IM.IAM Deployment Guide

Bundeskriminalamt – Oracle IAM-Projekt

Autor: Dieter Steding

Erstelldatum: 26. Januar 2019

Letzte Änderung: 2. Februar 2019

Kontrollnummer: <Document Reference Number>

Version: Entwurf

Freigabe:

|  |  |
| --- | --- |
| <Freigabe 1> |  |
| <Freigabe 2> |  |

# Dokumentenkontrolle

## Änderungshistorie

| Datum | Autor | Version | | Änderungsreferenz |
| --- | --- | --- | --- | --- |
| 26. Januar 2019 | Dieter Steding | | Entwurf 1 | Kein vorheriges Dokument |
|  |  | |  |  |
|  |  | |  |  |
|  |  | |  |  |

## Reviewer

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

Inhalt

1 Dokumentenkontrolle ii

1.1 Änderungshistorie ii

1.2 Reviewer ii

2 Einführung 1

2.1 Ziele und Umfang 1

2.2 Bezugsdokumente 1

2.3 Hardware und Softwareumgebungen 1

3 Systemtechnisches Design 2

3.1 IAM Core Services 2

3.2 IAM Autoritative Datenquelle 2

3.2.1 Integration Autoritative Datenquelle – Initial On-Boarding 2

3.2.2 Integration Autoritative Datenquelle – Fortwährender Datenabgleich 2

3.3 IAM Identity Service 3

4 Pre-Deployment Anforderungen 4

4.1 Hardware und Software Zertifizierung 4

4.2 Überprüfung der Anforderungen 4

4.2.1 Erforderliche Komponentenversionen 4

4.2.2 Erforderliche Patches 4

4.2.3 Weitere erforderliche Software 4

4.3 Checkliste für die Bereitstellung 5

4.3.1 E-Mail Server 5

4.3.2 Oracle Metadata Repository 5

4.3.3 Oracle Identity Manager 6

4.3.4 Oracle SOA Suite 7

4.3.5 Oracle BI Publisher 7

5 Pre-Deployment Konfiguration 9

5.1 Datensicherung 9

5.2 Konfiguration Protokollierung Identity Manager 9

5.2.1 Schematischer Ablauf 9

5.2.2 Hierarchie der Protokollierung 11

5.2.3 Konfiguration 11

5.2.4 Konfiguration der Standard Logger 12

5.3 Systemeigenschaften 12

5.4 Deployment Pakete 13

5.4.1 Paket 0000 systemCustomization 14

5.4.2 Paket 0100 systemFramework 14

5.4.3 Paket 0101 entityCustomization 15

5.4.4 Paket 0102 systemIntegration 15

5.4.5 Paket 0200 trustedSource ??? 15

6 Bereitstellung des Deployment 17

6.1 Vorbereitung 17

6.1.1 Bezug der Ablaufsteuerung 17

6.1.2 Festlegung der-Konfiguration 18

6.1.2.1 Anlegen und Einrichten des Wallet 23

6.1.2.2 Anlegen und Einrichten der Parameter 26

6.1.2.3 Substitution der Platzhalter in der Konfiguration 30

6.2 Bezug des Deployments 33

7 Bereitstellungsprozess 34

7.1 Setup 34

7.1.1 Multi-Language Support 35

7.1.2 Plug-In Store Konfiguration 36

7.1.3 Standard Workflow Konfiguration 36

7.1.4 Notifikation Services Konfiguration 36

7.1.5 Konfiguration System Eigenschaften 36

7.1.6 Frontend Customization Konfiguration 36

7.2 Neustart 40

7.3 Deployment 40

7.3.1 Deployment Entity Konfiguration und Integration 40

7.4 Initial On-Boarding 41

7.4.1 Identitäten 41

7.5 Post Deployment 41

7.5.1 Entitlement Transformation 41

7.5.2 Catalog Synchronisation 42

8 Umsetzung des Berechtigungskonzepts 43

8.1 Berechtigungsobjekte Oracle Identity Manager 43

9 Anhang 44

9.1 Verwalten der IT Ressourcen 44

9.2 Verwalten der Hintergrundprozess 44

# Einführung

## Ziele und Umfang

Dieses Dokument beschreibt das Vorgehen für die Bereitstellung der konfigurierten Konnektoren im Oracle Identity Manager. Alle notwendigen Einstellungen, die nach der Bereitstellung der Konnektoren notwendig sind, sind ebenso aufgeführt.

Die Informationen zu Unternehmensstruktur und Benutzerdaten sind in Datenquelle des Bundeskriminalamtes hinterlegt. Diese Informationen werden durch eine direkte Kopplung aus der Datenquelle in den Oracle Identity Manager geladen.

Die dadurch erzeugten Identitätsprofile im Oracle Identity Manager wiederum dienen dazu jedem dieser Profile in den entsprechenden Zielsystemen ein Benutzerkonto und Berechtigungen zuzuweisen, falls dass für die Interaktion einer natürlichen Person mit dem Zielsystem notwendig ist.

Aus technischer Sicht sind diese Kopplungen Konnektoren, die in Oracle Identity Manager geladen, anschließend konfiguriert und durch diese Systemkomponente ausgeführt werden.

## Bezugsdokumente

| ID | Dokument | Version | Datum | Verantwortlicher |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Hardware und Softwareumgebungen

| Umgebung | Beschreibung |
| --- | --- |
| Entwicklung | Die Systemumgebung, auf der Entwickler die Implementierung vornehmen. |
| Akzeptanz / Test | Testumgebung für den Test neuer Softwareversionen. Hier werden die funktionalen Tests durch Endanwender vorgenommen |
| Pre-Produktion | Die Systemumgebung, in der die durch einzelne Entwickler bereitgestellten Artefakte zusammengeführt werden und umfängliche Integrationstests der einzelnen Module durchgeführt werden |
| Produktion | Die Umgebung auf der das eigentliche IT-System betrieben und von Benutzern bedient wird. |

# Systemtechnisches Design

* IAM Core Services
* IAM Autoritative Datenquellen
* IAM Identity Service

## IAM Core Services

Die konzipierte Systemlandschaft des IAM Core Services ist in nachfolgender Abbildung dargestellt:

TBD

## IAM Autoritative Datenquelle

Die Datenquelle des Bundeskriminalamts wird als primäre Quelle für die Identitäten (Personen) und Organisationen angebunden. Hierfür wird eine Systemverbindung über das Datenprotokoll zwischen Oracle Identity Manager und Datenquelle eingerichtet. Für die Übertragung der Attributwerte aus Datenquelle in das Datenmodell des Oracle Identity Manager wird je nach Entitätstyp ein entsprechendes Schema verwendet.

### Integration Autoritative Datenquelle – Initial On-Boarding

Initial On-Boarding bezeichnet den Vorgang des Ladens der Identitätsdaten aus der autoritativen Datenquelle. Dieser Vorgang wird zu einem Zeitpunkt durchgeführt, zu dem die Automatismen der Lebenszyklusverwaltung von Identitäten im System noch nicht vorhanden bzw. deaktiviert sind. Nur so können Konflikte mit der zu einem späteren Zeitpunkt durchzuführenden Integration von Zielsystemen und deren Account Discovery vermieden werden.

### Integration Autoritative Datenquelle – Fortwährender Datenabgleich

Die IDM Lösung stützt sich auf Identitätsdaten der Datenquelle des Bundeskriminalamtes ab, die fortwährend abgeglichen werden, um Benutzerkonten und deren Berechtigungen zu verwalten. Die Identitätsdaten werden in der gleichen Weise aus dieser Datenquelle bezogen, wie es während des Initial On-Boarding vorgenommen wurde. Nach dem Ausrollen der IDM Lösung werden durch Verschieben der Identitäten in der Datenquelle die unterschiedlichen Zustände des Anstellungsverhältnisses einer Identität wiedergespiegelt. Diese Verschiebung löst die entsprechenden Ereignisse in der IDM Lösung aus. Derartige Ereignisse beinhalten Aktivitäten zu:

* Identity Create
* Identity Modify
* Identity Delete

die wiederum Auswirkungen auf die in der Lösung vorgehaltenen Identitätsdaten einer Person haben.

Änderungen werden durch den Konnektor basierend auf den Attributen

erkannt.

Ist der Stammsatz einer Identität gelöscht, verbleiben diese Daten in der IDM Lösung. In Datenquelle befinden sich die Identitätsdaten nicht mehr. In der IDM-Lösung verändert sich der Zustand der Identität zu gelöscht.

## IAM Identity Service

# Pre-Deployment Anforderungen

## Hardware und Software Zertifizierung

Die plattformspezifischen Anforderungen an Hardware und Software, die in diesem Deployment Guide 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 Applikationsserver | Oracle® WebLogic 12c (12.2.1.3.0) |
| Oracle Datenbank | Oracle® RDBMS 12c (12.2.0.1.0 oder höher |
| Oracle Identity Manager | Oracle® Identity Manager 12c Release 12.2.1.3.0 |
| Oracle SOA Suite | Oracle® SOA Suite 12c Release 12.2.1.3.0 |

### Erforderliche Patches

| Komponente | Patch |
| --- | --- |
| Oracle Identity Manager | Patch 28492345 (Oracle® Identity Management Suite Bundle Patch 12.2.1.3.181016)  Patch 28682376 |
| Oracle Access Manager | Patch 28492345 (Oracle® Identity Management Suite Bundle Patch 12.2.1.3.181016)  Patch 28595514 |

### Weitere erforderliche Software

| Komponente | Patch |
| --- | --- |
| Version Control System Repository | Apache™ Subversion® 1.9 oder höher |
| Version Control System Kommandozeile | Apache™ Subversion® 1.9 oder höher |
| Oracle Fusion Middleware Stack (SOA) | Oracle® Fusion Middleware 12c Release 12.1.3.0 |
| Oracle Identity Manager Client | Oracle® Identity Manager 12c Release 12.1.3.0 |

## Checkliste für die Bereitstellung

Während der Bereitstellung werden für die abschließende Konfiguration folgende Daten abverlangt:

### E-Mail Server

| Parameter | Bedeutung |
| --- | --- |
| Server Name | Der vollqualifizierte DNS-Name des technischen Systems, auf dem der anzusprechende Mail-Dienst bereitgestellt ist |
| Benutzeranmeldung | Der technische Benutzername mit dem sich Oracle Identity Manager gegenüber dem Mail-Dienst authentisiert. |
| Benutzerkennwort | Das Kennwort für den technischen Benutzernamen für eine erfolgreiche Authentisierung. |
| Authentication | Entweder true oder false je nachdem, ob der Mail-Dienst eine Authentisierung voraussetzt oder nicht. |

### Oracle Metadata Repository

| Parameter | Bedeutung |
| --- | --- |
| Database Server | Der vollqualifizierte DNS-Name des technischen Systems, auf dem die Datenbank für das Oracle Identity Manager zugeordnete Metadata Repository bereitgestellt wurde.  **Beispiel**: buster.vm.oracle.com |
| Port | Der Port, der durch den Oracle Listener verwendet wird, um den Zugriff auf die Datenbank des Metadata Repository zu vermitteln.  Beispiel: 7021 |
| Database Service | Der Name des Datenbankdienstes der Oracle Listener-Konfiguration.  **Beispiel**: mdr.vm.oracle.com |
| Principal Name | Der Name des Datenbankbenutzers, für den das Datenbankschema des Metadata Repository während der Ausführung des Repository Creation Utilities (RCU) angelegt wurde.  **Beispiel**: igd\_mds |
| Principal Password | Das Kennwort des Datenbankbenutzers, für den das Datenbankschema des Metadata Repository während der Ausführung des Repository Creation Utilities (RCU) angelegt wurde.  **Beispiel**: wmkah1mdFh@nuhr |

### Oracle Identity Manager

| Parameter | Bedeutung |
| --- | --- |
| Database Server | Der vollqualifizierte DNS-Name des technischen Systems, auf dem die Datenbank für Oracle Identity Manager bereitgestellt wurde.  **Beispiel**: buster.vm.oracle.com |
| Port | Der Port, der durch den Oracle Listener verwendet wird, um den Zugriff auf die Datenbank zu vermitteln.  **Beispiel**: 7021 |
| Database Service | Der Name des Datenbankdienstes der Oracle Listener-Konfiguration.  **Beispiel**: mdr.vm.oracle.com |
| OIM Database User Name | Der Name des Datenbankbenutzers, für den das Datenbankschema des Oracle Identity Managers während der Ausführung des Repository Creation Utilities (RCU) angelegt wurde.  **Beispiel**: igd\_oim |
| System User Password | Das Kennwort des Datenbankbenutzers *SYSTEM* das bei der Erzeugung der Datenbank vergeben wurde.  **Beispiel**: wmkah1mdFh@nuhr. |
| Server Name | Der vollqualifizierte DNS-Name des technischen Systems, auf dem Oracle Identity Manager während der Erzeugung der WebLogic Server Domain bereitgestellt wurde.  **Beispiel**: buster.vm.oracle.com |
| Server Port | Der Port, der dem Managed Server der WebLogic Server Domain zugweisen wurde, um Anfragen zu bearbeiten.  **Beispiel**: 8005 |
| Principal Name | Der Name des Systemadministrators für Oracle Identity Manager.  **Standard**: XELSYSADM |
| Principal Password | Das Kennwort des Systemadministrators für Oracle Identity Manager das bei der Konfiguration der WebLogic Domain vergeben wurde.  **Beispiel**: wmkah1mdFh@nuhr |
| Installation | Das Oracle Home Verzeichnis, in das die Softwareinstallation der Systemkomponente vorgenommen wurde.  **Beispiel**: /opt/oracle/product/iam/12.2.1/idm/server |

### Oracle SOA Suite

| Parameter | Bedeutung |
| --- | --- |
| Server Name | Der vollqualifizierte DNS-Name des technischen Systems, auf dem die Oracle SOA Suite während der Erzeugung der WebLogic Server Domain bereitgestellt wurde.  **Beispiel**: buster.vm.oracle.com |
| Server Port | Der Port, der dem Managed Server der WebLogic Server Domain zugweisen wurde, um Anfragen zu bearbeiten.  **Beispiel**: 8001 |
| Principal Name | Der Name des Benutzerkontos, das während der Erzeugung der WebLogic Server Domain als Standard Administrator festgelegt wurde.  **Standard**: weblogic |
| Principal Password | Das Kennwort für den Standard Administrator der WebLogic Server Domainvergeben wurde.  **Beispiel**: wmkah1mdFh@nuhr |
| Installation | Das Oracle Home Verzeichnis, in das die Softwareinstallation der Systemkomponente vorgenommen wurde.  **Beispiel**: /opt/oracle/product/iam/12.2.1/soa |

### Oracle BI Publisher

| Parameter | Bedeutung |
| --- | --- |
| Server Name | Der vollqualifizierte DNS-Name des technischen Systems, auf dem die Oracle BI Enterprise Edition während der Erzeugung der WebLogic Server Domain bereitgestellt wurde.  **Beispiel**: buster.vm.oracle.com |
| Server Port | Der Port, der dem Managed Server der WebLogic Server Domain zugweisen wurde, um Anfragen zu bearbeiten.  **Beispiel**: 8019 |
| Principal Name | Der Name des Benutzerkontos, das während der Erzeugung des Berichtsdienstes Standard Administrator festgelegt wurde.  **Standard**: weblogic |
| Principal Password | Das Kennwort für den Standard Administrator des Berichtsdienstes bei der Konfiguration der WebLogic Domain vergeben wurde.  **Beispiel**: wmkah1mdFh@nuhr |
| Installation | Das Oracle Home Verzeichnis, in das die Softwareinstallation der Systemkomponente vorgenommen wurde.  **Beispiel**: /opt/oracle/product/bis/12.2.1 |

# Pre-Deployment Konfiguration

## Datensicherung

Bevor mit der Bereitstellung der Konnektoren begonnen wird, wird empfohlen eine Datensicherung der bestehenden Konfiguration vorzunehmen. Diese Datensicherung erlaubt es den ursprünglichen Zustand wiederherzustellen, für den Fall, dass während der Bereitstellung irreversible Fehler auftreten.

Um die bestehende Konfiguration durch eine Datensicherung zu sichern, sind folgende Schritte auszuführen:

1. Jede laufende Instanz der SOA Suite und des Oracle Identity Managers ist herunterzufahren
2. Erzeugen eines neuen Verzeichnisses, z.B. OIM\_ADMIN/backup
3. Exportieren der Datenbankschemata
4. Sichern folgender Verzeichnisse  
     
   OIM\_ORACLE\_HOME/apps/oim.ear/META-INF  
   OIM\_ORACLE\_HOME/apps/oim.ear/APP-INF/classes  
   OIM\_ORACLE\_HOME/apps/oim.ear/xlWebApp/WEB-INF/classes  
     
   OIM\_ORACLE\_HOME/server/ConnectorDefaultDirectory  
   OIM\_ORACLE\_HOME/server/customResources  
   OIM\_ORACLE\_HOME/server/icf/intg  
   OIM\_ORACLE\_HOME/server/bundles

## Konfiguration Protokollierung Identity Manager

Die Ausgabe in Protokolldateien basiert auf dem Framework Oracle Diagnostic Logging (ODL). Dieses Framework wiederum ist eine Erweiterung des Java EE Frameworks.

### Schematischer Ablauf

Anstatt auftretende Fehler und Infomeldungen auf der Standardausgabe auszugeben, dient ODL dazu, die Meldungen über sogenannte Logger an einen oder mehrere Handler weiterzuleiten. Neben der Auswahl des Handlers wird gleichzeitig auf Grund der Wichtigkeit der Meldung entschieden, ob diese überhaupt weitergeleitet wird. Die Filterung und die Formate der Ausgabe können zur Laufzeit konfiguriert werden.

ODL besteht aus zwei Hauptkomponenten:

* Logger  
  Dabei handelt es sich um Namenskonventionen, welche von der Applikation benutzt werden. Üblicherweise werden in der Konfigurationsdatei Logger für ganze (Super-)Pakete beschrieben, in der Applikation selbst wird mittels Logger.getLogger(java.lang.Class) der entsprechende Logger anhand des Klassen- und Paketnamens bestimmt. Damit können die Ausgaben entsprechend der Softwarestruktur separat gefiltert und ausgegeben werden. In der Konfigurationsdatei wird neben den Namen der Logger auch deren Level gesetzt. Damit ist es möglich, unterschiedlichen Paketen und somit unterschiedlichen Komponenten verschiedene Log-Level zuzuordnen. Darüber hinaus können entweder allgemein oder auch zu jedem Logger spezifisch ein oder mehrere Handler definiert werden. Somit ist es beispielsweise möglich, fatale Fehler nicht nur in eine Datei zu schreiben, sondern auch gleichzeitig per E-Mail an einen Administrator zu schicken.
* Handler  
  Diese bestimmen mittels Konfiguration der entsprechenden Handler-Klasse, wohin die Protokollausgaben geschrieben werden sollen, und mittels Konfiguration des Formats, wie dorthin geschrieben werden soll. Neben der reinen Nachricht können mittels Muster zusätzlich Wichtigkeit, Datum, Logger-Name, Klassenname und Methodenname bis hin zur genauen Codezeile ausgegeben werden. Nachfolgende Abbildung veranschaulicht das generelle Prinzip.



### Hierarchie der Protokollierung



### Konfiguration

Es gibt Möglichkeiten, die Anzahl der Meldungen innerhalb der Konfigurationsdatei unter Zuhilfenahme der Anweisung „Level“ zu beeinflussen. "Level" legt die Art und Menge der Eintragungen fest, die in der Protokolldatei abgelegt werden sollen. Mögliche Werte sind:

| Typ | Level | Beschreibung |
| --- | --- | --- |
| INCIDENT\_ERROR | 1 |  |
| ERROR | 1 |  |
| WARNING | 1 |  |
| MOTIFICATION | 1 |  |
| NOTIFICATION | 16 |  |
| TRACE | 1 |  |
| TRACE | 16 |  |
| TRACE | 32 |  |

Die Einrichtung der Nachrichtentypen und –Level ist auch unter der Perspektive Performanz zu betrachten.

### Konfiguration der Standard Logger

| Kategorie | Typ | Level |
| --- | --- | --- |
| XELLERATE.ACCOUNTMANAGEMENT | ERRRO | 1 |
| XELLERATE.ADAPTERS | ERROR | 1 |
| XELLERATE.AUDITOR | ERROR | 1 |
| XELLERATE.APIS | NOTIFICATION | 1 |
| XELLERATE.CACHEMANAGEMENT | ERROR | 1 |
| XELLERATE.CSRFILTER | ERROR | 1 |
| XELLERATE.DATABASE | ERROR | 1 |
| XELLERATE.DDM | ERROR | 1 |
| XELLERATE.DDM.EXPORT | ERROR | 1 |
| XELLERATE.DDM.IMPORT | ERROR | 1 |
| XELLERATE.DDM.RESOLUTION | ERROR | 1 |
| XELLERATE.DDM.STATS | ERROR | 1 |
| XELLERATE.JAVACLIENT | ERROR | 1 |
| XELLERATE.PERFORMANCE | ERROR | 1 |
| XELLERATE.PREPAREDSTATEMENT | ERROR | 1 |
| XELLERATE.POLICIES | ERROR | 1 |
| XELLERATE.REQUESTS | ERROR | 1 |
| XELLERATE.RULES | ERROR | 1 |
| XELLERATE.SCHEDULER | ERROR | 1 |
| XELLERATE.SCHEDULER.TASK | ERROR | 1 |
| XELLERATE.SCHEDULER.WEBSTARTUP | ERROR | 1 |
| XELLERATE.SERVER | ERROR | 1 |
| XELLERATE.WEBAPP | ERROR | 1 |
| XELLERATE.XSSFILTER | ERROR | 1 |

## Systemeigenschaften

Während des Deployment-Vorgangs wird die Systemkonfiguration von Oracle Identity Manager geändert. Die Notwendigkeit dieser Änderungen ergibt sich aus den Anforderungen der an das Verhalten des Systems gestellt wird. Nachfolgende Tabelle führt alle Systemeigenschaften auf, die durch das Deployment automatisch geändert werden.

| Systemeigenschaft | Auslieferung | Änderung |
| --- | --- | --- |
| AllowDisabledManagers | false | true |
| Recon.SEND\_NOTIFICATION | false | true |
| XL.UserNameDomain | oracle.com | bka.bund.de |
| XL.SendEmailNotificationBasedOnUserLocal | false | true |
| XL.AllowAPHarvesting | false | true |
| XL.AllowAPBasedMultipleAccountProvisioning | false | true |
| XL.RoleAuditLevel |  | Role |
| XL.CatalogAuditDataCollection |  | catalog |
| OIG.IsIdentityAuditorEnabled | false | true |
| XL.AllowRoleHierarchicalPolicyEval | false | true |

## Deployment Pakete

Basierend auf den Erfahrungen von Oracle Consulting sind alle Implementierungen strukturiert in Deployment Paketen abgelegt.

Diese Pakete basieren auf der technischen Konnektor-Struktur. Dadurch wird ein nahezu vollautomatischer Deployment-Prozess erreicht. Der Deployment-Prozess basiert auf dem Oracle Identity Manager Deployment Manager.

Nachfolgende Tabelle führt alle Pakete auf, die für das Deployment bereitstehen.

| Verzeichnis/Datei | Beschreibung | Version |
| --- | --- | --- |
| 0000 systemCustomization | Systemeigenschaften und Komponentenkonfiguration | 12.2.1.3.0 |
| 0100 systemFramework | Standardartefakte von Oracle Consulting | 12.2.1.3.0 |
| 0101 entityCustomization | Anpassung der Datenmodelle und der Benutzeroberfläche für die Standardentitäten Benutzer und Organisation | 12.2.1.3.0 |
| 0102 systemIntegration | Gemeinsam durch Systemkonnektoren verwendete Basiskomponenten wie Java Bibliotheken, Task Adapter und Scheduler Tasks. | 12.2.1.3.0 |
| 0200 trustedSource ??? | Konfigurationen der Datenquelle | 12.2.1.3.0 |

Wie aus der ersichtlich wird, beginnen die einzelnen Deployment-Pakete mit einer Nummer. Diese Nummer ist wichtig für die Einhaltung des Ablaufs des Deployment-Vorgangs. Auf Grund der Abhängigkeiten zwischen den einzelnen Paketen ist es wesentlich, dass Pakete mit einer niedrigeren Nummer vor einem Paket mit einer höheren Nummer installiert werden. Das Deployment ist demzufolge hierarchisch aufgebaut. Die Anhängigkeiten werden durch nachfolgende Abbildung verdeutlicht:

Der Inhalt der einzelnen Pakete wird in den nachfolgenden Kapiteln beschrieben.

### Paket 0000 systemCustomization

| Verzeichnis/Datei | Beschreibung |
| --- | --- |
| lib/bka.iam.identity.library.war | Bibliothek für die UI Anpassungen |
| lib/customResources.properties | Property Bundle für UI Anpassungen der Standard Entitäten in der Sprachausprägung Common |
| lib/customResources\_de.properties | Property Bundle für UI Anpassungen der Standard Entitäten in der Sprachausprägung Deutsch |
| lib/customResources\_en.properties | Property Bundle für UI Anpassungen der Standard Entitäten in der Sprachausprägung Englisch |
| lib/customResources\_en\_US.properties | Property Bundle für UI Anpassungen der Standard Entitäten in der Sprachausprägung Englisch in der Variante Amerikanisch |
| xml/oim-looup-dm.xml |  |
| xml/oim-properties-dm.xml | System Eigenschaften |
| xml/ps2-properties-dm.xml | System Eigenschaften |
| xml/ps3-properties-dm.xml | System Eigenschaften |

### Paket 0100 systemFramework

| Verzeichnis/Datei | Beschreibung |
| --- | --- |
| lib/hst-foundation.jar | Java Implementierungen für die Bereitstellung allgemeiner Klassen und deren Methoden in JEE Umgebungen. |
| lib/ocs-adapter.jar | Java Implementierungen für die Bereitstellung wiederkehrender Anwendungsfälle während der Provisionierung. |
| lib/ocs-common.jar | Java Implementierungen gemeinsam durch in ocs-adapter.jar und ocs-scheduler verwendeter allgemeiner Datenmodelle und Klassen. |
| lib/ocs-foundation.jar | Basis Implementierungen zur Abstraktion das API’s von Oracle Identity Manager für die Standardisierung von Abläufen während des Datenabgleichs und der Provisionierung. |
| lib/ocs-scheduler.jar | Java Implementierungen für die Bereitstellung wiederkehrender Anwendungsfälle für den internen und Internen Datenabgleich. |
| lib/ocs-utility.jar | Wiederverwendbare Softwarekomponenten wie Transformationen, Datei‑ oder Datenbankzugriffe, die in Prozesse für den Datenabgleich oder die Provisionierung zur Laufzeit eingebunden werden können |
| xml/ocs-adapter-dm.xml | Mapping für die Adapter Factory des Oracle Identity Managers für die Einbindung der durch ocs-adapter.jar bereitgestellten Implementierungen in Oracle Identity Manager. |
| xml/ocs-lookup-dm.xml | Standardisierte Wertelisten wie Sprache, Zeitzonen usw. |

### Paket 0101 entityCustomization

| Verzeichnis/Datei | Beschreibung |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

### Paket 0102 systemIntegration

| Verzeichnis/Datei | Beschreibung |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

### Paket 0200 trustedSource ???

| Verzeichnis/Datei | Beschreibung |
| --- | --- |
|  |  |
|  |  |
|  |  |

# Bereitstellung des Deployment

## Vorbereitung

Für die halbautomatische Bereitstellung sind einige vorbereitende Schritte notwendig, um das Deployment durchführen zu können. Diese Schritte sind im Einzelnen:

* Bezug der Ablaufsteuerung
* Vereinbarung der Konfiguration
* Anlegen und Einrichten des Wallet
* Substitution der Platzhalter in der Konfiguration
* Bezug des Deployment

### Bezug der Ablaufsteuerung

Die Ablaufsteuerung wird über das Version Control Repository bezogen. Der Bezug dieser Steuerung wird durch die Kommandozeilenfolge vorgenommen.

mkdir –p <working>

cd <working>

svn -–username <username> export –-force <sourceurl> .

| Parameter | Beschreibung |
| --- | --- |
| <working> | Der Name des Verzeichnisses, in das der Export vorgenommen wird und aus dem heraus alle nachfolgenden Operationen gestartet werden. |
| <username> | Der Benutzername der durch das Kommando svn für die Anmeldung am Repository zu verwenden ist. |
| <sourceurl> | Die URL zum Versions Control System über die die Deployment-Steuerung in das lokale Dateisystem exportiert wird.  **Beispiel**: https://gcdpsource.oracle.com/svn/iam-bka/internal/1.0/trunk/IdentityTransition |

Bei erstmaliger Ausführung des Exports aus dem Version Control System wird das Kennwort für das spezifizierte Benutzerkonto <username> interaktiv abgefragt.

Authentication realm: <<https://gcdpsource.oracle.com:443>> GCDP Subversion

Password for ‘dieter.steding@oracle.com’:

Bei Eingabe eines falschen Kennworts wird der ausführende Benutzer wiederholt aufgefordert sich durch erneute Eingabe von Benutzername und Kennwort gegenüber dem Version Control System zu authentisieren.

Ist die Kennwortprüfung erfolgreich besteht die Möglichkeit das Kennwort unverschlüsselt zu speichern.

-----------------------------------------------------------------------

ATTENTION! Your password for authentication realm:

<<https://gcdpsource.oracle.com:443>> GCDP Subversion

Can only be stored to disk unencrypted! You are advised to configure

Your system so that Subversion can store passwords encrypted, if

Possible. See the documentation for details.

You can avoid future appearances of this warning by setting the value

Of the ‘store-plaintext-passwords’ option to either ‘yes’ or ‘no’ in

‘/home/dsteding/.subversion/servers’.

-----------------------------------------------------------------------

Store password unencrypted (yes/no)?

Diese Abfrage sollte temporär mit yes beantwortet werden.

Es wird empfohlen, dass das aktuelle Arbeitsverzeichnis gegen unberechtigte Zugriffe geschützt wird. Dazu wird folgende Kommandozeilen verwendet:

find ./ -type f -exec chmod 600 {} \;

find ./ -type d -exec chmod 700 {} \;

Anschließend ist für das zentrale Shell-Skript der Ausführungsmodus auf Benutzerebene freizugeben. Dazu wird folgende Kommandozeile verwendet:

chmod u+x install installAll configAll onboard onboard-identity onboard-system

### Festlegung der-Konfiguration

Das Deployment kann von einem zentralen Server aus auf alle für diesen Server erreichbaren Systemkomponenten über die Ablaufsteuerung vorgenommen werden.

Bestimmte Konfigurationsparameter sind ausgelagert und werden über externe Dateien gespeist. Das betrifft:

* Umgebungsabhängige Einstellungen wie Sever Namen und Ports
* Kennwörter
* Absenderadressen von E-Mail-Benachrichtigungen
* Konfigurationen der Bereitstellung der SOA Composites

Diese Konfigurationsparameter sind durch Platzhalter in der jeweiligen Konfigurationsdatei deklariert und werden nach dem Bezug des Deployment aus dem Version Control System entsprechenden substituiert. Nachfolgende Tabelle führt alle Platzhalter auf, die verwendet werden.

| Wert | Zieldatei | Beschreibung |
| --- | --- | --- |
| \_\_BIP\_PROT\_\_ | bip-server.xml | Protokoll das Oracle Identity Manager verwendet um Berichte in Oracle BI Publisher abzurufen.  **Standard**: http |
| \_\_BIP\_HOST\_\_ | bip-server.xml | Der vollqualifizierte DNS-Name des technischen Systems, auf dem der anzusprechende Dienst bereitgestellt ist.  **Beispiel**: buster.vm.oracle.com |
| \_\_BIP\_PORT\_\_ | bip-server.xml | Der Port, der dem Managed Server der WebLogic Server Domain zugweisen wurde, um Anfragen zu bearbeiten.  **Beispiel**: 8019 |
| \_\_BIP\_USER\_\_ | bip-server.xml | Der Name des Benutzerkontos, das während der Erzeugung des Berichtsdienstes als Standard Administrator des Berichtsdienstes festgelegt wurde.  **Standard**: weblogic |
| \_\_BIP\_PASS\_\_ | bip-server.xml | Das Kennwort das für den Standard Administrator des Berichtsdienstes vergeben wurde.  **Beispiel**: wmkah1mdFh@nuhr |
| \_\_BIP\_HOME\_\_ | bip-server.xml | Das Oracle Home Verzeichnis, in das die Softwareinstallation der Systemkomponente vorgenommen wurde.  **Beispiel**: /opt/oracle/product/bis/12.2.1 |
| \_\_BIP\_CONF\_\_ | bip-server.xml |  |
| \_\_JEE\_PROT\_\_ | jee-server.xml | Protokoll, das während des Deployments für die Kommunikation mit dem Admin Server der WebLogic Domain verwendet wird.  **Standard**: t3 |
| \_\_JEE\_HOST\_\_ | jee-server.xml | Der vollqualifizierte DNS-Name des technischen Systems, auf dem der Admin Server der WebLogic Domain bereitgestellt ist  **Beispiel**: buster.vm.oracle.com |
| \_\_JEE\_PORT\_\_ | jee-server.xml | Der Port, der dem Admin Server der WebLogic Server Domain zugweisen wurde, um Anfragen zu bearbeiten.  **Beispiel**: 7001 |
| \_\_JEE\_NAME\_\_ | jee-server.xml | Der Name des Admin Servers, der während der Erzeugung der WebLogic Domain festgelegt wurde.  **Standard**: AdminServer |
| \_\_JEE\_USER\_\_ | jee-server.xml | Der Name des Benutzerkontos, das während der Erzeugung der WebLogic Server Domain als Domain Administrator festgelegt wurde.  **Beispiel**: weblogic |
| \_\_JEE\_PASS\_\_ | jee-server.xml | Das Kennwort für den Domain Administrator der WebLogic Domain vergeben wurde.  **Beispiel**: wmkah1mdFh@nuhr |
| \_\_JEE\_HOME\_\_ | jee-server.xml | Das Oracle Home Verzeichnis, in das die Softwareinstallation des Oracle WebLogic Servers vorgenommen wurde.  **Beispiel**: /opt/oracle/product/wls/12.2.1 |
| \_\_LBR\_HOST\_\_ | oim-server.xml soa-server.xml | Der vollqualifizierte DNS-Name des technischen Systems, auf dem der Load Balancer, der die Frontend URL für Oracle Identity Manager bereitstellt, betrieben wird.  **Beispiel**: igd.vm.oracle.com |
| \_\_LBR\_PORT\_\_ | oim-server.xml | Der Port, der dem Load Balancer, um Anfragen zu bearbeiten.  **Beispiel**: 80 |
| \_\_OIM\_PROT\_\_ | oim-server.xml | Protokoll, das während des Deployments für die Kommunikation mit dem Managed Server der WebLogic Domain verwendet wird.  **Standard**: t3 |
| \_\_OIM\_HOST\_\_ | oim-server.xml | Der vollqualifizierte DNS-Name des technischen Systems, auf dem der Managed Server der WebLogic Domain bereitgestellt ist  **Beispiel**: buster.vm.oracle.com |
| \_\_OIM\_PORT\_\_ | oim-server.xml | Der Port, der dem Managed Server der WebLogic Server Domain zugweisen wurde, um Anfragen zu bearbeiten.  **Beispiel**: 8005 |
| \_\_OIM\_NAME\_\_ | oim-server.xml | Der Name des Managed Servers, der während der Erzeugung der WebLogic Domain festgelegt wurde.  **Beispiel**: oim |
| \_\_OIM\_USER\_\_ | oim-server.xml | Der Name des Systemadministrators für Oracle Identity Manager.  **Standard**: XELSYSADM |
| \_\_OIM\_PASS | oim-server.xml | Das Kennwort des Systemadministrators für Oracle Identity Manager.  **Beispiel**: wmkah1mdFh@nuhr |
| \_\_OIM\_HOME\_\_ | oim-server.xml | Das Oracle Home Verzeichnis, in das die Softwareinstallation der Systemkomponente vorgenommen wurde.  **Beispiel**: /opt/oracle/product/iam/12.2.1/idm/server |
| \_\_OIM\_AUTH\_\_ | oim-server.xml | **Beispiel**: /opt/oracle/product/iam/12.2.1/idm/designconsole/config/authwl.conf |
| \_\_MDS\_HOST\_\_ | mds-server.xml | Der vollqualifizierte DNS-Name des technischen Systems, auf dem die Datenbank für das Oracle Identity Manager zugeordnete Metadata Repository bereitgestellt wurde.  **Beispiel**: buster.vm.oracle.com |
| \_\_MDS\_PORT\_\_ | mds-server.xml | Der Port, der durch den Oracle Listener verwendet wird, um den Zugriff auf die Datenbank des Metadata Repository zu vermitteln.  **Beispiel**: 7021 |
| \_\_MDS\_NAME\_\_ | mds-server.xml | Der Name des Datenbankdienstes der Oracle Listener-Konfiguration.  **Beispiel**: mdr.vm.oracle.com |
| \_\_MDS\_USER\_\_ | mds-server.xml | Der Name des Datenbankbenutzers, für den das Datenbankschema des Metadata Repository während der Ausführung des Repository Creation Utilities (RCU) angelegt wurde.  **Beispiel**: igd\_mds |
| \_\_MDS\_PASS\_\_ | mds-server.xml | Das Kennwort des Datenbankbenutzers, für den das Datenbankschema des Metadata Repository während der Ausführung des Repository Creation Utilities (RCU) angelegt wurde.  **Beispiel**: wmkah1mdFh@nuhr |
| \_\_SMTP\_HOST\_\_ | oim-config-ant.xml | Der vollqualifizierte DNS-Name des technischen Systems, auf dem der SMTP Server betrieben wird.  **Beispiel**: dovecot.vm.oracle.com |
| \_\_SMTP\_PORT\_\_ | oim-config-ant.xml | Der Port, der dem SMTP Server zugweisen wurde, um Anfragen zu bearbeiten.  **Standard**: 25 |
| \_\_SMTP\_USER\_\_ | oim-config-ant.xml | Der technische Benutzername mit dem sich Oracle Identity Manager gegenüber dem Mail-Dienst authentisiert.  **Beispiel**: extmailadmin |
| \_\_SMTP\_PASS\_\_ | oim-config-ant.xml | Das Kennwort für den technischen Benutzernamen für eine erfolgreiche Authentisierung.  **Beispiel**: wmkah1mdFh@nuhr |
| \_\_SMTP\_ADDR\_ | oim-config-ant.xml | Absender der Nachrichten.  **Beispiel**: identity@vm.oracle.com |
| \_\_SCP\_HOST\_\_ | scp-server.xml | Der vollqualifizierte DNS-Name des technischen Systems, gegenüber dem das Deployment vorgenommen werden soll  **Beispiel**: buster.vm.oracle.com |
| \_\_SCP\_PORT\_\_ | scp-server.xml | Der Port, der für den SSH Daemon konfiguriert wurde, um Anfragen zu bearbeiten.  **Beispiel**: 7001 |
| \_\_SCP\_USER\_\_ | scp-server.xml | Das Benutzerkonto des Zielsystems des Deployments mit dem der Transfer von Dateien vorgenommen wird.  **Beispiel**: oracle |
| \_\_SCP\_PASS\_\_ | scp-server.xml | Das Kennwort Benutzerkonto des Zielsystems des Deployments mit dem der Transfer von Dateien vorgenommen wird.  **Beispiel**: wmkah1mdFh@nuhr |
| \_\_SCP\_CERT\_\_ | scp-server.xml | Der Pfad zur Datei des öffentlichen Schlüssels des Benutzerkontos das für den Transfer der Dateien verwendet wird.  **Beispiel**: /home/oracle/.ssh/dieter.steding@oracle.com |
| \_\_SOA\_PROT\_\_ | soa-server.xml | Protokoll, das während des Deployments für die Kommunikation mit dem Managed Server der WebLogic Domain verwendet wird.  **Standard**: t3 |
| \_\_SOA\_HOST\_\_ | soa-server.xml | Der vollqualifizierte DNS-Name des technischen Systems, auf dem die Oracle SOA Suite während der Erzeugung der WebLogic Server Domain bereitgestellt wurde.  **Beispiel**: buster.vm.oracle.com |
| \_\_SOA\_PORT\_\_ | soa-server.xml | Der Port, der dem Managed Server der WebLogic Server Domain zugweisen wurde, um Anfragen zu bearbeiten.  **Beispiel**: 8001 |
| \_\_SOA\_NAME\_\_ | soa-server.xml | Der Name des Managed Servers, der während der Erzeugung der WebLogic Domain festgelegt wurde.  **Beispiel**: soa |
| \_\_SOA\_USER\_\_ | soa-server.xml | Der Name des Benutzerkontos, das während der Erzeugung der WebLogic Server Domain als Standard Administrator festgelegt wurde.  **Standard**: weblogic |
| \_\_SOA\_PASS\_\_ | soa-server.xml | Das Kennwort das für den Standard Administrator der WebLogic Server Domain vergeben wurde.  **Beispiel**: wmkah1mdFh@nuhr |
| \_\_SOA\_HOME\_\_ | soa-server.xml | Das Oracle Home Verzeichnis, in das die Softwareinstallation der Systemkomponente vorgenommen wurde.  **Beispiel**: /opt/oracle/product/iam/12.2.1/soa |

#### Anlegen und Einrichten des Wallet

Aus Sicherheitsgründen sind in der Ablaufsteuerung keine Kennwörter in Klartext hinterlegt. Die zu verwendenden Kennwörter werden vor der Ausführung des Deployments in den entsprechenden Konfigurationsdateien substituiert. Der Bezug der dafür notwendigen Kennwörter wird über ein Wallet, welches durch Oracle Platform Security Services verwaltet wird, isoliert.

Das Wallet wird in einem Verzeichnis des Betriebssystems angelegt.

|  |  |
| --- | --- |
| warning | **Achtung**: |
| Die Lage dieses Verzeichnisses durch die Ablaufsteuerung vorgegeben  In diesem Verzeichnis darf kein anderes Oracle Wallet gespeichert sein. |

Zum Anlegen des Wallet wird das Werkzeug mkstore verwendet. Der Aufruf zum Anlegen sieht folgendermaßen aus:

cd <working>

mkstore -wrl jps/identity -create

| Parameter | Beschreibung |
| --- | --- |
| <working> | Der Name des Verzeichnisses, in das der Export vorgenommen wird und aus dem heraus alle nachfolgenden Operationen gestartet werden. |

Es wird ein Passwort abgefragt, mit dem das Wallet vor unbefugtem Öffnen geschützt wird. Das Passwort muss aus 8 bis 30 Zeichen bestehen und mindestens ein alphanumerisches sowie ein numerisches Zeichen enthalten.

Enter

Das Wallet wird - wie oben bereits angemerkt - mit dem Namen ewallet.p12 angelegt. Außerdem wird im selben Verzeichnis eine ebenfalls verschlüsselte Datei namens cwallet.sso angelegt. Diese Datei enthält das Passwort für das Wallet und wird zum Zugriff auf das Wallet genutzt. Das Wallet wird durch diesen Mechanismus zu einem sogenannten auto open wallet.

Die Einträge erfolgen wiederum mit mkstore

echo <credential> | mkstore -wrl jps/identity -createUserCredential <stage> <alias> <password>

| Parameter | Beschreibung |
| --- | --- |
| <credential> | Das Kennwort, das bei der Anlage des Wallet vergeben wurde.  **Beispiel**: wmkah1mdFh@nuhr |
| <stage> | Der Name der logischen Gruppe von Credential‘s.  **Beispiel**: extdev |
| <alias> | Der Aliasname des Credential‘s welcher später im Schritt Substitution für die Extraktion des Kennworts verwendet wird.  **Beispiel**: oim |
| <password> | Das Credential welches im Schritt Substitution zu verwenden ist.  **Beispiel**: wmkah1mFh@nuhr |

Die Werte für den Parameter <stage> zu unterliegen folgenden Wertevorrat:

| Wert | Beschreibung |
| --- | --- |
| intdev | Logischen Gruppe von Credential’s für die Entwicklungsumgebung des Internen Identity Managements. |
| intint | Logischen Gruppe von Credential’s für die Akzeptanz / Test des Internen Identity Managements |
| intedu | Logischen Gruppe von Credential’s für die Schulungsumgebung des Internen Identity Managements |
| intppr | Logischen Gruppe von Credential’s für die Pre Produktionsumgebung des Internen Identity Managements |
| intppa | Logischen Gruppe von Credential’s für die Produktionsumgebung des Internen Identity Managements |

Die Werte für den Parameter <alias> zu unterliegen folgenden Wertevorrat:

| Alias | Zielvariable | Beschreibung |
| --- | --- | --- |
| bip@oig | \_\_BIP\_PASS\_\_ | Das Kennwort das für den Standard Administrator des Berichtsdienstes vergeben wurde.  **Beispiel**: wmkah1mdFh@nuhr |
| jee@oig | \_\_JEE\_PASS\_\_ | Das Kennwort für den Standard Administrator der WebLogic Domain vergeben wurde.  **Beispiel**: wmkah1mdFh@nuhr |
| mds@oig | \_\_MDS\_PASS\_\_ | Das Kennwort des Datenbankbenutzers, für den das Datenbankschema des Metadata Repository während der Ausführung des Repository Creation Utilities (RCU) angelegt wurde.  **Beispiel**: wmkah1mdFh@nuhr |
| oim@oig | \_\_OIM\_PASS\_\_ | Das Kennwort des Systemadministrators für Oracle Identity Manager.  **Beispiel**: wmkah1mdFh@nuhr |
| scp@oig | \_\_SCP\_\_PASS\_\_ | Das Kennwort Benutzerkonto des Zielsystems des Deployments mit dem der Transfer von Dateien vorgenommen wird.  **Beispiel**: wmkah1mdFh@nuhr |
| soa@oig | \_\_SOA\_PASS\_\_ | Das Kennwort das für den Standard Administrator der WebLogic Server Domain vergeben wurde.  **Beispiel**: wmkah1mdFh@nuhr |

#### Anlegen und Einrichten der Parameter

Die Parameter für die Substitution der übrigen Parameter wird über Textdateien vorgenommen. Die Dateien mit den Parametern werden in einem Verzeichnis des Betriebssystems angelegt.

|  |  |
| --- | --- |
| warning | **Achtung**: |
| Die Lage dieses Verzeichnisses durch die Ablaufsteuerung vorgegeben. |

Die Namen dieser Dateien folgen der Namensgebung des Parameters <stage>.

Der Aufruf zum Anlegen der Textdatei sieht folgendermaßen aus:

cd <working>

cp ./tpl/intoig.properties ./cfg/<stage>.properties

| Parameter | Beschreibung |
| --- | --- |
| <working> | Der Name des Verzeichnisses, in das der Export vorgenommen wird und aus dem heraus alle nachfolgenden Operationen gestartet werden. |
| <stage> | Der Name der logischen Gruppe von Parametern.  **Beispiel**: intdev |

Die Werte für den Parameter <stage> zu unterliegen folgenden Wertevorrat:

| Datei | Beschreibung |
| --- | --- |
| intdev | Substitutionswerte für die Entwicklungsumgebung des Internen Identity Managements. |
| intint | Substitutionswerte für die Akzeptanz / Test des Internen Identity Managements |
| intedu | Substitutionswerte für die Schulungsumgebung des Internen Identity Managements |
| intppr | Substitutionswerte für die Pre Produktionsumgebung des Internen Identity Managements |
| intppa | Substitutionswerte für die Produktionsumgebung des Internen Identity Managements |

Die Deklaration der Werte für die Substitution der Platzhalter in jeder der Dateien ist dann folgendermaßen vorzunehmen:

|  |  |
| --- | --- |
| info | **Hinweis**: |
| Die in der Spalte Beschreibung als Standard bzw. Beispiel aufgeführten Werte sind in der Kopiervorlage entsprechend vorbelegt. |

| Wert | Zielvariable | Beschreibung |
| --- | --- | --- |
| BIP\_PROT | \_\_BIP\_PROT\_\_ | Protokoll das Oracle Identity Manager verwendet um Berichte in Oracle BI Publisher abzurufen.  **Standard**: http |
| BIP\_HOST | \_\_BIP\_HOST\_\_ | Der vollqualifizierte DNS-Name des technischen Systems, auf dem der anzusprechende Dienst bereitgestellt ist.  **Beispiel**: buster.vm.oracle.com |
| BIP\_PORT | \_\_BIP\_PORT\_\_ | Der Port, der dem Managed Server der WebLogic Server Domain zugweisen wurde, um Anfragen zu bearbeiten.  **Beispiel**: 8019 |
| BIP\_USER | \_\_BIP\_USER\_\_ | Der Name des Benutzerkontos, das während der Erzeugung des Berichtsdienstes als Standard Administrator des Berichtsdienstes festgelegt wurde.  **Standard**: weblogic |
| BIP\_HOME | \_\_BIP\_HOME\_\_ | Das Oracle Home Verzeichnis, in das die Softwareinstallation der Systemkomponente vorgenommen wurde.  **Beispiel**: /opt/oracle/product/bis/12.2.1 |
| BIP\_CONF | \_\_BIP\_CONF\_\_ | **Beispiel**: /dbs/oracle/XDO |
| JEE\_PROT\_ | \_\_JEE\_PROT\_\_ | Protokoll, das während des Deployments für die Kommunikation mit dem Admin Server der WebLogic Domain verwendet wird.  **Standard**: t3 |
| JEE\_HOST | \_\_JEE\_HOST\_\_ | Der vollqualifizierte DNS-Name des technischen Systems, auf dem der Admin Server der WebLogic Domain bereitgestellt ist.  **Beispiel**: buster.vm.oracle.com |
| JEE\_PORT | \_\_JEE\_PORT\_\_ | Der Port, der dem Admin Server der WebLogic Server Domain zugweisen wurde, um Anfragen zu bearbeiten.  **Beispiel**: 7001 |
| JEE\_NAME | \_\_JEE\_NAME\_\_ | Der Name des Admin Servers, der während der Erzeugung der WebLogic Domain festgelegt wurde.  **Standard**: adm |
| JEE\_USER | \_\_JEE\_USER\_\_ | Der Name des Benutzerkontos, das während der Erzeugung der WebLogic Server Domain als Domain Administrator festgelegt wurde.  **Beispiel**: weblogic |
| JEE\_HOME | \_\_JEE\_HOME\_\_ | Das Oracle Home Verzeichnis, in das die Softwareinstallation des Oracle WebLogic Servers vorgenommen wurde.  **Beispiel**: /opt/oracle/product/wls/12.2.1 |
| OIM\_PROT | \_\_OIM\_PROT\_\_ | Protokoll, das während des Deployments für die Kommunikation mit dem Managed Server der WebLogic Domain verwendet wird.  **Standard**: t3 |
| OIM\_HOST | \_\_OIM\_HOST\_\_ | Der vollqualifizierte DNS-Name des technischen Systems, auf dem der Managed Server der WebLogic Domain bereitgestellt ist.  **Beispiel**: buster.vm.oracle.com |
| OIM\_PORT | \_\_OIM\_PORT\_\_ | Der Port, der dem Managed Server der WebLogic Server Domain zugweisen wurde, um Anfragen zu bearbeiten.  **Beispiel**: 8005 |
| OIM\_NAME | \_\_OIM\_NAME\_\_ | Der Name des Managed Servers, der während der Erzeugung der WebLogic Domain festgelegt wurde.  **Beispiel**: oim |
| OIM\_USER | \_\_OIM\_USER\_\_ | Der Name des Systemadministrators für Oracle Identity Manager.  **Standard**: XELSYSADM |
| OIM\_HOME | \_\_OIM\_HOME\_\_ | Das Oracle Home Verzeichnis, in das die Softwareinstallation der Systemkomponente vorgenommen wurde.  **Beispiel**: /opt/oracle/product/iam/12.2.1/idm/server |
| OIM\_AUTH | \_\_OIM\_AUTH\_\_ | **Beispiel**: /opt/oracle/product/iam/12.2.1/idm/designconsole/config/authwl.conf |
| MDS\_HOST | \_\_MDS\_HOST\_\_ | Der vollqualifizierte DNS-Name des technischen Systems, auf dem die Datenbank für das Oracle Identity Manager zugeordnete Metadata Repository bereitgestellt wurde.  **Beispiel**: buster.vm.oracle.com |
| MDS\_PORT | \_\_MDS\_PORT\_\_ | Der Port, der durch den Oracle Listener verwendet wird, um den Zugriff auf die Datenbank des Metadata Repository zu vermitteln.  **Beispiel**: 7021 |
| MDS\_NAME | \_\_MDS\_NAME\_\_ | Der Name des Datenbankdienstes der Oracle Listener-Konfiguration.  **Beispiel**: mdr.vm.oracle.com |
| MDS\_USER | \_\_MDS\_USER\_\_ | Der Name des Datenbankbenutzers, für den das Datenbankschema des Metadata Repository während der Ausführung des Repository Creation Utilities (RCU) angelegt wurde.  **Beispiel**: igd\_mds |
| SMTP\_HOST | \_\_SMTP\_HOST\_\_ | Der vollqualifizierte DNS-Name des technischen Systems, auf dem der SMTP Server betrieben wird.  **Beispiel**: mail.vm.oracle.com |
| SMTP\_PORT | \_\_SMTP\_PORT\_\_ | Der Port, der dem SMTP Server zugweisen wurde, um Anfragen zu bearbeiten.  **Standard**: 25 |
| SMTP\_USER | \_\_SMTP\_USER\_\_ | Der technische Benutzername mit dem sich Oracle Identity Manager gegenüber dem Mail-Dienst authentisiert.  **Beispiel**: xelsysadm |
| SMTP\_ADDR | \_\_SMTP\_ADDR\_\_ | Absender der Nachrichten.  **Beispiel**: identity@vm.oracle.com |
| SCP\_HOST | \_\_SCP\_HOST\_\_ | Der vollqualifizierte DNS-Name des technischen Systems, gegenüber dem das Deployment vorgenommen werden soll.  **Beispiel**: buster.vm.oracle.com |
| SCP\_PORT | \_\_SCP\_PORT\_\_ | Der Port, der für den SSH Daemon konfiguriert wurde, um Anfragen zu bearbeiten.  **Beispiel**: 7022 |
| SCP\_USER | \_\_SCP\_USER\_\_ | Das Benutzerkonto des Zielsystems des Deployments mit dem der Transfer von Dateien vorgenommen wird.  **Beispiel**: oracle |
| SCP\_CERT | \_\_SCP\_CERT\_\_ | Der Pfad zur Datei des öffentlichen Schlüssels des Benutzerkontos das für den Transfer der Dateien verwendet wird.  **Beispiel**: /home/oracle/.ssh/dieter.steding@oracle.com |
| SOA\_PROT | \_\_SOA\_PROT\_\_ | Protokoll, das während des Deployments für die Kommunikation mit dem Managed Server der WebLogic Domain verwendet wird.  **Standard**: t3 |
| SOA\_HOST | \_\_SOA\_HOST\_\_ | Der vollqualifizierte DNS-Name des technischen Systems, auf dem die Oracle SOA Suite während der Erzeugung der WebLogic Server Domain bereitgestellt wurde.  **Beispiel**: buster.vm.oracle.com |
| SOA\_PORT | \_\_SOA\_PORT\_\_ | Der Port, der dem Managed Server der WebLogic Server Domain zugweisen wurde, um Anfragen zu bearbeiten.  **Beispiel**: 8001 |
| SOA\_NAME | \_\_SOA\_NAME\_\_ | Der Name des Managed Servers, der während der Erzeugung der WebLogic Domain festgelegt wurde.  **Beispiel**: soa |
| SOA\_USER | \_\_SOA\_USER\_\_ | Der Name des Benutzerkontos, das während der Erzeugung der WebLogic Server Domain als Standard Administrator festgelegt wurde.  **Standard**: weblogic |
| SOA\_HOME | \_\_SOA\_HOME\_\_ | Das Oracle Home Verzeichnis, in das die Softwareinstallation der Systemkomponente vorgenommen wurde.  **Beispiel**: /opt/oracle/product/iam/12.2.1/soa |

#### Substitution der Platzhalter in der Konfiguration

Die Substitution der Platzhalter in den Konfigurationsdateien erfolgt über eine Shell‑Skript.

Für dessen Ausführung werden Umgebungsvariablen vorausgesetzt. Diese Umgebungsvariablen werden vorzugsweise in einer Datei global für alle die Infrastruktur umfassenden Systemkomponenten erzeugt. Somit wird sichergestellt, dass unabhängig von einem Systemkomponenten-Deployment alle notwendigen Informationen deklariert sind. Vorzugsweise ist die Datei im Dateipfad des ausführenden Benutzers auffindbar. Die empfohlene Lokation für diese Datei ist:

${HOME}/bin

Die Namen dieser Dateien sollten der Namensgebung des Parameters <stage> folgen.

| Datei | Beschreibung |
| --- | --- |
| intdev | Deklaration der Umgebungsvariablen für die Entwicklungsumgebung des Internen Identity Managements. |
| intint | Deklaration der Umgebungsvariablen für die Akzeptanz / Test des Internen Identity Managements |
| intedu | Deklaration der Umgebungsvariablen für die Schulungsumgebung des Internen Identity Managements |
| intppr | Deklaration der Umgebungsvariablen für die Pre Produktionsumgebung des Internen Identity Managements |
| intppa | Deklaration der Umgebungsvariablen für die Produktionsumgebung des Internen Identity Managements |

Für die Ausführung des Shell-Skript werden die nachfolgend aufgeführten Umgebungsvariablen vorausgesetzt:

| Umgebungsvariable | Bedeutung |
| --- | --- |
| ORACLE\_BASE | The root of the Oracle Component directory tree. If you install an OFA-compliant database using Oracle Universal Installer defaults, then ORACLE\_BASE is /opt/products/fmw. |
| FMW\_HOME | Location of the middleware home on which Oracle Identity Manager, Oracle Access Manager, Oracle SOA Suite and Oracle BI Publisher are installed. |
| JAVA\_HOME | Location of the Java Development Kit installation. It is usually parallel to FMW\_HOME.  **Example**: ${FMW\_HOME}/../jdk |
| JAVA\_VENDOR | Specifies the vendor of the JDK.  **Example**: Sun |
| ANT\_HOME | Location of the ANT installation. It is usually under *FMW\_HOME.*  **Example**: ${FMW\_HOME}/modules/thirdparty/org.apache.ant/1.9.8.0.0/apache-ant-1.9.8 |
| OIG\_PREFIX | The deployment specific prefix to pick up Identity Manager related artifacts during the deployment.  **Example**: extdev |
| SOA\_PREFIX | The deployment specific prefix to pick up Workflow related artifacts during the deployment.  **Example**: extdev |
| WLS\_HOME | Directory on which WebLogic server is installed. It is usually under *FMW\_HOME.*  **Example**: ${FMW\_HOME}/wls |
| BIP\_HOME | Directory on which Oracle BI Publisher is installed server is installed. It is usually under *FMW\_HOME.*  **Example**: ${FMW\_HOME}/bis |
| IAM\_HOME | Directory on which Oracle IAM Suite is installed server is installed. It is usually under *FMW\_HOME.*  **Example**: ${FMW\_HOME}/iam |
| OIG\_HOME | Directory on which Oracle Identity Manager is installed server is installed. It is usually under *IAM\_HOME*.  **Example**: ${IAM\_HOME}/server |
| SOA\_HOME | Directory on which Oracle SOA Suite is installed. It is usually under *FMW\_HOME*.  **Example**: ${FMW\_HOME}/soa |
| OIG\_SRC\_URL | The URL from which Identity Manager related deployment artifacts are exported.  **Example**: https://gcdpsource.oracle.com/svn/iam-bka/internal/1.0/trunk/IdentityManager |
| BIP\_SRC\_URL | The URL from which Oracle BI Publisher related deployment artifacts are exported.  **Example**: https://gcdpsource.oracle.com/svn/iam-bka/internal/1.0/trunk/IdentityReports |

|  |  |
| --- | --- |
| warning | **Achtung**: |
| Ab diesem Zeitpunkt ist das technische System auf dem die weiteren Schritte der Bereitstellung vorgenommen als unsicher zu betrachten. |

cd <working>

. <stage>

./install replace

| Parameter | Beschreibung |
| --- | --- |
| <working> | Der Name des Verzeichnisses, in das der Export vorgenommen wird und aus dem heraus alle nachfolgenden Operationen gestartet werden. |
| <stage> | Der logische Name des Infrastrukturumgebung. |

## Bezug des Deployments

Ist das Deployment bereits vorhanden kann es mittels

./install verify

überprüft werden. Es wird eine Konsistenzprüfung der exportierten Konfigurationsdateien und eine Syntaxprüfung aller XML Dateien ausgeführt.

**Alternativ** wird das Deployment ebenfalls über das Version Control Repository bezogen. Der Bezug wird durch die Kommandozeile

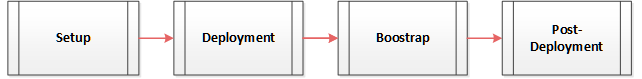
./install update

ausgeführt. Diese Operation führt neben dem Bezug des Deployment eine Konsistenzprüfung der exportierten Konfigurationsdateien und eine Syntaxprüfung aller XML Dateien aus.

# Bereitstellungsprozess

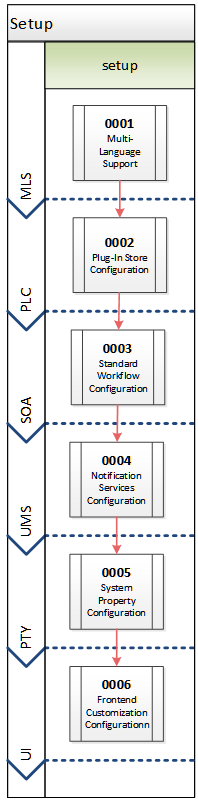
Das Deployment ist ein Prozess, der in seinem Ablauf die Bereitstellung von Konfigurationen, Entitäten sowie den Bezug von Daten aus diversen Quellsystemen umfasst. Dabei sind zu einem gegebenen Zeitpunkt Artefakte des Deployments auf bereits geladene Daten angewiesen, um fehlerfrei im Oracle Identity Manager bereitgestellt werden zu können. Andererseits haben einzelne Artefakte Abhängigkeiten untereinander die Einhaltung einer bestimmten Reihenfolge innerhalb des Bereitstellungsprozesses erfordern (siehe Kapitel 5.4).

Der Bereitstellungprozess selbst untergliedert sich in wesentliche Teilprozesse:



## Setup

Im Teilprozess Setup werden die Server-Komponenten in ihrer Konfiguration geändert und miteinander verbunden. Dazu werden folgende einzelne Task durchlaufen:



### Multi-Language Support

Viele Artefakte in Oracle Identity Manager unterstützen Mehrsprachigkeit.

Im Auslieferungszustand ist Oracle Identity Manager mit der Sprachoption Englisch bestückt. Durch nachfolgende Konfigurationsschritte wird der verfügbare Sprachumfang um alle weiteren vordefinierten Sprachen erweitert. Die weiteren Sprachen werden durch Ausführung von

./install setup 0001

dem System bekannt gemacht.

### Plug-In Store Konfiguration

Das Ladeverhalten der Plug-In’s im Identity Manager wird durch Ausführung von

./install setup 0002

angepasst.

### Standard Workflow Konfiguration

Die Standard Workflows werden mit den TaskFlows des Identity Managers durch Ausführung von

./install setup 0003

verbunden.

### Notifikation Services Konfiguration

Oracle Identity Manager 12c Release 2 (12.2.1) unterstützt das Senden von Nachrichten per E-Mail. Zum Senden von E-Mail-Benachrichtigungen wird der User Messaging Service (UMS) verwendet. UMS speichert Informationen über den Sendestatus der E-Mails und stellt diese Informationen für die Fehlerbehandlung zur Verfügung. Die Systemkomponenten Identity Manager und User Masseging Service (UMS) werden durch Ausführung von

./install setup 0004

aufeinander abgestimmt.

### Konfiguration System Eigenschaften

Einige System Eigenschaften sind auf Grund der fachlichen und technischen Anforderungen gegenüber dem Auslieferungszustand zu ändern. Durch Ausführung von

./install setup 0005

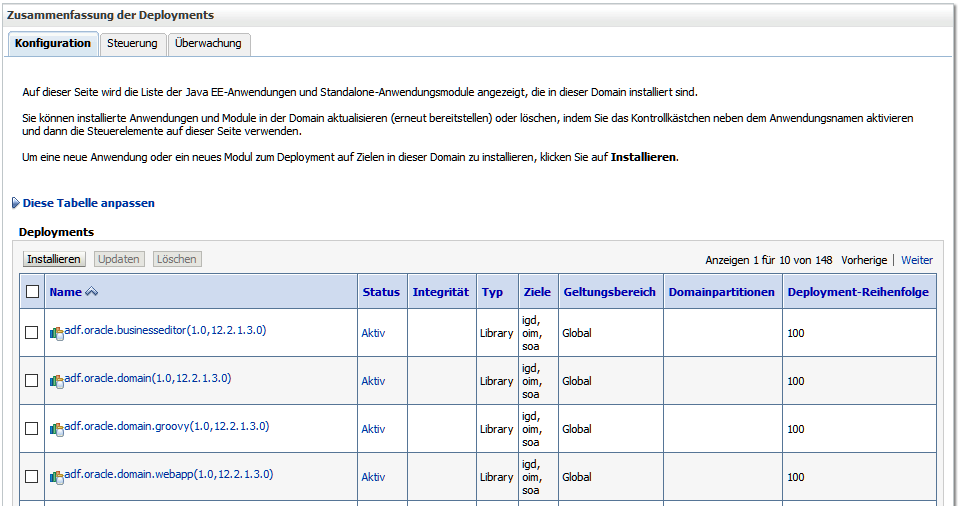
werden diese Änderungen vorgenommen.

### Frontend Customization Konfiguration

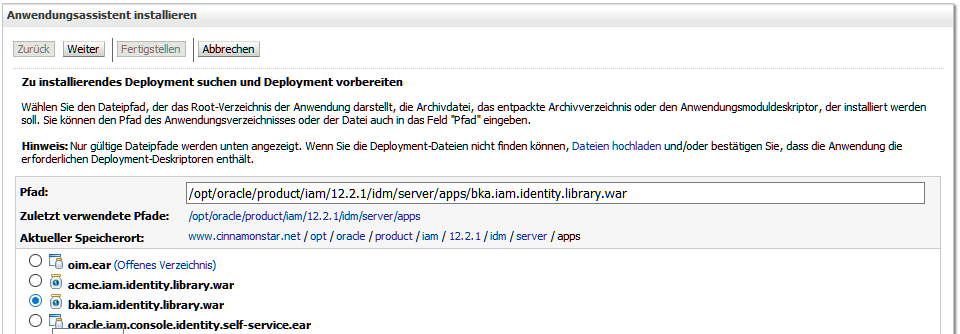
Für die Anpassung der Oberflächenelemente wird eine Anwendungsbibliothek bereitgestellt.

./install setup 0006

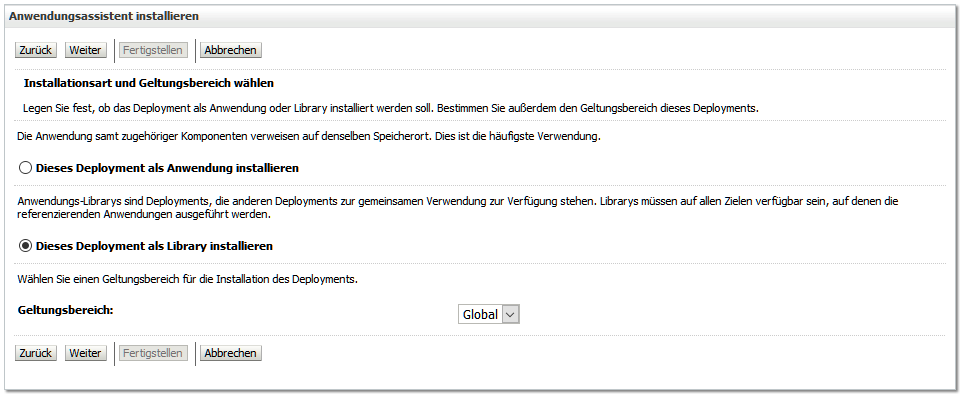
Anschließend im Panel **Domainstruktur**-> über den Link **Deployments** in die Auflistung der existierenden Deployment der Domain wechseln.



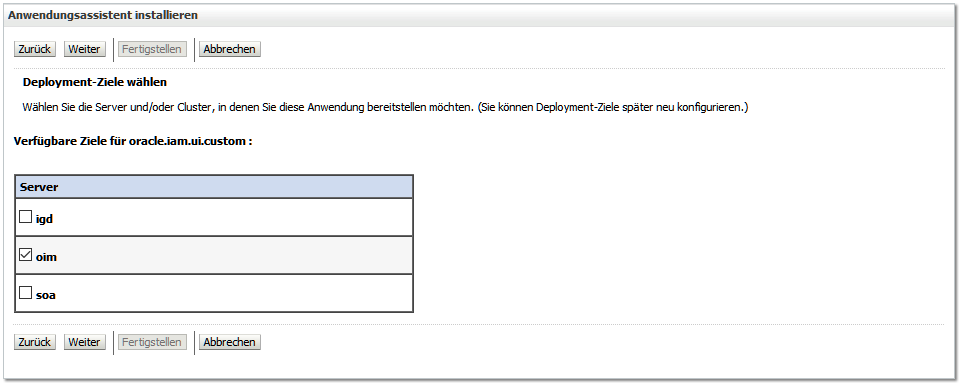
Die Bereitstellung der Bibliothek erfolgt über die Schaltfläche **Installieren**. Im Darauffolgend angezeigten Assistenten wird in den entsprechenden Verzeichnispfad navigiert und die Datei bka.iam.ui.identity.library.war ausgewählt.



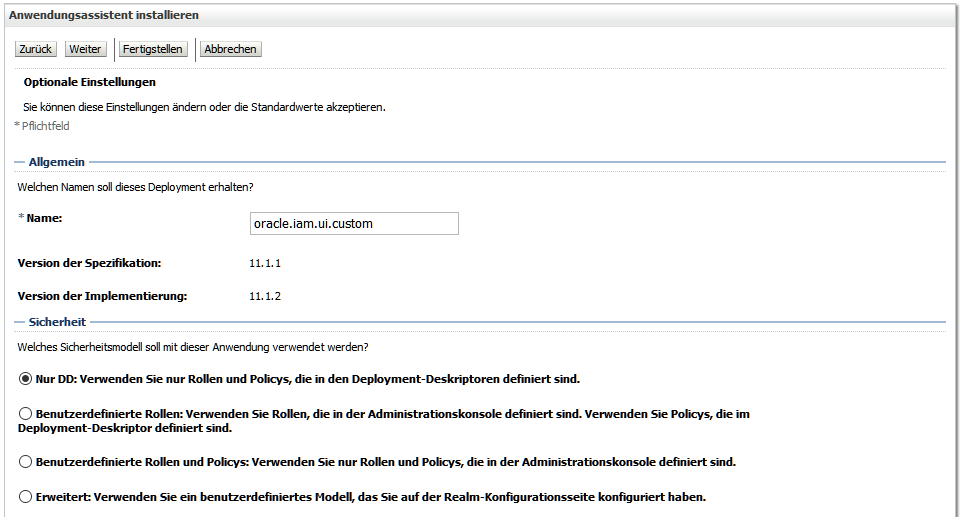
Über die Schaltfläche **Weiter** wird in der Bereitstellung der Bibliothek fortgefahren. Als Art des Deployment ist sicherzustellen, dass die Option **Dieses Deployment als Library installieren ausgewählt wurde**.



Über die Schaltfläche **Weiter** wird in der Bereitstellung der Bibliothek fortgefahren. Als Ziel des Deployment wird aus den verfügbaren Zielen der Cluster ausgewählt, in dem Oracle Identity Manager bereitgestellt wurde, Innerhalb des Clusters wird die Option **Alle Server im Cluster** verwendet, um das Deployment auf alle Server vorzunehmen.



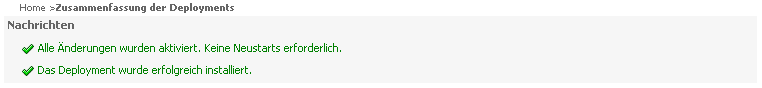
Über die Schaltfläche **Weiter** wird in der Bereitstellung der Bibliothek fortgefahren. In den daraufhin angezeigten **Optionalen Einstellungen** sind keine Veränderungen vorzunehmen.



Wichtig ist, dass folgende Parameter exakt eingehalten werden

| Parameter | Wert |
| --- | --- |
| Name | oracle.iam.custom.ui |
| Version der Spezifikation | 11.1.1 |
| Version der Implementierung | 11.1.2 |

Über die Schaltfläche **Fertigstellen** wird nun die Bereitstellung der Bibliothek vorgenommen. Die erfolgreiche Bereitstellung wird durch das System entsprechend bestätigt.



Als Ergebnis dieses Vorgangs werden nun zwei Bibliotheken mit gleichem Namen und unterschiedlichen Versionsnummern in der Deployment Übersicht angezeigt.

ScreenShot

Allerdings wird zurzeit nur die Anwendungsbibliothek mit der niedrigeren Versionsnummer verwendet. Erst nach einem Neustart der Managed Server wird die Anwendungsbibliothek mit der höheren Versionsnummer entsprechend referenziert.

ScreenShot

Es muss nun noch die Deployment-Reihenfolge der Anwendungsbibliothek angepasst werden. Standardmäßig wird 100 für diese Reihenfolge festgelegt. Wichtig ist, dass bei Änderung dieses Wertes die Deployment-Reihenfolge so eingestellt wird, dass die Anwendungsbibliothek vor den eigentlichen Anwendungen bereitsteht, die sie referenzieren und nach den Modulen, die die Anwendungsbibliothek selbst verwendet.

| Parameter | Version | Reihenfolge |
| --- | --- | --- |
| oracle.iam.ui.model |  |  |
| oracle.iam.ui.view |  |  |
| oracle.iam.ui.oia-view |  |  |
| oracle.iam.ui.custom |  |  |
| oracle.iam.ui.custom |  |  |
| oracle.iam.console.identity.self-service.ear |  |  |
| oracle.iam.console.identity.sysadmin.ear |  |  |

## Neustart

|  |  |
| --- | --- |
| warning | **Achtung**: |
| Alle Mitglieder des Clusters in dem Oracle Identity Manager bereitgestellt wurde sind danach neu zu starten |

## Deployment

Im Teilprozess Deployment werden die Entwicklungsartefakte in den Oracle Identity Manager eingebracht und konfiguriert. Dazu werden folgende einzelne Task durchlaufen:

Insert Flow Picture here

### Deployment Entity Konfiguration und Integration

Die Deployment-Pakete 0100 bis 0102 (siehe Kapitel 5.4) werden in einem Deployment-Schritt zusammengefasst. Das Deployment wird durch das Kommando gestartet.

./install deploy 001

Anschließend werden die für das Benutzer Frontend notwendigen Deployment-Pakete durch Ausführung des Kommandos

./install request 001

## Initial On-Boarding

Initial On-Boarding ist ein Prozess, in dem erstmals alle notwendigen Informationen aus den verschiedenen Datenquellen im Oracle Identity Manager zusammengetragen werden.

Initial On-Boarding wird durch das Ausführen der dafür zuständigen Hintergrundprozesse erreicht. Zum Zeitpunkt des Deployments werden diese Prozesse Skript-gesteuert angestoßen.

Die durch das Deployment erzeugten Hintergrundprozesse sind in ihrer Attribut Konfiguration bereits vollständig ausgeprägt. Es ist also ausreichend den entsprechenden Prozess zu starten.

Es wird empfohlen, die Prozesse in der nachfolgend beschriebenen Reihenfolge durchzuführen

|  |  |
| --- | --- |
| info | **Hinweis**: |
| Alle Mitglieder des Clusters in dem Oracle Identity Manager bereitgestellt wurde sind danach neu zu starten |

Insert Flow Picture here

### Identitäten

Alle weiteren Ladeprozesse erfordern Daten, die aus Datenquelle des Bundeskriminalamtes geladen sein müssen, bevor die weiteren Ladeprozesse verlustarm ausgeführt werden können. Hierbei handelt es sich um die Benutzerdaten und ihren Beziehungen zur Organisationsstruktur und anderen Benutzerdaten (Führungskräfte).

## Post Deployment

Die Berechtigungsobjekte werden dem vorgegebenen Ablauf zur Erzeugung von Businessrollen zugeführt. Dieser Prozess beinhaltet die Bereitstellung der Berechtigungsobjekte als Entitlements in Oracle Identity Manager.

### Entitlement Transformation

Die Entitlement Transformation wird durch den Hintergrundprozess

Entitlement List Job

angestoßen. Je nach Füllungsgrad des Oracle Identity Managers kann dieser Prozess einige Zeit in Anspruch nehmen. Dieser Prozess startet nach seiner Beendigung selbsttätig den Hintergrundprozess

### Catalog Synchronisation

Die Entitlement Transformation wird durch den Hintergrundprozess

Catalog Synchronization Job

angestoßen. Je nach Füllungsgrad des Oracle Identity Managers kann dieser Prozess einige Zeit in Anspruch nehmen.

# Umsetzung des Berechtigungskonzepts

Das Berechtigungskonzept legt fest welche Aktoren innerhalb der Geschäftsprozesse mit entsprechenden Berechtigungen in Oracle Identity Manager auszustatten sind. Dies erfordert die Anlage von Berechtigungsobjekten in Oracle Identity Manager.

## Berechtigungsobjekte Oracle Identity Manager

Entsprechend den Anforderungen aus dem Berechtigungskonzept sind weitere Rollendefinitionen in Oracle Identity Manager zu erzeugen. Die im Auslieferungszustand vorhandenen Rollen verbleiben dabei unverändert. Folgende Rollen sind in Oracle Identity Manager zusätzlich angelegt.

### Administrative Rollen

| Rolle | Kategorie | Verwendungszweck |
| --- | --- | --- |
| FIM System Administrators | OIM Roles |  |
| FIM Identity Administrators | OIM Roles |  |

|  |  |
| --- | --- |
| info | **Hinweis**: |
| Durch die Einsufung in die Kategorie *OIM Roles* sind diese Rollen im Katalog nicht sichtbar und können somit nicht beantragt werden. |

### Administrative Rollen

| Rolle | Kategorie | Verwendungszweck |
| --- | --- | --- |
| efbsAccountPasswordRSSuper | Admin | Admin Rolle die berechtigt die Kennwörter des Benutzerkontos *rssupe*r im Active Directory der Cirtix Terminal Server Zugänge zu ändern. |
| efbsAccountPasswordPropertyUser | Admin | Admin Rolle die berechtigt die Kennwörter des Benutzerkontos *PROPERTY\_USER* im Active Directory der Cirtix Terminal Server Zugänge zu ändern. |
| efbsAccountPasswordPropertyUserGlobal | Admin | Admin Rolle die berechtigt die Kennwörter des Benutzerkontos *PROPERTY\_USER \_GLOB* im Active Directory der Cirtix Terminal Server Zugänge zu ändern. |

# Anhang

## Verwalten der IT Ressourcen

IT Ressourcen definieren die technischen Parameter, die Oracle Identity Manager verwendet, um zu den entsprechenden Backend Systemen eine Verbindung aufzubauen und sich gegenüber diesem technischen System zu authentisieren.

Die IT Ressourcen wurden während der Phase des Deployments erzeugt und durch die Substitution der Parameter entsprechend konfiguriert.

TBD

## Verwalten der Hintergrundprozess

Die Hintergrundprozesse wurden während der Phase des Deployments erzeugt und durch die Substitution der Parameter entsprechend konfiguriert.

TBD