



Hewlett Packard
Enterprise

Operations Orchestration

Softwareversion: 10.60 Betriebssysteme
Windows und Linux

Architekturhandbuch

Datum der Dokumentveröffentlichung: Mai 2016

Datum des Software-Release: Mai 2016

Rechtliche Hinweise

Garantie

Die Garantiebedingungen für Produkte und Services von Hewlett Packard Enterprise sind in der Garantieerklärung festgelegt, die diesen Produkten und Services beiliegt. Keine der folgenden Aussagen kann als zusätzliche Garantie interpretiert werden. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen.

Die hierin enthaltenen Informationen können ohne vorherige Ankündigung geändert werden.

Eingeschränkte Rechte

Vertrauliche Computersoftware. Gültige Lizenz von Hewlett Packard Enterprise für den Besitz, Gebrauch oder die Anfertigung von Kopien erforderlich. Entspricht FAR 12.211 und 12.212. Kommerzielle Computersoftware, Computersoftwareokumentation und technische Daten für kommerzielle Komponenten werden an die US-Regierung per Standardlizenz lizenziert.

Copyright-Hinweis

© 2005-2016 Hewlett Packard Enterprise Development LP

Markenhinweise

Adobe™ ist eine Marke von Adobe Systems Incorporated.

Microsoft® und Windows® sind in den USA eingetragene Marken der Microsoft Corporation.

UNIX® ist eine eingetragene Marke von The Open Group.

Dieses Produkt enthält eine Schnittstelle der freien Programmbibliothek zum Komprimieren, 'zlib', geschützt durch Copyright © 1995-2002 Jean-loup Gailly und Mark Adler.

Aktualisierte Dokumentation

Auf der Titelseite dieses Dokuments befinden sich die folgenden identifizierenden Informationen:

- Software-Versionsnummer, die Auskunft über die Version der Software gibt.
- Datum der Dokumentveröffentlichung, das bei jeder Änderung des Dokuments ebenfalls aktualisiert wird.
- Datum des Software-Release, das angibt, wann diese Version der Software veröffentlicht wurde.

Unter der unten angegebenen Internetadresse können Sie überprüfen, ob neue Updates verfügbar sind, und sicherstellen, dass Sie mit der neuesten Version eines Dokuments arbeiten: <https://softwaresupport.hp.com/>.

Für die Anmeldung bei dieser Website benötigen Sie einen HP Passport. Um sich für eine HP Passport-ID zu registrieren, klicken Sie auf **Register** (Registrieren) auf der HP Software Support-Site oder auf **Create an Account** (Konto erstellen) auf der HP Passport-Anmeldeseite.

Wenn Sie sich beim Support-Service eines bestimmten Produkts registrieren, erhalten Sie ebenfalls aktualisierte Softwareversionen und überarbeitete Ausgaben der zugehörigen Dokumente. Weitere Informationen erhalten Sie bei Ihrem HPE-Kundenbetreuer.

Inhalt

Systemarchitektur	4
Operations Orchestration-Komponenten	4
Einfache Bereitstellung	4
Einfacher Cluster	5
Skalierbarkeit	6
Hinzufügen eines RAS	6
RAS-Hochverfügbarkeit	8
Verwenden eines Load Balancers in der OO-Bereitstellung	10
Load Balancer - Anforderungen	10
Load Balancer - Sicherheit	10
Konfigurieren von Load Balancer und OO Central-Systemen für TLS- Verschiebung	11

Systemarchitektur

Operations Orchestration-Komponenten

HPE OO Studio ist ein eigenständiges Authoring-Programm für das Erstellen, Ändern und Testen von Flows.

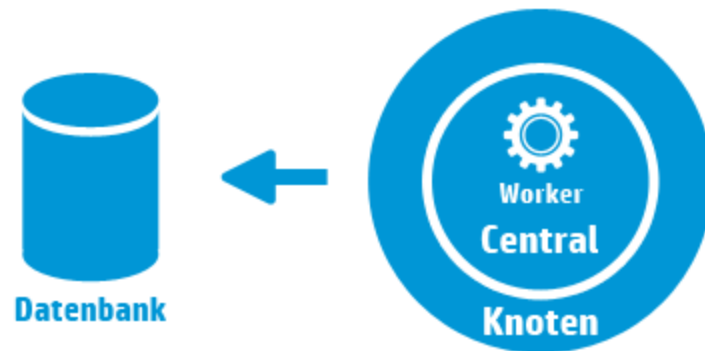
HPE OO Central ist die Laufzeitumgebung von HPE OO. Es wird für die Ausführung von Flows, die Überwachung der verschiedenen Ausführungen und das Generieren von Reports verwendet.

Ein **RAS** ist ein Server für Remoteaktionen, der einen Worker und ein Remoteprotokoll für die Verbindung mit Central einschließt.

Weitere Informationen zu HPE OO-Komponenten finden Sie im *HPE OO-Konzepthandbuch*.

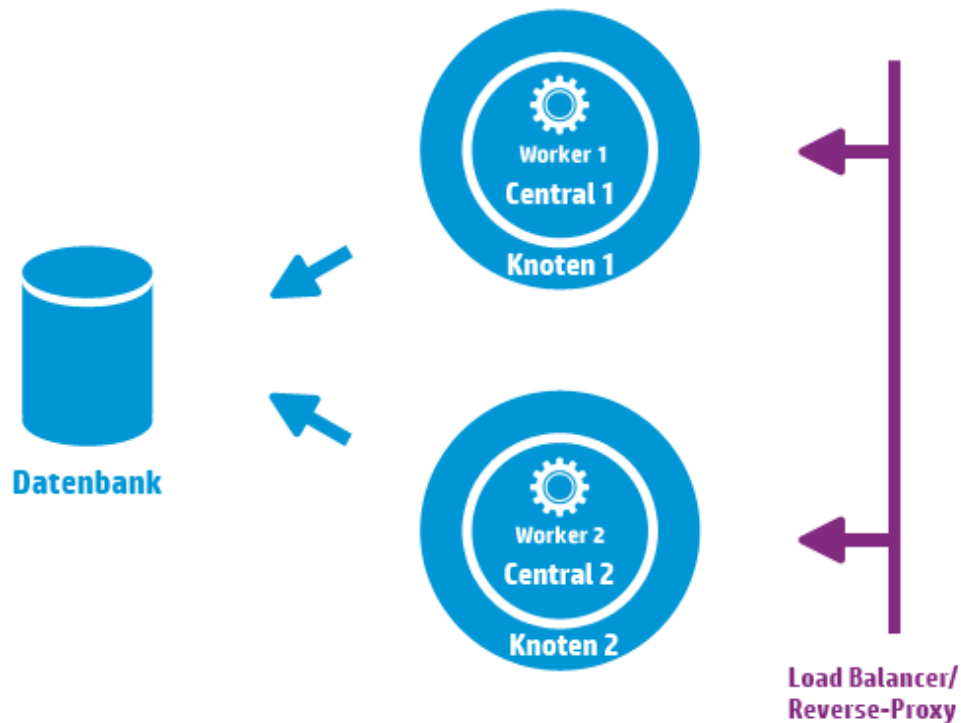
Einfache Bereitstellung

Die einfache HPE OO-Bereitstellung besteht aus einer einzelnen Central-Instanz (siehe Abbildung unten).



Einfacher Cluster

Um zu verhindern, dass die Central-Instanz zum Single Point of Failure wird, empfiehlt sich eine Hochverfügbarkeitsbereitstellung. Sie können einen Cluster aus mehreren Central-Knoten einrichten, der in der einfachsten Form zwei Central-Knoten enthält, die mit demselben Datenbankschema verbunden sind. Wie die folgende Abbildung zeigt, kann vor dem Central-Cluster ein Load Balancer eingerichtet werden, um eine einzelne URL für die Endbenutzer bereitzustellen. Das Bereitstellen einer einzelnen URL kann auch mittels DNS-Lastausgleich erfolgen.



Der Load Balancer/Reverse Proxy sollte an die Central-Instanzen umleiten, die die Ports 8443 und 8080 verwenden, wenn während der Installation die Standardwerte ausgewählt wurden. Weitere Informationen finden Sie unter *HPE OO-Systemanforderungen*.

Änderung gegenüber OO 9.x: Im Gegensatz zu früheren Versionen besteht weder eine Notwendigkeit zur Verwendung externer Clustersoftware, noch wird ein gemeinsam genutztes

Dateisystem benötigt.

Skalierbarkeit

HPE OO ermöglicht das horizontale Skalieren für die Erhöhung des Durchsatzes bei der Ausführung.

Sie können mehrere Central-Instanzen zum HPE OO-Cluster hinzufügen. HPE OO unterstützt die Live-Skalierbarkeit. Dies bedeutet, dass beim Hinzufügen eines Central-Knotens keine Ausfallzeit erforderlich ist. Installieren Sie einfach eine weitere Central-Instanz und konfigurieren Sie sie so, dass sie auf das vorhandene Datenbankschema verweist.

Weitere Informationen finden Sie im Dokument *HPE OO 10 Benchmark* in HPLN unter <https://hpln.hp.com/node/17617/attachment>.

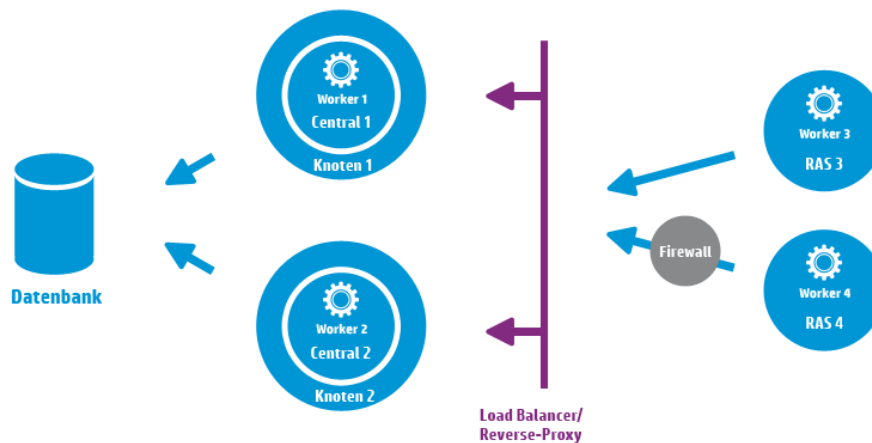
Hinzufügen eines RAS

Eine RAS-Instanz ist eine optionale OO-Komponente. Ein RAS kann verwendet werden, wenn HPE OO Flows in einem Netzwerksegment ausführen muss, das über die HPE OO Central-Knoten nicht erreichbar ist. In diesem Fall können Sie eine RAS-Instanz im Zielnetzwerksegment installieren, die dann die erforderlichen Flows aus der Central-Instanz abrufen und lokal ausführt.

Als weiterer Anwendungsfall kann ein RAS verwendet werden, wenn der ausgeführte Flow bestimmte Binärdateien auf dem lokalen Computer erfordert. Die Binärdateien müssen nicht auf jedem HPE OO-Knoten installiert werden. Es reicht aus, sie auf einem Host zu installieren, auf dem ein RAS installiert ist, und die Flows (oder bestimmte Schritte) so zu konfigurieren, dass die Ausführung auf diesem RAS erfolgt. Dies kann mit der als Worker-Gruppe bezeichneten Funktionalität erreicht werden.

Weitere Informationen zu Worker-Gruppen finden Sie im *HPEOO-Konzepthandbuch*.

RAS-Instanzen können Sie einer HPE OO Central-Instanz oder einem Cluster aus HPE OO Central-Knoten zuordnen. Die folgende Abbildung zeigt, wie RAS3 und RAS4 mit dem HPE OO Central-Cluster kommunizieren. Beachten Sie, dass sich RAS4 hinter einer Firewall befindet.



Konfigurieren der RAS-Verbindungsrichtung

Ab OO 10.60 können Sie RAS-Instanzen so konfigurieren, dass einige die Verbindung zu Central initiieren, während andere darauf warten, dass Central die Verbindung initiiert.

Wenn zum Beispiel Central und ein RAS in unterschiedlichen Netzwerken installiert sind, wobei sich Central in einem sichereren Netzwerk befindet, und Ihre Sicherheitsrollen keine Verbindung vom weniger sicheren Netzwerk zum sichereren Netzwerk zulassen, können Sie Central die Verbindung zum RAS initiieren lassen.

Während der Installation eines RAS müssen Sie zwischen zwei Optionen wählen:

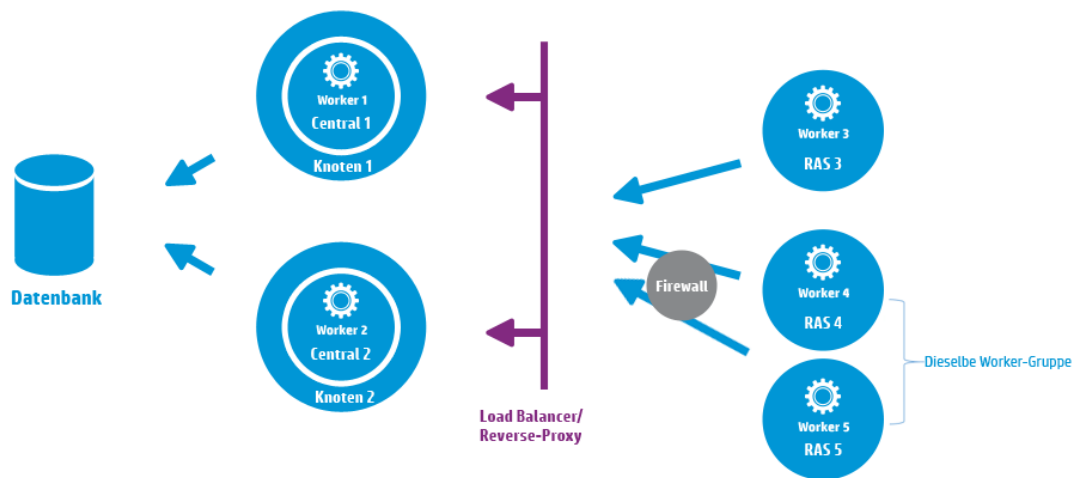
- **Standard-RAS - RAS initiiert Kommunikation zu Central** - Dies ist die einfachste Option, die empfohlen wird, wenn Ihre Sicherheitsregeln dies zulassen.
- **Reverse RAS - Central initiiert Kommunikation zu RAS** - Wählen Sie diese Option, wenn Central in einem anderen, sichereren Netzwerk installiert wurde und Ihre Sicherheitsrollen keine Verbindung vom weniger sicheren Netzwerk zum sichereren Netzwerk zulassen.

Sie müssen dann den RAS so konfigurieren, dass er die Verbindung von Central akzeptiert, und Central so konfigurieren, dass der RAS registriert wird (auf der Registerkarte **Systemkonfiguration** > **Topologie** > **Worker**).

Wenn der RAS gestartet wird, bleibt er im Leerlauf und wartet darauf, dass Central die Verbindung initiiert.

RAS-Hochverfügbarkeit

Wenn ein RAS in einem Netzwerksegment bereitgestellt wird, um die Computer in diesem Segment zu verwalten, brauchen Sie dazu nicht nur eine Instanz zu verwenden. Um Hochverfügbarkeit zu erreichen, können Sie in diesem Segment eine zusätzliche RAS-Instanz bereitstellen. Stellen Sie dabei sicher, dass sie mit derselben Worker-Gruppe verknüpft wird. Dies ist in der folgenden Abbildung dargestellt:



Änderung gegenüber HPE OO 9.x: Zwischen RAS-Cluster und Central (oder Central-Cluster) ist kein zusätzlicher Load Balancer erforderlich. Da sowohl RAS 4 als auch RAS 5 derselben Worker-Gruppe angehören, teilen sie die Last bei der Ausführung der Flows\Schritte, die für diese Worker-Gruppe bestimmt sind, und realisieren damit die Hochverfügbarkeit.

Verwenden eines Load Balancers in der OO-Bereitstellung

Weitere Informationen über das Installieren eines Load Balancers finden Sie in der Dokumentation vom Anbieter Ihres Load Balancers.

Load Balancer - Anforderungen

Wir empfehlen, den Load Balancer mit zwei separaten virtuellen IPs für die Benutzeroberfläche und für RAS-Instanzen zu konfigurieren:

- Für die HPE OO-Benutzeroberfläche und die Kundenportale sollte die virtuelle IP eine Richtlinie für **Sticky-Sitzungen** verwenden. Die Sticky-Sitzung stellt sicher, dass alle nachfolgenden Anforderungen an den Server gesendet werden, der die erste Anmeldeanforderung bearbeitet hat. Dies bedeutet, dass sich der Benutzer nur einmal bei der HPE OO-Schnittstelle anmelden muss.
- Für RAS-Instanzen sollte die virtuelle IP eine **Round-Robin**-Richtlinie verwenden, um die Last nach dem Umlaufverfahren zwischen den verschiedenen Servern zu verteilen.

Hinweis: Wenn Sie eine andere Konfiguration verwenden, die diese Anforderungen erfüllt, kann auch diese verwendet werden. Beispiel: Wenn Sie einen Load Balancer verwenden, der JSESSION unterstützt, können Sie den Parameter JSESSIONID verwenden, um für alle Quellen eine einzelne virtuelle IP mit einer Richtlinie für Sticky-Sitzungen einzurichten. Da RAS-Anforderungen zustandslos sind (keine JSESSIONID), wird hierdurch eine Round Robin-Richtlinie für RAS-Instanzen realisiert.

Central verwendet die folgende URL, um zu überprüfen, welcher Server live ist:

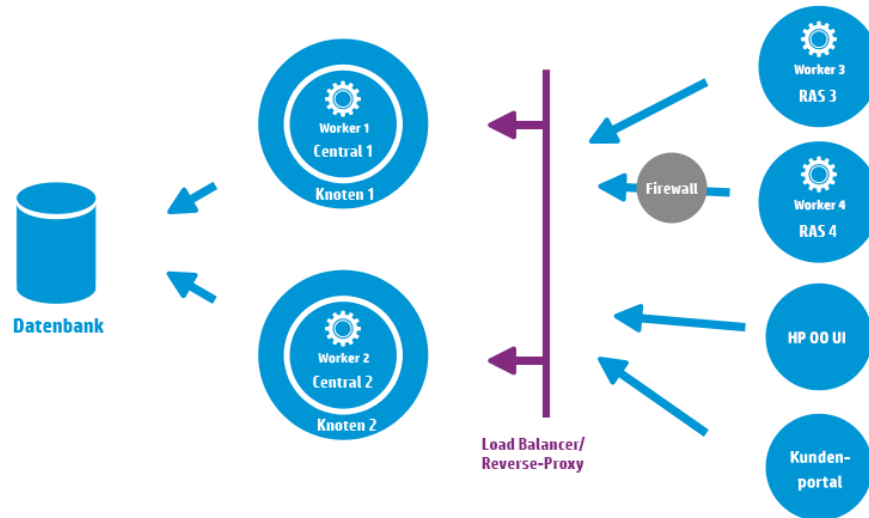
HTTP://<IP>:<PORT>/oo/hello.html

Load Balancer - Sicherheit

In einer verstärkten Hochverfügbarkeitsumgebung sollte der Load Balancer für TLS konfiguriert werden. Weitere Informationen zum Konfigurieren von TLS finden Sie unter "Authentifizierung mit Server- und Clientzertifikat" im *HPE OO-Sicherheits- und Optimierungshandbuch*.

Die Kommunikation zwischen der HPEOO-Schnittstelle und Load Balancer kann über HTTPS erfolgen. Wir empfehlen, das TLS-Zertifikat auf dem Load Balancer zu installieren, sodass dies der

Abschlusspunkt für die Verschlüsselung ist. Hinter dem Load Balancer erfolgt die Kommunikation über HTTP mit höherer Geschwindigkeit.



Konfigurieren von Load Balancer und OO Central-Systemen für TLS-Verschiebung

Wenn ein Load Balancer für den Zugriff auf die Central-Server verwendet wird, sollte der Load Balancer für das TLS Offloading konfiguriert werden.

1. Fügen Sie in einem Editor zum Beispiel den folgenden Text in die Tomcat-Datei **Server.xml** ein:

```
<Engine name="Catalina" defaultHost= "localhost" >
. . .
<Valve
className="org.apache.catalina.valves.RemoteIpValve"protocolHeader="X-
Forwarded-Proto" />
. . .
</Engine>
```

2. Konfigurieren Sie den Load Balancer so, dass allen Anforderungen der Clients ein neuer Header hinzugefügt wird.

Der Headername ist konfigurierbar und muss der oben angegebenen Tomcat-Konfiguration entsprechen. In diesem Beispiel lautet der Name "X-Forwarded-Proto".

Im F5 Load Balancer würde dann die Konfiguration etwa wie folgt aussehen:

```
when HTTP_REQUEST {  
  HTTP::header insert "X-Forwarded-Proto" "https";  
}
```

