

Loadbalancer & HTTP Proxy Konfiguration

Oracle® Access Manager Guide für
OpenIdConnect Erweiterung

Release 1.0.0

Loadbalancer & HTTP Proxy Konfiguration

Copyright © 2022, 2024 Oracle Consulting Services

Veröffentlicht 27.06.2023

von Sophie Strecke, Dieter Steding, Sylvert Bernet, Adrien Farkaš, Tomas Sebo und Jovan Lakic

| | | | |
|--------------------------------|------------|-------------------------------|---|
| | | | |
| Programm | | Polizei 20/20 | |
| Programmleiter | | Holger Gadorosi | |
| Projektleiter/Verantwortlicher | | Norbert Linde | |
| Dokumententitel | | P20 OpenIdConnect Erweiterung | |
| Version | | 1.1 | |
| Erstellt am | | 08.06.20228 | |
| Erstellt von | | Dieter Steding | |
| Zuletzt bearbeitet am | | 27.06.2023 | |
| Zuletzt bearbeitet von | | Dieter Steding | |
| | | | |
| Versionshistorie | | | |
| Version | Datum | Autor | Verweis |
| 1.0 | 29.08.2022 | Dieter Steding | Kein vorheriges Dokument |
| 1.1 | 16.05.2023 | Dieter Steding | Beschreibung der Ressourcen vervollständigt |

Inhaltsverzeichnis

| | |
|--|---|
| Vorwort | 1 |
| Audience | 1 |
| Bezugsdokumente | 1 |
| Vertraulichkeit | 1 |
| Typografische Konventionen | 1 |
| Symbolkonventionen | 1 |
| Einführung zur Access Manager OIDC-Erweiterung | 3 |
| Erforderliche Komponenten | 3 |
| Erforderliche Versionen | 3 |
| Erforderliche Patches | 3 |
| Anwendungsempfehlung | 4 |
| Unterstützte Sprachen | 5 |

Vorwort

In diesem Handbuch wird beschrieben, wie die OIDC-Erweiterung in Oracle Access Manager integriert wird.

Diese Konfiguration ist erforderlich, um den vom Standard abweichenden Anforderungen des Programms P20 zu genügen.

Audience

Dieses Dokument richtet sich sowohl an Personen, die sich mit der Administration von Ressourcen, als auch an Teams, die sich mit der Integration von Zielsystemen befassen.

Bezugsdokumente

Informationen zur Installation und Verwendung von Oracle Identity & Access Management Suite finden Sie auf der folgenden Oracle Help Center-Seite:

- <https://docs.oracle.com/en/middleware/identity/oracle-identity-suite/12.2.1.3/index.html>
- <https://docs.oracle.com/en/middleware/identity/oracle-identity-suite/12.2.1.4/index.html>

Vertraulichkeit

Das in dieser Dokumentation enthaltene Material stellt geschützte, vertrauliche Informationen zu Produkten und Methoden von Oracle dar.

Der Leserkreis erklärt sich damit einverstanden, dass die Informationen in dieser Dokumentation nicht außerhalb von Oracle weitergegeben und zu keinem anderen Zweck als der Bewertung dieses Verfahrens verwendet, vervielfältigt oder weitergegeben werden dürfen.

Typografische Konventionen

In der folgenden Tabelle werden die typografischen Konventionen beschrieben, die in diesem Dokument verwendet werden.

| Konvention | Bedeutung |
|------------------------|---|
| fett | Fettdruck kennzeichnet grafische Benutzeroberflächenelemente, die mit einer Aktion verknüpft sind, oder im Text oder Glossar definierte Begriffe. |
| <i>kursiv</i> | Kursivschrift kennzeichnet Buchtitel, Hervorhebungen oder Platzhaltervariablen, für die Sie bestimmte Werte angeben |
| <code>monospace</code> | Monospace-Schrift innerhalb eines Absatzes kennzeichnet Befehle, URLs, Code in Beispielen, auf dem Bildschirm angezeigten Text oder von Ihnen einzugebenden Text. |

Symbolkonventionen

In der folgenden Tabelle werden die Symbole erläutert, die in diesem Dokument verwendet werden können.

| Symbol | Bedeutung |
|--------|---|
| [] | Enthält optionale Argumente und Befehlsoptionen. |
| { } | Enthält eine Reihe von Auswahlmöglichkeiten für eine erforderliche Befehlsoption. |
| \${ } | Zeigt eine Variablenreferenz an. |
| - | Verbindet mehrere gleichzeitige Tastenanschläge. |
| + | Verbindet mehrere aufeinanderfolgende Tastenanschläge. |
| > | Zeigt die Auswahl eines Menüelements in einer grafischen Benutzeroberfläche an. |

Einführung zur Access Manager OIDC- Erweiterung

Oracle® Access Management ist eine Komplettlösung, die eine sichere Geschäftstransformation mit Mobil- und Social-Networking-Technologien, der Bereitstellung hybrider Anwendungen vor Ort und in der Cloud sowie einer hybriden Bereitstellung von Zugriffsverwaltung ermöglicht und gleichzeitig ein nahtloses Benutzererlebnis, eine zentralisierte Verwaltung sowie marktführende Leistung und Skalierbarkeit gewährleistet.

Die folgenden Abschnitte geben einen allgemeinen Überblick über die Erweiterung:

- [Erforderliche Komponenten](#)
- [Anwendungsempfehlung](#)
- [Unterstützte Sprachen](#)

Erforderliche Komponenten

Die in diesem Dokument aufgeführten plattformspezifischen Hardware- und Softwareanforderungen sind zum Zeitpunkt der Erstellung dieses Dokuments gültig. Da nach der Veröffentlichung dieses Dokuments möglicherweise neue Plattformen und Betriebssysteme zertifiziert werden, wird empfohlen, die Zertifizierungsmatrix im Oracle Technology Network zu konsultieren. Die aktuellen Aussagen zu zertifizierten Plattformen und Betriebssystemen finden Sie dort.

Die entsprechende Zertifizierungsmatrix für Produkte der Oracle Identity and Access Management Suite ist unter den folgenden URLs verfügbar:

- [Oracle® Fusion Middleware 12c \(12.2.1.4.0\)](#)
- [Oracle® Fusion Middleware 12c \(12.2.1.3.0\)](#)

Erforderliche Versionen

Dies sind die Softwarekomponenten und Versionen, die zur Installation und den Einsatz der Erweiterung erforderlich sind.

| Komponente | Version |
|------------------------------|--|
| Oracle® Java Development Kit | JDK 1.8.0_131 oder höher |
| Oracle® Infrastruktur | Oracle® WebLogic 12c (12.2.1.4.0) |
| Oracle® Database | Oracle® RDBMS 12c (12.2.0.1.0) oder höher |
| Oracle® Access Management | Oracle® Access Management 12c Release 12.2.1.4.0 |

Erforderliche Patches

Dies sind die Softwarekomponenten und Versionen, die zur Installation und den Einsatz der Erweiterung erforderlich sind.

| Komponente | Version |
|---------------------------|--|
| Oracle® Access Management | Oracle® Fusion Middleware Bundle Patch 12.2.1.4.240415 |

Anwendungsempfehlung

Single-Sign-On-Systeme (SSO) ermöglichen es Benutzern, sich einmal zu authentifizieren und danach auf mehrere verschiedene Systeme zuzugreifen. Es gibt viele SSO-Systeme für Webanwendungen, es sieht jedoch so aus, als ob diese Systeme alle das gleiche grundlegende Funktionsprinzip verwenden. Dieser allgemeine Ablauf der Zugriffsverwaltung wird im Folgenden beschrieben:

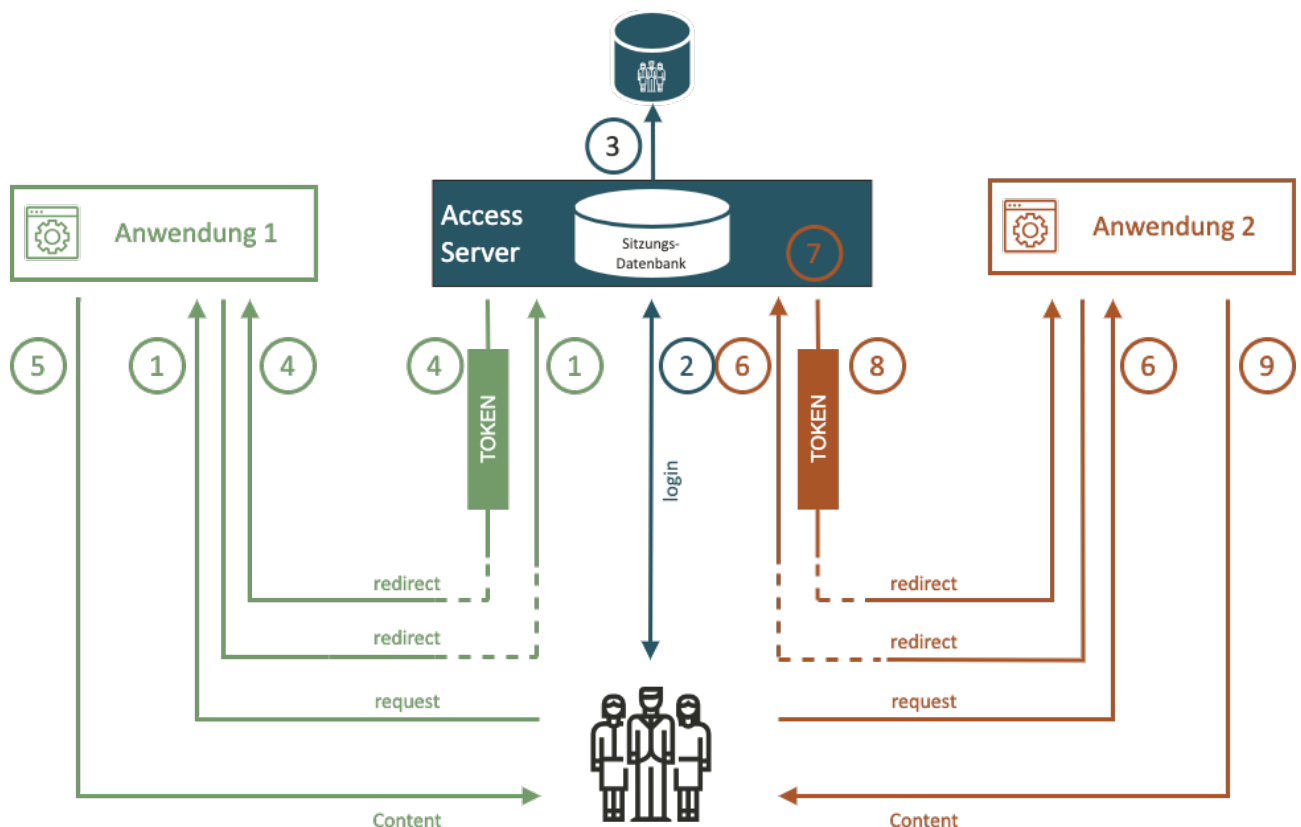


Abbildung 1. Access Manager im Kontext Single Sign On

1. Ein Benutzer fordert Zugriff auf Anwendung 1 an worauf diese prüft, ob eine lokale Sitzung für den Benutzer existiert. Ist diese nicht vorhanden, leitet die Anwendung den Benutzer zum Dienst Access Server der Zugriffssteuerung weiter.
2. Der Access Server der Zugriffssteuerung prüft, ob eine SSO-Sitzung vorhanden ist. Da noch keine Sitzung besteht, fordert der Access Server der Zugriffssteuerung den Benutzer zur Authentifizierung auf.
3. Nach Bereitstellung der Daten für die Authentifizierung werden diese an einen externen Dienst zur Authentifizierung (IdP) zur Verwendung eines externen Dienstes vorgenommen. Im einfachsten Fall ist dies ein Verzeichnisdienst, in komplexeren Umgebungen werden auch externe IdP-Provider (IdP) hinzugezogen. Die Zugriffssteuerung richtet bei erfolgreicher Authentifizierung eine Sitzung (SSO-Sitzung) für den Webbrowser des Benutzers ein. Dies ist der entscheidende Teil des SSO-Mechanismus.

4. Der Benutzer wird zurück zu Anwendung 1 umgeleitet und die Anwendung erstellt normalerweise ihrerseits eine lokale Sitzung für den Benutzer.
5. Der Benutzer interagiert mit Anwendung 1.
6. Wenn der Benutzer versucht, auf Anwendung 2 zuzugreifen, prüft diese, wie Anwendung 1 zunächst auf die Existenz einer lokalen Sitzung für den Benutzer. Ist diese nicht vorhanden, leitet die Anwendung den Benutzer zu Anwendung 1 an den Access Server der Zugriffssteuerung weiter.
7. Die Zugriffssteuerung prüft erneut, ob eine SSO-Sitzung vorhanden ist. Da der Benutzer zuvor am Access Server der Zugriffssteuerung authentifiziert wurde, liegt eine gültige SSO-Sitzung vor.
8. Die Zugriffssteuerung muss den Benutzer nicht erneut authentifizieren und den Benutzer sofort zurück zu Anwendung 2.
9. Anwendung 2 richtet ihrerseits eine lokale Sitzung mit dem Benutzer ein und fährt normal fort.

Unterstützte Sprachen

Die Erweiterung unterstützt die folgenden Sprachen:

- English