhängige Softwareprogramme installiert werden. |

### Roadmap

Die Installation erfolgt nachfolgendem Vorgehen

1. Installation eines zertifizierten Java Development KIT (JDK)
2. Festlegung der Lokation des Oracle Inventory
3. Installation Fusion Middleware
4. Installation Oracle HTTP Server
5. Konfiguration der Domains

### Java Development KIT (JDK)

|  | Wichtig: |
| --- | --- |
| Dieser Installationsschritt erfordert administrative Rechte auf dem Zielsystem |

|  |  |
| --- | --- |
| icon-note-16 | Hinweis: |
| Die Installation erfolgt in das Verzeichnis */usr/java/jdk1.8.0\_131* |

|  |  |
| --- | --- |
|  | Kommando: |
| rpm -ivh *<stage>*/jdk-8u131-linux-x64.rpm  update-alternatives --install /usr/bin/java /usr/java/jdk1.8.0\_131/bin/java 2  /usr/sbin/alternatives --config java  update-alternatives --install /usr/bin/java /usr/java/jdk1.8.0\_131/bin/javac 1  /usr/sbin/alternatives --config javac |

### Festlegung der Lokation des Oracle Inventory

Für die Installation wird ein Oracle Inventory benötigt, welches über folgende Kommandozeile festgelegt wird:

|  | Kommando: |
| --- | --- |
| touch /opt/oracle/fmwInst.loc  cat >> /opt/oracle/fmwInst.loc << EOF  inventory\_loc=/opt/oracle/inventory  inst\_group=asa  EOF |

### Fusion Middleware

| icon-note-16 | Hinweis: |
| --- | --- |
| Die Installation erfolgt in das Verzeichnis */opt/oracle/product/fmw/12.2.1* |

|  |  |
| --- | --- |
|  | Kommando: |
| <STAGE>/ORACLE\_FMW\_12.2.1.3\_Download/12.2.1.3.0\_WebTier/fmw\_12.2.1.3.0\_ohs\_linux64.bin –invPtrLoc /opt/oracle/fmwInst.loc |

Dadurch wird der Installationsassistent der Softwarekomponente gestartet, in dem die nachfolgenden Schritte abgearbeitet werden:

| **Bildschirm** | **Parameter** | **Wert** |
| --- | --- | --- |
| **Welcome** |  |  |
| **Auto Updates** | Skip Auto Updates | ausgewählt |
| **Installation Location** | Oracle Home | /opt/oracle/product/fmw/12.2.1 |
| **Prerequisite Checks** |  |  |
| **Installation Summary** |  |  |
| **Installation Process** |  |  |
| **Installation Complete** |  |  |

### Oracle HTTP Server

#### Vorgabe

| **Vorgaben** | **Verwendung** |
| --- | --- |
| **Verzeichnis** | *<ORACLE\_BASE>*/fmw/12.2.1 |

#### Installation

Die Installation erfolgt über das Kommando:

|  |  |
| --- | --- |
|  | Kommando: |
| cd *<STAGE>*/12.2.1.3.0\_WebTier  ./fmw\_12.2.1.3.0\_ohs\_linux64.bin |

Dadurch wird der Installationsassistent der Softwarekomponente gestartet, in dem die nachfolgenden Schritte abgearbeitet werden:

| **Bildschirm** | **Parameter** | **Wert** |
| --- | --- | --- |
| **Welcome** |  |  |
| **Auto Updates** | Skip Auto Updates | ausgewählt |
| **Installation Location** | Oracle Home | /opt/oracle/product/fmw/12.2.1 |
| **Installation Type** | Collocated HTTP Server (Managed through WebLogic server) | ausgewählt |
| **JDK Selection** | JDK Home | /usr/java/latest |
| **Prerequisite Checks** |  |  |
| **Installation Summary** |  |  |
| **Installation Process** |  |  |
| **Installation Complete** |  |  |

#### Patch

Nach erfolgreicher Installation erfolgt die Applizierung der letzten Bundle Patches für die Software Komponente.

##### HTTP Server

|  |  |
| --- | --- |
|  | Kommando: |
| . fmw.oui  cd *<STAGE>/*WWW/29307387  opatch apply -jdk /usr/java/latest |

##### WebGate

|  |  |
| --- | --- |
|  | Kommando: |
| . fmw.oui  cd *<STAGE>/*WWW/29034045  opatch apply -jdk /usr/java/latest |

## Domain Konfiguration

Wenn Sie einer vorhandenen Domäne eine Oracle HTTP Server-Instanz hinzufügen, stellen Sie sicher, dass die Ports verfügbar sind, die Sie der neuen Komponenten zuweisen.

|  |  |
| --- | --- |
|  | Wichtig: |
| Der Konfigurationsassistent führt keine automatische Überprüfung der zugewiesenen Ports durch. |

Vor dem Starten des Konfigurationsassistenten ist es wichtig, den Administrationsserver herunterzufahren. Dadurch wird verhindert, dass während der Konfiguration der Instanz Konfigurationssperren, -speicherungen oder -aktivierungen auftreten.

Um den Administrationsserver zu stoppen führen Sie folgende Schritte aus:

TBD

#### HTTP Service

| **Topik** | **Wert** | |
| --- | --- | --- |
| **Name** | WWW | |
| **Port** | **non-SSL** | **SSL** |
|  | 80 | 443 |

### Verzeichnis

Die Konfiguration der Instanz erfolgt über Erweitern der Domain config.

Aus diesem Grund wird die Option **Update an existing domain** ausgewählt.

| **Komponente** | **Template** |
| --- | --- |
| **Domain Location** | /opt/Anwendungen/domains/config |

### Auswahl Template

Für Oracle http Server wird folgend Komponente ausgewählt:

| **Komponente** | **Template** |
| --- | --- |
| **HTTP Server** | Oracle http Server (Collocated) – 12.2.1.3.0 [ohs] |

### Konfiguration Datenbank

Die Datenbankschemata wurden im Abschnitt Anforderung der Konfiguration der Datenbank Schemata erzeugt und in *Common Infrastructure Services* persistiert. Der Abruf der voreingestellten Datenbankkonfiguration erfolgt durch Zugriff auf dieses Schema.

| **Option** | **Wert** |
| --- | --- |
| **Auto Configuration** | RCU Data |
| **Vendor** | Oracle |
| **Driver** | Oracle's Driver (Thin) for Service connections; Versions: Any |
| **Host Name** | <???> |
| **DBMS/Service** | <???> |
| **Port** | 1521 |
| **Schema Owner** | ICD\_STB |
| **Schema Password** |  |

Der Abruf der Konfiguration erfolgt über die Schaltfläche **Get RCU Configuration**. Das führt zur Überprüfung der eingegebenen Optionen und bei Erfolg zur Anzeige der gespeicherten Konfiguration.

| D:\tt\icon-warning-16.png | **Warnung** |
| --- | --- |
| Zu diesem Zeitpunkt sind die Werte so konfiguriert, dass eine Verbindung zu einer Single Instanz hergestellt wird. Für die hier vorgenommene Konfiguration wird jedoch eine hochverfügbare RAC-Datenbank verwendet. |

| D:\tt\icon-tip-16.png | **Tipp** |
| --- | --- |
| Oracle empfiehlt, dass jedes der Komponentenschemata eine Active GridLink-Datenquelle verwenden. |

Folgendes Vorgehen ist anzuwenden, um alle Datenquellen nach GridLink zu konvertieren:

1. Wählen alle Schemas auswählen, indem das Kontrollkästchen in der ersten Kopfzeile der Schematabelle aktiviert wird.
2. Auf **Convert to GridLink** klicken

| **Option** | **Wert** |
| --- | --- |
| **SCAN, Host Name, and Port** |  |
| **ONS Host and Port** |  |
| **Enable Fan** | <checked> |

### Erweiterte Konfiguration

In der Erweiterten Konfiguration sind die Optionen

1. System Components

auszuwählen.

#### System Components

Verwenden Sie den Bildschirm Systemkomponenten, um Details zu Oracle HTTP Server-Instanzen anzugeben.

Auf dem Bildschirm Systemkomponenten:

1. Klicken Sie auf **Add**, um eine neue Oracle HTTP Server-Instanz zu erstellen.
2. Geben Sie im Feld Systemkomponente *<Name>* an.
3. Geben Sie *OHS* im Feld Komponententyp an.
4. Restart Interval Seconds  
   Geben Sie die Anzahl der Sekunden an, die gewartet werden soll, bevor ein Neustart versucht wird, wenn eine Anwendung nicht reagiert.
5. Restart Delay Second  
   : Geben Sie die Anzahl der Sekunden an, die zwischen den Neustartversuchen gewartet werden soll.

Verwenden Sie hierfür die Werte aus nachfolgender Tabelle.

| **System Component** | **Component Type** |
| --- | --- |
| **ohs1** | OHS |
| **ohs2** | OHS |
| **ohs3** | OHS |

#### OHS Server

Verwenden Sie den Bildschirm OHS-Server, um die Oracle HTTP Server-Instanzen in der Domäne zu konfigurieren.

Geben Sie im Feld Listen Address die IP-Adresse des Hosts an, auf dem sich die Oracle HTTP Server-Instanz befinden soll.

|  |  |
| --- | --- |
|  | Wichtig: |
| Verwenden Sie nicht **localhost**. |

##### ohs1

| **Vorgaben** | **Verwendung** |
| --- | --- |
| **System Component** | ohs1 |
| **Admin Host** | vwasc181.zds.bka.bund.de |
| **Admin Port** | 7005 |
| **Listen Address** | vwasc181.zds.bka.bund.de |
| **Listen Port** | 80 |
| **SSL Listen Port** | 443 |
| **Server Name** | http:// vwasc181.zds.bka.bund.de |

##### ohs2

| **Vorgaben** | **Verwendung** |
| --- | --- |
| **System Component** | ohs2 |
| **Admin Host** | vwasc181.zds.bka.bund.de |
| **Admin Port** | 7005 |
| **Listen Address** | vwasc182.zds.bka.bund.de |
| **Listen Port** | 80 |
| **SSL Listen Port** | 443 |
| **Server Name** | http:// vwasc182.zds.bka.bund.de |

##### Ohs3

| **Vorgaben** | **Verwendung** |
| --- | --- |
| **System Component** | ohs3 |
| **Admin Host** | Vwasc181.zds.bka.bund.de |
| **Admin Port** | 7005 |
| **Listen Address** | vwasc281.zds.bka.bund.de |
| **Listen Port** | 80 |
| **SSL Listen Port** | 443 |
| **Server Name** | http:// vwasc282.zds.bka.bund.de |

### Machines

Dieser Schritt wird übersprungen.

### Assign Server To Maschines

| D:\tt\icon-warning-16.png | **Warnung** |
| --- | --- |
| Alle Systemkomponenten werden den erzeugten UNIX Maschine zugeordnet. |

Die Zuordnung erfolgt nach dem Muster:

| **Unix Machine** | **Systemkomponente** |
| --- | --- |
| **vwasc181** | ohs1 |
| **vwasc182** | ohs2 |
| **vwasc291** | ohs3 |

### Summary

Vorgenommene Konfigurationen prüfen und den „Update“ drücken.

Die Konfiguration der WebLogic Server Domain wir vorgenommen.

### Post Conditions

## Component Logging

#### Error Log

##### General

| **Kategorie** | **Wert** |
| --- | --- |
| **Log File/Directory** | /var/opt/Anwendungen/logs/instances/config/${COMPONENT\_NAME}-server.log |
| **Level** | WARNING:32 |

##### Rotation Policy

| **Kategorie** | **Wert** |
| --- | --- |
| **Time Based** | <checked> |
| **Rotation Frequency** | Day(s) 1 |
| **Retention Period** | Day(s) 7 |

#### Access Log

##### General

| **Kategorie** | **Wert** |
| --- | --- |
| **Log File/Directory** | /var/opt/Anwendungen/logs/instances/config/${COMPONENT\_NAME}-access.log |
| **Log Formt** | common |

##### Rotation Policy

| **Kategorie** | **Wert** |
| --- | --- |
| **Time Based** | <checked> |
| **Rotation Frequency** | Day(s) 1 |
| **Retention Period** | Day(s) 7 |

## Ausrollen des Clusters

Nachdem die Konfiguration für den ersten Knoten erfolgreich war, wird sie an die weiteren Knoten weitergeben. Dazu wird die Domain auf dem ersten Knoten gepackt und auf den anderen Knoten entpackt.

### Packen der Domain Konfiguration

|  | **Kommando** |
| --- | --- |
| . fmw.env  ${ORACLE\_HOME}/oracle\_common/common/bin/pack.sh -domain=/opt/Anwendungen/domains/config -app\_dir=/opt/Anwendungen/applications/config -template=${TEMP}/confg-domain.jar |

| D:\tt\icon-warning-16.png | **Warnung** |
| --- | --- |
| Die mit dem Parameter *template* spezifizierte Datei ist gegebenenfalls vor Ausführung des Kommandos zu löschen |

### Entpacken der Domain Konfiguration

Das Entpacken der Domain wird auf jedem weiteren Knoten mit folgendem Kommando vorgenommen:

|  | **Kommando** |
| --- | --- |
| . fmw.env  ${ORACLE\_HOME}/oracle\_common/common/bin/unpack.sh -domain=/opt/Anwendungen/domains/config -app\_dir=/opt/Anwendungen/applications/config -template=${TEMP}/config-domain.jar |

### Post Conditions

Nach dem Ausrollen der Domain auf einem weiteren Knoten ist als erstes der WebLogic Nodemanager auf diesem Knoten zu starten.

Anschließend können über die WebLogic Console der Domain die für diesen Knoten konfigurierten Managed Server gestartet werden.

| **Machine** | **HTTP Server** |
| --- | --- |
| **vwasc182** | ohs2 |
| **vwasc291** | ohs3 |

## Domain Verwaltung

Damit die Umgebung funktioniert, müssen die folgenden Dienste und Komponenten betriebsbereit sein (dies impliziert die Reihenfolge des Starts in derselben Reihenfolge).

1. Starten wlst Shell

|  | **Kommando** |
| --- | --- |
| . fmw.env  ${JRF\_HOME}/common/bin/wlst.sh |

1. Verbindung zur Domain

|  | **Kommando** |
| --- | --- |
| nmConnect('weblogic','wmkah1mdkh','vwase052.entw.bka.bund.de','5556','config','/opt/Anwendungen/domains/config','PLAIN') |

| icon-note-16 | Hinweis |
| --- | --- |
| Dir Benutzername und das Kennwort werden nur zur Authentifizierung der Verbindungen zwischen Nodemanager und dem Client verwendet.  Sie sind unabhängig von den Sicherheitsdaten, die für die Verwaltung der Domain definiert und im Verzeichnis /opt/Anwendungen/domains/config/config/ in der Datei nm\_password.properties gespeichert. |

1. Starten des Manage Server oam

|  | **Kommando** |
| --- | --- |
| nmStart(serverName= 'ohs1', serverType= 'OHS')  nmStart(serverName= 'ohs2', serverType= 'OHS')  nmStart(serverName= 'ohs3', serverType= 'OHS') |