IGS ZeRo Services Deployment

Identity Governance Service

Release 1.0.0

GEMEINSAM. DIGITAL. VERNETZT.

IGS ZeRo Services Deployment

1 Ausgabe

von Adrien Farkas, Dieter Steding und Sylvert Bernet

Programm	Polizei 20/20
Programmleiter	Holger Gadorosi
Projektleiter/Verantwortlicher	Norbert Linde
Dokumententitel	IGS.ZeRo Services Deployment
Version	1.2
Erstellt am **Erstellt von**	31.03.2023 Adrien Farkas
Zuletzt bearbeitet am **Zuletzt bearbeitet von**	2023-07-15 Dieter Steding

Versionshistorie

Version	Datum	Autor	Verweis
1.0	31.03.2023	A. Farkas	Kein vorheriges Dokument
1.1	26.05.2023	A. Farkas	Abschnitt Codebase Grant's hinzugefügt
1.2	15.07.2023	D. Steding	Provisioning Service hinzugefügt

Inhaltsverzeichnis

Vorwort

In diesem Vorwort werden die in diesem Handbuch verwendeten Funktionen und Konventionen sowie zur Barrierefreiheit von Dokumenten beschrieben.

Leserkreis

Dieser Leitfaden richtet sich an Administratoren einer Oracle Identity Governance Infrastruktur.

Reference Documents

For information about installing and using Oracle Identity and Access Management, visit the following Oracle Help Center page:

- *https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/index.html*
- *https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.3/asadm/index.html*

Vertraulichkeit

Das in dieser Dokumentation enthaltene Material stellt geschützte, vertrauliche Informationen dar, die sich auf Produkte und Methoden von Oracle beziehen.

Die Leser stimmen zu, dass die Informationen in diesem Dokument nicht außerhalb des Projekts offengelegt und zu keinem anderen Zweck als zur Bewertung dieses Verfahrens vervielfältigt, verwendet oder offengelegt werden dürfen.

Typogarfische Konventionen

In diesem Dokument werden die folgenden typografische Konventionen verwendet.

Konvention	Bedeutung
fett	Fettschrift 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 Platzhaltervariablen, für die Sie bestimmte Werte angeben.
`monospace`	Monospace-Schrift kennzeichnet Befehle innerhalb eines Absatzes, URLs, Code in Beispielen, Text, der auf dem Bildschirm angezeigt wird, oder Text, den Sie eingeben.

Symbol Konventionen

In diesem Dokument werden die folgenden Konventionen für Symbole verwendet.

Symbol	Bedeutung
[ ]	Enthält optionale Argumente und Befehlsoptionen.

Symbol	Bedeutung
{ | }	Enthält eine Reihe von Auswahlmöglichkeiten für eine erforderliche Befehlsoption.
${ }	Referenziert eine Variable.
-	Verbindet gleichzeitig mehrere Tastenanschläge.
+	Verbindet mehrere aufeinanderfolgende Tastenanschläge.
>	Zeigt die Auswahl eines Menüpunkts in der grafischen Benutzeroberfläche an.

Bereitstellung

Um die Dienste bereitzustellen, sind die folgenden Schritte zu befolgen:

- Bereitstellen der Webanwendung
- Zuweisen von Codebase Grant's

Bereitstellen der Webanwendung

Alle Dienste werden als Webanwendung in der gleich Weblogic Server Domain bereitgestellt, wie die Applikationen der Oracle Identity Governance Suite selbst. Dadurch wird eine hohe Grad an Wiederverwendbarkeit der von der Oracle Identity Governance Suite bereitgestellten Bibliotheken erreicht.

In diesem Abschnitt wird nur die Bereitstellung mit dem Deployment Assistant in der Administrationskonsole der WebLogic Domain behandelt. Andere Techniken, wie die Verwendung von Apache Ant-Skripts mit benutzerdefinierten WebLogic-Tasks oder der API für die Bereiststellung, werden nicht behandelt.

WebLogic Server unterstützt die Bereitstellung von Webanwendungen aus WAR-Dateien und aus expadierten Verzeichnissen.

Der Bereitstellungsmodus *staging* bestimmt, wie die Archivdatei eines Moduls den Zielservern die das Modul bereitstellen müssen, zur Verfügung gestellt werden. WebLogic Server bietet drei verschiedene Optionen zum Staging von Archivdateien: den *stage*-Modus, den *nostage*-Modus und den *external_stage*-Modus. Sie können den Staging-Modus entweder auf der Ebene des WebLogic Server oder auf Ebene der Anwendung festlegen, wodurch der Ebene des WebLogic Server überschrieben wird.

Modus Stage

Der Modus *stage* bedeutet, dass der Administrationsserver die Dateien von ihrem ursprünglichen Speicherort in die Staging-Verzeichnisse jedes Zielservers kopiert. Wenn Sie beispielsweise eine JEE-Anwendung auf drei Servern in einem Cluster bereitstellen, kopiert der Administrationsserver die Bereitstellungsdateien in Verzeichnisse auf jedem der drei Servercomputer. Anschließend stellt jeder Server die JEE-Anwendung mithilfe seiner lokalen Kopie der Archivdateien bereit.

Der Modus *stage* ist der standardm?ßige (und bevorzugte) Modus bei der Bereitstellung auf mehr als einer WebLogic Server-Instanz.

Modus Nostage

Der Modus *nostage* bedeutet, dass der Administrationsserver die Archivdateien nicht von ihrem Speicherort kopiert. Stattdessen muss jeder Zielserver für die Bereitstellung von einem einzigen gleichnaimigen Verzeichnis aus auf die Archivdateien zugreifen können. Wenn Sie beispielsweise eine JEE-Anwendung auf drei Servern in einem Cluster bereitstellen, muss jeder Server auf identischen Archivdateien der Anwendung zugreifen können (von einem freigegebenen oder im Netzwerk bereitgestellten Verzeichnis), um die Anwendung bereitzustellen.

Im Modus *nostage* erkennt der Container automatisch Änderungen an JSP's und Servlets.

Der Modus *nostage* ist der Standardmodus, wenn die Bereitstellung nur auf dem Administrationsserver erfolgt (z. B. in einer Dom?ne mit einem einzigen Server). Sie können den

Modus *nostage* auch ausw?hlen, wenn Sie einen Cluster von Serverinstanzen auf demselben Computer ausführen.

Modus External_stage

Der Modus *external_stage* ?hnelt dem Modus *stage*, da sich die Bereitstellungsdateien lokal auf jedem Zielserver befinden müssen. Allerdings kopiert der Administrationsserver die Bereitstellungsdateien nicht automatisch auf Zielserver im Modus *external_stage*; dtattdessen müssen Sie sicherstellen, dass die Dateien in das Staging-Verzeichnis jedes Zielservers kopiert werden.

Der Modus *external_stage* ist der am wenigsten verbreitete Bereitstellungsmodus. Es wird im Allgemeinen nur in Umgebungen verwendet, die von Werkzeugen von Drittanbietern verwaltet werden, die das erforderliche Kopieren von Dateien automatisieren.

Zuweisen von Codebase Grant's

Zum Zweck der Authentisierung und Authorisierung verwenden die Anwendungen entweder technische oder personalisierte Benutzerkonten, um diese Konten gegenüber den Serviceschnittstellen, die Oracle Identity Governance Suite offeriert, zu authentifizieren und zu autorisieren.

Um diese Authentisierung und Autorisierung vornehmen zu können, müssen die Applikationen dafür berechtigt werden. Dies wird erreicht, indem den binäre Archivdateien entsprechende Berechtigungen (*Codebase Grant*'s) erteilt werden. Bei *Codebase Grant*'s handelt es sich um Richtlinien, die die Ausführungsrechte von Code regeln, der in einer Java Virtual Machine (JVM) ausgef?hrt wird.

ZeRo Provisioning Service

Die folgenden *Codebase Grant*'s sind erforderlich, um den Dienst betriebsbereit zu machen:

- Identity Governance Identity Assertion
- Identity Governance Credential Access
- Webservice Manager Credential Access

Identity Governance Identity Assertion

Element	Value
Resource Name	IdentityAssertion
Permission Actions	execute
Permission Class	oracle.security.jps.JpsPermission

Identity Governance Credential Access

Element	Value
Resource Name	context=SYSTEM,mapName=oim,keyName=*
Permission Actions	read

Element	Value
Permission Class	oracle.security.jps.service.credstore.CredentialAccessPermission

Webservice Manager Credential Access

Element	Value
Resource Name	context=SYSTEM,mapName=oracle.wsm.security,keyName=*
Permission Actions	read
Permission Class	oracle.security.jps.service.credstore.CredentialAccessPermission

Sicherheit

Für den Zugriff auf die bereitgestellten Dienste müssen Konten authentifiziert und autorisiert werden. Dazu sind im angeschlossenen Verzeichnisdienst folgende Objekte erstellen:

- Enterprise Rollen
- Technische Benutzerkonten

Enterprise Rollen

Die Anwendung geht davon aus, dass die Namen der Rollen (groupOfUniqueName) wie folgt lauten:

- `zero_admin`
- `zero_viewer`

Wenn die Namen von der, w?hrend der Bereitstellung, verwendeten Namenskonvention abweichen, muss die Datei **WEB-INF/weblogic.xml** entsprechend ge?ndert und die Anwendung erneut bereitgestellt werden.

Der tats?chliche Speicherort f?r die Gruppen im Verzeichnisdiesnt sollte den geltenden IAM-Konventionen entsprechen. F?r die Anwendung ist nur der **Gruppenname** (`cn`-Attribut) ausschlaggebend.

Technische Benutzerkonten

HTTP-Proxy Konfiguration

Aus Sicherheitsgründen erfolgt der Zugriff auf die Dienste über einen HTTP-WebServer, der als Reverse Proxy in der DMZ eingesetzt wird. Die Verwendung von *reverse* hat seinen Ursprung im entsprechenden *forward*-Proxy, da der *reverse*-Proxy näher am Anwendungsserver sitzt und nur eine begrenzte Anzahl von Sites bedient.

Daher muss dieser HTTP-WebServer so konfiguriert werden, dass er den Datenverkehr über seinen Server umleitet und an den Anwendungsserver weiterleitet.

- TDB