Administrator Guide

IP.IAM Konfiguration

Autor: Dieter Steding  
 Sophie Strecke

Erstelldatum: 28-01-2020

Letzte Änderung: 01-05-2020

Kontrollnummer: OC\_DE/300516442/DO.081/0020

Version: 1.0

**Freigabe:**

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

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

## Dokumentenkontrolle

### Änderungshistorie

| Date | Autor | Version | | Änderungsreferenz |
| --- | --- | --- | --- | --- |
|  |  |  |  | |
| 28-01-20 | Dieter Steding | 1.0 | Kein vorheriges Dokument | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |

### Reviewer

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

Inhalt

[Dokumentenkontrolle ii](#_Toc59098623)

[Änderungshistorie ii](#_Toc59098624)

[Reviewer ii](#_Toc59098625)

[Einführung 1](#_Toc59098626)

[Leserkreis 1](#_Toc59098627)

[Bezugsdokumente 1](#_Toc59098628)

[Vertraulichkeit 1](#_Toc59098629)

[Typografische Konventionen 1](#_Toc59098630)

[Anforderungen 2](#_Toc59098631)

[Hardware und Software Zertifizierung 2](#_Toc59098632)

[Überprüfung der Anforderungen 2](#_Toc59098633)

[Erforderliche Komponentenversionen 2](#_Toc59098634)

[Erforderliche Patches 2](#_Toc59098635)

[Konventionen Verzeichnisvariablen 2](#_Toc59098636)

[Komponenten Konfiguration 4](#_Toc59098637)

[Konfiguration Access Server 5](#_Toc59098638)

[Konfiguration Identity Store 6](#_Toc59098639)

[Allgemein 6](#_Toc59098640)

[Verzeichnis und Zugangsdaten 6](#_Toc59098641)

[Benutzer und Gruppen 6](#_Toc59098642)

[Verbindungsdetails 7](#_Toc59098643)

[Kennwortverwaltung 7](#_Toc59098644)

[Konfiguration Föderation 8](#_Toc59098645)

[Einstellungen 8](#_Toc59098646)

[Service Provider 8](#_Toc59098647)

[Allgemein 8](#_Toc59098648)

[Konfiguration Authentifizierungsmodul 9](#_Toc59098649)

[Konfiguration Authentifizierungsschema 9](#_Toc59098650)

[Konfiguration Load Balancer Regeln 10](#_Toc59098651)

[WebLogic Console 10](#_Toc59098652)

[Umleitungsregel 10](#_Toc59098653)

[Umleitungsparameter 10](#_Toc59098654)

[WebLogic Console Help 10](#_Toc59098655)

[Umleitungsregel 10](#_Toc59098656)

[Umleitungsparameter 11](#_Toc59098657)

[Fusion Middleware Control 11](#_Toc59098658)

[Umleitungsregel 11](#_Toc59098659)

[Umleitungsparameter 11](#_Toc59098660)

[Access Manager Console 12](#_Toc59098661)

[Umleitungsregel 12](#_Toc59098662)

[Umleitungsparameter 12](#_Toc59098663)

[Policy Manager Console 12](#_Toc59098664)

[Umleitungsregel 12](#_Toc59098665)

[Umleitungsparameter 13](#_Toc59098666)

[Access Manager 13](#_Toc59098667)

[Umleitungsregel 13](#_Toc59098668)

[Umleitungsparameter 13](#_Toc59098669)

[Platform Security Services 14](#_Toc59098670)

[Umleitungsregel 14](#_Toc59098671)

[Umleitungsparameter 14](#_Toc59098672)

[OAuth/OpenID Provider 14](#_Toc59098673)

[Umleitungsregel 15](#_Toc59098674)

[Umleitungsparameter 15](#_Toc59098675)

[Credential Collector 15](#_Toc59098676)

[Umleitungsregel 15](#_Toc59098677)

[Umleitungsparameter 15](#_Toc59098678)

## Einführung

### Leserkreis

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

### 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

### Vertraulichkeit

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

Die Leserschaft 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 Datenbank** | Oracle® RDBMS 12c (12.2.0.1.0 oder höher |
| **Oracle Access Manager** | Oracle® Access Manager 12c Release 12.2.1.3.0 |

#### Erforderliche Patches

| **Komponente** | **Patch** |
| --- | --- |
| **Oracle Access Manager** | Patch 28922534 (Oracle® Access Management Bundle Patch 12.2.1.3.0 (ID:191201.0123.S) |

### Konventionen Verzeichnisvariablen

|  |  |
| --- | --- |
| **Variable** | **Bedeutung** |
| *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 gängige Oracle Fusion Middleware-Produkte gespeichert sind. |
| *JAVA\_HOME* | Der Speicherort, an dem das unterstützte Java Development Kit (JDK) installiert wurde. |
| *STAGE* | Das Basisverzeichnis, unter dem Oracle-Produkt Medien aufzufinden sind. |
| *DOMAIN\_BASE* | Das Basisverzeichnis, unter dem WebLogic Domains konfiguriert werden. |

## Komponenten Konfiguration

Für die föderierte Identity und Access Management ist Access Manager entsprechend zu konfigurieren. Eine wesentliche Voraussetzung hierfür ist die Aktivierung von Access-Komponenten.

Freizuschalten sind die Dienste:

1. Identity Föderation

|  |  |
| --- | --- |
| icon-note-16 | **Hinweis** |
| Die Freischaltung des OAuth-Service ist zum gegenwärtigen Zeitpunkt nicht notwendig, da die hierfür erforderlichen Anforderungen nicht definiert sind. |

Um den genannten Dienst zu aktivieren, ist folgendermaßen zu verfahren:

1. Anmeldung als WebLogic Administrator in der Access Management Console,
2. Nach erfolgreicher Anmeldung befinden Sie im Modul **Anwendungssicherheit** des Access Managers.
3. In diesem Modul navigieren Sie über die Schaltfläche **Konfiguration** in die Ansicht Basis Konfigurationseinstellungen des Access Managers.
4. Die Aktivierung der Dienste **Identity Federation** erfolgt in der Kachel **Verfügbare Services**.
5. Im der Ansicht **Verfügbare Dienste** ist der Dienst **Identity Federation** zu aktivieren

## Konfiguration Access Server

Die nach dem Erzeugen der Domain vorzufindende Konfiguration der Access Server ist gegebenenfalls anzupassen.

Nachfolgende Tabelle für die korrekte Konfiguration für jeden Access Server auf:

| **Name** | **Instanz** | | **Proxy** | | |
| --- | --- | --- | --- | --- | --- |
|  | **Host** | **Port** | **ID** | **Port** | **Mode** |
| **oam1** | vwasc181ext.zds.bka.bund.de | 8009 | AccessServerConfigProxy | 5575 | Open |
| **oam2** | vwasc182ext.zds.bka.bund.de | 8009 | AccessServerConfigProxy | 5575 | Open |
| **oam3** | vwasc281ext.zds.bka.bund.de | 8009 | AccessServerConfigProxy | 5575 | Open |

## Konfiguration Identity Store

Die Systemkomponenten Access Manager verwendet den Identity Store *Federation Identity Proxy* für die Authentisierung von Benutzer.

Der *Federation Identity Proxy* exponiert die Datenbank des Identity Managers als Verzeichnisdienst.

Über diesen Identity Stores werden all die Benutzer authentisiert, deren Teilnehmer keinen eigenen Identity Provider für eine föderierte Authentisierung bereitstellen.

#### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Speichername** | FederationIdentityProxy |
| **Speichertype** | OUD: Oracle Unified Directory |
| **Beschreibung** | The Identity Store providing entries to authenticate accounts where participants have not their own infrastructure. |
| **SSL aktivieren** | <unchecked> |
| **nativen ID-Speichers verwende** | <unchecked> |
| **Im Voraus abgerufene Attribute** | uid,mail,cn,sn,givenName |

#### Verzeichnis und Zugangsdaten

| **Parameter** | **Wert** |
| --- | --- |
| **Verzeichnis** | fimvip.bka.bund.de:7389 |
| **Bind DN** | uid=oamadmin,cn=System,dc=bka,dc=bund,dc=de |
| **Kennwort** |  |

#### Benutzer und Gruppen

| **Parameter** | **Wert** |
| --- | --- |
| **Anmelde-ID-Attribut** | uid |
| **Benutzerkennwortattribut** | userPassword |
| **Benutzersuchbasis** | cn=Participants,dc=fim,dc=bund,dc=de |
| **Objektklassen für Benutzerfilter** | person |
| **Gruppennameattribut** | cn |
| **Basis für die Gruppensuche** | ou=Gropus,dc=bka,dc=bund,dc=de |
| **Gruppenfilterklassen** | groupOfUniqueNames |
| **Gruppenmitgliedschafts-Cache aktivieren** | <unchecked> |

#### Verbindungsdetails

| **Parameter** | **Wert** |
| --- | --- |
| **Minimale Poolgröße** | 50 |
| **Maximale Poolgröße** | 100 |
| **Wait Timeout (in milliseconds)** | 1000 |
| **Inaktivitätstimeout (in Sekunden)** | 0 |
| **Zeitgrenze für Ergebnisse (in Sekunden)** | 0 |
| **Anzahl Wiederholungen** | 3 |
| **Referral Policy** | <empty> |

#### Kennwortverwaltung

Die Kennwortverwaltung verbleibt deaktiviert.

## Konfiguration Föderation

### Einstellungen

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Provider Id** | https://idp.bka.extraprol.de/oam/fed |
| **Signaturschlüssel** | access\_signing |
| **Verschlüsselungsschlüssel** | access\_encrypt |

### Service Provider

#### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | FederationIdentityProxy |
| **Beschreibung** | Service Provider for sharing the common Loopback Identity Provider |
| **Partner aktivieren** | <checked> |

##### Serviceinformationen

| **Parameter** | **Wert** |
| --- | --- |
| **Protokoll** | SAML 2.0 |
| **Servicedetails** | Aus Providermetadaten laden |
| **Provider-ID** | http://idp.bka.extrapol.de/oam/fed |

##### Signaturzertifikat

| icon-note-16 | **Hinweis** |
| --- | --- |
| Das Laden der Metadatendatei findet nach Bereitstellung durch das Bundeskriminalamt statt. |

##### Name ID Format

| **Parameter** | **Wert** |
| --- | --- |
| **NameID-Format** | Persistent |
| **NameID-Value** | Benutzer-ID-Speicherattribute |
| **Expression** | userPrincipalName |

##### Attribute Zuordnung

| **Attributprofil** | **Wert** |
| --- | --- |
| **Attribute Profil** | sp-attribute-profile |

### Konfiguration Authentifizierungsmodul

| **Parameter** | **Wert** |
| --- | --- |
| **Typ** | LDAP-Authentifizierungsmodul |
| **Name** | FederationIdentityProxy |
| **Benutzeridentitätsspeicher** | FederationIdentityProxy |

### Konfiguration Authentifizierungsschema

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | FederationProxyScheme |
| **Beschreibung** | Authentication scheme for all proxied Resources |
| **Authentifizierungsebene** | 2 |
| **Standard** | <unchecked> |
| **Challenge-Methode** | FORM |
| **Challenge-Umleitungs-URL** | /oam/server |
| **Authentifizierungsmodul** | FederationIdentityProxy |
| **Challenge-URL** | https://idp.extrapol.bund.de/ecc |
| **Kontexttyp** | external |
| **Challenge-Parameter** | <empty> |

## Konfiguration Load Balancer Regeln

### WebLogic Console

Diese Location leitet die HTTP‑Requests für den Zugriff auf die Konfiguration der WebLogic Domain. um

#### Umleitungsregel

| **Regel** | **Kontext** |
| --- | --- |
| **Location** | /console |

#### Umleitungsparameter

| **Parameter** | **Wert** |
| --- | --- |
| **WLSRequest** | ON |
| **WLProxySSL** | ON |
| **WLProxyPassThrough** | ON |
| **WLIOTimeoutSecs** | 590 |
| **WLSocketTimeoutSecs** | 30 |
| **WebLogicHost** | vwasc181.zds.bka.bund.de |
| **WebLogicPort** | 7003 |
| **Require ip** | 126..???.???.???/24 |

|  | **Wichtig** |
| --- | --- |
| Die Kontext URL der WebLogic Server Console wird nicht durch einen Access Agent geschützt.  Aus diesem Grund wird der Zugriff auf diesen Kontext auf das interne Netzwerk des Bundeskriminalamts durch auf einen entsprechenden IP-Bereich über den Parameter **Require ip** eingeschränkt. |

### WebLogic Console Help

Diese Location leitet die HTTP‑Requests für den Zugriff auf die kontextsensitive Hilfe der WebLogic Domain. um

#### Umleitungsregel

| **Regel** | **Kontext** |
| --- | --- |
| **Location** | /consolehelp |

#### Umleitungsparameter

| **Parameter** | **Wert** |
| --- | --- |
| **WLSRequest** | ON |
| **WLProxySSL** | ON |
| **WLProxyPassThrough** | ON |
| **WLIOTimeoutSecs** | 590 |
| **WLSocketTimeoutSecs** | 30 |
| **WebLogicHost** | vwasc181.zds.bka.bund.de |
| **WebLogicPort** | 7003 |
| **Require ip** | 126..???.???.???/24 |

|  | **Wichtig** |
| --- | --- |
| Die Kontext URL des WebLogic Server Console Hilfe wird nicht durch einen Access Agent geschützt.  Aus diesem Grund wird der Zugriff auf diesen Kontext auf das interne Netzwerk des Bundeskriminalamts durch auf einen entsprechenden IP-Bereich über den Parameter **Require ip** eingeschränkt. |

### Fusion Middleware Control

Diese Location leitet die HTTP‑Requests für den Zugriff auf das Fusion Middleware Control der Access Manager Domain um.

#### Umleitungsregel

| **Regel** | **Kontext** |
| --- | --- |
| **Location** | /em |

#### Umleitungsparameter

| **Parameter** | **Wert** |
| --- | --- |
| **WLSRequest** | ON |
| **WLProxySSL** | ON |
| **WLProxyPassThrough** | ON |
| **WLIOTimeoutSecs** | 590 |
| **WLSocketTimeoutSecs** | 30 |
| **WebLogicHost** | vwasc181.zds.bka.bund.de |
| **WebLogicPort** | 7003 |
| **Require ip** | 126..???.???.???/24 |

|  | **Wichtig** |
| --- | --- |
| Die Kontext URL des Fusion Middleware Control wird nicht durch einen Access Agent geschützt.  Aus diesem Grund wird der Zugriff auf diesen Kontext auf das interne Netzwerk des Bundeskriminalamts durch auf einen entsprechenden IP-Bereich über den Parameter **Require ip** eingeschränkt. |

### Access Manager Console

Diese Location leitet die http Request für den Zugriff auf die Konsole der Access Manager Konfiguration um.

#### Umleitungsregel

| **Regel** | **Kontext** |
| --- | --- |
| **Location** | /oamconsole |

#### Umleitungsparameter

| **Parameter** | **Wert** |
| --- | --- |
| **WLSRequest** | ON |
| **WLProxySSL** | ON |
| **WLProxyPassThrough** | ON |
| **WLIOTimeoutSecs** | 590 |
| **WLSocketTimeoutSecs** | 30 |
| **WebLogicHost** | vwasc181.zds.bka.bund.de |
| **WebLogicPort** | 7003 |
| **Require ip** | 126..???.???.???/24 |

|  | **Wichtig** |
| --- | --- |
| Die Kontext URL der Access Manager Console wird nicht durch einen Access Agent geschützt.  Aus diesem Grund wird der Zugriff auf diesen Kontext auf das interne Netzwerk des Bundeskriminalamts durch auf einen entsprechenden IP-Bereich über den Parameter **Require ip** eingeschränkt. |

### Policy Manager Console

Diese Location leitet die http Request für den Zugriff auf die Konsole der Policy Manager Konfiguration um.

#### Umleitungsregel

| **Regel** | **Kontext** |
| --- | --- |
| **Location** | /access |

#### Umleitungsparameter

| **Parameter** | **Wert** | |
| --- | --- | --- |
| **WLSRequest** | ON | |
| **WLProxySSL** | ON | |
| **WLProxyPassThrough** | ON | |
| **WLIOTimeoutSecs** | 590 | |
| **WLSocketTimeoutSecs** | 30 | |
| **WebLogicCluster** | **Server Name** | **Port** |
|  | vwasc181.zds.bka.bund.de | 8011 |
|  | vwasc182.zds.bka.bund.de | 8011 |
|  | vwasc281.zds.bka.bund.de | 8011 |
| **Require ip** | 126..???.???.???/24 | |

|  | **Wichtig** |
| --- | --- |
| Die Kontext URL der Policy Manager Console wird nicht durch einen Access Agent geschützt.  Aus diesem Grund wird der Zugriff auf diesen Kontext auf das interne Netzwerk des Bundeskriminalamts durch auf einen entsprechenden IP-Bereich über den Parameter **Require ip** eingeschränkt. |

### Access Manager

Diese Location leitet die http Request für den Zugriff auf die Access Manager Server um.

#### Umleitungsregel

| **Regel** | **Kontext** |
| --- | --- |
| **Location** | /oam |

#### Umleitungsparameter

| **Parameter** | **Wert** | |
| --- | --- | --- |
| **WLSRequest** | ON | |
| **WLProxySSL** | ON | |
| **WLProxyPassThrough** | ON | |
| **WLIOTimeoutSecs** | 590 | |
| **WLSocketTimeoutSecs** | 30 | |
| **WebLogicCluster** | **Server Name** | **Port** |
|  | vwasc181.zds.bka.bund.de | 8009 |
|  | vwasc182.zds.bka.bund.de | 8009 |
|  | vwasc281.zds.bka.bund.de | 8009 |

|  | **Wichtig** |
| --- | --- |
| Die Kontext URL des Access Managers wird nicht durch einen Access Agent geschützt. |

### Platform Security Services

Diese Location leitet die http Request für den Zugriff auf die Access Manager Platform Security Services um.

#### Umleitungsregel

| **Regel** | **Kontext** |
| --- | --- |
| **Location** | /opss |

#### Umleitungsparameter

| **Parameter** | **Wert** | |
| --- | --- | --- |
| **WLSRequest** | ON | |
| **WLProxySSL** | ON | |
| **WLProxyPassThrough** | ON | |
| **WLIOTimeoutSecs** | 590 | |
| **WLSocketTimeoutSecs** | 30 | |
| **WebLogicCluster** | **Server Name** | **Port** |
|  | vwasc181.zds.bka.bund.de | 8009 |
|  | vwasc182.zds.bka.bund.de | 8009 |
|  | vwasc281.zds.bka.bund.de | 8009 |

|  | **Wichtig** |
| --- | --- |
| Die Kontext URL der Platform Security Services wird nicht durch einen Access Agent geschützt. |

### OAuth/OpenID Provider

Diese Location leitet die http Request für den Zugriff auf die Access Manager Platform Security Services um.

#### Umleitungsregel

| **Regel** | **Kontext** |
| --- | --- |
| **Location** | /.well-known/oidc-configuration |

#### Umleitungsparameter

| **Parameter** | **Wert** | |
| --- | --- | --- |
| **WLSRequest** | ON | |
| **WLProxySSL** | ON | |
| **WLProxyPassThrough** | ON | |
| **WLIOTimeoutSecs** | 590 | |
| **WLSocketTimeoutSecs** | 30 | |
| **PathTrim** | /.well-known | |
| **PathPrepend** | /oauth2/rest | |
| **WebLogicCluster** | **Server Name** | **Port** |
|  | vwasc181.zds.bka.bund.de | 8009 |
|  | vwasc182.zds.bka.bund.de | 8009 |
|  | vwasc281.zds.bka.bund.de | 8009 |

|  | **Wichtig** |
| --- | --- |
| Die Kontext URL der OAuth/OpenID Provider wird nicht durch einen Access Agent geschützt. |

### Credential Collector

Diese Location leitet die http Request für den Zugriff auf die Access Manager Platform Security Services um.

#### Umleitungsregel

| **Regel** | **Kontext** |
| --- | --- |
| **Location** | /ecc |

#### Umleitungsparameter

| **Parameter** | **Wert** | |
| --- | --- | --- |
| **WLSRequest** | ON | |
| **WLProxySSL** | ON | |
| **WLProxyPassThrough** | ON | |
| **WLIOTimeoutSecs** | 590 | |
| **WLSocketTimeoutSecs** | 30 | |
| **WebLogicCluster** | **Server Name** | **Port** |
|  | vwasc181.zds.bka.bund.de | 8009 |
|  | vwasc182.zds.bka.bund.de | 8009 |
|  | vwasc281.zds.bka.bund.de | 8009 |

|  | **Wichtig** |
| --- | --- |
| Die Kontext URL des Credential Collectors wird nicht durch einen Access Agent geschützt. |