



Hewlett Packard
Enterprise

HPE Application Performance Management

Softwareversion: 9.30

APM-Installationshandbuch

Dokument-Releasedatum: Juli 2016
Software-Releasedatum: Juli 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. HPE 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 HPE für den Besitz, Gebrauch oder die Anfertigung von Kopien erforderlich. Entspricht FAR 12.211 und 12.212; kommerzielle Computersoftware, Computersourcedokumentation und technische Daten für kommerzielle Komponenten werden an die US-Regierung per Standardlizenz lizenziert.

Urheberrechtshinweise

© Copyright 2005-2016 Hewlett Packard Enterprise Development LP

Marken

Adobe® und Acrobat® sind Marken der Adobe Systems Incorporated.

AMD und das AMD Arrow-Logo sind eingetragene Marken von Advanced Micro Devices, Inc.

Google™ und Google Maps™ sind eingetragene Marken von Google Inc.

Intel®, Itanium®, Pentium® und Intel® Xeon® sind eingetragene Marken der Intel Corporation in den Vereinigten Staaten und anderen Ländern.

iPod ist eine Marke der Apple Computer, Inc.

Java ist eine eingetragene Marke von Oracle und/oder der zugehörigen Tochtergesellschaften.

Microsoft®, Windows®, Windows NT®, Windows Server® und Windows Vista™ sind eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Oracle ist eine eingetragene Marke von Oracle und/oder der zugehörigen Tochtergesellschaften.

UNIX® ist eine eingetragene Marke von The Open Group.

Dokumentationsaktualisierungen

Die Titelseite dieses Dokuments enthält die folgenden bezeichnenden Informationen:

- Software-Versionsnummer zur Angabe der Software-Version.
- Dokument-Releasedatum, das sich mit jeder Aktualisierung des Dokuments ändert.
- Software-Releasedatum zur Angabe des Releasedatums der Software-Version.

Um nach Aktualisierungen des Dokuments zu suchen, oder um zu überprüfen, ob Sie die aktuellste Version des Dokuments verwenden, wechseln Sie zu: <https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=>.

Um diese Website verwenden zu können, müssen Sie über ein HPE Passport-Konto verfügen. Wenn Sie nicht über ein Konto verfügen, klicken Sie auf der HPE Passport-Anmeldeseite auf **Create an account**.

Unterstützung

Besuchen Sie die HPE-Website zur Software-Unterstützung unter: <https://softwaresupport.hpe.com>

Auf dieser Website finden Sie Kontaktinformationen und Details zu Produkten, Services und Supportleistungen von HPE Software.

HPE Software-Unterstützung stellt Kunden online verschiedene Tools zur eigenständigen Problemlösung zur Verfügung. Sie bietet schnelle und effiziente Wege, auf interaktive Werkzeuge für den technischen Support

zuzugreifen, die für die Führung des Unternehmens erforderlich sind. Als Kunde mit Supportvertrag stehen Ihnen beim Support folgende Optionen zur Verfügung:

- Suchen nach interessanten Wissensdokumenten
- Absenden und Verfolgen von Support-Fällen und Erweiterungsanforderungen
- Herunterladen von Software-Patches
- Verwalten von Supportverträgen
- Nachschlagen von HPE-Supportkontakten
- Einsehen von Informationen über verfügbare Services
- Führen von Diskussionen mit anderen Softwarekunden
- Suchen und Registrieren für Softwareschulungen

Bei den meisten Support-Bereichen ist die Registrierung und Anmeldung als HPE Passport-Benutzer erforderlich. Einige Angebote setzen den Abschluss eines Supportvertrags voraus. Um sich für eine HPE Passport-ID zu registrieren, wechseln Sie zu <https://softwaresupport.hpe.com> und klicken Sie dann auf **Register**.

Weitere Informationen über die für den Zugriff erforderlichen Voraussetzungen erhalten Sie unter:
<https://softwaresupport.hpe.com/web/softwaresupport/access-levels>

HPE Software-Integrationen, -Lösungen sowie Best Practices

Besuchen Sie die Website der Hewlett Packard Enterprise Software-Unterstützung (<https://softwaresupport.hpe.com/manuals>), um auf eine breite Palette der Dokumente und Materialien für Best Practices zuzugreifen.

Inhalt

Einführung	6
Teil I: Installationsworkflow	7
Kapitel 1: Überblick über die APM 9.30-Installation	8
Kapitel 2: Allgemeine Voraussetzungen	9
Voraussetzungen für die Installation - Windows	10
Voraussetzungen für die Installation - Linux	12
Kapitel 3: Installieren von BSM 9.30	16
Kapitel 4: Aufgaben nach der Installation	17
Allgemeine Aufgaben nach der Installation	18
Starten und Beenden von APM	21
An- und Abmelden	22
Hinzufügen weiterer APM-Server	23
Kapitel 5: Konfigurieren des sicheren Zugriffs auf den APM-Reverse Proxy	24
Reverse Proxy-Konfiguration	24
Workflow der Reverse Proxy-Konfiguration	26
Konfigurieren eines Reverse Proxys - Apache	27
Konfigurieren von Apache als Reverse Proxy	27
Referenz – Unterstützung für die APM-Applikationsbenutzer	29
Referenz - Unterstützung für APM-Daten-Collectoren	30
Konfigurieren eines Reverse Proxys – IIS	32
Konfigurieren des IIS als Reverse Proxy	32
Konfigurieren des IIS-Reverse Proxys für die Verwendung von SSL	32
Konfigurieren von IIS für das Anfordern der Clientauthentifizierung – optional	34
Spezifische HPE APM-Konfiguration	35
Hinweise und Einschränkungen	37
Unterstützung des spezifischen und des generischen Reverse Proxy-Modus in APM	37
Spezifischer Modus	37
Generischer Modus	37
Kapitel 6: Installieren und Konfigurieren von zusätzlichen Komponenten	39
Teil II: Anhänge	40
Anhang A: Installieren von APM auf einer Windows-Plattform	41
Vorbereiten der für die Installation erforderlichen Informationen	42
Arbeiten mit dem IIS-Webserver	44
Installieren von APM-Servern auf einer Windows-Plattform	46
Anhang B: Installieren von APM auf einer Linux-Plattform	49
Vorbereiten der für die Installation erforderlichen Informationen	50

Arbeiten mit dem Apache-Webserver	51
Installieren von APM-Servern auf einer Linux-Plattform	52
Anhang C: Serverbereitstellung und Festlegen von Datenbankparametern	54
Dienstprogramm für die Setup- und Datenbankkonfiguration – Übersicht	55
Festlegen von Datenbankparametern	56
Erforderliche Informationen zum Festlegen der Datenbankparameter	58
Ausführen des Dienstprogramms für das Setup und die Datenbankkonfiguration	60
Anhang D: Unbeaufsichtigte Installation von APM	63
Vollständige APM 9.30-Installation im Hintergrund	64
Generieren einer Antwortdatei zum unbeaufsichtigtem Ausführen des Post-Installations- Assistenten und des Dienstprogramms für das Setup und die Datenbankkonfiguration	66
Konfigurieren der Windows-Authentifizierung während der unbeaufsichtigten Ausführung des Dienstprogramms für das Setup und die Datenbankkonfiguration	67
Verschlüsselung von Kennwörtern in der Antwortdatei	68
Anhang E: Notfallwiederherstellung für APM	69
Einführung in die Notfallwiederherstellung für APM	69
Vorbereiten der Umgebung für die Notfallwiederherstellung	72
Bereinigungsverfahren	76
Konfigurieren der neuen Umgebung	81
Konfigurieren der Daten-Collectoren	82
Anhang F: Hochverfügbarkeit für APM	84
Übersicht über die Optionen für hohe Verfügbarkeit	85
Lastenausgleich für den Gateway-Server	86
Hochverfügbarkeit für den Gateway-Server	89
Hochverfügbarkeit für den Datenverarbeitungsserver	90
Konfigurieren der APM-Daten-Collectoren in einer verteilten Umgebung	102
Anhang G: Deinstallation von APM 9.30	103
Deinstallieren von BSM-Servern vor der Installation von APM	105
Anhang H: Ändern von Benutzern des APM-Diensts	108
Wechseln des Windows-Benutzers	108
Wechseln des Linux-Benutzers	109
Anhang I: Wechseln von Webservern	110
Anhang J: Fehlerbehebung	111
Ressourcen für die Fehlerbehebung	112
Beheben von Installations- und Verbindungsproblemen	113
Senden von Feedback zur Dokumentation	119

Einführung

Willkommen beim Handbuch zur Installation von APM. Dieses Handbuch enthält einen detaillierten Überblick über die Installation von APM.

Dieses Handbuch richtet sich an Kunden, die nicht über eine Version von APM verfügen.

Wenn Sie eine frühere Version von APM installiert haben, finden Sie dazu Informationen im **APM Upgrade Guide**.

Aufbau dieses Handbuchs

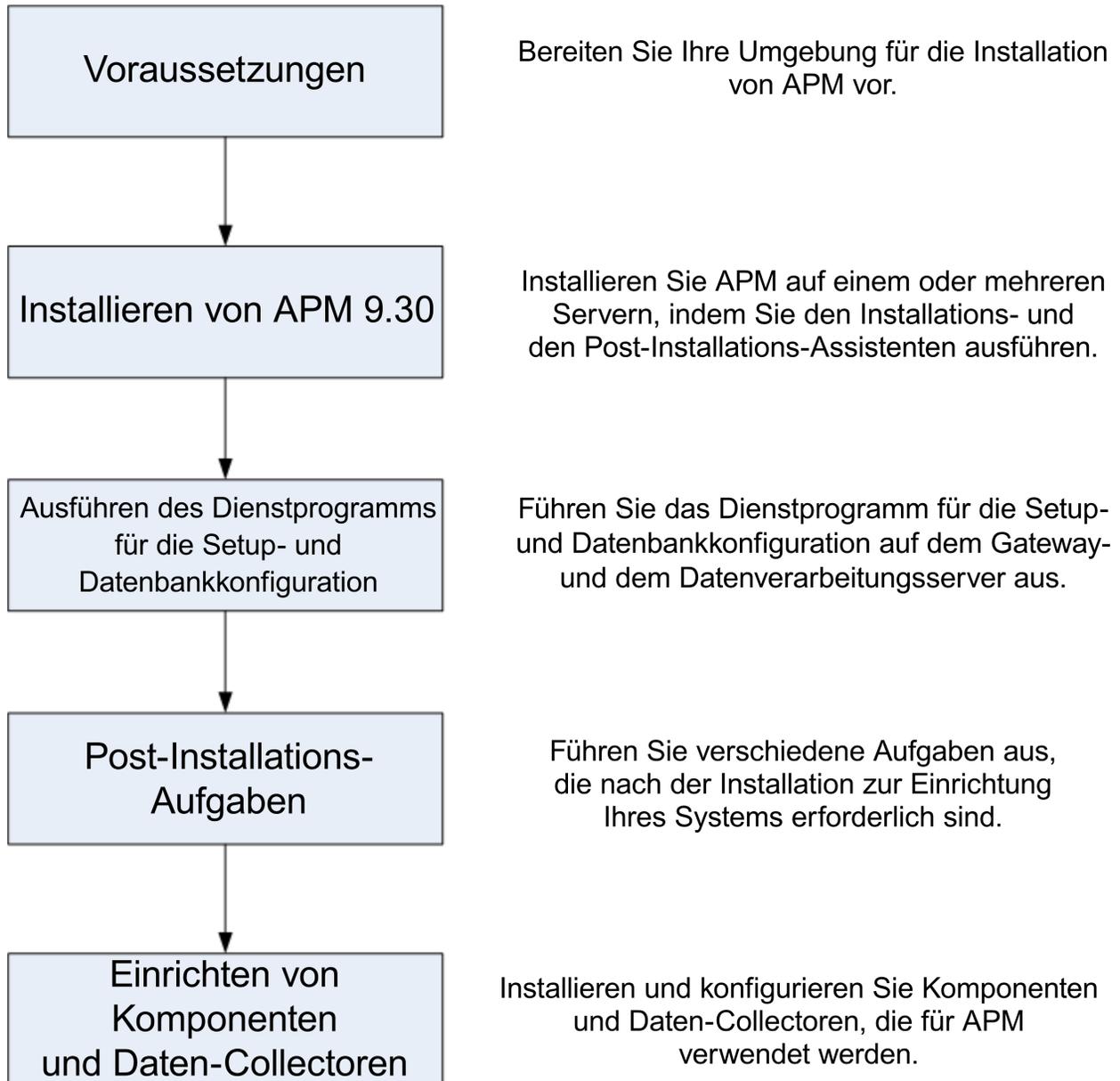
Dieses Buch ist in zwei Teile unterteilt:

- Teil I enthält eine schrittweise Anleitung für die Installation von APM.
- Teil II, der Anhang, enthält Referenzinformationen und optionale Verfahren.

Teil I: Installationsworkflow

Kapitel 1: Überblick über die APM 9.30-Installation

Die Installation von APM 9.30 umfasst die folgenden Hauptschritte:



Kapitel 2: Allgemeine Voraussetzungen

Führen Sie die folgenden Schritte aus, bevor Sie mit der Installation beginnen:

1. Erstellen eines Bereitstellungsplans

Erstellen Sie einen vollständigen Bereitstellungsplan einschließlich erforderlicher Software, Hardware und Komponenten. Details finden Sie im *APM Getting Started Guide* und in den APM-Systemanforderungen und den Tabellen für die APM-Unterstützung.

2. Bestellen und Registrieren von Lizenzen

Bestellen Sie die Lizenzen basierend auf dem Bereitstellungsplan bei einem Vertriebsmitarbeiter. Registrieren Sie Ihre Kopie von APM, um Zugriff auf technischen Support und Informationen zu allen HPE-Produkten zu erhalten. Ihnen stehen auch Aktualisierungen und Upgrades zu. Sie können Ihre Kopie von APM auf der Website [HPE Support](https://softwaresupport.hpe.com) (<https://softwaresupport.hpe.com>) registrieren.

3. Vorbereiten der Hardware

Richten Sie die APM-Server und den APM-Datenbankserver ein. Informationen zum Einrichten des Datenbankservers finden Sie im *APM Database Guide*.

4. Einrichten des Webservers (optional)

APM installiert während der Installation den Apache-Webserver auf allen APM-Gateway-Servern. Wenn Sie den Apache-Webserver verwenden möchten, jedoch den IIS-Webserver bereits installiert haben, beenden Sie den Dienst **IIS-Webserver** vor der Installation von APM. Ändern Sie nicht die Einstellung **Starttyp** für diesen Dienst. Entfernen Sie nicht die Rolle **IIS-Webserver**. Wenn Sie den IIS-Webserver verwenden möchten, müssen Sie ihn vor der Installation von APM auf allen Gateway-Servern installieren und starten.

Hinweis: Es darf sich nur ein ausgeführter Webserver auf einem Servercomputer befinden, der denselben Port wie APM verwendet. Wenn Sie sich z. B. während der APM-Serverinstallation zur Verwendung des Apache HTTP-Servers entschließen und die Installation auf einem Computer durchführen, auf dem bereits IIS ausgeführt wird, müssen Sie den IIS-Dienst beenden und den Startstatus des Diensts auf **Manuell** festlegen, bevor Sie mit der Installation beginnen. Weitere Informationen finden Sie unter:

- Für Linux: ["Arbeiten mit dem Apache-Webserver" auf Seite 51](#)
- Für Windows: ["Arbeiten mit dem IIS-Webserver" auf Seite 44](#)

Voraussetzungen für die Installation - Windows

Beachten Sie vor der Installation der APM-Server auf einer Windows-Plattform folgende Punkte:

- Sie sollten die APM-Server auf einem Laufwerk mit mindestens 40 GB freiem Speicherplatz installieren. Weitere Details zu den Serversystemanforderungen finden Sie unter Systemanforderungen für APM und Tabellen für die APM-Unterstützung.
- Wenn APM-Server, einschließlich der Datenbankserver, in mehreren Netzwerksegmenten installiert werden, sollten Sie unbedingt die Anzahl der Hops und die Latenz zwischen den Servern minimieren. Durch das Netzwerk verursachte Latenz kann negative Auswirkungen auf die APM-Applikation haben und zu Leistungs- und Stabilitätsproblemen führen. Die Netzwerklatenz sollte unabhängig von der Anzahl an Hops nicht mehr als 5 Millisekunden betragen. Weitere Informationen erhalten Sie über den HPE Support.
- Die APM-Server müssen sich auf ausschließlich für sie vorgesehenen Computern befinden und dürfen keine anderen Applikationen ausführen. Bestimmte APM-Komponenten können gleichzeitig auf APM-Servern installiert sein. Weitere Informationen zu Komponenten, die zusammen installiert werden können finden Sie in den Systemanforderungen für APM und Tabellen für die APM-Unterstützung.
- Wenn Sie den IIS-Webserver verwenden möchten, müssen Sie ihn vor der APM-Installation installieren und nach Abschluss der Installation aktivieren. Weitere Informationen finden Sie unter ["Arbeiten mit dem IIS-Webserver" auf Seite 44](#).
- APM-Server dürfen nicht auf einem Laufwerk installiert werden, das einer lokalen oder einer Netzwerkressource zugeordnet ist.
- Aufgrund bestimmter Webbrowserbeschränkungen dürfen die Namen von Servercomputern mit dem Gateway-Server nur aus alphanumerischen Zeichen (a bis z, A bis Z, 0 bis 9), Bindestrichen (-) und Punkten (.) bestehen. Wenn die Namen der Computer mit dem Gateway-Server beispielsweise Unterstriche enthalten, ist es eventuell nicht möglich, sich mit Microsoft Internet Explorer 7.0 oder höher an der APM-Website anzumelden.
- Während der APM-Serverinstallation können Sie einen anderen Pfad für das APM-Verzeichnis angeben (standardmäßig ist das Verzeichnis **C:\HPBSM**). Beachten Sie dabei aber, dass der vollständige Pfad zum Verzeichnis keine Leerzeichen enthalten, höchstens 15 Zeichen aufweisen darf und mit **HPBSM** enden muss.
- Der Name des Installationsverzeichnisses darf nur alphanumerische Zeichen (a-z, A-Z, 2-9) enthalten.

Hinweis: Die Ziffern 0 und 1 dürfen in Installationsverzeichnisnamen nicht verwendet werden.

- Die UAC (User Access Control, Benutzerkontensteuerung) muss vor der Installation von APM deaktiviert werden. Die Benutzerkontensteuerung ist bei einigen Versionen von Windows Server (z. B.: 2008 SP2) standardmäßig aktiviert.
- Wenn Sie APM-Server auf einer Plattform mit verstärkter Sicherheit (einschließlich der Nutzung des HTTPS-Protokolls) ausführen möchten, lesen Sie die im APM Hardening Guide beschriebenen Verfahren zur verstärkten Sicherheit.
- Öffnen Sie im APM-Cluster den Port 21212 auf dem Datenverarbeitungsserver.

Hinweis: Während der Installation wird der Wert für den Windows-Registrierungsschlüssel HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ReservedPorts so aktualisiert, dass er den folgenden Portbereich beinhaltet, der für APM erforderlich ist: 1098-1099, 2506-2507, 8009-8009, 29000-29000, 4444-4444, 8083-8083, 8093-8093.

Diese Portbereiche werden nicht aus dem Registrierungsschlüssel entfernt, wenn APM deinstalliert wird. Sie sollten die Ports daher nach der Deinstallation von APM manuell aus dem Registrierungsschlüssel entfernen, wenn sie nicht mehr von einer anderen Applikation benötigt werden.

Voraussetzungen für die Installation - Linux

Beachten Sie vor der Installation der APM-Server auf einer Linux-Plattform folgende Punkte:

- Sie sollten die APM-Server auf einem Laufwerk mit mindestens 40 GB freiem Speicherplatz installieren. Das **/tmp**-Verzeichnis muss mindestens 2,5 GB freiem Speicherplatz aufweisen. Sie können das **/tmp**-Verzeichnis mit dem folgenden Befehl wechseln:

```
export IATEMPDIR=/new/tmp/dir
```

```
export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp/dir
```

wobei **/new/tmp/dir** das neue **/tmp**-Verzeichnis darstellt.

Weitere Details zu den Serversystemanforderungen finden Sie unter Systemanforderungen für APM und Tabellen für die APM-Unterstützung.

- Wenn APM-Server, einschließlich der Datenbankserver, in mehreren Netzwerksegmenten installiert werden, sollten Sie unbedingt die Anzahl der Hops und die Latenz zwischen den Servern minimieren. Durch das Netzwerk verursachte Latenz kann negative Auswirkungen auf die APM-Applikation haben und zu Leistungs- und Stabilitätsproblemen führen. Die Netzwerklatenz sollte unabhängig von der Anzahl an Hops nicht mehr als 5 Millisekunden betragen. Weitere Informationen erhalten Sie über den HPE Support.
- Die APM-Server müssen sich auf ausschließlich für sie vorgesehenen Computern befinden und dürfen keine anderen Applikationen ausführen. Bestimmte APM-Komponenten können gleichzeitig auf APM-Servern installiert sein. Weitere Informationen zu Komponenten, die zusammen installiert werden können, finden Sie in den Systemanforderungen für APM und Tabellen für die APM-Unterstützung.
- Stellen Sie vor der Installation von APM auf einem Linux-Rechner sicher, dass SELinux die Installation nicht blockiert. Dazu können Sie SELinux entweder deaktivieren oder es so konfigurieren, dass Java 32-Bit ausgeführt werden kann.

Um SELinux zu deaktivieren, öffnen Sie die Datei **/etc/selinux/config**, legen Sie den Wert **SELINUX=disabled** fest und starten Sie den Computer neu.

Auf den Systemen, auf denen SELinux deaktiviert ist, ist die Option **SELINUX=disabled** in der Datei **/etc/selinux/config** festgelegt:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Darüber hinaus gibt der Befehl **getenforce** die Einstellung **Disabled** zurück:

```
~]$ getenforce
Disabled
```

Verwenden Sie das Dienstprogramm **rpm**, um sicherzustellen, dass die zuvor erwähnten Pakete installiert sind:

```
~]$ rpm -qa | grep selinux
selinux-policy-3.12.1-136.el7.noarch
libselinux-2.2.2-4.el7.x86_64
selinux-policy-targeted-3.12.1-136.el7.noarch
libselinux-utils-2.2.2-4.el7.x86_64
libselinux-python-2.2.2-4.el7.x86_64
```

```
~]$ rpm -qa | grep policycoreutils
policycoreutils-2.2.5-6.el7.x86_64
policycoreutils-python-2.2.5-6.el7.x86_64
```

```
~]$ rpm -qa | grep setroubleshoot
setroubleshoot-server-3.2.17-2.el7.x86_64
setroubleshoot-3.2.17-2.el7.x86_64
setroubleshoot-plugins-3.0.58-2.el7.noarch
```

Vor der Aktivierung von SELinux muss jede Datei im Dateisystem mit dem SELinux-Kontext gelabelt werden. Andernfalls ist es möglich, dass beschränkten Domänen der Zugriff verweigert wird, wodurch das System nicht ordnungsgemäß gebootet werden kann.

Um dies zu verhindern, konfigurieren Sie `SELINUX=permissive` in der Datei `/etc/selinux/config`:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Starten Sie das System als root-Benutzer. Beim nächsten Booten werden die Dateisysteme gelabelt. Der Label-Prozess labelt alle Dateien mit dem SELinux-Kontext:

```
~]# reboot
```

Im Permissive-Modus wird die SELinux-Richtlinie nicht durchgesetzt, jedoch werden Verweigerungen für Aktionen protokolliert, die bei der Ausführung im Enforcing-Modus verweigert worden wären.

Vor der Umstellung auf den Enforcing-Modus müssen Sie den folgenden Befehl als root-Benutzer ausführen, um zu überprüfen, dass SELinux keine Aktionen während des letzten Bootens verweigert hat. Wenn SELinux während des letzten Bootens keine Aktionen verweigert hat, liefert dieser Befehl keine Ausgabe.

```
~]# grep "SELinux is preventing" /var/log/messages
```

Wenn keine Meldungen über Verweigerungen in der Datei `/var/log/messages` enthalten sind, legen Sie `SELINUX=enforcing` in der Datei `/etc/selinux/config` fest.

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
```

```
# targeted - Targeted processes are protected.  
# mls - Multi Level Security protection.  
SELINUXTYPE=targeted
```

Booten Sie das System neu. Stellen Sie nach dem Booten sicher, dass `getenforce` die Einstellung **Enforcing** zurückgibt:

```
~]$ getenforce  
Enforcing
```

```
~]# sestatus  
SELinux status:                enabled  
SELinuxfs mount:              /sys/fs/selinux  
SELinux root directory:       /etc/selinux  
Loaded policy name:           targeted  
Current mode:                  enforcing  
Mode from config file:        enforcing  
Policy MLS status:            enabled  
Policy deny_unknown status:    allowed  
Max kernel policy version:    28
```

- Um SELinux so zu konfigurieren, dass Java 32-Bit ausgeführt werden kann, führen Sie den Befehl **setsebool -P allow_execmod on** aus.
- APM-Server dürfen nicht auf einem Laufwerk installiert werden, das einer Netzwerkressource zugeordnet ist.
- Aufgrund bestimmter Webbrowserbeschränkungen dürfen die Namen von Servercomputern mit dem Gateway-Server nur aus alphanumerischen Zeichen (a bis z, A bis Z, 0 bis 9), Bindestrichen (-) und Punkten(.) bestehen. Wenn die Namen der Computer mit dem Gateway-Server beispielsweise Unterstriche enthalten, ist es möglicherweise nicht möglich, sich an der APM-Website anzumelden. Um in diesem Fall auf die APM-Website zuzugreifen, verwenden Sie die IP-Adresse des Computers statt des Computernamens mit dem Unterstrich.
- Wenn Sie APM-Server auf einer Plattform mit verstärkter Sicherheit (einschließlich der Nutzung des HTTPS-Protokolls) ausführen möchten, lesen Sie die im APM Hardening Guide beschriebenen Verfahren zur verstärkten Sicherheit.
- Sie müssen ein root-Benutzer sein, um APM auf dem Servercomputer zu installieren.
- Die Umgebungsvariable **DISPLAY** muss auf dem APM-Servercomputer ordnungsgemäß konfiguriert werden. Auf dem Computer, über den Sie den Installation durchführen, muss X-Server ausgeführt werden, da das Upgrade nicht unbeaufsichtigt durchgeführt werden kann. Details finden Sie unter ["Unbeaufsichtigte Installation von APM" auf Seite 63](#).
- Öffnen Sie im APM-Cluster den Port 21212 auf dem Datenverarbeitungsserver.
- Vor der Installation von APM 9.30 unter Oracle Linux (OEL)- oder Red Hat Enterprise Linux-Betriebssystemen für unterstützte 6.x- und 7.x-Versionen, müssen Sie die folgenden RPM-Pakete auf allen Computern installieren, auf denen APM ausgeführt wird:

<ul style="list-style-type: none">• glibc	<ul style="list-style-type: none">• libXext
<ul style="list-style-type: none">• glibc-common	<ul style="list-style-type: none">• libXtst
<ul style="list-style-type: none">• nss-softokn-freebl	<ul style="list-style-type: none">• compat-libstdc++-33

• libXau	• libXrender
• libxcb	• libgcc
• libX11	• openssl1.0.2g
• compat-expat1	• rpm-devel

Um die in der Tabelle oben aufgelisteten RPM-Pakete zu installieren, führen Sie das RPM-Installationswerkzeug auf allen Computern aus, auf denen APM ausgeführt wird:

<APM_Installationsordner>/rhel_oel_installation_fix/rpm_installer.sh.

- Wenn das Skript keines der RPM-Pakete installieren kann, wird die folgende Meldung angezeigt:

```
!!! ERROR: package <package name> has not been installed successfully  
In this case, refer the problem to your system administrator.
```

- Wenn das Skript feststellt, dass ein RPM-Paket bereits installiert ist, überspringt es dieses Paket und fährt mit dem nächsten Paket fort.

Sie können jedoch die Neuinstallation der Pakete erzwingen, indem Sie das Werkzeug mit dem Parameter **f** aufrufen:

<APM_Installationsordner>/rhel_oel_installation_fix/rpm_installer.sh

Beispiel:

```
<APM_Installationsordner>/rhel_oel_installation_fix/rpm_installer.sh f
```

Wenn der Linux-Upgrade-Dienst Yum auf Ihrem Computer nicht ausgeführt wird, müssen Sie die notwendigen RPM-Pakete manuell mithilfe des folgenden Befehls herunterladen und installieren:

```
yum install -y openssl1.0.2g glibc.i686 glibc-common.i686 nss-softokn-freebl.i686 libXau.i686  
libxcb.i686 libX11.i686 libXext.i686 libXtst.i686 compat-libstdc++-33.i686 libXrender.i686  
libgcc.i686 compat-expat1 rpm-devel
```

Die Version dieser Pakete ist von System zu System unterschiedlich. Sie können die Pakete von einer beliebigen RPM Repository-Website herunterladen, die Ihrem System entspricht. Das folgende RPM-Suchwerkzeug kann Ihnen dabei nützlich sein (<http://rpm.pbone.net/>).

Um die Version des Pakets ermitteln zu können, müssen Sie dieses herunterladen und den folgenden Befehl in einem Terminalfenster ausführen:

rpm -qa \${PAKETNAME} (z. B.: rpm -qa glibc)

Der Befehl gibt den folgenden Text zurück:

```
# rpm -qa glibc  
glibc-2.12-1.132.el6.x86_64
```

Dieser Text zeigt die für den Computer erforderliche Paketversion an.

In diesem Fall müssten Sie das Paket für die i686-Architektur mit derselben Version – glibc-2.12-1.132.el6.i686 – herunterladen und manuell installieren.

Kapitel 3: Installieren von BSM 9.30

Installieren Sie APM 9.30 auf einer Gruppe von Servern. Hierbei kann es sich entweder um einen Gateway-Server und einen Datenverarbeitungsserver oder um einen Ein-Computer-Server handeln. Führen Sie im ersten Fall den Assistenten zuerst auf dem Datenverarbeitungsserver aus. Der Assistent weist Sie an, wann Sie mit der Installation auf dem Gateway-Server beginnen müssen.

Der Installations-Assistent weist Sie an, wann Sie den Post-Installations-Assistenten ausführen müssen. Nach der Ausführung des Post-Installations-Assistenten können Sie entscheiden, ob Sie das Dienstprogramm für das Setup und die Datenbankkonfiguration gleichzeitig oder zu einem späteren Zeitpunkt ausführen möchten.

Hinweis: Wenn Sie APM 9.30 auf einem Windows Server 2008 R2- oder 2012 R2-Server installieren:

1. Suchen Sie unter **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System** den Wert **Enable LUA** und ändern Sie ihn auf **0**.
2. Starten Sie den Computer neu.

Herunterladen der Software

1. Wechseln Sie zur Website [HPE SMTA](http://prssc.int.hpe.com/smta/smta.cgi) (<http://prssc.int.hpe.com/smta/smta.cgi>) und melden Sie sich an.
2. Wählen Sie neben **Release-Name** den Eintrag **APM0930** aus und klicken Sie auf **Suchen**.
3. Laden Sie die erforderliche ZIP-Datei herunter:
 - **HPE_APM_9.30_Windows_Setup.zip**
 - **HPE_APM_9.30_Linux_Setup.zip**
4. Entpacken Sie die Datei und führen Sie das Installationsprogramm aus.

Ausführen des Installations- und Post-Installations-Assistenten

- ["Installieren von APM auf einer Windows-Plattform" auf Seite 41](#)
- ["Installieren von APM auf einer Linux-Plattform" auf Seite 49](#)

Wenn ein Patch verfügbar ist, wechseln Sie zur Website [HPE Software Support](https://softwaresupport.hpe.com) (<https://softwaresupport.hpe.com>) und laden Sie den gewünschten Patch herunter.

Alternativ dazu können Sie den Installations- und Post-Installations-Assistenten im unbeaufsichtigten Modus ausführen. Details finden Sie unter ["Unbeaufsichtigte Installation von APM" auf Seite 63](#).

Hinweis: Der unbeaufsichtigte Modus wird nicht bei Upgrade-Assistenten unterstützt.

Kapitel 4: Aufgaben nach der Installation

Dieses Kapitel umfasst die folgenden Themen:

- Allgemeine Aufgaben nach der Installation 18
- Starten und Beenden von APM21
- An- und Abmelden 22
- Hinzufügen weiterer APM-Server 23

Allgemeine Aufgaben nach der Installation

Führen Sie die folgenden Aufgaben aus, um die Installation abzuschließen.

- **Upgrade angepasster Service-Zustand-KPIs**

In BSM wurde das interne Format des KPI-Parameters "KPI ist kritisch, wenn" geändert. Somit ist dieser Wert nach einem Upgrade möglicherweise nicht mehr richtig, wenn Sie KPIs erstellt oder angepasst haben.

Hinweis: APM muss zum Ausführen dieses Schritts gestartet sein.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- a. Greifen Sie über die Adresse **http://<Gateway-Servername>:29000/** auf die JMX-Konsole auf dem Gateway-Server zu und geben Sie Ihren Benutzernamen und das Kennwort ein.
- b. Klicken Sie im Abschnitt **Topaz** auf **service=repositories_manager**.
- c. Suchen Sie nach **upgradeCriticalIf()** und geben Sie **1** als Kunden-ID im Feld **Parameter** ein.
- d. Klicken Sie auf **Invoke**.

- **Entfernen von OMi-KPIs**

Wenn Geschäftsapplikationen, BTFs oder BTs OMi_KPIs zugeordnet sind, werden die KPIs beschädigt, da OMi in APM 9.30 nicht unterstützt wird. So entfernen Sie die beschädigten KPIs:

- a. Führen Sie die Synchronisierung für Zustandsindikatoren (**Verwaltung > Service-Zustand > Zuweisungen > Registerkarte Zustandsindikatorzuweisungen**) aus.
- b. Führen Sie die Synchronisierung für KPIs (**Verwaltung > Service-Zustand > Zuweisungen > Registerkarte KPI-Zuweisungen**) aus.
- c. Wählen Sie im Abschnitt **CI-Typen** den Eintrag **Root-Element** und klicken Sie auf jeder Registerkarte auf **CIT synchronisieren**.

- **Löschen von temporären Internetdateien**

Wenn Sie sich nach der Aktualisierung das erste Mal bei APM anmelden, löschen Sie die temporären Internetdateien des Browsers. Dieser Vorgang sollte für jeden Browser durchgeführt werden, der auf APM zugreift.

- **Deaktivieren Sie die Firewall zwischen den APM-Gateway- und -Datenverarbeitungsservern.**

Im Allgemeinen wird das Einfügen von Firewalls zwischen APM-Servern nicht unterstützt. Wenn auf einem APM-Servercomputer eine Betriebssystem-Firewall aktiviert ist (GW oder DPS), muss ein Kanal geöffnet bleiben, um den Datenaustausch zwischen den APM-Gateway- und -Datenverarbeitungsservern zu ermöglichen.

Zusätzlich dazu müssen die entsprechenden Ports (abhängig von Ihrer APM-Konfiguration) geöffnet bleiben, damit die Kommunikation zwischen APM-Benutzern und -Daten-Collectoren mit den APM Gateway-Servern möglich ist. Die erforderlichen Ports sind in der Regel 443 oder 80 und 383. Details finden Sie unter "Port Usage" im APM-Plattformverwaltungshandbuch.

- **Erstellen der Profildatenbank**

Das Profildatenbankschema wird nach dem Ausführen der Installations-Assistenten erstellt. Weitere Informationen finden Sie unter "Creating Databases" im APM-Plattformverwaltungshandbuch.

- **Hochladen zusätzlicher Lizenzen**

Die APM-Hauptlizenz wird während der APM-Basisinstallation eingegeben. Für eine Reihe von APM-Applikationen sind jedoch zusätzliche Lizenzen erforderlich. Damit Sie diese Applikationen verwenden können, müssen Sie Lizenzen bei HPE erwerben. Weitere Informationen finden Sie auf der Website [HPE Software Support](https://softwaresupport.hpe.com) (<https://softwaresupport.hpe.com>).

Die Lizenzdateien werden in den Lizenzmanager hochgeladen. Weitere Informationen finden Sie unter "Seite 'Lizenzverwaltung'" im APM-Plattformverwaltungshandbuch.

- **Konfigurieren von LW-SSO, wenn sich der Load Balancer in einer separaten Domäne befindet**

Wenn Sie einen Load Balancer verwenden und dieser sich nicht in derselben Domäne wie die in APM integrierten Server (z. B. NNMi, OO) befindet, müssen Sie eine LW-SSO-Konfiguration anpassen. Details finden Sie unter "LW-SSO Configuration for Multi-Domain and Nested Domain Installations" im APM-Plattformverwaltungshandbuch.

- **Ausführen der Optimierungsverfahren**

Führen Sie die Verfahren unter "Using TLS in APM" im APM Hardening Guide aus, wenn Sie die Kommunikation zwischen den APM-Servern schützen möchten.

- **Sicherstellen des ordnungsgemäßen Starts aller Prozesse**

Sie können überprüfen, ob alle Prozesse ordnungsgemäß gestartet wurden. Details finden Sie unter "How to View the Status of Processes and Services" im APM-Plattformverwaltungshandbuch.

- **Installieren und Konfigurieren von System Health**

Mit System Health können Sie die Leistung der Server, der Datenbanken und der Daten-Collectoren überwachen, die in Ihrem APM-System ausgeführt werden, und deren ordnungsgemäße Funktionsfähigkeit sicherstellen. Es empfiehlt sich, System Health nach der Bereitstellung der APM-Server zu installieren und zu konfigurieren. Details finden Sie unter System Health Guide.

- **Überprüfen der Installationsprotokolldateien**

Sie können die Installationsprotokolldatei anzeigen, indem Sie unten im Installationsfenster auf den Link **Protokolldateien anzeigen** klicken.

In einer Windows-Umgebung befindet sich diese Protokolldatei zusammen mit anderen Protokolldateien für separate Installationspakete im Verzeichnis `%temp%\..\HPOvInstaller\HPEApm_<Version>`.

In einer Linux-Umgebung befinden sich die Protokolldateien im Verzeichnis `/tmp/HPOvInstaller/HPEApm_<Version>`.

Der Name der Installationsprotokolldatei weist folgendes Format auf:

HPEApm_<VERSION>_<DATUM>_HPOvInstallerLog.html oder **HPEApm_<VERSION>_<DATUM>_HPOvInstallerLog.txt** (z. B.: HPEApm_9.30_2016.05.23_15_48_HPOvInstallerLog.html).

Die Namen von individuellen Protokolldateien für Installationspakete weisen folgendes Format auf:

Package_<PAKETTYP>_HPEApm_<PAKETNAME>_install.log (z. B.: Package_msi_HPEApm_BPMPkg_install.log).

Hinweis: Wenn der Server neu gestartet wird, werden standardmäßig alle Dateien aus dem Ordner **tmp** automatisch gelöscht. Sichern Sie somit nach der Installation von APM alle Protokolldateien, bevor Sie den Server neu starten.

• Installieren der Setupdateien von Komponenten

Mit den Setupdateien von Komponenten werden die Komponenten installiert, die von APM verwendet werden. Die Setupdateien von Komponenten werden nicht im Rahmen einer einfachen APM-Installation installiert. Sie sind getrennt im Downloadbereich des Webbereitstellungspakets gespeichert. Sie können diese in die APM-Seite für Downloads hochladen. Die Setupdateien für Komponenten können von APM heruntergeladen und bei Bedarf verwendet werden. Details zur Verwendung der APM-Seite für Downloads finden Sie unter "Downloads" im APM-Plattformverwaltungshandbuch.

Hinweis:

- Die Komponenten auf der Seite für Downloads werden für alle Haupt- und Nebenversionen aktualisiert (z. B. 9.00 und 9.20). Um die aktualisierten Komponenten für Minor-Minor-Releases und Patches (z. B. 9.26) herunterzuladen, wechseln Sie zur Website [HPE Software Support](https://softwaresupport.hpe.com) (<https://softwaresupport.hpe.com>).
- Sie können eine Komponente mit der Setupdatei der Komponente direkt über das Netzwerk installieren. Details zur Installation einer Komponente finden Sie in der jeweiligen Dokumentation der Komponente, die Sie installieren möchten. Die jeweiligen Dokumentationen stehen auf der Downloadseite in APM zur Verfügung, nachdem die Setupdateien einer Komponente auf die Downloadseite kopiert wurden.

Um die Setupdateien für Komponenten zu installieren, kopieren Sie die Komponentensetupdateien, die Sie auf der Seite für Downloads zur Verfügung stellen möchten, aus dem entsprechenden Verzeichnis im Release-Downloadbereich in das Verzeichnis **<HEP APM-**

Stammverzeichnis>\AppServer\webapps\site.war\admin\install

auf dem APM-Gateway-Server. Erstellen Sie bei Bedarf die Verzeichnisstruktur **admin\install**.

• Neustart von APM

Starten Sie APM neu, indem Sie alle Server deaktivieren und anschließend aktivieren. Details finden Sie unter "[Starten und Beenden von APM](#)" auf Seite 21.

Starten und Beenden von APM

Starten Sie nach Abschluss der APM-Serverinstallation den Computer neu. Sie sollten dies so bald wie möglich machen. Wenn der Computer neu gestartet wird, müssen Sie sich wieder als derselbe Benutzer anmelden, als der Sie vor dem Neustart des Computers angemeldet waren.

Hinweis: Wenn der Server neu gestartet wird, werden standardmäßig alle Dateien aus dem Ordner **tmp** automatisch gelöscht. Sichern Sie somit nach der Installation von APM alle Protokolldateien, bevor Sie den Server neu starten.

Starten Sie APM auf jedem Servercomputer, nachdem Sie die APM-Server (entweder zusammen auf einem Computer oder mindestens eine Instanz jedes Servertyps in einer verteilten Bereitstellung) installiert und eine Verbindung zwischen den Servercomputern und den Datenbanken hergestellt haben.

Hinweis: Sie können überprüfen, welche APM-Server und -Funktionen auf einem APM-Servercomputer installiert sind, indem Sie den Abschnitt [INSTALLED_SERVERS] der Datei **<APM-Serverstammverzeichnis>\conf\TopazSetup.ini** anzeigen. Mit `Data_Processing_Server=1` wird beispielsweise angegeben, dass der Server für die Datenverarbeitung auf dem Computer installiert ist.

So starten und beenden Sie APM unter Windows:

Wählen Sie **Start > Alle Programme > HPE Application Performance Management > Verwaltung > HPE Application Performance Management aktivieren | deaktivieren**. Aktivieren Sie in einer verteilten Umgebung zuerst den Datenverarbeitungsserver und dann den Gateway-Server.

So starten und beenden Sie APM unter Linux:

```
/opt/HP/BSM/scripts/run_hpbsm {start | stop | restart}
```

So starten oder beenden Sie APM mit einem Daemon-Skript bzw. führen einen Neustart durch:

```
/etc/init.d/hpbsmd {start| stop | restart}
```

Hinweis: Wenn Sie APM anhalten, wird der APM-Dienst nicht aus dem Microsoft-Fenster für Dienste entfernt. Der Dienst wird erst nach der Deinstallation von APM entfernt.

An- und Abmelden

Die Anmeldung bei APM erfolgt über die Anmeldeseite in einem Browser auf dem Clientcomputer. LW-SSO ist die standardmäßige Authentifizierungsmethode von APM. Details finden Sie unter "Logging into APM with LW-SSO" im Handbuch APM-Plattformverwaltungshandbuch.

Sie können die Single Sign-On-Authentifizierung vollständig deaktivieren, oder Sie können LW-SSO deaktivieren und eine andere unterstützte Authentifizierungsstrategie verwenden. Details zur Auswahl einer Authentifizierungsmethode finden Sie unter "Festlegen der Authentifizierungsstrategien" im APM-Plattformverwaltungshandbuch.

So greifen Sie auf die APM-Anmeldeseite zu und melden sich zum ersten Mal an:

1. Geben Sie im Webbrowser die URL `http://<Servername>.<Domänenname>/HPBSM` ein. Dabei stehen **Servername** und **Domänenname** für den vollqualifizierten Domännennamen des APM-Servers. Sind mehrere Server vorhanden oder wurde APM in einer verteilten Architektur bereitgestellt, geben Sie ggf. die Lastenausgleichs- oder Gateway-Server-URL an.

Hinweis: Benutzer, die frühere Versionen von APM ausführen, können weiterhin Textmarken verwenden, die für den Zugriff auf die URL `http://<Servername>.<Domänenname>/mercuriam` und `http://<Servername>.<Domänenname>/topaz` festgelegt wurden.

2. Geben Sie die Angaben für den Standardadministratorbenutzer ("admin") und das Kennwort ein, die im Dienstprogramm für die Setup- und Datenbankkonfiguration festgelegt wurden, und klicken Sie auf **Anmelden**. Nach der Anmeldung wird oben rechts der Benutzername angezeigt.
3. (Empfehlung) Erstellen Sie weitere Administratorbenutzer, damit APM-Administratoren auf das System zugreifen können. Details zur Erstellung von Benutzern im APM-System finden Sie unter "User Management" im APM-Plattformverwaltungshandbuch.

- Informationen zur Fehlerbehebung bei der Anmeldung finden Sie unter "Fehlerbehebung und Einschränkungen" im APM-Plattformverwaltungshandbuch.
- Details zu Authentifizierungsmethoden für die Anmeldung, die in APM verwendet werden können, finden Sie unter "Authentication Strategies — Overview" im APM-Plattformverwaltungshandbuch.
- Details zum sicheren Zugriff auf APM finden Sie im APM Hardening Guide.

Wenn Sie die Sitzung beendet haben, sollten Sie sich von der Website abmelden, um unberechtigten Zugriff zu verhindern.

So melden Sie sich ab:

Klicken Sie oben auf der Seite auf **Abmelden**.

Hinzufügen weiterer APM-Server

Nachdem die Funktionsweise der APM-9.30-Umgebung sichergestellt ist, können Sie nach Bedarf weitere Gateway-Server und Datenverarbeitungsserver hinzufügen.

So fügen Sie neue APM-Server zu einer bestehenden APM-Umgebung hinzu:

1. Wechseln Sie zur Website [HPE SMTA](http://prssc.int.hpe.com/smta/smta.cgi) (<http://prssc.int.hpe.com/smta/smta.cgi>) und melden Sie sich an.
2. Wählen Sie neben **Release-Name** den Eintrag **APM0930** aus und klicken Sie auf **Suchen**.
3. Laden Sie die erforderliche ZIP-Datei herunter:
 - **HPE_APM_9.30_Windows_Setup.zip**
 - **HPE_APM_9.30_Linux_Setup.zip**
4. Entpacken Sie die Datei und führen Sie das Installationsprogramm auf allen APM-Servern (Gateway und Datenverarbeitung) aus.
5. Führen Sie das Dienstprogramm für das Setup und die Datenbankkonfiguration aus.
 - **Windows:** Wählen Sie auf dem APM-Server **Start > Alle Programme > HPE Application Performance Management > Verwaltung > HPE Application Performance Management konfigurieren**. Alternativ dazu können Sie die Datei auch direkt über **<HPE APM_Installationsverzeichnis>\bin\config-server-wizard.bat** ausführen.
 - **Linux:** Öffnen Sie auf dem APM-Servercomputer eine Terminalbefehlszeile und starten Sie **/opt/HP/BSM/bin/config-server-wizard.sh**.

Weitere Informationen zu diesem Hotfix finden Sie unter "[Serverbereitstellung und Festlegen von Datenbankparametern](#)" auf [Seite 54](#).

6. Starten Sie alle APM-Server neu.

Nachdem Sie alle zusätzlichen Server installiert haben, starten Sie alle anderen APM-Server und -Daten-Collectoren erneut, damit diese die neuen Server erkennen können.

Kapitel 5: Konfigurieren des sicheren Zugriffs auf den APM-Reverse Proxy

In diesem Abschnitt werden die Auswirkungen von Reverse Proxys auf die Sicherheit sowie Anweisungen für den Einsatz eines Reverse Proxys zusammen mit APM beschrieben.

Dieses Kapitel behandelt nur die Sicherheitsaspekte eines Reverse Proxys. Andere Aspekte bei Reverse Proxys, wie z. B. das Zwischenspeichern und die Lastverteilung bleiben unbeachtet.

Bei einem Reverse Proxy handelt es sich um einen Server, der sich zwischen dem Clientcomputer und dem Web Server befindet. Für den Clientcomputer erscheint der Reverse Proxy wie ein Standardwebserver, der die HTTP- oder HTTPS-Protokollanforderungen des Clientcomputers verarbeitet, ohne dass eine dedizierte Clientkonfiguration erforderlich ist.

Der Clientcomputer sendet gewöhnliche Anforderungen für Webinhalte und verwendet dabei anstatt des Webservernamens den Namen des Reverse Proxys. Der Reverse Proxy sendet die Anforderung dann an einen der Webserver. Obwohl die Antwort wieder vom Webserver über den Reverse Proxy zum Clientcomputer gesendet wird, scheint es für den Clientcomputer, als ob die Antwort vom Reverse Proxy kommt.

APM unterstützt einen Reverse Proxy in der DMZ-Architektur. Der Reverse Proxy ist ein HTTP- oder HTTPS-Vermittler zwischen den APM-Daten-Collectoren/-Applikationsbenutzern und dem APM-Server.

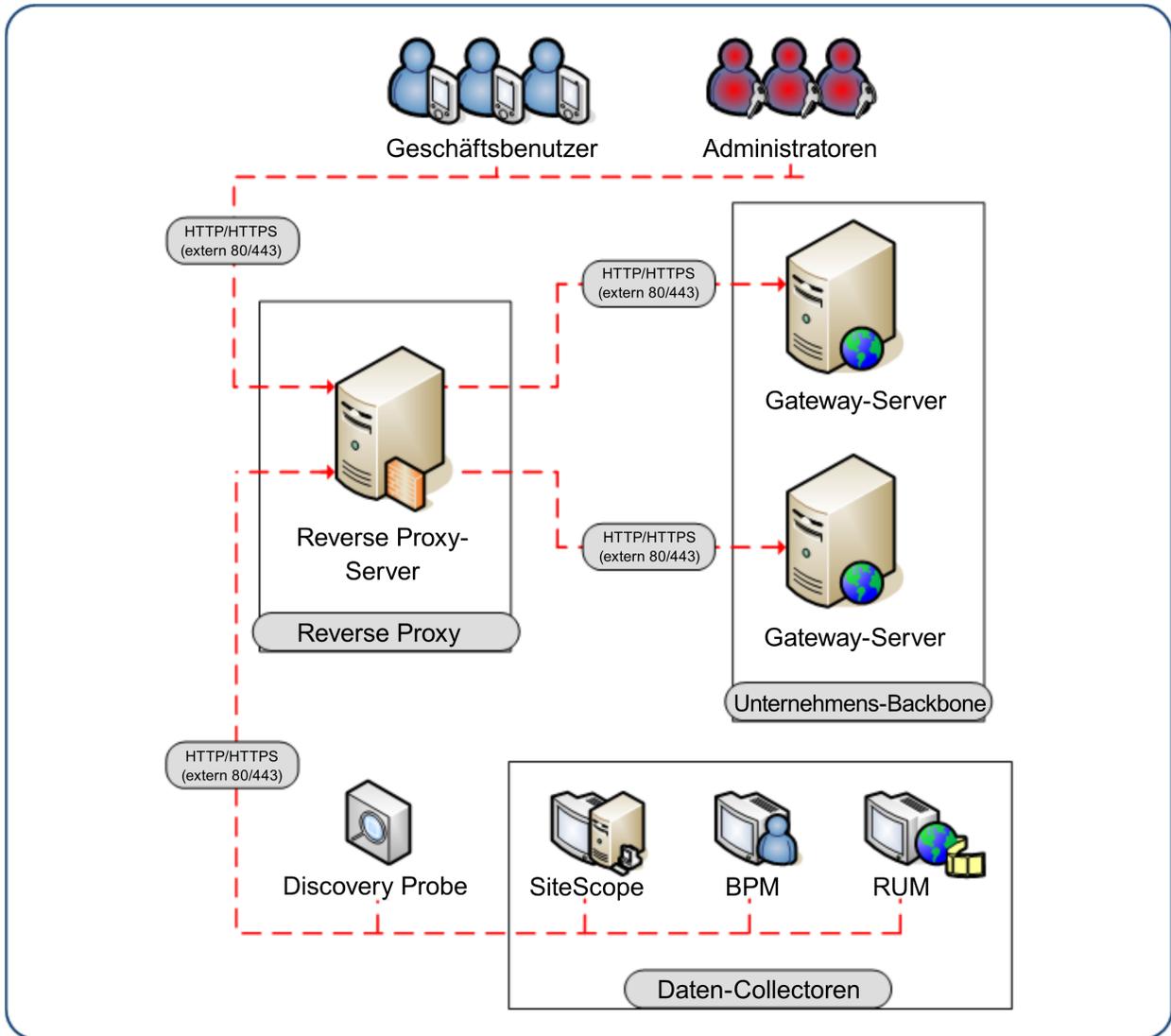
Ihre Daten-Collectoren können auf APM über denselben virtuellen Host oder über einen anderen virtuellen Host wie Ihre Applikationsbenutzer zugreifen.

Reverse Proxy-Konfiguration

In dieser Topologie ist der Reverse Proxy-Kontext in zwei Abschnitte unterteilt:

- die Kommunikation, die an den virtuellen Host für Daten-Collectoren umgeleitet wird.
- die Kommunikation, die an den virtuellen Host für Applikationsbenutzer umgeleitet wird.

Die Verwendung eines Reverse Proxys ist in der folgenden Abbildung dargestellt. Ihre Daten-Collectoren können auf APM über denselben virtuellen Host oder über einen anderen virtuellen Host wie Ihre Applikationsbenutzer zugreifen. Ihre Umgebung kann z. B. einen Load Balancer für Applikationsbenutzer und einen Load Balancer für Daten-Collectoren verwenden werden.



Die APM-Unterstützung für einen Reverse Proxy muss in jedem der folgenden Fälle anders konfiguriert werden:

Szenario-Nr.	APM-Komponenten hinter dem Reverse Proxy
1	Daten-Collectoren (Business Process Monitor, Real User Monitor, SiteScope, Data Flow Probe)
2	Applikationsbenutzer
3	Daten-Collectoren und Applikationsbenutzer

Workflow der Reverse Proxy-Konfiguration

In diesem Abschnitt wird der gesamte Workflow für die Konfiguration eines Reverse Proxys für die Zusammenarbeit mit APM-Servern beschrieben. Das Verfahren ist abhängig von dem Webserver Ihres Reverse Proxys.

1. Wenn Sie einen Load Balancer verwenden, der als Reverse Proxy dient, müssen Sie keinen zusätzlichen Reverse Proxy konfigurieren. Details finden Sie unter ["Lastenausgleich für den Gateway-Server" auf Seite 86](#).
2. Führen Sie das entsprechende Verfahren durch – je nachdem, ob der Reverse Proxy den Apache- oder den IIS-Webserver verwendet.
Apache. ["Konfigurieren eines Reverse Proxys - Apache" auf Seite 27](#).
IIS. ["Konfigurieren eines Reverse Proxys – IIS" auf Seite 32](#).
3. Konfigurieren Sie APM für die Unterstützung Ihres Reverse Proxys. Details finden Sie unter ["Spezifische HPE APM-Konfiguration" auf Seite 35](#).

Konfigurieren eines Reverse Proxys - Apache

Dieser Abschnitt enthält die Beschreibung zur Konfiguration eines Reverse Proxys unter Verwendung von Apache-2.2.x-Webservern.

Hinweis: Das Sichern des Zugriffs auf den Reverse Proxy sollte als Teil des Hardening-Workflows durchgeführt werden. Details finden Sie unter "Hardening Workflow" im *Hardening Guide*.

Dieser Abschnitt umfasst die folgenden Themen:

- ["Konfigurieren von Apache als Reverse Proxy" auf Seite 27](#)
- ["Referenz – Unterstützung für die APM-Applikationsbenutzer" auf Seite 29.](#)
- ["Referenz - Unterstützung für APM-Daten-Collectoren" auf Seite 30.](#)

Konfigurieren von Apache als Reverse Proxy

Hinweis: Das Sichern des Zugriffs auf den Reverse Proxy sollte als Teil des Hardening-Workflows durchgeführt werden. Details finden Sie unter "Hardening Workflow" im *Hardening Guide*.

1. Konfigurieren Sie Apache für die Verwendung als Reverse Proxy.

Apache muss manuell konfiguriert werden, um als Reverse Proxy verwendet werden zu können.

Beispiel:

- a. Öffnen Sie die Datei `<Apache-Installationsverzeichnis>\Webserver\conf\httpd.conf`.
- b. Aktivieren Sie die folgenden Module:
 - `LoadModule proxy_module modules/mod_proxy.so`
 - `LoadModule proxy_http_module modules/mod_proxy_http.so`
- c. Fügen Sie die folgenden Zeilen hinzu:

```
ProxyRequests off
```

```
<Proxy *>  
    Order deny,allow  
    Deny from all  
    Allow from all  
</Proxy>  
ProxyTimeout 300
```

2. Fügen Sie Unterstützung für Applikationsbenutzer und Daten-Collectoren, wie im folgenden Beispiel gezeigt, hinzu. Details zu dieser Aufgabe finden Sie unter ["Referenz – Unterstützung für die APM-Applikationsbenutzer" auf Seite 29](#) und ["Referenz - Unterstützung für APM-Daten-Collectoren" auf Seite 30](#).

Daten-Collectoren:

```
ProxyPass          /ext          http://DATA/ext  
ProxyPassReverse  /ext          http://DATA/ext
```

ProxyPass	/topaz/topaz_api	http://DATA/topaz/topaz_api
ProxyPassReverse	/topaz/topaz_api	http://DATA/topaz/topaz_api
ProxyPass	/mam-collectors	http://DATA/mam-collectors
ProxyPassReverse	/mam-collectors	http://DATA/mam-collectors

Applikationsbenutzer:

ProxyPass	/mercuryam	http://USERS/mercuryam
ProxyPassReverse	/mercuryam	http://USERS/mercuryam
ProxyPass	/hpbsm	http://USERS/hpbsm
ProxyPassReverse	/hpbsm	http://USERS/hpbsm
ProxyPass	/topaz	http://USERS/topaz
ProxyPassReverse	/topaz	http://USERS/topaz
ProxyPass	/webinfra	http://USERS/webinfra
ProxyPassReverse	/webinfra	http://USERS/webinfra
ProxyPass	/filters	http://USERS/filters
ProxyPassReverse	/filters	http://USERS/filters
ProxyPass	/TopazSettings	http://USERS/TopazSettings
ProxyPassReverse	/TopazSettings	http://USERS/TopazSettings
ProxyPass	/opal	http://USERS/opal
ProxyPassReverse	/opal	http://USERS/opal
ProxyPass	/mam	http://USERS/mam
ProxyPassReverse	/mam	http://USERS/mam
ProxyPass	/mam_images	http://USERS/mam_images
ProxyPassReverse	/mam_images	http://USERS/mam_images
ProxyPass	/mcrs	http://USERS/mcrs
ProxyPassReverse	/mcrs	http://USERS/mcrs
ProxyPass	/rumproxy	http://USERS/rumproxy
ProxyPassReverse	/rumproxy	http://USERS/rumproxy
ProxyPass	/odb	http://USERS/odb
ProxyPassReverse	/odb	http://USERS/odb
ProxyPass	/uim	http://USERS/uim
ProxyPassReverse	/uim	http://USERS/uim
ProxyPass	/ucmdb-api	http://USERS/ucmdb-api
ProxyPassReverse	/ucmdb-api	http://USERS/ucmdb-api
ProxyPass	/ucmdb-ui	http://USERS/ucmdb-ui
	connectiontimeout=1000 timeout=1000	
ProxyPassReverse	/ucmdb-ui	http://USERS/ucmdb-ui
ProxyPass	/excite-runtime	http://USERS/excite-runtime
ProxyPassReverse	/excite-runtime	http://USERS/excite-runtime
ProxyPass	/excite	http://USERS/excite
ProxyPassReverse	/excite	http://USERS/excite
ProxyPass	/OVPM	http://USERS/OVPM
ProxyPassReverse	/OVPM	http://USERS/OVPM
ProxyPass	/topaz/sitescope	http://USERS/topaz/sitescope
ProxyPassReverse	/topaz/sitescope	http://USERS/topaz/sitescope
ProxyPass	/cm	http://USERS/cm
ProxyPassReverse	/cm	http://USERS/cm

Hinweis: Wenn Sie IDM-SSO verwenden, müssen Sie möglicherweise die folgenden Zeilen

hinzufügen (ersetzen Sie **siteminderagent** in der Syntax unten durch den Namen Ihres IDM-SSO Anbieters):

```
ProxyPass          /siteminderagent    http://USERS/siteminderagent
ProxyPassReverse   /siteminderagent    http://USERS/siteminderagent
```

3. Überprüfen Sie die Reverse Proxy-Punkte zu APM.

- Starten Sie Apache neu.
- Wechseln Sie zu **http://<RP>/topaz** und stellen Sie sicher, dass die APM-Anmeldeseite angezeigt wird. Wenn Sie zu diesem Zeitpunkt Ihre Anmeldeinformationen eingeben, wird eine leere Seite angezeigt, da APM noch nicht für die Verwendung eines Reverse Proxys konfiguriert ist.

Referenz - Unterstützung für die APM-Applikationsbenutzer

Die folgende Tabelle kann als Referenz für Applikationsbenutzer zum Herstellen einer Verbindung über den Reverse Proxy verwendet werden.

Anforderungen für ... auf dem Reverse Proxy-Server	Anforderung an Proxy verarbeitet von:
/hpbsm/*	http://[Virtueller Host für Applikationsbenutzer]/hpbsm/* https://[Virtueller Host für Applikationsbenutzer]/hpbsm/*
/excite/*	http://[Virtueller Host für Applikationsbenutzer]/excite/* https://[Virtueller Host für Applikationsbenutzer]/excite/*
/excite-runtime/*	http://[Virtueller Host für Applikationsbenutzer]/excite-runtime/* https://[Virtueller Host für Applikationsbenutzer]/excite-runtime/*
/filters/*	http://[Virtueller Host für Applikationsbenutzer]/filters/* https://[Virtueller Host für Applikationsbenutzer]/filters/*
/mam/*	http://[Virtueller Host für Applikationsbenutzer]/mam/* https://[Virtueller Host für Applikationsbenutzer]/mam/*
/mam_images/*	http://[Virtueller Host für Applikationsbenutzer]/mam_images/* https://[Virtueller Host für Applikationsbenutzer]/mam_images/*
/mcrs/*	http://[Virtueller Host für Applikationsbenutzer]/mcrs/* https://[Virtueller Host für Applikationsbenutzer]/mcrs/*
/mercuryam/*	http://[Virtueller Host für Applikationsbenutzer]/mercuryam/* https://[Virtueller Host für Applikationsbenutzer]/mercuryam/*
/odb/*	http://[Virtueller Host für Applikationsbenutzer]/odb/* https://[Virtueller Host für Applikationsbenutzer]/odb/*
/opal/*	http://[Virtueller Host für Applikationsbenutzer]/opal/* https://[Virtueller Host für Applikationsbenutzer]/opal/*

Anforderungen für ... auf dem Reverse Proxy-Server	Anforderung an Proxy verarbeitet von:
/OVPM/*	http://[Virtueller Host für Applikationsbenutzer]/OVPM/* https://[Virtueller Host für Applikationsbenutzer]/OVPM/*
/rumproxy/*	http://[Virtueller Host für Applikationsbenutzer]/rumproxy/* https://[Virtueller Host für Applikationsbenutzer]/rumproxy/*
/topaz/*	http://[Virtueller Host für Applikationsbenutzer]/topaz/* https://[Virtueller Host für Applikationsbenutzer]/topaz/*
/TopazSettings/*	http://[Virtueller Host für Applikationsbenutzer]/TopazSettings/* https://[Virtueller Host für Applikationsbenutzer]/TopazSettings/*
/ucmdb-api/*	http://[Virtueller Host für Applikationsbenutzer]/ucmdb-api/* https://[Virtueller Host für Applikationsbenutzer]/ucmdb-api/*
/ucmdb-ui/*	<p>http://[Virtueller Host für Applikationsbenutzer]/ucmdb-ui/* https://[Virtueller Host für Applikationsbenutzer]/ucmdb-ui/*</p> <p>Hinweis: Wenn Sie einen Reverse-Proxy verwenden und eine Integration mit HPE Universal CMDB nutzen, stellen Sie sicher, dass die Einstellung für die Zeitüberschreitung des Reverse Proxys mindestens 1000 Sekunden beträgt).</p> <p>Ändern Sie zum Beispiel in der http.conf-Datei des Reverse Proxys die Zeile, die mit ProxyPass beginnt wie folgt:</p> <pre>ProxyPass /ucmdb-ui http://<MeinAPM GW-Server>/ucmdb-ui connectiontimeout=1000 timeout=1000</pre>
/uim/*	http://[Virtueller Host für Applikationsbenutzer]/uim/* https://[Virtueller Host für Applikationsbenutzer]/uim/*
/webinfra/*	http://[Virtueller Host für Applikationsbenutzer]/webinfra/* https://[Virtueller Host für Applikationsbenutzer]/webinfra/*

Referenz - Unterstützung für APM-Daten-Collectoren

Die folgende Tabelle kann als Referenz für Daten-Collectoren zum Herstellen einer Verbindung über den Reverse Proxy verwendet werden.

Anforderungen für ... auf dem Reverse Proxy-Server	Anforderung an Proxy verarbeitet von:
/topaz/topaz_api/*	http://[Virtueller Host für Daten-Collectoren]/topaz/* https://[Virtueller Host für Daten-Collectoren]/topaz/*
/topaz/sitescope/*	http://[Virtueller Host für Daten-Collectoren]/topaz/sitescope/* https://[Virtueller Host für Daten-Collectoren]/topaz/sitescope/*

Anforderungen für ... auf dem Reverse Proxy-Server	Anforderung an Proxy verarbeitet von:
/ext/*	http://[Virtueller Host für Daten-Collectoren]/ext/* https://[Virtueller Host für Daten-Collectoren]/ext/*
/cm/*	http://[Virtueller Host für Daten-Collectoren]/cm/* https://[Virtueller Host für Daten-Collectoren]/cm/*
/mam-collectors/*	http://[Virtueller Host für Daten-Collectoren]/mam-collectors/* https://[Virtueller Host für Daten-Collectoren]/mam-collectors/*
/axis2/*	http://[Virtueller Host für Daten-Collectoren]/axis2/* https://[Virtueller Host für Daten-Collectoren]/axis2/* Hinweis: Erforderlich, wenn der SOAP-Adapter mit eingebettetem Run-Time Service Model (RTSM) für die Replikation in eine gesicherte APM-Installation über Reverse Proxy verwendet wird.

Hinweis:

- Stellen Sie sicher, dass der Reverse Proxy die Logik der Verarbeitung nach Priorität unterstützt, d. h. dass bei Bedarf spezifischere Ausdrücke vor allgemeineren Ausdrücken verarbeitet werden. So muss zum Beispiel der Ausdruck **/topaz/topaz_api/*** vor dem Ausdruck **/topaz/*** verarbeitet werden.
- Für einige Reverse Proxies ist ebenfalls ein Reverse Pass erforderlich. Dieser Reverse Pass ändert die vom Server zurückgegebenen HTTP- oder HTTPS-Header in relative Header. Ein Beispiel für einen Reverse Pass finden Sie unter ["Konfigurieren von Apache als Reverse Proxy "](#) auf Seite 27.

Konfigurieren eines Reverse Proxys - IIS

Dieser Abschnitt enthält die Beschreibung zur Konfiguration eines Reverse Proxys unter Verwendung eines IIS-Webserver. Die Prozeduren mit den Schritten, die in anderen Produkten als APM durchgeführt werden müssen, sind nur Beispiele aufgeführt.

Hinweis: Das Sichern des Zugriffs auf den Reverse Proxy sollte als Teil des Hardening-Workflows durchgeführt werden. Details finden Sie unter "Hardening Workflow" im *Hardening Guide*.

Dieser Abschnitt umfasst die folgenden Themen:

"Konfigurieren des IIS als Reverse Proxy " auf Seite 32

"Konfigurieren des IIS-Reverse Proxys für die Verwendung von SSL" auf Seite 32

"Konfigurieren von IIS für das Anfordern der Clientauthentifizierung – optional" auf Seite 34

Konfigurieren des IIS als Reverse Proxy

Diese Prozedur ist von der IIS-Version abhängig.

Beispiel:

1. Installieren Sie die Application Request Routing (ARR)-Erweiterung. Details finden Sie unter <http://www.iis.net/downloads/microsoft/application-request-routing>.
2. Öffnen Sie den IIS-Manager.
3. Erstellen Sie eine neue IIS-Website, oder verwenden Sie die Standardwebsite.
4. Erstellen Sie eine neue IIS-Serverfarm mit dem Namen APM.
 - a. Fügen Sie der Farm einen neuen Server mit der IP-Adresse Ihres APM-Gateway-Servers hinzu.
 - b. Wenn Sie dazu aufgefordert werden, lassen Sie das Erstellen einer URL-Rewrite-Regel zu.
5. Aktivieren Sie die Verwendung des IIS als Proxy.
 - a. Wählen Sie den Hauptstrukturknoten (Servername) > **Application Request Routing Cache** > **Server Proxy Settings**.
 - b. Aktivieren Sie das Kontrollkästchen **Enable proxy**.
 - c. Legen Sie als **HTTP version** die Einstellung **Pass through** fest.
 - d. Aktivieren Sie das Kontrollkästchen **Reverse rewrite host in response headers**.
 - e. Klicken Sie auf **Apply**.
6. Überprüfen Sie die Reverse Proxy-Punkte zu APM.

Wechseln Sie zu **http://<Reverse Proxy FQDN>/topaz** und stellen Sie sicher, dass die APM-Anmeldeseite angezeigt wird. Wenn Sie zu diesem Zeitpunkt Ihre Anmeldeinformationen eingeben, wird eine leere Seite angezeigt, da APM noch nicht für die Verwendung eines Reverse Proxys konfiguriert ist.

Konfigurieren des IIS-Reverse Proxys für die Verwendung von SSL

Hinweis: Das Sichern des Zugriffs auf den Reverse Proxy sollte als Teil des Hardening-Workflows

durchgeführt werden. Details finden Sie unter *Hardening Workflow* im *Hardening Guide*.

1. Richten Sie auf dem Reverse Proxy eine Vertrauensbeziehung zu der Zertifizierungsstelle ein, die das Serverzertifikat ausgestellt hat.

Importieren Sie mithilfe der Microsoft Management Console das CA-Stammzertifikat der Zertifizierungsstelle, die das Serverzertifikat für diesen Server ausgestellt hat, in den Computer-Truststore.

Beispiel:

- a. Öffnen Sie auf dem Reverse Proxy die Microsoft Management Console (**Ausführen > mmc**).
- b. Fügen Sie ein Snap-In hinzu **Datei > Snap-In hinzufügen/entfernen**).
- c. Wählen Sie **Zertifikate** und klicken Sie auf **Hinzufügen**.
- d. Wählen Sie **Computerkonto** aus, und klicken Sie auf **Weiter**.
- e. Wählen **Lokalen Computer** und klicken Sie auf **Fertig stellen**.
- f. Klicken Sie auf **OK**.
- g. Importieren Sie das Zertifikat
Importieren Sie **ca.cer** in die Liste **Vertrauenswürdige Stammzertifizierungsstellen**.

2. Importieren Sie das Serverzertifikat in die Microsoft Management Console

Importieren Sie das zuvor erhaltene Serverzertifikat in **Eigene Zertifikate** in der Microsoft Management Console.

3. Aktivieren Sie SSL auf dem IIS

Beispiel:

- a. Wählen Sie im IIS-Manager Ihre Website.
- b. Wählen Sie im Ausschnitt **Aktionen** die Option **Bindungen**.
- c. Fügen Sie eine HTTPS-Bindung für Port 443 hinzu.
- d. Geben Sie Ihr Serverzertifikat im Feld **SSL-Zertifikat** ein.

4. Konfigurieren Sie den Reverse Proxys für die Anforderung von SSL

Beispiel:

- a. Wählen Sie im IIS-Manager Ihre Website, und wählen Sie **SSL-Einstellungen**.
- b. Aktivieren Sie das Kontrollkästchen **SSL erforderlich**.

5. Konfigurieren der SSL-Verschiebung

Wenn Ihr SSL auf dem Reverse Proxy endet, führen Sie die folgenden Schritte aus:

- a. Führen Sie den folgenden Befehl aus, um IIS so zu konfigurieren, dass große Datenstichproben (1 MB) durchgereicht werden:

**C:\Windows\System32\inetsrv>appcmd.exe set config -
section:system.webserver/serveuruntime /uploadreadaheadsize:1048576 /commit:apphost**

- b. Wählen Sie im IIS-Manager den Hauptstrukturknoten (Servename) > **Application Request Routing Cache > Server Proxy Settings**.
- c. Aktivieren Sie das Kontrollkästchen **enable SSL offloading**.

Konfigurieren von IIS für das Anfordern der Clientauthentifizierung - optional

1. Erstellen Sie die SSL-Bindung neu, um die Clientaushandlung zu aktivieren

Die vorherige Bindung funktioniert, könnte möglicherweise aber Leistungsprobleme verursachen. Diese Bindung ermöglicht die Aushandlung, wodurch die Leistung bei Verwendung der Clientauthentifizierung erhöht wird.

- a. Entfernen Sie die aktuelle Bindung mit der IIS Manager-Benutzeroberfläche
- b. Führen Sie die folgenden Befehle auf dem IIS-Server aus:

```
c:\windows\system32\inetsrv\appcmd set site /site.name:"Default Web Site" /+bindings.  
[protocol='https',bindingInformation='*:443:']
```

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=<Hash-Wert Ihres Serverzertifikats>  
appid={00112233-4455-6677-8899-AABBCCDDEEFF} clientcertnegotiation=enable
```

Hinweis: Den Hash-Wert Ihres Zertifikats können Sie über die MMC anzeigen. Zeigen Sie dazu in den Details des Zertifikats den Fingerabdruck an.

2. Konfigurieren Sie den Reverse Proxy für die Anforderung eines Clientzertifikats

Beispiel:

- a. Wählen Sie im IIS-Manager Ihre Website, und wählen Sie **SSL-Einstellungen**.
- b. Wählen Sie unter **Clientzertifikate** die Option **Erforderlich**.

3. Geben Sie im base64-Format den Header an, den der Reverse Proxy für die Clientauthentifizierung an APM übergibt.

Beispiel:

- a. Wählen Sie im IIS-Manager Ihre Farm, und wählen Sie **Proxy**.
- b. Aktivieren Sie das Kontrollkästchen **Reverse rewrite host in response headers**.
- c. Geben Sie in das Feld **forward encoded client certificate in the following header** den Header-Namen **CLIENT_CERT_HEADER** ein.
- d. Klicken Sie auf **Apply**.

Spezifische HPE APM-Konfiguration

Zusätzlich zur Konfiguration des Reverse Proxys zur Verwendung mit APM müssen Sie APM für die Verwendung des Reverse Proxys konfigurieren.

Hinweis: APM muss nur konfiguriert werden, wenn Applikationsbenutzer über einen Reverse Proxy mit APM verbunden sind. Wenn der Reverse Proxy nur für die Daten-Collectoren verwendet wird, überspringen Sie die Anweisungen in diesem Abschnitt.

So konfigurieren Sie Apache für die Verwendung mit dem Reverse Proxy:

1. Wählen Sie **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen**. Klicken Sie auf **Foundation**, und wählen Sie den Kontext **Plattformverwaltung** aus der Dropdownliste aus.
2. Legen Sie im Ausschnitt **Plattformverwaltung - Host-Konfiguration** die folgenden Parameter fest:
 - **"URL des virtuellen Gateway-Servers für Applikationsbenutzer" und "URL des virtuellen Gateway-Servers für Daten-Collectoren"**. Stellen Sie sicher, dass diese Parameter die URL des Computers (Reverse Proxy, Load Balancer oder ein anderer Computertyp) enthalten, der für den Zugriff auf den Gateway-Server verwendet wird. Beispiel:
`http://mein_reverse_proxy.beispiel.com:80`
Wenn Sie ein NAT-Gerät für den Zugriff auf den Gateway-Server verwenden, geben Sie die vollständige URL des NAT-Gerätes ein. Beispiel:
`http://nat_gerät.beispiel.com:80`
URL des virtuellen Gateway-Servers für Applikationsbenutzer und URL des virtuellen Gateway-Servers für Daten-Collectoren (optional). Wenn Sie mehr als eine URL (die für die virtuellen Server-URLs oben definierten) für den Zugriff auf den Gateway-Server verwenden müssen, definieren Sie eine lokale Server-URL für jeden Computer über den Sie auf den Gateway-Server zugreifen möchten. Beispiel:
`http://mein_specifischer_virtueller_server.beispiel.com:80`
Wenn der Parameter **Local Virtual Services Server URL** für einen bestimmten Computer definiert ist, wird diese URL anstelle der **Default Virtual Services URL** für diesen speziell definierten Computer verwendet.
 - **URL des direkten Gateway-Servers für Applikationsbenutzer**. Klicken Sie auf die Schaltfläche **Bearbeiten** und löschen Sie die URL im Feld **value**.
 - **URL des direkten Gateway-Servers für Daten-Collectoren**. Klicken Sie auf die Schaltfläche **Bearbeiten** und löschen Sie die URL im Feld **value**.
3. Legen Sie im Ausschnitt **Reverse Proxy-Konfiguration** die folgenden Parameter fest:
 - **Reverse Proxy aktivieren**. Legen Sie diesen Parameter auf **true** fest. Beachten Sie, dass dies durchgeführt werden muss, nachdem die obigen Parameter konfiguriert wurden.
 - **HTTP- oder HTTPS-Reverse Proxy-IPs**. Geben Sie die internen IPs der Reverse Proxys oder Load Balancer ein, die für die Kommunikation mit dem Gateway-Server verwendet werden.
 - Wenn die IP-Adresse des Reverse Proxys, der die HTTP/S-Anforderung sendet, enthalten ist, ist die an den Client zurückgegebene URL entweder die Standard-URL des virtuellen Servers oder die lokale URL des virtuellen Servers (falls definiert).

- Wenn für diesen Parameter keine IP-Adressen definiert sind (nicht empfohlen), wird APM im generischen Modus ausgeführt. Das bedeutet, dass Sie sich nicht direkt am Gateway, sondern nur über die virtuelle URL bei APM anmelden können.

Hinweis: Wenn sich Ihr Reverse Proxy und die APM-Gateway-Server nicht in derselben Domäne befinden, müssen Sie die IP des Reverse Proxys zum Parameter **HTTP- oder HTTPS-Reverse Proxy-IPs** hinzufügen. Weitere Details finden Sie unter "LW-SSO Configuration for Multi-Domain and Nested Domain Installations" im *APM Platform Administration Guide*.

So ermitteln Sie die interne IP Ihres Reverse Proxys oder Load Balancer:

- Melden Sie sich über den Reverse Proxy oder Load Balancer bei APM an.
 - Öffnen Sie das Protokoll am folgendem Speicherort: **<HPE APM-Gateway-Stammverzeichnis>\log\EJBContainer\UserActionsServlet.log**.
 - Die in diesem Protokoll in der letzten **login**-Zeile angezeigte IP ist die IP des Reverse Proxys oder Load Balancer. Der Eintrag sollte Ihren Benutzernamen enthalten.
4. Erhöhen Sie den Wert für die Zeitüberschreitung des Reverse Proxys.
 5. Starten Sie den HPE APM-Dienst auf den APM-Gateway- und Datenverarbeitungsservern erneut.

Hinweis: Nach dem Ändern der APM-Basis-URL, wird davon ausgegangen, dass der Client HTTP- oder HTTPS-Sitzungen mit der neuen Basis-URL initiiert. Sie müssen deshalb sicherstellen, dass der HTTP- oder HTTPS-Kanal des Clients zur neuen URL aktiviert ist.

Hinweise und Einschränkungen

APM erfordert, dass für den Reverse Proxy eine Zeitüberschreitung von mindestens 300 Sekunden eingestellt ist. Dies ist die Standardeinstellung bei einigen Apache-Versionen, aber möglicherweise haben Sie eine kürzere Zeitspanne festgelegt. Für einzelne Prozesse, wie z. B. das Installieren eines Content Packs, muss die Zeitüberschreitung sogar auf 1000 Sekunden festgelegt sein (siehe ["Konfigurieren von Apache als Reverse Proxy"](#) auf Seite 27).

Wenn Sie APM für den Betrieb im generischen Modus konfiguriert haben, muss der Zugriff aller APM-Clients auf den APM-Computer über den Reverse Proxy erfolgen.

Unterstützung des spezifischen und des generischen Reverse Proxy-Modus in APM

APM-Server antworten Applikationsbenutzern durch Senden einer Basis-URL, die zur Berechnung der richtigen Verweise im vom Benutzer angeforderten HTML-Code verwendet wird. Wenn ein Reverse Proxy verwendet wird, muss APM so konfiguriert werden, dass im HTML-Code mit der Antwort an den Benutzer die Basis-URL des Reverse Proxy anstatt der APM-Basis-URL zurückgegeben wird.

Wenn der Reverse Proxy nur für Daten-Collectoren verwendet wird, ist die Konfiguration nur auf den Daten-Collectoren und dem Reverse Proxy; jedoch nicht auf den APM-Servern erforderlich.

Es gibt zwei Proxy-Modi zur Steuerung des Benutzerzugriffs auf APM-Servern:

- ["Spezifischer Modus"](#) auf Seite 37.
- ["Generischer Modus"](#) auf Seite 37.

Spezifischer Modus

Dieser Modus sollte verwendet werden, wenn der Zugriff auf die APM-Server über spezifische Reverse Proxies und gleichzeitig auch direkt erfolgen soll. Direkter Zugriff auf den Server bedeutet, dass Sie die Firewall und den Proxy-Server umgehen, da Sie in Ihrem Intranet arbeiten.

Wenn Sie in diesem Modus arbeiten, wird jedes Mal, wenn APM aufgrund einer HTTP/S-Anforderung eines Applikationsbenutzers eine Basis-URL berechnen muss, diese Basis-URL durch den für **Default Virtual Gateway Server URL** oder **Local Virtual Gateway Server URL** (falls definiert) festgelegten Wert ersetzt, wenn die HTTP/S-Anforderung über eine der im Parameter **HTTPs-Reverse Proxy-IPs** oder **HTTPs-Reverse Proxy-IPs** definierten IP-Adressen empfangen wird. Wenn die HTTP/S-Anforderung nicht über eine dieser IP-Adressen empfangen wird, entspricht die Basis-URL, die APM in der HTTP/S-Anforderung empfängt, der Basis-URL, die an den Client zurückgegeben wird.

Generischer Modus

Dieser Modus wird verwendet, wenn Sie versuchen, über den Reverse Proxy auf den Gateway-Server zuzugreifen. Alle angeforderten URLs werden umgeschrieben und mit der virtuellen IP des Gateway-Servers zurück gesendet.

Wenn Sie in diesem Modus arbeiten, wird jedes Mal, wenn APM aufgrund einer HTTP/S-Anforderung eine Basis-URL berechnen muss, diese Basis-URL durch den für **Default Virtual Gateway Server URL** oder **Local Virtual Gateway Server URL** (falls definiert) festgelegten Wert ersetzt.

Beachten Sie, dass Sie bei Verwendung dieses Modus sicherstellen müssen, dass alle APM-Clients auf die APM-Server über die URL zugreifen, die im Parameter **Default Virtual Gateway Server URL** oder **Local Virtual Gateway Server URL** festgelegt ist.

Kapitel 6: Installieren und Konfigurieren von zusätzlichen Komponenten

Einen umfassenden, detaillierten Workflow für das Einrichten von APM sowie Informationen über APM-Komponenten und -Konzepte finden Sie im **APM Getting Started Guide**, der Teil der APM-Hilfe ist.

Verwenden Sie die folgenden Referenzen beim Installieren und Konfigurieren zusätzlicher Komponenten:

Element	Ressource
APM-Plattform	Informationen zum Konfigurieren der APM-Plattform finden Sie im APM-Plattformverwaltungshandbuch, der Teil der APM-Hilfe ist.
APM-Integrationen	Informationen zu Integrationen zwischen APM und anderen Produkten finden Sie im HPESW Solution and Integration-Portal unter https://hpenterprise.sharepoint.com/teams/aztec/ .
APM-Komponenten	<ul style="list-style-type: none">• Real User Monitor: Siehe Real User Monitor Administration Guide.• Business Process Monitor: Siehe Business Process Monitor Deployment Guide.• SiteScope: Siehe HPE SiteScope-Bereitstellungshandbuch.• Diagnostics: Siehe Diagnostics Installation and Configuration Guide.• System Health: Siehe System Health Guide.• Data Flow Probe: Siehe Data Flow Probe Installation Guide.

Sie können wie folgt auf die oben stehenden Ressourcen zugreifen:

- Die Seite **Planning and Deployment Guides** finden Sie im APM-Installationsstammverzeichnis (**Get_documentation.htm**). Sie können auch in **APM Hilfe > Planning and Deployment Guides** wählen.
- Die Seite **Downloads** finden Sie unter **Admin > Plattform > Setup und Verwaltung > Downloads**.
- Die HPE Software Support-Website <https://softwaresupport.hpe.com>.

Teil II: Anhänge

Anhang A: Installieren von APM auf einer Windows-Plattform

Diese Anhang umfasst die folgenden Themen:

- [Vorbereiten der für die Installation erforderlichen Informationen](#) 42
- [Arbeiten mit dem IIS-Webserver](#) 44
- [Installieren von APM-Servern auf einer Windows-Plattform](#) 46

Vorbereiten der für die Installation erforderlichen Informationen

Bereiten Sie vor der Installation die folgenden Informationen vor:

- **Zielverzeichnisnamen.** Während der Installation werden die HPE L-Core-Pakete von APM installiert. Ist bereits eine frühere Version dieser Pakete installiert, werden diese automatisch aktualisiert. Andernfalls wird die aktuell installierte Version nicht überschrieben. Diese Änderung kann nicht rückgängig gemacht werden.
- Während der Installation müssen Sie die Installationsverzeichnisse für die freigegebenen Pakete auswählen. Dazu gehören die folgenden Komponenten:
 - HPE Cross Platform Component
 - HPE Cross Platform Component Java
 - HPE Security Core
 - HPE HTTP Communication
 - HPE Certificate Management Client
 - HPE Security Core Java
 - HPE HTTP Communication Java
 - HPE Performance Access Java
 - HPE Graphing Component
 - HPE Process Control
 - HPE Certificate Management Server
 - HPE Configuration
 - HPE Deployment
- **Lizenzschlüssel.** Sie haben die Wahl zwischen einer Evaluierungslizenz (60 Tage) oder dem Import einer dauerhaften Lizenz. Sie können in ein lokales oder in ein Netzwerkverzeichnis wechseln, um die .DAT-Lizenzdatei zu speichern.

Wenn Sie zu einem späteren Zeitpunkt den Lizenzschlüssel aktualisieren müssen (falls Sie z. B. eine Lizenz für eine oder mehrere neue APM-Komponenten erwerben), können Sie dazu die APM-Website nutzen: Wählen Sie **Admin > Plattform > Setup und Verwaltung > Lizenzverwaltung** aus, und klicken Sie auf die Schaltfläche **Lizenz aus Datei hinzufügen**. Informationen zum Aktualisieren des Lizenzschlüssels finden Sie unter "Licenses" im APM-Plattformverwaltungshandbuch.
- **Verwaltungsnummer.** Dies ist die Verwaltungsnummer, die Sie zusammen mit Ihrem APM-Paket erhalten haben.
- **E-Mail-Adresse des Administrators.**

- **Vom Webserver verwendete Portnummer.** Dies ist der Port für den Zugriff auf APM. Der Standardport ist 80.
- **Name des Gateway-Servercomputers.** Dieser Name muss auch den Domännennamen umfassen.
- **Name des Load Balancer** (falls vorhanden). Dies ist der Load Balancer, der für den Zugriff auf die APM-Website verwendet wird.
- **Name des SMTP-E-Mail-Servers.**
- **SMTP-Sendername.** Dieser Name erscheint auf Benachrichtigungen, die von APM gesendet werden. Der Name darf keine Leerzeichen enthalten. Wenn der eingegebene Name Leerzeichen aufweist, werden die Reports nicht übermittelt.

Hinweis: Nach dem Start von APM können Sie einen alternativen SMTP-Server über **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** konfigurieren.

Arbeiten mit dem IIS-Webserver

Wenn APM auf einer Windows-Plattform installiert wird, kann Apache HTTP Server oder Microsoft Internet Information Server (IIS) verwendet werden. Den Webservertyp geben Sie im Post-Installations-Assistenten an. Sie können den Post-Installations-Assistenten erneut ausführen, um diese Einstellungen zu ändern.

Hinweis: Es darf sich nur ein ausgeführter Webserver auf einem Servercomputer befinden, der denselben Port wie APM verwendet. Wenn Sie sich z. B. während der APM-Serverinstallation zur Verwendung von Apache HTTP Server entschließen und die Installation auf einem Computer durchführen, auf dem bereits IIS ausgeführt wird, müssen Sie den IIS-Dienst anhalten und den Startstatus des Diensts auf **Manuell** festlegen, bevor Sie mit der Installation beginnen.

Apache HTTP Server

APM verwendet eine Apache HTTP-Serverversion, die von HPE zur Verwendung mit APM angepasst wurde. Sie wird während der Serverinstallation installiert.

Standardmäßig ist Apache HTTP Server nicht für die SSL-Verwendung aktiviert. Details zum Konfigurieren des Webserver zur Verwendung von SSL finden Sie unter <http://httpd.apache.org/docs/2.2/ssl/>. SSL sollte für alle von APM genutzten Verzeichnisse aktiviert werden, wie in der Apache-Konfigurationsdatei (**httpd.conf** und **httpd-ssl.conf**) konfiguriert ist.

Microsoft Internet Information Server (IIS)

- Informationen zu Microsoft Windows Server 2008 mit IIS 7.x-Webserver finden Sie unter "[Microsoft Windows Server 2008 mit IIS 7.x-Webserver](#)" auf Seite 44.
- Informationen zu Microsoft Windows Server 2012 mit IIS 8-Webserver finden Sie unter "[Microsoft Windows Server 2012 mit IIS 8-Webserver](#)" auf Seite 45.

Microsoft Windows Server 2008 mit IIS 7.x-Webserver

Wenn Sie die Installation unter Microsoft Windows Server 2008 mit IIS 7.X-Webserver durchführen, müssen Sie die folgenden Schritte durchführen:

1. Wählen Sie in der **Systemsteuerung** die Option **Verwaltung > Server-Manager** aus.
2. Klicken Sie mit der rechten Maustaste auf **Rollen** und wählen Sie **Rollen hinzufügen** aus, um den Assistenten **Rollen hinzufügen** zu starten.
3. Wählen Sie auf der Seite **Serverrollen auswählen** die Option **Webserverrolle (IIS)** für die Installation aus.

Wenn ein Popup-Fenster mit der Frage angezeigt wird, ob die für den Webserver (IIS) erforderlichen Features hinzugefügt werden sollen, klicken Sie auf die Schaltfläche **Erforderliche Features hinzufügen**.

4. Klicken Sie zweimal auf **Weiter**.
5. Wählen Sie im Ausschnitt **Rollendienste auswählen** die folgenden Rollen aus:
 - a. Im Abschnitt **Allgemeine HTTP-Funktionen: Statischer Inhalt** (normalerweise standardmäßig aktiviert)
 - b. Im Abschnitt **Anwendungsentwicklung: ISAPI-Erweiterungen** und **ISAPI-Filter**.

c. Im Abschnitt **Verwaltungstools: IIS-Verwaltungsskripts und -tools**

6. Klicken Sie auf **Installieren**.

Microsoft Windows Server 2012 mit IIS 8-Webserver

Wenn Sie die Installation unter Microsoft Windows Server 2012 mit IIS 8-Webserver durchführen, müssen Sie die folgenden Schritte durchführen:

1. Wählen Sie in der **Systemsteuerung** die Option **Verwaltung > Server-Manager** aus.
2. Klicken Sie auf **Verwalten > Rollen und Funktionen hinzufügen**.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Rollenbasierte oder featurebasierte Installation**.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie **Einen Server aus dem Serverpool auswählen**.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Serverrollen auswählen** die Option **Webserverrolle (IIS)** für die Installation aus.
Wenn ein Popup-Fenster mit der Frage angezeigt wird, ob die für den Webserver (IIS) erforderlichen Features hinzugefügt werden sollen, klicken Sie auf die Schaltfläche **Erforderliche Features hinzufügen**.
9. Klicken Sie zweimal auf **Weiter**.
10. Wählen Sie im Ausschnitt **Rollendienste auswählen** die folgenden Rollen aus:
 - a. Im Abschnitt **Allgemeine HTTP-Funktionen**:
 - o **Statischer Inhalt** (normalerweise standardmäßig aktiviert)
 - o **HTTP-Umleitung**
 - b. Im Abschnitt **Anwendungsentwicklung: ISAPI-Erweiterungen und ISAPI-Filter**.
 - c. Im Abschnitt **Verwaltungstools: IIS-Verwaltungsskripts und -tools**
11. Klicken Sie auf **Weiter**.
12. Klicken Sie auf **Installieren**.

Installieren von APM-Servern auf einer Windows-Plattform

Die APM-Server (Gateway-Server und Datenverarbeitungsserver) werden vom APM-Distributionspaket installiert. Wenn Sie die Installation nicht auf einem Computer mit IIS ausführen, installiert APM den Apache HTTP-Server während der Installation.

Sie benötigen Administratorberechtigungen für die Computer, auf denen Sie APM-Server installieren.

Hinweis: Stellen Sie sicher, dass keine anderen Installationen oder Prozesse den Windows Installer verwenden. In diesem Fall reagiert die APM-Installation nicht mehr und die Installation kann nicht fortgesetzt werden. Sie müssen die andere Installation beenden, die APM-Installation durch Klicken auf die Schaltfläche **Abbrechen** im Installations-Assistenten beenden und die APM-Installation erneut ausführen.

Der erste Assistent kopiert die Dateien und Pakete auf den Computer. Mithilfe des Assistenten für die Aufgaben nach der Installation können Sie die Registrierung sowie die Konfiguration von Verbindungs-, Webserver- und SMTP-Einstellungen durchführen.

Sie können APM auch im unbeaufsichtigten Modus installieren. Details finden Sie unter "[Unbeaufsichtigte Installation von APM](#)" auf Seite 63.

So installieren Sie APM-Server:

1. Wechseln Sie zur Website [HPE SMTA](http://prssc.int.hpe.com/smta/smta.cgi) (<http://prssc.int.hpe.com/smta/smta.cgi>) und melden Sie sich an.
2. Wählen Sie neben **Release-Name** den Eintrag **APM0930** aus und klicken Sie auf **Suchen**.
3. Laden Sie **HPE_APM_9.30_Windows_Setup.zip** herunter.
4. Entzippen Sie die Datei in ein lokales Verzeichnis.
5. Wählen Sie im Menü **Start** den Befehl **Ausführen** aus.
6. Geben Sie den Speicherort, von dem Sie die Installation ausführen, gefolgt von **HPApm_9.30_setup.exe**, ein. Die Setupdatei für APM-Server befindet sich im Verzeichnis **Windows_Setup**. Geben Sie beispielsweise `d:\Windows_Setup\HPApm_9.30_setup.exe` ein.

Hinweis: Wenn Sie die Installation auf einem virtuellen Computer durchführen, müssen Sie die .exe-Datei sowie das Verzeichnis der Pakete lokal kopieren. Falls Sie versuchen, die Installation auf dem virtuellen Computer über das Netzwerk durchzuführen, schlägt die Installation fehl.

7. Klicken Sie auf **OK**. Das Setup beginnt.
8. Folgen Sie den Anweisungen auf dem Bildschirm für die Serverinstallation.
 - **Sprache.** Wenn das Installationsprogramm in zusätzlichen Sprachen vorliegt, wählen Sie eine der verfügbaren Optionen aus.

Möglicherweise erhalten Sie eine Antiviruswarnung. Sie können mit der Installation fortfahren, ohne Aktionen durchzuführen und während die Antivirussoftware auf dem Computer ausgeführt wird.

- **Setuptyp:**

- Wählen Sie den Setuptyp **Gateway** aus, um den Gateway-Server auf dem aktuellen Computer zu installieren.
- Wählen Sie den Setuptyp **Datenverarbeitung** aus, um den Datenverarbeitungsserver auf dem aktuellen Computer zu installieren.
- Wählen Sie als Setuptyp **Typisch** aus, um den Gateway-Server und den Server für die Datenverarbeitung auf demselben Computer zu installieren.

Hinweis: Wenn Sie die Installation unter Windows 2008 R2 Server vornehmen, erhalten Sie möglicherweise die folgende Meldung: The installation folder for shared content is not valid. Eine mögliche Ursache ist, dass Sie nicht über die notwendigen Administratorberechtigungen für die Installation von APM auf dem Computer verfügen. Wenden Sie sich an den Systemadministrator.

- **Installationsverzeichnisse.** Die folgenden Verzeichnisse müssen für die Installation ausgewählt werden.
 - Wählen Sie das Installationsverzeichnis für den freigegebenen Inhalt von HPE aus. Weitere freigegebene Daten befinden sich unter `%ALLUSERSPROFILE%\HP\BSM\`.
 - Wählen Sie das Installationsverzeichnis für den produktspezifischen Inhalt aus. In Microsoft Windows-Umgebungen darf dieser Pfad aus maximal 15 Zeichen bestehen und keine Leerzeichen enthalten. Wenn der Name mehr Zeichen aufweist oder nicht mit **HPBSM** endet, werden Sie im nächsten Installationsschritt aufgefordert, einen anderen Namen einzugeben.

Hinweis: Während der Installation wird möglicherweise die folgende Meldung angezeigt: The necessary ports are in use. Wenn gemeldet wird, dass die benötigten Ports verwendet werden, schlägt die Installation nicht fehl. Es wird jedoch empfohlen, die Verwendung der benötigten Ports aufzuheben. Andernfalls müssen Sie APM erneut für die Verwendung anderer Ports konfigurieren.

Diese Installationsphase kann in einer virtuellen Umgebung etwa 30-60 Minuten in Anspruch nehmen.

Nach Abschluss dieses Verfahrens werden die erfolgreich bereitgestellten Pakete und Applikationen mit Häkchen markiert. Sollten Fehler aufgetreten sein, werden die fehlgeschlagenen Installationskripts in einem Fenster angezeigt.

9. Der Assistent für Aufgaben nach der Installation wird geöffnet. Gehen Sie wie folgt vor:

- **Registrieren Sie das Produkt.**
- **Konfigurieren Sie die Verbindungseinstellungen:**
 - i. **Apache HTTP Server.** Falls Port 80, der Standardport, bereits von einem vorhandenen Webserver verwendet wird, werden Sie von APM aufgefordert, den Konflikt zu lösen. Wenn Sie sich für diese Version entscheiden, müssen Sie auch die E-Mail-Adresse des APM-Administrators eingeben.
 - ii. **Microsoft IIS.** Falls IIS nicht den Port 80 verwendet, geben Sie den IIS-Port an. Wenn Sie sich für diese Option entscheiden, müssen Sie auch die IIS Website-Adresse für die Verwendung durch APM auswählen.
- **Wählen Sie den Webservertyp aus:**
 - Wird von APM keine Installation von Microsoft IIS auf dem Computer erkannt, wird Ihnen nur die Option **Apache HTTP-Server** angezeigt. Wenn Sie APM mit Microsoft IIS ausführen möchten,

klicken Sie auf **Abbrechen**, um den Assistenten zu beenden. Installieren Sie IIS und führen Sie die Post-Installation erneut aus.

• **Geben Sie den SMTP-E-Mail-Server an:**

- Sie sollten die vollständige Internetadresse des SMTP-Servers angeben. Verwenden Sie nur alphanumerische Zeichen.
- Geben Sie im Feld **Absendername** den Namen ein, der in geplanten Reports und in Warnungen angezeigt werden soll, die von APM gesendet werden. Wenn APM bereits einmal auf demselben Computer installiert war, wird möglicherweise der Standardname **HP_BSM_Notification_Manager** angezeigt. Sie können diesen Standardnamen akzeptieren oder einen anderen Namen eingeben.
- Nach dem Start von APM können Sie einen alternativen SMTP-Server über **Plattformverwaltung > Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** konfigurieren.

Führen Sie bei einer Bereitstellung auf mehreren Servern die oben aufgeführten Schritte aus, um weitere APM-Server zu installieren.

Hinweis: Sie können den Post-Installations-Assistenten erneut ausführen, um Einstellungen zu ändern. Der Post-Installations-Assistent kann von folgendem Ort ausgeführt werden: **<HPE APM-Stammverzeichnis>\bin\postinstall.bat**. Wenn Sie den Post-Installations-Assistenten jedoch zum ersten Mal ausführen oder er vor Abschluss geschlossen wurde, verwenden Sie stattdessen die Datei **<HPE APM-Stammverzeichnis>\bin\ovii-postinstall.bat <TOPAZ_HOME>**, wobei **<TOPAZ_HOME>** das APM-Installationsverzeichnis (normalerweise **C:\HPBSM**) ist.

Anhang B: Installieren von APM auf einer Linux-Plattform

Diese Anhang umfasst die folgenden Themen:

- [Vorbereiten der für die Installation erforderlichen Informationen](#) 50
- [Arbeiten mit dem Apache-Webserver](#) 51
- [Installieren von APM-Servern auf einer Linux-Plattform](#) 52

Vorbereiten der für die Installation erforderlichen Informationen

Bereiten Sie vor der Installation die folgenden Informationen vor:

- **Verwaltungsnummer.** Dies ist die Nummer, die Sie zusammen mit Ihrem APM-Paket erhalten haben.
- **Webservername.** Dieser Name muss auch den Domännennamen umfassen.

Hinweis: Bei der Installation auf einer Linux-Plattform muss der Domänenname manuell eingegeben werden.

- **E-Mail-Adresse des Administrators.**
- **Name des SMTP-E-Mail-Servers.**
- **SMTP-Sendername.** Dieser Name erscheint auf Benachrichtigungen, die von APM gesendet werden.
- **Name des Gateway-Servercomputers.**
- **Name des Load Balancer** (falls vorhanden). Dies ist der Load Balancer, der für den Zugriff auf die APM-Website verwendet wird.
- **Vom Webserver verwendete Portnummer.** Der Standardport ist 80.

Arbeiten mit dem Apache-Webserver

Wird APM auf einer Linux-Plattform installiert, kann es mit Apache HTTP-Server verwendet werden.

Hinweis: Auf einem APM-Servercomputer darf es nur einen aktiven Webserver geben.

Apache HTTP Server

APM verwendet eine Apache HTTP-Serverversion, die von HPE für APM angepasst wurde. Sie wird während der Serverinstallation installiert.

APM führt Apache HTTP-Server standardmäßig über Port 80 aus. Wird Port 80 bereits verwendet, kann der Portkonflikt auf zwei Arten gelöst werden:

- Bevor Sie mit der APM-Installation beginnen, konfigurieren Sie den Dienst, der diesen Port verwendet, mit einem anderen Port neu.
- Wählen Sie während der APM-Installation einen anderen Port für den Apache HTTP-Server aus.

Standardmäßig ist Apache HTTP Server nicht für die SSL-Verwendung aktiviert. Details zum Konfigurieren des Webservers zur Verwendung von SSL finden Sie unter <http://httpd.apache.org/docs/2.2/ssl/>. SSL sollte für alle von APM genutzten Verzeichnisse aktiviert werden, wie in der Apache-Konfigurationsdatei (**httpd.conf** und **httpd-ssl.conf**) konfiguriert ist.

Installieren von APM-Servern auf einer Linux-Plattform

Sie können die APM-Server (den Gateway-Server und den Datenverarbeitungsserver) vom APM-Installationspaket installieren.

Um zu überprüfen, ob es sich bei den Installationsdateien um von HPE bereitgestellten Originalcode handelt und keine Manipulation durch Dritte erfolgt ist, können Sie den öffentlichen Schlüssel von HPE verwenden und die Überprüfungsanweisungen auf dieser HPE-Website befolgen:

<https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>.

Sie können APM auch im unbeaufsichtigten Modus installieren. Details finden Sie unter "[Unbeaufsichtigte Installation von APM](#)" auf Seite 63.

Hinweis: Es wird empfohlen, zum Installieren von APM keine Emulatorapplikation wie Exceed zu verwenden. Die Installation über einen Emulator kann die Installation verlangsamen und negative Auswirkungen auf das Erscheinungsbild und die Funktionalität der Benutzeroberfläche haben.

So installieren Sie APM-Server:

1. Melden Sie sich am Server als Benutzer **root** an.
2. Wechseln Sie zur Website [HPE SMTA](http://prssc.int.hpe.com/smta/smta.cgi) (<http://prssc.int.hpe.com/smta/smta.cgi>) und melden Sie sich an.
3. Wählen Sie neben **Release-Name** den Eintrag **APM0930** aus und klicken Sie auf **Suchen**.
4. Laden Sie **HPE_APM_9.30_Linux_Setup.zip** herunter.
5. Entzippen Sie die Datei in ein lokales Verzeichnis.
6. (Optional) Um zu überprüfen, ob es sich bei den Installationsdateien um von HPE bereitgestellten Originalcode handelt und keine Manipulation durch Dritte erfolgt ist, können Sie den öffentlichen Schlüssel von HPE verwenden und die Überprüfungsanweisungen auf der folgenden Website befolgen: <https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>.
7. Führen Sie das folgende Skript aus:
/HPApm_9.30_setup.bin
8. Folgen Sie den Anweisungen auf dem Bildschirm für die Serverinstallation.

Hinweis: Falls APM eine frühere Installation auf dem Computer findet, wird eine Meldung angezeigt, mit der Sie darüber informiert werden, dass angepasste Konfigurationsdaten überschrieben werden.

- Auswählen des Setuptyps:
 - Wählen Sie den Setuptyp **Gateway** aus, um den Gateway-Server auf dem aktuellen Computer zu installieren.
 - Wählen Sie den Setuptyp **Datenverarbeitung** aus, um den Datenverarbeitungsserver auf dem aktuellen Computer zu installieren.

- Wählen Sie als Setuptyp **Typisch** aus, um den Gateway-Server und den Server für die Datenverarbeitung auf demselben Computer zu installieren.
- Das Verzeichnis, in das die APM-Dateien kopiert werden, ist **/opt/HP/BSM**.
- Das Datenverzeichnis für von HPE freigegebenen Inhalt ist **/var/opt/OV**.

Hinweis: Während der Installation wird möglicherweise die folgende Meldung angezeigt:

The necessary ports are in use. Wenn gemeldet wird, dass die benötigten Ports verwendet werden, schlägt die Installation nicht fehl. Es wird jedoch empfohlen, die Verwendung der benötigten Ports aufzuheben.

Diese Installationsphase kann in einer virtuellen Umgebung etwa 30-60 Minuten in Anspruch nehmen.

Nach Abschluss dieses Verfahrens werden die erfolgreich bereitgestellten Pakete und Applikationen mit Häkchen markiert. Wenn Fehler aufgetreten sind, wird eine Registerkarte mit Details zu den möglicherweise aufgetretenen Fehlern geöffnet.

9. Der Assistent für Aufgaben nach der Installation wird geöffnet. Gehen Sie wie folgt vor:

- **Registrieren Sie das Produkt.** Geben Sie **Name**, **Firma** und **Wartungsnummer** ein.
- **Konfigurieren Sie die Verbindungseinstellungen:**
 - **Host.** Muss der vollständig qualifizierte Domänenname (FQDN) sein. Der Name des Servers wird möglicherweise standardmäßig angezeigt, die Domäne müssen Sie jedoch manuell hinzufügen. Wenn Sie einen Load Balancer verwenden, müssen Sie hier den Computernamen für den Load Balancer eingeben.
 - **Port.** Falls Port 80, der Standardport, bereits von einem vorhandenen Webserver verwendet wird, werden Sie von APM aufgefordert, den Konflikt zu lösen.
- **Zeigen Sie den Webservertyp an und geben Sie die E-Mail-Adresse des APM-Administrators ein.** APM installiert den Apache HTTP-Server. Dies ist der in Linux-Umgebungen zu verwendende Webserver.
- **Geben Sie den SMTP-E-Mail-Server an:**
 - Sie sollten die vollständige Internetadresse des SMTP-Servers angeben. Verwenden Sie nur alphanumerische Zeichen.
 - Geben Sie als Absendernamen den Namen ein, der in geplanten Reports und in Warnungen erscheinen soll, die von APM gesendet werden.

Hinweis: Sie können den Post-Installations-Assistenten erneut ausführen, um Einstellungen zu ändern. Der Post-Installations-Assistent kann von folgendem Ort ausgeführt werden: **<HPE APM-Stammverzeichnis>/bin/postinstall.sh**. Wenn Sie den Post-Installations-Assistenten jedoch zum ersten Mal ausführen oder er vor Abschluss geschlossen wurde, verwenden Sie stattdessen die Datei **<HPE APM-Stammverzeichnis>/bin/ovii-postinstall.sh <TOPAZ_HOME>**, wobei **<TOPAZ_HOME>** das APM-Installationsverzeichnis (normalerweise **/opt/HP/BSM**) ist.

Anhang C: Serverbereitstellung und Festlegen von Datenbankparametern

Diese Anhang umfasst die folgenden Themen:

- Dienstprogramm für die Setup- und Datenbankkonfiguration – Übersicht 55
- Festlegen von Datenbankparametern 56
- Erforderliche Informationen zum Festlegen der Datenbankparameter 58
- Ausführen des Dienstprogramms für das Setup und die Datenbankkonfiguration 60

Hinweis: Wenn Sie Oracle Server verwenden, ersetzen Sie in diesem Abschnitt den Begriff **Datenbank** durch den Begriff **Benutzerschema**.

Dienstprogramm für die Setup- und Datenbankkonfiguration - Übersicht

Sie konfigurieren die Serverbereitstellung und führen die Erstellung von und Verbindung mit Datenbanken/Benutzerschemas mithilfe des Dienstprogramms für die Setup- und Datenbankkonfiguration durch.

Sie können das Dienstprogramm für das Setup und die Datenbankkonfiguration als Teil der APM-Serverinstallation ausführen, indem Sie es auf der letzten Seite des Post-Installations-Assistenten auswählen. Sie können das Dienstprogramm für die Setup- und Datenbankkonfiguration aber auch eigenständig nach der Serverinstallation ausführen. Bei beiden Verfahren sind dieselben Schritte erforderlich.

Bei der Installation in einer verteilten Umgebung führen Sie das Dienstprogramm zuerst auf dem Datenverarbeitungsserver und anschließend auf dem Gateway-Server aus.

Wenn Sie zu einem späteren Zeitpunkt den Typ oder die Verbindungsparameter ändern möchten, können Sie das Dienstprogramm für die Setup- und Datenbankkonfiguration erneut ausführen. Der APM-Server, auf dem Sie das Dienstprogramm ausführen, muss deaktiviert sein. Details finden Sie unter ["Starten und Beenden von APM" auf Seite 21](#).

Starten Sie nach dem Ändern des Typs oder der Verbindungsparameter der Datenbanken aller APM-Server und -Daten-Collectoren neu.

Hinweis: Wenn Sie die Verbindungsparameter für die Verwaltung ändern, wenn APM ausgeführt wird, kann die RTSM-Datenbank schwerwiegende Datenverluste und Integritätsprobleme hervorrufen.

Bevor Sie diese Schritte durchführen, sollten Sie die Abschnitte ["Festlegen von Datenbankparametern" auf Seite 56](#) und ["Erforderliche Informationen zum Festlegen der Datenbankparameter" auf Seite 58](#) nochmals durchsehen.

Ausführliche Informationen zum Vorbereiten von MS SQL Server oder Oracle Server in Ihrem System für den Einsatz mit APM finden Sie im APM Database Guide.

Hinweis: Verwenden Sie nicht das Dienstprogramm für das Setup und die Datenbankkonfiguration anstelle des oder vor dem Upgrade-Assistenten. Verwenden Sie dieses nur nachdem das Upgrade abgeschlossen und sich die Zielumgebung im Produktionsmodus befindet.

Festlegen von Datenbankparametern

Sie können die Verbindungsparameter für die folgenden Datenbanken festlegen:

- Verwaltung
- RTSM

Folgende Maßnahmen sind für das Konfigurieren der Verbindungen für diese Datenbanken erforderlich:

- Auswählen des Datenbanktyps, den Sie verwenden möchten: MS SQL Server oder Oracle Server.
- Auswählen, ob die Datenbank in MS SQL Server oder das Benutzerschema in Oracle Server erstellt oder erneut verwendet wird. Siehe ["Erstellen von Datenbanken" auf Seite 56](#).
- Angeben der Verbindungsparameter für die Datenbank oder das Benutzerschema. Siehe ["Herstellen einer Verbindung zu vorhandenen Datenbanken" auf Seite 56](#).

Hinweis: Wenn Sie eine aktive Verwaltungsdatenbank für APM ändern müssen, wenden Sie sich an den HPE Support.

Erstellen von Datenbanken

Sie können das Dienstprogramm für die Setup- und Datenbankkonfiguration dazu verwenden, die Datenbanken für MS SQL Server oder Oracle Server zu erstellen. Sie können diese Datenbanken aber auch manuell direkt auf dem jeweiligen Datenbankserver erstellen (beispielsweise wenn in Ihrer Organisation die Nutzung von Administratoranmeldeinformationen während des Setups nicht zulässig ist). Wenn Sie die Datenbanken manuell erstellt haben, müssen Sie das Dienstprogramm für die Setup- und Datenbankkonfiguration weiterhin ausführen, um eine Verbindung mit den Datenbanken herzustellen.

Anweisungen zum manuellen Erstellen von Datenbanken in MS SQL Server finden Sie unter "Creating and Configuring Microsoft SQL Server Databases" im APM Database Guide. Anweisungen zum manuellen Erstellen von Benutzerschemas in Oracle Server finden Sie unter "Manually Creating the Oracle Server Database Schemas" im APM Database Guide.

Hinweis: Jede in APM erstellte Datenbank und jedes Benutzerschema muss über einen eindeutigen Namen verfügen (dabei spielt es keine Rolle, ob sie auf einem oder mehreren Datenbankservern erstellt wurden).

Herstellen einer Verbindung zu vorhandenen Datenbanken

Bei der Ausführung des Dienstprogramms für die Setup- und Datenbankkonfiguration wählen Sie aus, ob Sie eine neue Datenbank/ein neues Benutzerschema erstellen möchten oder eine Verbindung mit einer vorhandenen Datenbank bzw. einem Benutzerschema herstellen möchten.

Im Allgemeinen verwenden Sie die Option **Mit einem vorhandenen Schema verbinden** in den folgenden Szenarien:

- Wenn Sie eine Verbindung mit einer Datenbank/einem Benutzerschema herstellen, die/das Sie manuell in MS SQL Server/Oracle Server erstellt haben.
- Wenn Sie APM in einer verteilten Umgebung installieren und das Dienstprogramm auf Servern nach dem ersten Server ausführen. In diesem Fall müssen Sie den Assistenten zuerst auf dem Datenverarbeitungsserver und dann auf den Gateway-Servern ausführen.

Sie stellen eine Verbindung mit den Datenbanken/Benutzerschemas her, die Sie während der Installation des ersten Datenverarbeitungsservers erstellt haben. Nachdem Sie eine Verbindung mit der Management-Datenbank hergestellt haben, indem Sie dieselben Verbindungsparameter festlegen, die Sie während der Installation des ersten Servers angegeben haben, werden die Verbindungsparameter für die anderen Datenbanken standardmäßig auf den entsprechenden Bildschirmen angezeigt. Bei der Ausführung auf dem Gateway-Server werden nicht alle Datenbanken angezeigt.

Informationen zur Implementierung einer verteilten Bereitstellung von APM finden Sie unter "Bereitstellungskonfiguration" im *APM Getting Started Guide*.

Erforderliche Informationen zum Festlegen der Datenbankparameter

Vor dem Festlegen der Datenbankparameter sollten Sie die in den folgenden Abschnitten beschriebenen Informationen bereithalten.

Konfigurieren von Verbindungsparametern für MS SQL Server

Sie benötigen die folgenden Informationen, um neue Datenbanken zu erstellen und um eine Verbindung mit vorhandenen herzustellen:

- **Hostname.** Der Name des Computers, auf dem MS SQL Server installiert ist. Wenn Sie eine Verbindung mit einer nicht standardmäßigen MS SQL Server-Instanz im dynamischen Modus herstellen, geben Sie Folgendes ein: <Hostname>\<Instanzname>

Achtung: Bei der Ausführung des Dienstprogramms besteht eine Beschränkung auf 26 Zeichen für das Feld **Hostname**. Wenn die Verwendung eines Hostnamens ohne einen Domännennamen in Ihrer Umgebung nicht zulässig ist, führen Sie eine der folgenden Problemlösungen aus.

- Verwenden Sie die IP-Adresse anstelle des Hostnamens im Feld **Hostname**.
 - Ordnen Sie den Hostnamen der IP-Adresse in der Windows-Hostdatei zu. Verwenden Sie den Hostnamen, den Sie im Feld **Hostname** verwendet haben.
- **Port.** Der TCP/IP-Port des MS SQL-Servers. APM zeigt automatisch den Standardport an, **1433**.
 - Wenn Sie eine Verbindung mit einer benannten Instanz im statischen Modus herstellen, geben Sie die Portnummer ein.
 - Wenn Sie eine Verbindung mit einer benannten Instanz im dynamischen Modus herstellen, ändern Sie die Portnummer in **1434**. Dieser Port kann dynamisch den richtigen Datenbankport abhören.
 - **Name der Datenbank.** Der Name der vorhandenen Datenbank, die manuell erstellt wurde, oder der Name, den Sie der neuen Datenbank geben (z. B. APM_Verwaltung).

Hinweis: Datenbanknamen, die mit Zahlen beginnen, werden nicht unterstützt.

- **Benutzername und Kennwort.** (Bei Verwendung der MS SQL Server-Authentifizierung) Der Benutzername und das Kennwort eines Benutzers mit Administratorrechten für MS SQL Server. Beachten Sie, dass ein Kennwort angegeben werden muss.

Tipp: Aus Sicherheitsgründen empfehlen wir, nicht den standardmäßigen Benutzer **sa** zu verwenden.

Sie können mit der Windows-Authentifizierung, statt der MS SQL Server-Authentifizierung, eine Datenbank erstellen und eine Verbindung mit der Datenbank herstellen. Dazu müssen Sie sicherstellen, dass der Windows-Benutzer, der den APM-Dienst ausführt, über die erforderlichen Berechtigungen für den Zugriff auf die MS SQL Server-Datenbank verfügt. Weitere Informationen dazu, wie Sie einem Windows-Benutzer die Ausführung des APM-Diensts zuweisen, finden Sie unter "[Ändern von Benutzern des APM-Diensts](#)" auf [Seite 108](#). Weitere Informationen darüber, wie Sie einem MS SQL-Server einen Windows-Benutzer hinzufügen, finden Sie unter "Using Windows Authentication to Access Microsoft SQL Server Databases" im APM Database Guide.

Hinweis: In Linux-Umgebungen wird die Windows-Authentifizierung nicht unterstützt.

Konfigurieren der Verbindungsparameter für Oracle Server

Hinweis: Wenn sich Oracle Server auf einem Real Application Cluster (Oracle RAC) befindet, müssen Sie einigen Parametern in diesem Abschnitt andere Werte zuweisen. Details finden Sie im Abschnitt "Support for Oracle Real Application Cluster" im APM Database Guide.

Stellen Sie vor der Festlegung der Datenbankparameter sicher, dass Sie zumindest ein Tablespace für jedes Benutzerschema erstellt haben, um die Persistenz von Applikationsdaten zu gewährleisten. Zudem müssen Sie mindestens einen temporären Tablespace entsprechend den Anforderungen festgelegt haben. Details zum Erstellen und Dimensionieren der Tablespaces für APM-Benutzerschemas finden Sie unter "Oracle Server Configuration and Sizing Guidelines" im APM Database Guide.

Sie benötigen die folgenden Informationen, um ein neues Benutzerschema zu erstellen und um eine Verbindung mit einem vorhandenen herzustellen:

- **Hostname.** Der Name des Hostcomputers, auf dem Oracle Server installiert ist.

Achtung: Bei der Ausführung des Dienstprogramms besteht eine Beschränkung auf 26 Zeichen für das Feld **Hostname**. Wenn die Verwendung eines Hostnamens ohne einen Domännennamen in Ihrer Umgebung nicht zulässig ist, führen Sie eine der folgenden Problemumgehungen aus.

- Verwenden Sie die IP-Adresse anstelle des Hostnamens im Feld **Hostname**.
- Ordnen Sie den Hostnamen der IP-Adresse in der Windows-Hostdatei zu. Verwenden Sie den Hostnamen, den Sie im Feld **Hostname** verwendet haben.

- **Port.** Der Oracle-Listenerport. APM zeigt automatisch den Standardport an, **1521**.
- **SID.** Der Oracle-Instanzname, mit dem die von APM verwendete Oracle-Datenbankinstanz eindeutig identifiziert wird.
- **Schemaname und Kennwort.** Der Name und das Kennwort des vorhandenen Benutzerschemas oder der Name, den Sie dem neuen Benutzerschema zuweisen (z. B. APM_VERWALTUNG).

Wenn Sie ein neues Benutzerschema erstellen, benötigen Sie die folgenden zusätzlichen Informationen:

- **Administratorbenutzername und -kennwort.** (Um als Administrator eine Verbindung herzustellen) Der Name und das Kennwort eines Benutzers mit Administratorberechtigungen für Oracle Server (z. B. ein Systembenutzer).
- **Standard-Tablespace.** Der Name des speziellen Standard-Tablespaces, den Sie für das Benutzerschema erstellt haben.
- **Temporärer Tablespace.** Der Name des temporären Tablespaces, den Sie dem Benutzerschema zugewiesen haben. Der standardmäßige temporäre Oracle-Tablespace ist **temp**.

Hinweis: Zum Erstellen eines neuen APM-Benutzerschemas müssen Sie über Administratorberechtigungen sowie die Berechtigungen CREATE USER, CONNECT, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, UNLIMITED TABLESPACE, CREATE VIEW und CREATE PROCEDURE für Oracle Server verfügen.

Ausführen des Dienstprogramms für das Setup und die Datenbankkonfiguration

Sie können das Dienstprogramm für das Setup und die Datenbankkonfiguration während der APM-Installation oder unabhängig davon ausführen. Wenn Sie das Dienstprogramm für das Setup und die Datenbankkonfiguration unabhängig von der APM-Installation ausführen, beachten Sie die folgenden wichtigen Punkte:

- Wenn ein Eingabeaufforderungsfenster auf dem APM-Servercomputer geöffnet ist, müssen Sie es schließen, bevor Sie mit dem Dienstprogramm für das Setup und die Datenbankkonfiguration fortfahren.
- Wenn Sie diesen Assistenten nach der Installation zum Ändern der bestehenden Konfiguration und nicht während der Erstinstallation verwenden, müssen Sie APM deaktivieren, bevor Sie das Dienstprogramm für das Setup und die Datenbankkonfiguration ausführen (wählen Sie **Start > Programme > HPE Application Performance Management > Verwaltung > HPE Application Performance Management deaktivieren**).
- Verwenden Sie bei der Eingabe von Datenbankparametern nur englische Zeichen.

Hinweis: Sie können das Dienstprogramm auch im unbeaufsichtigten Modus ausführen. Details finden Sie unter "[Unbeaufsichtigte Installation von APM](#)" auf Seite 63.

So legen Sie Datenbankparameter fest und konfigurieren die Serverbereitstellung:

1. Starten Sie das Dienstprogramm für die Setup- und Datenbankkonfiguration auf eine der folgenden Arten:
 - Wählen Sie nach Abschluss des Post-Installations-Assistenten die Option zum Ausführen des Dienstprogramms für das Setup und die Datenbankkonfiguration.
 - **Windows:** Wählen Sie auf dem APM-Server **Start > Programme > HPE Application Performance Management > Verwaltung > HPE Application Performance Management konfigurieren**. APM startet das Dienstprogramm für das Setup und die Datenbankkonfiguration. Alternativ dazu können Sie die Datei auch direkt über `<HPE APM_Installationsverzeichnis>\bin\config-server-wizard.bat` ausführen.
 - **Linux:** Öffnen Sie auf dem APM-Servercomputer eine Terminalbefehlszeile und starten Sie `/opt/HP/BSM/bin/config-server-wizard.sh`.
2. Folgen Sie den Anweisungen auf dem Bildschirm, um die Datenbanken zu konfigurieren:
 - a. **Lizenz.** Wenn Sie dieses Dienstprogramm zum ersten Mal ausführen, haben Sie die Wahl zwischen der Evaluierungslizenz und dem Herunterladen von neuen Lizenzen. Sollten Sie das Dienstprogramm nicht zum ersten Mal ausführen, können Sie diesen Schritt überspringen oder zusätzliche Lizenzen herunterladen. Die Lizenzdatei verfügt über eine .DAT-Erweiterung und muss so lokal oder im Netzwerk gespeichert werden, dass der Server, auf dem das Dienstprogramm ausgeführt wird, darauf zugreifen kann.

Sie können Ihre Lizenzen nach der Installation von APM auf der Seite für die Lizenzverwaltung der Plattformverwaltung aktualisieren. Details finden Sie unter "Licenses" im APM-Plattformverwaltungshandbuch.
 - b. **Serverbereitstellung.** Der empfohlene Arbeitsablauf ist das Eingeben der Bereitstellungsinformationen in den Kapazitätsrechner, um den Umfang der Bereitstellung und die auszuführenden Applikationen und Funktionen zu ermitteln. Sie können die gespeicherte Exceldatei

mit dem Kapazitätsrechner auf dieser Seite des Dienstprogramms hochladen. Die erforderlichen Felder werden automatisch mit den Daten aus dem Kapazitätsrechner auf Grundlage Ihrer Einträge im Excel-Datenblatt ausgefüllt. Details hierzu finden Sie im APM Getting Started Guide.

- **Benutzer.** Die Anzahl der angemeldeten Benutzer legt fest, ob die Benutzerbelastung **klein**, **mittel** oder **groß** ist.
- **Modell.** Die Anzahl der Konfigurationselemente in Ihrem Modell legt fest, ob das Modell **groß**, **mittel**, **groß** oder **extragroß** ist.
- **Metrikdaten.** Die Anzahl der überwachten Applikationen, Transaktionen, Standorte und Hosts legt fest, ob die Messdatenbelastung **klein**, **mittel** oder **groß** ist.
- **<Liste der Applikationen>.** Wählen Sie die Applikationen aus, die für diese Bereitstellung aktiviert oder deaktiviert werden sollen, oder heben Sie die Aktivierung auf. Heben Sie die Aktivierung für nicht verwendete Applikationen auf, um Speicherplatz und Prozessorgeschwindigkeit für die Applikationen zu gewinnen, die Sie verwenden.

Hinweis: Wenn Sie während der Ausführung des Dienstprogramms keine Funktionen aktivieren, stehen den Benutzern keine zur Verfügung. Details zu den Applikationsoptionen finden Sie in den QuickInfos im Kapazitätsrechner.

Wenn die Installation abgeschlossen ist und Sie die Bereitstellung ändern möchten, können Sie Kapazitätsstufen anpassen sowie Applikationen und Funktionen auf der Seite für die Serverbereitstellung in der Plattformverwaltung aktivieren oder deaktivieren.

Sie können die Informationen auf dieser Seite auch manuell eingeben; es wird jedoch dringend empfohlen, den Kapazitätsrechner zu verwenden, um den Umfang und die Kapazität Ihrer Bereitstellung festzulegen.

- c. **Anmeldeeinstellungen.** Geben Sie Kennwörter für den Administratorbenutzer ("admin") ein, um auf APM und die JMX-Konsole zuzugreifen.

Optional können Sie ein **Kennwort für den Zugriff auf RTSM** festlegen, um die Kommunikation zwischen Run-time Service Model und RUM zu sichern.

Hinweis: Wenn Sie das Kennwort für den Zugriff auf RTSM während der APM-Installation ändern, müssen Sie das Kennwort auch in Diagnostics und RUM ändern.

- d. **IIS-Konfiguration.** Wenn Sie Microsoft Internet Information Server (IIS) Version 7.X unter Microsoft Windows Server 2008 verwenden, müssen für APM die folgenden IIS-Rollen aktiviert werden:

- ISAPI-Erweiterungen
- ISAPI-Filter
- IIS-Verwaltungsskripts und -tools
- Statischer Inhalt

Wenn sie bereits aktiviert sind, wird der Bildschirm für die IIS-Konfiguration nicht angezeigt.

Wenn eine der Rollen nicht aktiviert ist, können Sie ihre automatische Konfiguration anfordern, indem Sie nun **IIS-Rollen automatisch aktivieren** auswählen und auf **Weiter** klicken.

Wenn Sie sie manuell konfigurieren möchten, wählen Sie **IIS-Rollen manuell aktivieren** aus, und klicken Sie auf **Weiter**.

- e. **Firewall-Konfiguration.** Wenn Sie APM hinter einer Firewall ausführen, haben Sie beim Ausführen des Dienstprogramms auf einem Gateway-Server die Option, die Firewall automatisch oder manuell zu konfigurieren.

- Möglicherweise müssen Sie zusätzliche Ports öffnen, wenn auf dem Server eine Firewall aktiviert ist. Details finden Sie unter "Port Usage" im APM-Plattformverwaltungshandbuch.
 - Wenn Sie sich für die manuelle Konfiguration entscheiden, wird keine Portkonfiguration ausgeführt, und Sie müssen sowohl auf dem Gateway-Server als auch auf dem Datenverarbeitungsserver die manuelle Konfiguration durchführen.
- f. Zum Aktivieren der Datenbankverbindungen klicken Sie am Ende des Dienstprogramms auf **Fertig stellen**.
3. Wenn Sie das Dienstprogramm für das Setup und die Datenbankkonfiguration als Bestandteil der APM-Serverinstallation ausgeführt haben, dürfen Sie APM auf allen Servern nur nach dem erfolgreichen Festlegen der Parameter für alle Datenbanken starten. Details finden Sie unter "[Starten und Beenden von APM](#)" auf Seite 21.

Wenn Sie das Dienstprogramm für die Setup- und Datenbankkonfiguration ausgeführt haben, um einen neuen Gateway-Server hinzuzufügen oder bereits zuvor definierte Datenbanktypen oder Verbindungsparameter zu ändern, starten Sie alle APM-Server und -Daten-Collectoren neu, nachdem Sie die Parameteränderungen erfolgreich vorgenommen haben.

Hinweis: Wenn Sie dieses Dienstprogramm zum Ändern von Datenbanken in einer ausgeführten APM-Bereitstellung verwendet haben, enthalten MyBSM und Service-Zustand keine Seiten und Komponenten mehr. So stellen Sie MyBSM- und Service-Zustand-Seiten und -Komponenten wieder her:

- Öffnen Sie das folgende Verzeichnis: **<Stammverzeichnis des Gateway-Servers>\conflumashup\import**. Hier liegen zwei Verzeichnisse vor: **\loaded** und **\toload**.
- Kopieren Sie den Inhalt des Verzeichnisses **\loaded** in das Verzeichnis **\toload**. Starten Sie APM neu.

Anhang D: Unbeaufsichtigte Installation von APM

Die Assistenten zum Installieren und Konfigurieren von APM können im unbeaufsichtigten Modus ausgeführt werden. Beim unbeaufsichtigten Modus werden die Assistenten über eine Befehlszeile ausgeführt, ohne dass die Assistentenoberfläche angezeigt wird. Dies ermöglicht die Ausführung dieser Assistenten ohne X-Windows für Linux-Benutzer. Der Modus kann jedoch ebenfalls in Windows-Umgebungen verwendet werden.

Die Anweisungen wurden für die Verwendung unter Linux geschrieben. Um die Dateien in Windows-Umgebungen verwenden zu können, ersetzen Sie alle **.bin**-Dateitypen durch **.exe**-Dateitypen und alle **.sh**-Dateitypen durch **.bat**-Dateitypen.

Hinweis: Der unbeaufsichtigte Modus wird nicht bei Upgrade-Assistenten unterstützt.

Diese Anhang umfasst die folgenden Themen:

- [Vollständige APM 9.30-Installation im Hintergrund](#) 64
- [Generieren einer Antwortdatei zum unbeaufsichtigtem Ausführen des Post-Installations-Assistenten und des Dienstprogramms für das Setup und die Datenbankkonfiguration](#) 66
- [Konfigurieren der Windows-Authentifizierung während der unbeaufsichtigten Ausführung des Dienstprogramms für das Setup und die Datenbankkonfiguration](#) 67
- [Verschlüsselung von Kennwörtern in der Antwortdatei](#) 68

Vollständige APM 9.30-Installation im Hintergrund

Dieses Verfahren beschreibt die vollständige, unbeaufsichtigte Installation von APM, einschließlich des Installationsassistenten, des Post-Installations-Assistenten und der aktuellsten Minor-Minor-Version.

Hinweis: Der unbeaufsichtigte Modus wird nicht bei Upgrade-Assistenten unterstützt.

1. Führen Sie den APM-9.30-Installations-Assistenten unbeaufsichtigt aus, indem Sie die Installation über die Befehlszeile mit dem Parameter **-i silent** starten. Die Installationsdatei finden Sie im Stammordner **<APM-Installationsmedium>**.
 - Führen Sie den folgenden Befehl aus, um den Gateway-Server und den Datenverarbeitungsserver auf einem Computer (typische Installation) im Standardinstallationsverzeichnis zu installieren:
HPApm_9.30_setup.bin -i silent
 - Führen Sie die folgenden Schritte aus, um den Gateway-Server und Datenverarbeitungsserver auf verschiedenen Computern zu installieren:
 - i. Erstellen Sie eine leere Datei mit dem Namen **ovinstallparams.ini** in dem Verzeichnis auf beiden Servern, in dem sich die ausführbare Installationsdatei befindet.
 - ii. Kopieren Sie den folgenden Abschnitt in die **.ini**-Datei auf dem Gateway-Server:
[installer.properties]
setup=HPBsm
group=**gateway**
 - iii. Führen Sie den Installationsassistenten im unbeaufsichtigten Modus auf dem Gateway-Server wie folgt aus:
HPApm_9.30_setup.bin -i silent
 - iv. Kopieren Sie den folgenden Abschnitt in die **.ini**-Datei auf dem Datenverarbeitungsserver:
[installer.properties]
setup=HPBsm
group=**process**
 - v. Führen Sie den Installationsassistenten im unbeaufsichtigten Modus auf dem Datenverarbeitungsserver wie folgt aus:
HPApm_9.30_setup.bin -i silent
2. Öffnen Sie die Antwortdatei **<HPE APM-Stammverzeichnis>\TemplemptyRspFile.xml** und vervollständigen Sie die Werte im Abschnitt **Post Install**
3. Wenn Sie planen, eine APM-Konfiguration zu verwenden, die nicht unter dem root-Benutzer ausgeführt wird, erstellen Sie einen entsprechenden Benutzer.
4. Starten Sie den Post-Installations-Assistenten.
silentConfigureBSM.sh <HPE APM-Stammverzeichnis>\temp\emptyRspFile.xml postinstall
5. Melden Sie sich von Linux ab und erneut wieder an (optional). Wenn Sie APM in einer Linux-Umgebung installieren, und einen anderen als den root-Benutzer im Post-Installations -Assistenten angegeben haben, melden Sie sich ab und melden Sie sich mit dem ausgewählten Benutzer wieder an.
6. Führen Sie das Dienstprogramm für das Setup und die Datenbankkonfiguration aus.

<HPE APM-Stammverzeichnis>\bin\silentConfigureBSM.<HPE APM-Stammverzeichnis>\temp\emptyRspFile.xml postinstall

7. Aktivieren Sie APM. Details finden Sie unter "[Starten und Beenden von APM](#)" auf Seite 21.
8. Das erstmalige Aktivieren von APM kann bis zu einer Stunde dauern. Verwenden Sie die folgende URL zum Überprüfen des APM-Status:
http://localhost:11021/invoke?operation=showServiceInfoAsHTML&objectname=Foundations%3Atype%3DNannyManager
9. Den Upgrade-Assistent finden Sie auf allen Gateway- und Datenverarbeitungsservern sowie den Servern, auf denen beide gleichzeitig installiert sind, in den folgenden Speicherorten:
 - Unter Windows:
 - Upgrade von BSM 9.25: **<HPE APM-Stammverzeichnis>\bin\upgrade_wizard_run_from925.bat**
 - Upgrade von BSM 9.26: **<HPE APM-Stammverzeichnis>\bin\upgrade_wizard_run_from926.bat**
 - Unter Linux:
 - Upgrade von BSM 9.25: **/opt/HP/BSM/bin/upgrade_wizard_run_from925.sh**
 - Upgrade von BSM 9.26: **/opt/HP/BSM/bin/upgrade_wizard_run_from926.sh**
10. Wählen Sie in APM **Plattformverwaltung > Setup und Verwaltung > Serverbereitstellung**, um die APM-Applikationen zu aktivieren.

Generieren einer Antwortdatei zum unbeaufsichtigtem Ausführen des Post-Installations-Assistenten und des Dienstprogramms für das Setup und die Datenbankkonfiguration

Sie können eine XML-Datei mit den Werten erstellen, die Sie bei Ausführung des Dienstprogramms für das Setup und die Datenbankkonfiguration verwendet haben. Mit dieser Datei können Sie den Assistenten auf verschiedenen Computern ausführen.

1. Starten Sie das Dienstprogramm für das Setup und die Datenbankkonfiguration normal auf einem bestehenden APM-System.
2. Die Antwortdatei wird generiert und im Verzeichnis **<HPE APM-Stammverzeichnis>/temp** oder am angegebenen Speicherort gespeichert. In diese Datei werden die Werte geschrieben, die Sie bei Ausführung des Post-Installations-Assistenten und des Dienstprogramms für das Setup und die Datenbankkonfiguration verwendet haben.
3. Sie können nun mithilfe der folgenden Syntax und der Antwortdatei den Post-Installations-Assistenten und das Dienstprogramm für das Setup und die Datenbankkonfiguration auf jedem Computer im unbeaufsichtigten Modus ausführen:

silentConfigureBSM.sh <Pfad zur Antwortdatei>/<Name der Antwortdatei>.xml

Hinweis: Durch Anhängen des entsprechenden Befehls können Sie die beiden Assistenten unabhängig voneinander ausführen:

```
silentConfigureBSM.sh <Pfad zur Antwortdatei>/<Name der Antwortdatei>.xml [postinstall  
| configserver]
```

Die Datei **silentConfigureBSM.sh** finden Sie im Verzeichnis **<HPE APM-Stammverzeichnis>/bin**.

Konfigurieren der Windows-Authentifizierung während der unbeaufsichtigten Ausführung des Dienstprogramms für das Setup und die Datenbankkonfiguration

Mit dem Dienstprogramm für das Setup und die Datenbankkonfiguration kann APM so konfiguriert werden, dass die Anmeldeinformationen des Datenbankschemas direkt aus Anmeldeinformationen der Windows-Authentifizierung übernommen werden. Um diese Funktion bei der manuellen Erstellung einer Antwortdatei zu aktivieren, lassen Sie die Schlüssel **UserName** und **Password** für jedes relevante Schema leer. Das folgende Beispiel zeigt den Abschnitt **Management Schema** der Antwortdatei für die Verwendung der Windows-Authentifizierung:

```
<database name="management">
  <!--Enter 'create' to create a new database or 'connect' to connect to an
existing database-->
  <property key="operation" value="connect"/>
  <property key="dbName" value=" "/>
  <property key="hostName" value=""/>
  <property isEncrypted="true" key="password" value=" "/>
  <property key="server" value=" "/>
  <!--'sid' property is relevant only if you are using an Oracle database-->
  <property key="sid" value=" "/>
  <property key="UserName" value=" "/>
  <property key="port" value=""/>
  <!--Please enter your Management Database Server Type:'Oracle' or 'SQL
Server'-->
  <property key="dbType" value=" "/>
  <!--The following four items are only relevant if you are using an Oracle
database-->
  <property key="adminUserName" value=" "/>
  <property isEncrypted="true" key="adminPassword" value=" "/>
  <property key="defaultTablespace" value=" "/>
  <property key="temporaryTablespace" value=" "/>
</database>
```

Verschlüsselung von Kennwörtern in der Antwortdatei

Für eine erhöhte Sicherheit können die in der Antwortdatei gespeicherten Kennwörter verschlüsselt werden. Führen Sie zum Verschlüsseln das entsprechende Tool aus, das sich im folgenden Speicherort befindet:

<HPE APM-Stammverzeichnis>/bin/encrypt-password.sh

Sie geben Ihr Kennwort ein. Das Verschlüsselungstool gibt dann eine Zeichenfolge zurück. Kopieren Sie die Zeichenfolge in die Antwortdatei, in der Sie Ihr Kennwort eingegeben haben.

Einschränkung: Verschlüsselte Kennwörter sind nur auf dem Computer gültig, auf dem das Verschlüsselungstool ausgeführt wurde.

Um die Kennwortverschlüsselung zu entfernen, geben Sie die Kennwörter unverschlüsselt in die Antwortdatei ein, und legen Sie **IsEncrypted="false"** fest.

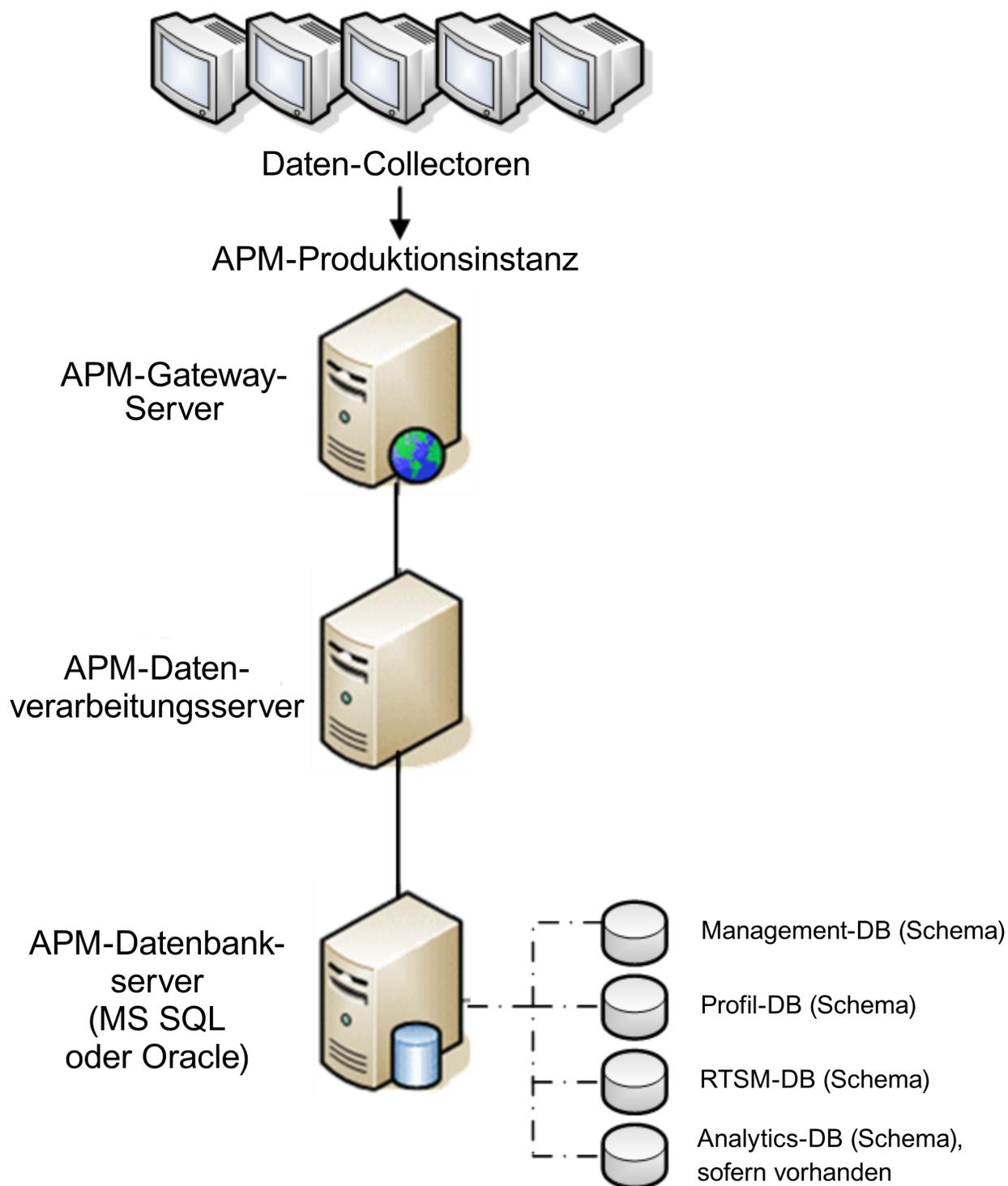
Anhang E: Notfallwiederherstellung für APM

- Einführung in die Notfallwiederherstellung für APM 69
- Vorbereiten der Umgebung für die Notfallwiederherstellung 72
- Bereinigungsverfahren 76
- Konfigurieren der neuen Umgebung 81
- Konfigurieren der Daten-Collectoren 82

Einführung in die Notfallwiederherstellung für APM

Sie können ein System für die Notfallwiederherstellung (Disaster Recovery) für Ihr APM-System einrichten und (bei Bedarf) aktivieren.

Nachfolgend werden die grundlegenden Prinzipien und Richtlinien für die Einrichtung eines Systems für die Notfallwiederherstellung beschrieben. Zudem wird erläutert, mit welchen Schritten das sekundäre APM-System als das neue primäre APM-System festgelegt wird.



Hinweis:

- Die Notfallwiederherstellung umfasst manuelle Schritte, da verschiedene Konfigurationsdateien und Aktualisierungen der APM-Datenbankschemas verschoben werden müssen. Für dieses Verfahren ist

mindestens ein APM-Administrator und ein Datenbankadministrator erforderlich, der mit den APM-Datenbanken und -Schemas vertraut ist.

- Es gibt eine Reihe unterschiedlicher möglicher Bereitstellungen und Konfigurationen für APM. Um zu überprüfen, ob das Szenario für die Notfallwiederherstellung in einer bestimmten Umgebung funktioniert, sollte es gründlich getestet und dokumentiert werden. Wenden Sie sich an HPE Professional Services, um sicherzustellen, dass bewährte Methoden beim Entwurf und im Workflow der Ausfallsicherung für jedes Szenario für die Notfallwiederherstellung eingesetzt werden.
- Der Computer für die Notfallwiederherstellung muss dasselbe Betriebssystem und Stammverzeichnis verwenden wie die ursprüngliche Umgebung.

Vorbereiten der Umgebung für die Notfallwiederherstellung

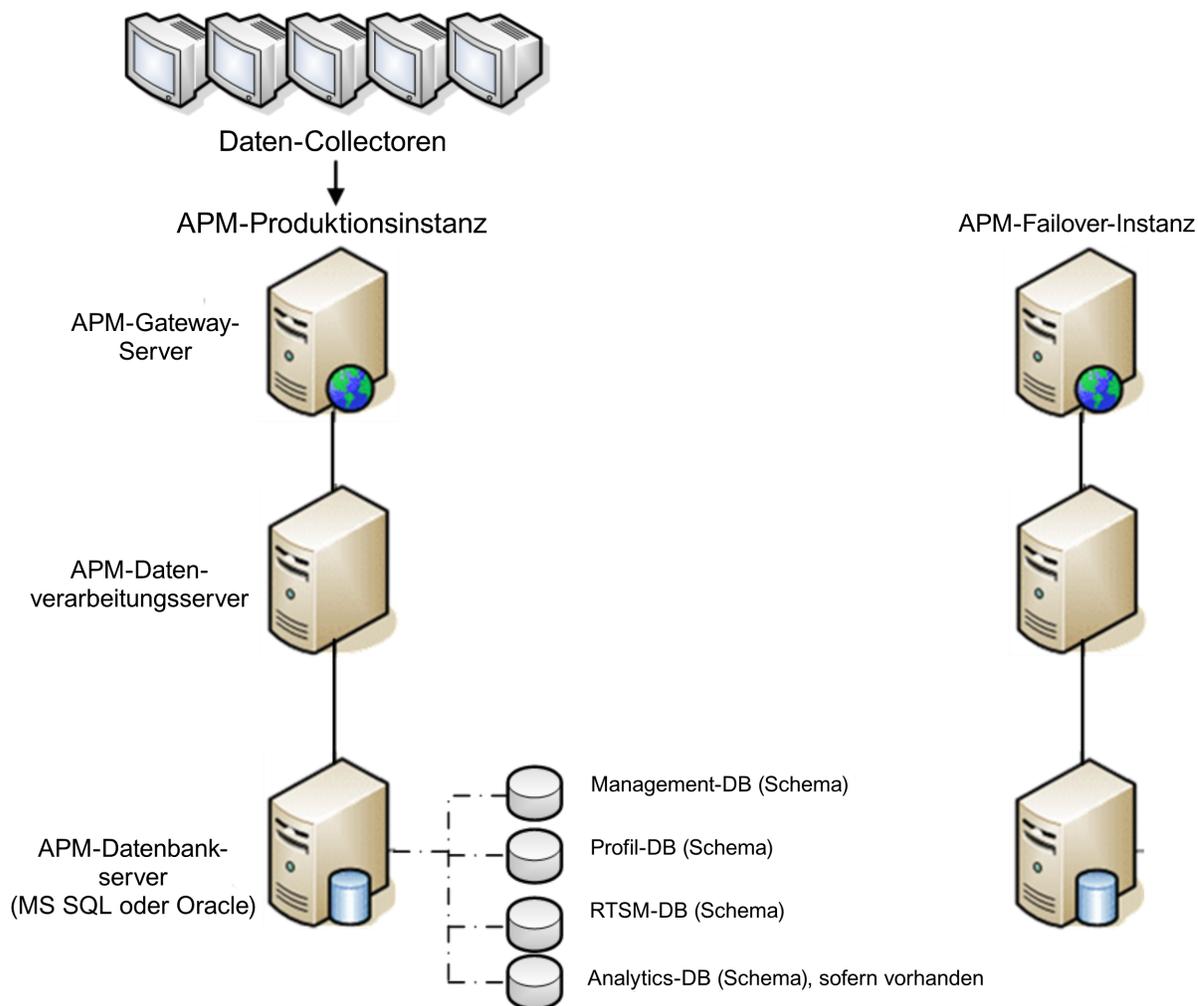
Folgende Schritte müssen zur Vorbereitung der Umgebung für die Notfallwiederherstellung ausgeführt werden:

1. Installieren einer Gruppe von APM-Servern

Installieren Sie eine zweite Instanz von APM, die der aktuellen Produktionsumgebung entspricht.

- Installieren Sie genau die gleiche Version von APM in der Sicherungsumgebung, die Sie auch in der Produktionsumgebung verwenden.
- Die Sicherungsumgebung sollte der Produktionsumgebung entsprechen (beispielsweise Bereitstellung auf einem oder zwei Computern, gleiche Hardware), sofern Sie mehr als ein GW oder DPS in der Produktionsumgebung verwenden. In diesem Fall müssen Sie lediglich eine Gruppe von APM-Servern (ein GW und ein DPS oder ein Server mit beiden Komponenten) als Umgebung für die Notfallwiederherstellung erstellen.
- Die Sicherungsumgebung muss dasselbe Betriebssystem und Installationsverzeichnis verwenden wie die ursprüngliche Umgebung.
- Führen Sie nicht das Dienstprogramm für die Server- und Datenbankkonfiguration aus, erstellen Sie keine Datenbanken, und aktivieren Sie keine Server.

In der folgenden Abbildung wird eine typische APM-Umgebung veranschaulicht, in der auch ein Ausfallsicherungssystem installiert ist:



2. Kopieren von Konfigurationsdateien vom ursprünglichen System

Kopieren Sie alle Dateien, die Sie manuell in einem der folgenden Verzeichnisse geändert haben, von der APM-Produktionsinstanz auf den gleichen Servertyp in der Failover-Instanz:

- odb/conf
- odb/content/
- BLE/rules/<custom rules>.jar

Wenn Sie Benutzerreports verwendet haben, um Excel-Reports zu erstellen, müssen Sie diese manuell zur Failover-Instanz kopieren. Die Reports sind im Verzeichnis **<HPE APM-Stammverzeichnis>\AppServer\webapps\site.war\openapi\excels** in Ordnern für jede Kunden-ID gespeichert.

Kopieren Sie außerdem alle anderen Dateien oder Verzeichnisse im System, die Sie angepasst haben.

Hinweis: Sie sollten zumindest täglich Sicherungen der APM-Server durchführen. Abhängig vom Umfang und den Intervallen der Konfigurationsänderungen kann es erforderlich sein, kürzere Intervalle einzuplanen, um umfangreiche Verluste an Konfigurationsänderungen bei einem Verlust

der Produktionsinstanz zu vermeiden.

3. Konfigurieren der Sicherungsdatenbank

Replizieren Sie die ursprüngliche Datenbank. Die ursprüngliche Datenbank kann nun als Sicherung verwendet werden, und die replizierte Datenbank fungiert als primäre Datenbank.

Hinweis: HPE empfiehlt, dass nur erfahrene Datenbankadministratoren diese Phase des Notfallwiederherstellungsszenarios durchführen.

• **Microsoft SQL – Konfigurieren des Protokolldateiversands für Datenbanken**

Um immer aktuelle Überwachungs- und Konfigurationsdaten bereitzustellen, ist es wichtig, den Protokolldateiversand zu aktivieren, sodass Lücken in den Daten minimiert werden. Mit dem Protokolldateiversand können Sie ein identisches Duplikat der ursprünglichen Datenbank erstellen, das nur durch die Verzögerung beim Kopieren und Laden leicht veraltet ist. Sie können dann den Standbydatenbankserver zum neuen primären Datenbankserver machen, wenn der ursprüngliche primäre Datenbankserver nicht mehr verfügbar ist. Wenn der ursprüngliche primäre Server dann wieder zur Verfügung steht, können Sie aus ihm einen neuen Standbyserver machen und vertauschen auf diese Weise die Serverrollen.

Der Protokolldateiversand muss für die folgenden APM-Datenbanken konfiguriert werden:

- Management
- RTSM
- Profile (alle Datenbanken)
- Analytic (sofern vorhanden)

Details zum Konfigurieren des Protokolldateiversands für Microsoft SQL finden Sie in der entsprechenden Microsoft SQL-Dokumentation.

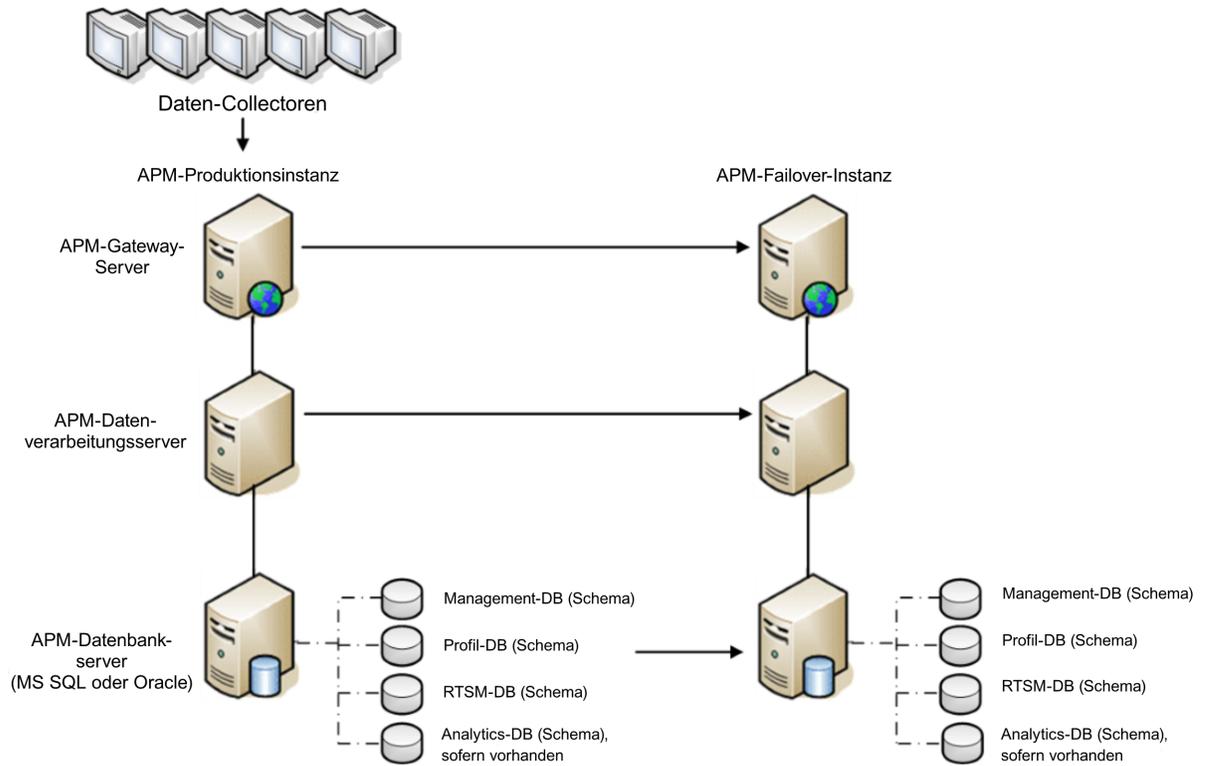
• **Oracle – Konfigurieren der Standbydatenbank (Data Guard)**

Oracle verfügt nicht über Protokolle für jedes Schema, sondern nur auf Datenbankebene. Sie können also keine Standbydatenbank auf Schemaebene anlegen und Sie müssen Kopien der Datenbanken des Produktionssystems in Ihrem Sicherungssystem erstellen.

Details zum Konfigurieren einer Standby-Datenbank finden Sie in der entsprechenden Oracle-Dokumentation.

Sobald die Konfiguration der Sicherungsdatenbank erfolgreich abgeschlossen wurde, sollte die APM-Ausfallsicherungsdatenbank mit der APM-Produktionsdatenbank synchron sein.

In der folgenden Abbildung sind das Produktionssystem und das Ausfallsicherungssystem mit aktiviertem Protokolldateiversand für die Datenbanken dargestellt:



Bereinigungsverfahren

Nachdem Sie die Originalumgebung repliziert haben, müssen bestimmte Einstellungen geändert werden, um Verwechslungen zwischen der ursprünglichen und der neuen Umgebung zu vermeiden. Mit diesem Verfahren werden alle computerspezifischen Verweise in den Konfigurationen aus der Produktionsinstanz entfernt.

Hinweis:

- Bevor mit der Aktivierung begonnen wird, sollte der APM-Administrator sicherstellen, dass auf die Ausfallsicherungsinstanz die richtige Lizenz angewendet wurde und dass alle verfügbaren Daten-Collectoren mit der Ausfallsicherungsinstanz kommunizieren können.
- HPE empfiehlt, dass ein erfahrener Datenbankadministrator die SQL-Anweisungen in diesem Verfahren ausführt.
- Die SQL-Anweisungen weiter unten müssen bis auf den letzten Schritt für die Management-Datenbank ausgeführt werden. Alle SQL-Anweisungen aus dem letzten Schritt müssen für die RTSM-Datenbank ausgeführt werden.

1. Löschen Sie veraltete Informationen aus Tabellen für hohe Verfügbarkeit (High Availability, HA).

Führen Sie die folgenden Abfragen für die Management-Datenbank der Umgebung für die Notfallwiederherstellung aus:

- **delete from HA_ACTIVE_SESS**
- **delete from HA_BACKUP_PROCESSES**
- **delete from HA_PROC_ALWD_SERVICES**
- **delete from HA_PROCESSES**
- **delete from HA_SRV_ALLWD_GRPS**
- **delete from HA_SERVICES_DEP**
- **delete from HA_SERVICES**
- **delete from HA_SERVICE_GRPS**
- **delete from HA_TASKS**
- **delete from HA_SERVERS**

2. Führen Sie die folgende Abfrage für die Management-Datenbank der DR-Umgebung aus:

Delete from PROPERTIES where NAME = 'HAServiceControllerUpgrade'

3. Ändern Sie Verweise in der Tabelle **SESSIONS** in der Management-Datenbank der DR-Umgebung auf die Sicherungssitzungsdatenbanken.

- a. Führen Sie die folgende Abfrage aus, um alle Datenbanknamen abzurufen:

SELECT * FROM SESSIONS
where SESSION_NAME like '%Unassigned%'

- b. Aktualisieren Sie die folgenden Spalten in allen zurückgegeben Zeilen mit den folgenden Werten:

- **SESSION_NAME:** Ersetzen Sie den Wert durch den neuen Namen der wiederhergestellten Datenbank (nur wenn **SESSION_NAME** gleich '%Unassigned%' ist). Verwenden Sie das folgende Skript:


```
UPDATE SESSIONS set SESSION_NAME='Unassigned<NEUER_DB_Servename><NEUER_Schemaname><DB_Benutzername>'
WHERE SESSION_NAME='Unassigned<ALTER_DB_Servename><ALTER_Schemaname><ALTER_DB_Benutzername>'
```
 - **SESSION_DB_NAME:** Ersetzen Sie den Wert durch den neuen Namen des wiederhergestellten Schemas. Verwenden Sie das folgende Skript:


```
UPDATE SESSIONS set SESSION_DB_NAME='<NEUER_Schemaname>'
WHERE SESSION_DB_NAME='<ALTER_Schemaname>'
```
 - **SESSION_DB_HOST:** Ersetzen Sie den Wert durch den neuen Namen des wiederhergestellten Datenbankhosts. Verwenden Sie das folgende Skript:


```
UPDATE SESSIONS set SESSION_DB_HOST='<NEUER_Hostname>'
WHERE SESSION_DB_HOST='<ALTER_Hostname>'
```
 - **SESSION_DB_PORT:** Ersetzen Sie den Wert durch den neuen Namen des wiederhergestellten Ports. Verwenden Sie das folgende Skript:


```
UPDATE SESSIONS set SESSION_DB_PORT='<NEUER_Portname>'
WHERE SESSION_DB_PORT='<ALTER_Portname>'
```
 - **SESSION_DB_SID:** Ersetzen Sie den Wert durch den neuen Namen der wiederhergestellten Sitzungs-ID. Verwenden Sie das folgende Skript:


```
UPDATE SESSIONS set SESSION_DB_SID='<NEUER_SID_Name>'
WHERE SESSION_DB_SID='<ALTER_SID_Name>'
```
 - **SESSION_DB_UID:** Ersetzen Sie den Wert durch den neu wiederhergestellten Namen. Verwenden Sie das folgende Skript:


```
UPDATE SESSIONS set SESSION_DB_UID='<NEUER_UID_Name>'
WHERE SESSION_DB_UID='<ALTER_UID_Name>'
```
 - **SESSION_DB_SERVER:** Ersetzen Sie den Wert durch den neuen Namen des wiederhergestellten Servers. Verwenden Sie das folgende Skript:


```
UPDATE SESSIONS set SESSION_DB_SERVER='<NEUER_Servename>'
WHERE SESSION_DB_SERVER='<ALTER_Servename>'
```
4. Ändern Sie Verweise in der Tabelle **Analytics** in der Management-Datenbank auf die Sicherungsdatenbanken.
- a. Führen Sie die folgende Abfrage aus, um alle Datenbanknamen abzurufen:


```
SELECT * FROM ANALYTICS_DATABASES
```
 - b. Aktualisieren Sie die folgenden Spalten in allen zurückgegebenen Zeilen mit den folgenden Werten:
 - **DB_HOST:** Ersetzen Sie den Wert durch den neuen Namen des wiederhergestellten Datenbankhosts. Verwenden Sie das folgende Skript:


```
update ANALYTICS_DATABASES set DB_HOST='NEUERDatenbankHostname' where DB_HOST='ALTERDatenbankHostname';
```
 - **DB_SERVER:** Ersetzen Sie den Wert durch den neuen Namen des wiederhergestellten Servers. Verwenden Sie das folgende Skript:

```
update ANALYTICS_DATABASES set DB_SERVER='NEUERDatenbankServename' where DB_SERVER='ALTERDatenbankServename'
```

- **DB_NAME:** Ersetzen Sie den Wert durch den neuen Namen des wiederhergestellten Servers. Verwenden Sie das folgende Skript:

```
update ANALYTICS_DATABASES set DB_NAME='NEUERDatenbankname' where DB_NAME='ALTERDatenbankname'
```

- **DB_SID:** Ersetzen Sie den Wert durch den neuen Namen der wiederhergestellten Sitzungs-ID. Verwenden Sie das folgende Skript:

```
update ANALYTICS_DATABASES set DB_SID = 'NEUESID' where DB_SID='ALTESID';
```

- **DB_PORT:** Ersetzen Sie den Wert durch den neuen Namen des wiederhergestellten Ports. Verwenden Sie das folgende Skript:

```
update ANALYTICS_DATABASES set DB_PORT= 'NeuerPort' where DB_PORT='AlterPort'
```

5. Löschen Sie die Informationen zum Bus-Cluster aus der Tabelle **PROPERTIES** in der Management-Datenbank.

Führen Sie folgende Abfrage aus:

Delete from PROPERTIES where

NAMESPACE='MessageBroker' or NAMESPACE='SonicMQ_Namespace' or

NAMESPACE='BrokerName' or NAMESPACE like 'hornetq-%'

6. Löschen Sie Computer aus der Tabelle **DEPLOYMENT** in der Management-Datenbank.

Führen Sie folgende Abfrage aus:

DELETE from DEPLOY_HW

7. Werte für "Setting Manager" der Tabelle **SETTING_PARAMETERS** in der Management-Datenbank.

Aktualisieren Sie die Werte für URLs und den LDAP-Server in der Tabelle **SETTING_PARAMETERS**.

In der folgenden Tabelle sind die Schlüssel der Tabelle **Setting Manager** aufgeführt, die aktualisiert werden müssen, sofern sie vorhanden sind:

SP_CONTEXT	SP_NAME	Beschreibung
platform	settings.smtp.server	Name des SMTP-Servers, der für die Warn-Engine verwendet wird
scheduledreports	settings.smtp.server	Name des SMTP-Servers, der für geplante Reports verwendet wird
platform	default.core.server.url	Die URL, die von den Daten-Collectoren für den Zugriff auf den Gateway-Server in APM verwendet wird
platform	default.centers.server.url	Die URL, die von den Benutzern für den Zugriff auf APM verwendet wird
platform	virtual.centers.server.url	

SP_CONTEXT	SP_NAME	Beschreibung
platform	virtual.core.server.url	

Ändern Sie für jeden Schlüssel in der Tabelle die folgende Abfrage und führen Sie sie aus:

update SETTING_PARAMETERS set SP_VALUE='<neuer Wert>'
where SP_CONTEXT='<Kontextwert>' and SP_NAME='<Namenswert>'

Nehmen Sie folgende Änderung vor:

- update SETTING_PARAMETERS set SP_VALUE='<neuer Computername>' where SP_CONTEXT='platform' and SP_NAME='settings.smtp.server'
- update SETTING_PARAMETERS set SP_VALUE='<neuer Computername>' where SP_CONTEXT='scheduledreports' and SP_NAME='settings.smtp.server'
- update SETTING_PARAMETERS set SP_VALUE='http://<neuer Computername>:80' where SP_CONTEXT='platform' and SP_NAME='default.core.server.url'
- update SETTING_PARAMETERS set SP_VALUE='http://<neuer Computername>:80' where SP_CONTEXT='platform' and SP_NAME='default.centers.server.url'

Die letzten beiden Einstellungen in der obigen Tabelle müssen nur aktualisiert werden, wenn Sie einen Load Balancer oder Reverse Proxy verwenden. Aktualisieren Sie in diesem Fall die Einstellungen wie folgt:

- update SETTING_PARAMETERS set SP_VALUE='http://<Load Balancer oder Reverse Proxy>:80' where SP_CONTEXT='platform' and SP_NAME='virtual.centers.server.url'
- update SETTING_PARAMETERS set SP_VALUE='http://<Load Balancer oder Reverse Proxy>:80' where SP_CONTEXT='platform' and SP_NAME='virtual.core.server.url'

8. Aktualisieren Sie SYSTEM-Schlüssel.

Aktualisieren Sie die folgenden Schlüssel in der Tabelle SYSTEM in der Management-Datenbank:

AdminServerURL	http://<DPS1>:port	Standardmäßig gibt es keine Portnummer.
GraphServerURL	http://<GW1>/topaz/	
GraphServerURL4.5.0.0	http://<GW1>/topaz/	
application.tac.path	http://<GW1>:port/AdminCenter	Standardmäßig ist dies Portnummer 80.
application.flipper.path	http://<GW1>:port/monitoring	Standardmäßig ist dies Portnummer 80.

Ändern Sie für jeden Wert in der Tabelle die folgende Abfrage und führen Sie sie aus:

update SYSTEM set SYS_VALUE='<neuer Wert>' where SYS_NAME='<key>'

Hierbei ist <neuer Wert> die neue URL im Format der ursprünglichen URL.

Beispiel:

```
update SYSTEM set SYS_VALUE='http://<neuer_Computer>:port' where SYS_
NAME='AdminServerURL'
```

Hinweis: Die standardmäßige Portnummer ist 80.

9. Leeren und aktualisieren Sie Tabellen in der RTSM-Datenbank.

Mit diesem Verfahren werden alle computerspezifischen Verweise in den RTSM-Konfigurationstabellen entfernt.

Führen Sie die folgenden SQL-Anweisungen für die RTSM-Datenbank aus:

- **update CUSTOMER_REGISTRATION set CLUSTER_ID=null**
- **truncate table CLUSTER_SERVER**
- **truncate table SERVER**
- **truncate table CLUSTERS**

Konfigurieren der neuen Umgebung

1. Führen Sie das Dienstprogramm für die Server- und Datenbankkonfiguration aus.

Führen Sie das Dienstprogramm für die Server- und Datenbankkonfiguration auf jedem Computer aus, um die erforderlichen Tabellen in der Datenbank wieder zu initialisieren. Um das Dienstprogramm für die Server- und Datenbankkonfiguration auszuführen, wählen Sie **Start > Alle Programme > HPE Application Performance Management > Verwaltung > HPE Application Performance Management konfigurieren** aus.

Hinweis: Stellen Sie bei der Ausführung des Dienstprogramms für die Server- und Datenbankkonfiguration sicher, dass Sie die Verbindung wieder mit denselben Datenbanken herstellen, die für die Ausfallsicherungsumgebung erstellt wurden (also die Datenbank, an die die Sicherungsdaten übertragen wurden). Sie könnten alle Konfigurationsdaten verlieren, wenn Sie versuchen, das Dienstprogramm für die Produktionsumgebung auszuführen.

Führen Sie das Dienstprogramm für die Server- und Datenbankkonfiguration auf den Computern in der gleichen Reihenfolge aus, in der APM ursprünglich in der Ausfallsicherungsumgebung installiert wurde.

2. Aktivieren von APM

Aktivieren Sie APM auf den neuen Servern.

3. Führen Sie das Bereinigungsverfahren nach dem Start aus, um veraltete Hosts zu deaktivieren, die nicht Bestandteil der Ausfallsicherungsinstanz sind.

So deaktivieren Sie veraltete Hosts:

- a. Wechseln Sie in APM zu **Admin > Plattform > Setup und Verwaltung > Serverbereitstellung** und wählen Sie **Deaktivieren von Maschine**.
- b. Deaktivieren Sie veraltete Hosts.

4. Wiederholen der Schritte zur verstärkten Sicherheit (optional)

Wenn für die ursprüngliche Umgebung die verstärkte Sicherheit eingerichtet wurde, müssen Sie die Schritte zur verstärkten Sicherheit für die neue Umgebung wiederholen.

Der Schritte für den Reverse Proxy müssen nicht wiederholt werden.

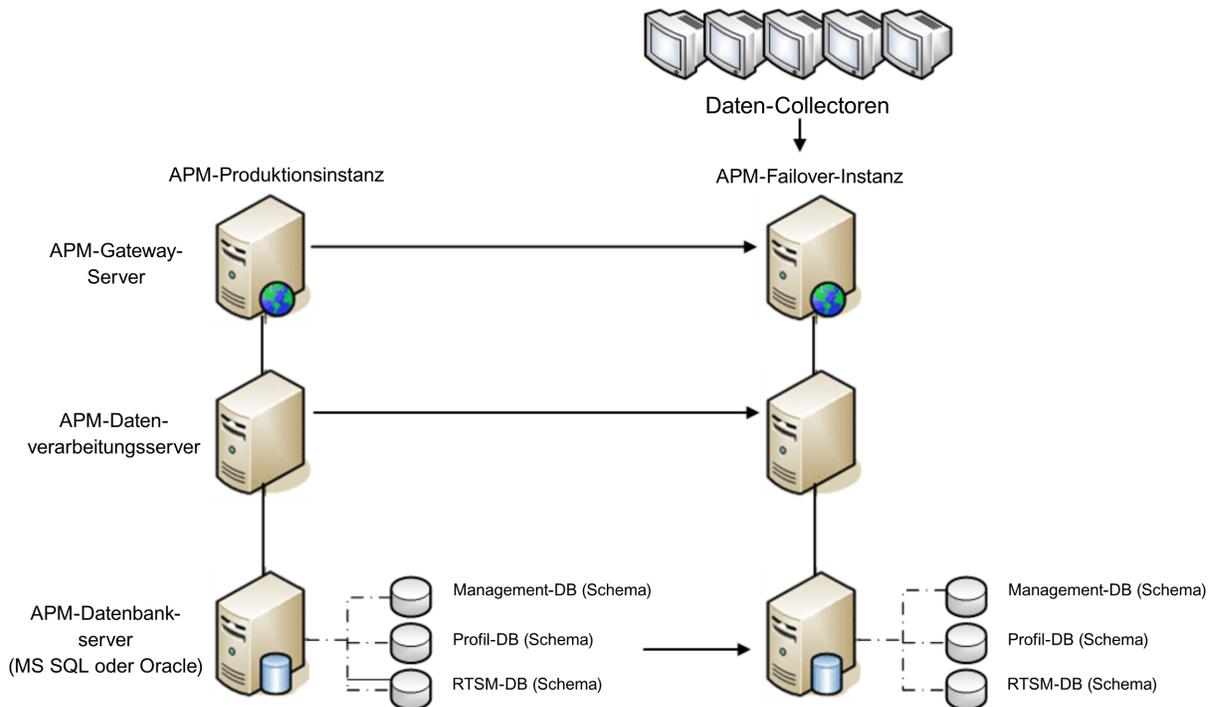
Details hierzu finden Sie im *APM Hardening Guide*.

Konfigurieren der Daten-Collectoren

1. Konfigurieren Sie die Datenerfassung.

Konfigurieren Sie alle Daten-Collectoren, einschließlich Business Process Monitor-Agents, Real User Monitor-Engines, SiteScopes, HPOM, Service Manager und Operations Orchestration (bei Installation auf einem separaten Server) für die Ausfallsicherungsinstanz. Details finden Sie in der relevanten Dokumentation für jede Datenerfassung.

In der folgenden Abbildung ist eine vollständig aktivierte Ausfallsicherungsinstanz dargestellt:



2. Konfigurieren Sie die Verbindungen der Datenerfassung für die Ausfallsicherung.

Wenn einer der Daten-Collectoren ausgefallen ist und auf einen anderen Computer verschoben wurde, müssen den APM-Servern die neuen URLs mitgeteilt werden. Dies wird in verschiedenen Applikationen in APM vorgenommen. Beispiel:

Daten-Collector	Verfahren
SiteScope	Verbinden Sie die SiteScope-Server erneut mit dem APM-Server in der SiteScope-Konsole.
Business Process Monitor	Verbinden Sie die BPM-Server erneut mit dem APM-Server in der BPM-Konsole.

Daten-Collector	Verfahren
Real User Monitor	Verbinden Sie die RUM-Server erneut mit dem APM-Server in der RUM-Konsole.
HP Operations Orchestration	Übernehmen Sie auf dem HP Operations Orchestration-Server die Konfiguration, um den neuen APM-Server widerzuspiegeln, wie im Verfahren im <i>Solutions and Integrations Guide</i> beschrieben ist.
HPE Service Manager	Übernehmen Sie auf dem HPE Service Manager-Server die Konfiguration, um den neuen APM-Server widerzuspiegeln, wie im Verfahren im <i>Solutions and Integrations Guide</i> beschrieben ist.
SHA PA-Daten-Collector	Verbinden Sie den SHA PA-Data Collector erneut durch erneutes Ausführen des Konfigurations-Assistenten.

Anhang F: Hochverfügbarkeit für APM

Diese Anhang umfasst die folgenden Themen:

- Übersicht über die Optionen für hohe Verfügbarkeit 85
- Lastenausgleich für den Gateway-Server 86
- Hochverfügbarkeit für den Gateway-Server 89
- Hochverfügbarkeit für den Datenverarbeitungsserver 90
- Konfigurieren der APM-Daten-Collectoren in einer verteilten Umgebung 102

Übersicht über die Optionen für hohe Verfügbarkeit

Sie können die Verfügbarkeit und die Zuverlässigkeit des Systems mit den Optionen für hohe Verfügbarkeit verbessern. Mit diesen Optionen werden mehrere Server, externer Lastenausgleich und Failoverprozeduren kombiniert.

Das Implementieren einer Konfiguration mit hoher Verfügbarkeit bedeutet, dass Sie die APM-Server so einrichten, dass der Dienst auch bei Stromausfällen, Computerausfällen und hohen Lasten immer verfügbar ist.

Lastenausgleich und hohe Verfügbarkeit können in Bereitstellungen auf einem Computer oder in verteilten Bereitstellungen implementiert werden. Sie konfigurieren den Lastenausgleich, indem Sie einen zusätzlichen Gateway-Server hinzufügen, und hohe Verfügbarkeit, indem Sie einen Sicherungsserver für die Datenverarbeitung hinzufügen.

Hohe Verfügbarkeit wird auf zwei Ebenen implementiert:

- **Hardwareinfrastruktur.** Diese Ebene umfasst redundante Server, Netzwerke, Stromversorgungen usw.
- **Applikation.** Diese Ebene weist zwei Komponenten auf:
 - **Lastenausgleich.** Mit dem Lastenausgleich wird die Arbeitslast zwischen verschiedenen Computern verteilt. Dadurch werden die Systemleistung und die Verfügbarkeit gesteigert.
Beim externen Lastenausgleich wird eine Software- und Hardwareeinheit von einem externen Anbieter bereitgestellt. Diese Einheit muss installiert und für die Funktionsfähigkeit mit APM-Applikationen konfiguriert werden.
 - **Failover.** Die Leistung eines Servers, beispielsweise des Datenverarbeitungsservers, wird von einem Sicherungsserver übernommen, falls der primäre Server oder die Komponente ausfällt bzw. vorübergehend nicht verfügbar ist.

Die Implementierung von Lastenausgleich und Failover wird in diesem Kapitel ausführlich erläutert.

Hinweis: HPE Professional Services bietet Beratungsservices, um Kunden im Hinblick auf die APM-Strategie sowie Planung und Bereitstellung zu unterstützen. Entsprechende Informationen erhalten Sie bei einem HPE-Kontakt.

Lastenausgleich für den Gateway-Server

Wenn Sie mehrere APM-Gateway-Server installieren, kann APM externe Mechanismen für den Lastenausgleich nutzen, um eine gleichmäßige Verteilung der Verarbeitungs- und Kommunikationsaktivitäten im Netzwerk sicherzustellen. Dies ist besonders bei hoher Last von Bedeutung, um eine Überlastung eines einzelnen Servers zu vermeiden.

Hinweis: Es wird empfohlen, APM hinter einem Load Balancer oder Reverse Proxy zu installieren. Hierdurch werden weitere Sicherheitsoptionen aktiviert und Notfallwiederherstellung sowie Upgradeverfahren vereinfacht.

Dieser Abschnitt umfasst die folgenden Themen:

["Konfigurieren des Lastenausgleichs" auf Seite 86](#)

["Hinweise und Einschränkungen" auf Seite 88](#)

Konfigurieren des Lastenausgleichs

1. Erstellen Sie zwei virtuelle Hostnamen. Der virtuelle Hostname muss ein vollqualifizierter Domänenname (Fully Qualified Domain Name, FQDN) im Format **<Servername>.<Domänenname>** sein. Dies ist eine notwendige Anforderung, um die Authentifizierung vom Typ Lightweight Single Sign On zu unterstützen, die standardmäßig aktiviert ist.

Der erste Hostname dient dem Zugriff auf die APM-Website auf dem Gateway-Server. Diese URL kann an APM-Benutzer verteilt werden. Der zweite Hostname ist dafür vorgesehen, dass die Daten-Collectoren auf den Gateway-Server zugreifen können. Diese URL muss verwendet werden, wenn die Kommunikation der Daten-Collectoren mit APM konfiguriert wird.
2. Geben Sie die Hostnamen für den jeweiligen Load Balancer in den Infrastruktureinstellungen für die virtuellen Server ein. Wählen Sie hierzu **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** aus, wählen Sie dann **Foundation** und anschließend **Plattformverwaltung** aus.
 - **URL des virtuellen Gateway-Servers für Applikationsbenutzer.** Virtueller Hostname für die APM-Website. Der Gateway-Server, auf dem Sie arbeiten, muss diese virtuelle IP-Adresse auflösen können. Das bedeutet, dass **nslookup** für den **virtuellen Hostnamen für die Applikationsbenutzer** bei Ausführung auf diesem Gateway-Server den Namen und die IP-Adresse zurückgeben muss.
 - **URL des virtuellen Gateway-Servers für Daten-Collectoren.** Virtueller Hostname für Daten-Collectoren. Alle Daten-Collectoren müssen diese virtuelle IP-Adresse auflösen können. Das bedeutet, dass **nslookup** für den **virtuellen Hostnamen für die Daten-Collectoren** bei Ausführung auf dem Daten-Collector-Server den Namen und die IP-Adresse zurückgeben muss.
3. Legen Sie im Ausschnitt **Reverse Proxy-Konfiguration** die folgenden Parameter fest:
 - **Parameter "Reverse Proxy aktivieren" = true.**
 - **HTTP-Reverse Proxy-IPs**
Fügen Sie die internen IP-Adressen der Load Balancer dieser Einstellung hinzu.

- Wenn die IP-Adresse des Load Balancer, der die HTTP/S-Anforderung sendet, enthalten ist, ist die an den Client zurückgegebene URL entweder die Standard-URL des virtuellen Servers oder die lokale URL des virtuellen Servers (falls definiert).
- Wenn für diesen Parameter keine IP-Adressen definiert sind (nicht empfohlen), wird APM im generischen Modus ausgeführt. Das bedeutet, dass Sie sich nicht direkt am Gateway, sondern nur über die virtuelle URL bei APM anmelden können.

Hinweis: Wenn sich Ihr Load Balancer und die APM-Gateway-Server nicht in derselben Domäne befinden, müssen Sie die IP des Reverse Proxys zum Parameter **HTTP- oder HTTPS-Reverse Proxy-IPs** hinzufügen. Weitere Details finden Sie unter "LW-SSO Configuration for Multi-Domain and Nested Domain Installations" im *APM Platform Administration Guide*.

So ermitteln Sie die interne IP Ihres Load Balancer:

- a. Melden Sie sich über den Load Balancer bei APM an.
 - b. Öffnen Sie das Protokoll am folgendem Speicherort: **<HPE APM-Gateway-Stammverzeichnis>\log\EJBContainer\UserActionsServlet.log**.
 - c. Die angezeigte IP in der letzten Anmeldezeile in diesem Protokoll ist die interne IP des Lastenausgleichmoduls. Der Eintrag sollte Ihren Benutzernamen enthalten.
4. Starten Sie nach dem Ändern der Reverse Proxy-Einstellungen den HPE APM-Dienst auf den APM-Gateway- und -Datenverarbeitungsservern neu.

Hinweis: Wenn Ihr Load Balancer die Auswahl zwischen Full-NAT- und Half-NAT-Topologien ermöglicht, wählen Sie **Full-NAT**.

5. Konfigurieren Sie den Load Balancer für den Zugriff der Daten-Collectoren. Alle Daten-Collectoren müssen auf die virtuelle IP des Load Balancer zugreifen können. Verwenden Sie die Standardeinstellungen für den Load Balancer, legen Sie aber Folgendes fest:
- Wir empfehlen die Verwendung eines Round Robin-Algorithmus, um die Last auf alle APM Gateway-Server gleichmäßig zu verteilen.
 - Verwenden Sie folgenden KeepAlive-URI:
 - Sendezeichenfolge: **GET /ext/mod_mdvr_wrap.dll?type=test**
 - Empfangszeichenfolge: **Web Data Entry is up**
6. Konfigurieren Sie den Load Balancer für den Benutzerzugriff.
- Verwenden Sie die Standardeinstellungen für den Load Balancer, aber legen Sie die Persistenz auf **stickiness by session enabled** oder **Destination Address Affinity** fest (je nach Load Balancer). Wenn keine dieser Optionen verfügbar ist und die Auswahl zwischen **cookiebasierter** Stickiness und **IP-basierter** Stickiness liegt, versuchen Sie es mit der **IP-basierten** Stickiness. Wenn dies nicht ordnungsgemäß funktioniert, treten möglicherweise zeitweise Benutzeroberflächenfehler auf.
 - Verwenden Sie folgenden KeepAlive-URI:
 - Sendezeichenfolge: **GET /topaz/topaz_api/loadBalancerVerify_centers.jsp**
 - Empfangszeichenfolge: **Erfolg**

Hinweise und Einschränkungen

- APM unterstützt Hardware- und Virtual Appliance-basierte Load Balancer. Aus Gründen der Leistung ist ein Hardware-basierter Load Balancer die bevorzugte Lösung. Alle Load Balancer müssen Sticky-Sitzungen für Benutzer sowie URL-basierte Zustandsmonitore konfigurieren können.
- Wenn Sie zwei Load Balancer für das Failover verwenden, müssen Sie die Hostnamen für beide Load Balancer auf dem DNS-Servercomputer konfigurieren. Dann können Sie den Computernamen, den FQDN des Hostnamens oder die URL von einem der Load Balancer angeben, wenn diese Informationen für die Daten-Collectoren erforderlich sind, oder auch im Browser, um die APM-Website zu öffnen.
- Wenn zwei Gateway-Server in unterschiedlichen Laufwerkspfaden installiert sind, z. B. einer auf Laufwerk C:\ und einer auf Laufwerk E:\, ist möglicherweise der Zugriff auf APM nicht möglich.
Problemumgehung: Erstellen Sie einen doppelten Pfad auf Laufwerk C:\, indem Sie **E:\<HPE APM-Stammverzeichnis>\confsettings** nach **C:\<HPE APM-Stammverzeichnis>\confsettings** kopieren.
- Wenn Sie zwei Load Balancer für das Failover verwenden und jeden Load Balancer für mehr als einen Servertyp eingesetzt wird, sollten Sie einen eindeutigen virtuellen Hostnamen in jedem Load Balancer für jeden Servertyp definieren, die virtuellen Hostnamen den tatsächlichen Hostnamen der entsprechenden Server zuordnen und alle virtuellen Hostnamen auf dem DNS-Servercomputer konfigurieren. Dann können Sie den jeweils relevanten virtuellen Hostnamen für jeden Daten-Collector angeben. Sie können ihn aber auch im Browser angeben, um die APM-Website zu öffnen.
- Stellen Sie beim Konfigurieren eines Load Balancer oder Reverse Proxys sicher, dass er von allen APM-Servern über die für die Verbindungen angegebenen virtuellen Adressen erreicht werden kann (Gateway und Datenverarbeitungserver).

Hochverfügbarkeit für den Gateway-Server

HPE Application Performance Management bietet Hochverfügbarkeit für die Gateway-Server, um sicherzustellen, dass die Daten ihr Ziel erreichen und dass die Benutzer APM-Applikationen auch bei einem Serverausfall verwenden können.

Geschützte Übermittlung eingehender Daten

APM ermöglicht eine geschützte Datenübermittlung für Monitor-Daten. Eine geschützte Datenübermittlung bedeutet, dass die Daten erst aus einem Datenspeicher gelöscht werden, nachdem sie an den nächsten Datenspeicher weitergeleitet und dort gespeichert wurden.

Hinweis: HPE Professional Services bietet Beratung zu den Best Practices im Hinblick auf dieses Thema. Informationen dazu, wie Sie diesen Service erhalten, bekommen Sie von Ihrem HPE-Kontakt.

APM unterstützt die folgenden Mechanismen, um eine hohe Verfügbarkeit von Rohdaten sicherzustellen:

- Wenn der Webserver des Gateway-Servercomputers ausfällt, werden die Daten entweder vom Load Balancer an einen anderen Gateway-Server weitergeleitet oder in die Warteschlange des Daten-Collectors aufgenommen, bis der Webserver wieder funktioniert.
- Wenn der Webserver des Gateway-Servercomputers Daten empfängt, der Bus aber ausgefallen ist, werden die Daten im Daten-Collector gespeichert, bis der Bus wieder funktioniert.
- Wenn der Bus die Daten empfängt, das Datenladeprogramm für die Überwachung aber ausgefallen ist, werden die Daten im Bus gespeichert, bis das Datenladeprogramm für die Überwachung wieder funktioniert. Die Daten werden dann an die Datenbank gesendet.

Hochverfügbarkeit für Service-Zustand

HPE Application Performance Management bietet Hochverfügbarkeit für Service-Zustand auf dem Gateway-Server, damit die Benutzer auch dann mit Service-Zustand arbeiten können, wenn ein Gateway-Server während einer Benutzersitzung ausfällt.

Wenn sich ein Benutzer bei APM anmeldet und die Arbeit mit Service-Zustand aufnimmt, werden die Sitzungsinformationen auf einem bestimmten Gateway-Server gespeichert, und der Load Balancer sendet die gesamte Kommunikation im Zusammenhang mit dieser Sitzung an den gleichen Gateway-Server. Fällt dieser Gateway-Server aus, leitet der Load Balancer die Sitzung an einen anderen Gateway-Server um, und die Sitzung wird auf dem neuen Gateway-Server erneut registriert. Der Benutzer setzt seine Arbeit ohne Unterbrechung des Diensts fort. Er muss sich auch nicht erneut bei APM anmelden.

Für den Load Balancer des Gateway-Servers muss **stickiness by session enabled** festgelegt sein. Details finden Sie unter "[Konfigurieren des Lastenausgleichs](#)" auf Seite 86.

Achtung: Es ist möglich, dass in bestimmten Situationen der Wechsel von einem Gateway-Server auf einen anderen einige Sekunden dauert. Während dieses Wechsels können einige Benutzeraktionen zu Fehlern führen.

Hochverfügbarkeit für den Datenverarbeitungsserver

Um die hohe Verfügbarkeit zu gewährleisten, sollten Sie einen Sicherungsserver für die Datenverarbeitung installieren. Damit APM ordnungsgemäß bei einem Ausfall des primären Datenverarbeitungsservers ausgeführt wird, kann der Sicherungsserver für die Datenverarbeitung dessen Funktionen übernehmen.

Tipp: Es wird empfohlen, bei der Installation des primären Servers und des Sicherungsservers für die Datenverarbeitung darauf zu achten, dass die Server im Hinblick auf Hardware, Speicher und Leistung vergleichbar sind.

Ist die hohe Verfügbarkeit für den Datenverarbeitungsserver aktiviert und ein Sicherungsserver definiert, führt der Hochverfügbarkeitscontroller automatisch ein Failover durch und verschiebt die Dienste auf den Sicherungsserver, falls ein oder mehrere Dienste nicht mehr zur Verfügung stehen. Der Server ruft die aktuelle Konfiguration aus der Verwaltungsdatenbank ab und bietet diese Dienste als neuen aktiven Server für die Datenverarbeitung an.

Sie können auch die JMX-Konsole verwenden, um dem Sicherungsserver Dienste manuell erneut zuzuweisen. Dies bietet sich beispielsweise an, wenn sie eine Wartung auf einem der Server für die Datenverarbeitung planen. Das manuelle Verschieben der Dienste kann die APM-Ausfallzeit reduzieren.

Hinweis: Bei der Bereitstellung einer neuen APM-Installation wird der zuerst gestartete Server für die Datenverarbeitung der Standardserver für zugewiesene Dienste des Servers für die Datenverarbeitung. Er wird also der primäre Server für die Datenverarbeitung. Wird ein zweiter Server für die Datenverarbeitung gestartet, können Sie ihn als Sicherungsserver nutzen. Details finden Sie unter "Understanding Service Reassignment" im APM-Plattformverwaltungshandbuch.

Dieser Abschnitt umfasst die folgenden Themen:

["Dienste, die dem Server zugewiesen werden" auf Seite 90](#)

["Dienste, die vom Hochverfügbarkeitscontroller \(HAC\) verwaltet werden" auf Seite 92](#)

["Konfigurieren des automatischen Failovers " auf Seite 96](#)

["Erneutes Zuweisen von Diensten mithilfe der JMX-Konsole" auf Seite 98](#)

["Manuelles Neuzuweisen von Diensten " auf Seite 99](#)

["Manuelles Deaktivieren der Datenaggregatordienste" auf Seite 101](#)

Dienste, die dem Server zugewiesen werden

Verschiedene Prozesse werden dem Gateway-Server und dem Server für die Datenverarbeitung zugewiesen. Jeder Prozess ist für die Ausführung bestimmter Dienste vorgesehen. Sie können die JMX-Konsole verwenden, um die Dienste anzuzeigen, die auf den APM-Servern oder auf einem bestimmten Server, z. B. dem Datenverarbeitungsserver, ausgeführt werden.

So zeigen Sie Dienste über die JMX-Webkonsole an:

1. Öffnen Sie in einem Webbrowser:
http://<Computername des Datenverarbeitungsservers>:29000
2. Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen zur Authentifizierung für die JMX-Konsole ein (wenden Sie sich an den Systemadministrator, falls Sie nicht über diese

Anmeldeinformationen verfügen).

3. Wählen Sie im Abschnitt **Topaz service=hac-manager** aus.
4. Klicken Sie unter **java.lang.String listAllAssignments()** aus der Datenbank auf **Invoke**.

Wenn Sie die Dienste eines bestimmten Servers, wie beispielsweise des Servers für die Datenverarbeitung, anzeigen möchten, geben Sie den Namen des Servers als Parameterwert ein.

Möchten Sie alle Dienste anzeigen, geben Sie keinen Wert für den Servernamen ein.

In einer Tabelle werden die Prozesse angezeigt, die auf dem Server ausgeführt werden. Die JMX-Onlinetabelle weist die folgenden Spalten auf:

Spaltenname	Beschreibung
Service	Der Name des zugewiesenen Diensts.
Kunde	Die ID des Kunden, dem der Dienst zugewiesen ist. Die standardmäßige Kunden-ID für ein einzelnes APM-System (ein System, das nicht von HPE Software-as-a-Service verwaltet wird) ist 1. Ein Dienst mit der Kunden-ID -1 ist ein globaler Dienst, der von allen Kunden in einer SaaS-Bereitstellung verwendet wird.
Process	Der Name des Servers für die Datenverarbeitung und der Name des JVM-Prozesses, der den Dienst verarbeitet. Die Dauer, für die der Server bereits aktiv ist, und der letzte Zeitpunkt, zu dem er per Ping erreicht wurde, werden ebenfalls angezeigt.
Assigned	Ob die Dienstzuweisung gerade aktiv ist, das Datum der Dienstzuweisung und die Dauer der Zuweisung werde angezeigt.
State	Der aktuelle Status des Diensts. Gültige Status: 1 – Angehalten 2 – Gestartet 3 – Wird angehalten 4 – Wird ausgeführt -1 – Fehler -2 – Fehler beim Anhalten -3 – Fehler beim Starten Das Datum, zu dem der Dienst den Status angenommen hat, und die Dauer, für die er in diesem Status ist, werden angezeigt.
Srv. Sign	Serversignatur.
State Sign	Statussignatur (sollte mit der Serversignatur übereinstimmen).

Dienste, die vom Hochverfügbarkeitscontroller (HAC) verwaltet werden

Die Dienste des Datenverarbeitungsservers, die von einem HAC verwaltet werden können, werden in der folgenden Tabelle beschrieben:

- Der Name des Prozesses in JVM
- Der Name, den der Hochverfügbarkeitscontroller (HAC) für den Prozess verwendet
- Die Dienste, die für einen Prozess ausgeführt werden
- Eine Beschreibung des Prozesses

JVM-Prozessname	HAC-Prozessname	Dienstname	Beschreibung des Diensts Speicherort der Protokolldatei
Mercury AS	mercury _as	KPI_ENRICHMENT	Mit dem Dienst KPI_Enrichment werden Dashboard-KPIs den CIs hinzugefügt, die dem Modell von externen Überwachungssystemen hinzugefügt wurden. Die hinzuzufügenden KPIs und die CIs, denen die KPIs hinzugefügt werden, können konfiguriert werden.
		BSM_DT	BSM_DT behandelt die konfigurierten Ausfallzeiten im System. Ausfallzeiten können für CIs konfiguriert werden und sich auf Alarme, Ereignisse, Reports, KPI-Berechnungen und die Überwachung auswirken.
		VERTICALS	Dieser Dienst gilt für SAP und stellt die Kompatibilität mit APM sicher. Der SAP-Dienst verknüpft Daten, die von SiteScope und Business Process Monitor abgerufen wurden, mit SAP-bezogenen Entitäten aus der RTSM.

JVM-Prozessname	HAC-Prozessname	Dienstname	Beschreibung des Diensts Speicherort der Protokolldatei
		EUM_ADMIN	EUM_ADMIN behandelt die End User Management-Verwaltung, wobei Instanzen von Business Process Monitor und Real User Monitor für die Überwachung konfiguriert werden.
mercury_odb	odb	BSM_ODB	RTSM ist ein zentrales Repository für Konfigurationsinformationen, die von verschiedenen APM-Applikationen und -Werkzeugen sowie Applikationen und Werkzeugen von Drittanbietern gesammelt werden. Diese Informationen werden beim Erstellen von APM-Ansichten verwendet.

JVM-Prozessname	HAC-Prozessname	Dienstname	Beschreibung des Diensts Speicherort der Protokolldatei
hpbsm_ bizImpact	businessimpact_service	BIZ_IMPACT	Die Business Impact-Komponente ermöglicht Ihnen die Anzeige von Geschäfts-CIs und SLAs, auf die sich ein anderes CI in Service-Zustand auswirkt.
		LIV_SERVICE	Dieser Dienst ermöglicht Ihnen das Erstellen von Ansichten mit lokaler Auswirkung in Service-Zustand. Diese sind von allen andern Ansichten unabhängig. Wenn Sie Indikatordefinitionen für ein CI innerhalb einer Ansicht mit lokaler Auswirkung ändern, hat dies keine Auswirkung auf das CI in allen anderen Ansichten.
hpbsm_ _offline _engine	offline_ engine	NOA	Der Dienst New Offline Aggregator überprüft und synchronisiert stündlich oder täglich neue Aufgaben für den Offlineaggregator.
hpbsm_ _marble _supervisor	marble_ supervisor	DASHBOARD	Der Dashboard-Dienst auf dem Datenverarbeitungsserver nimmt Onlineberechnungen der Geschäftslogik für Service-Zustand vor.

JVM-Prozessname	HAC-Prozessname	Dienstname	Beschreibung des Diensts Speicherort der Protokolldatei
hpbsm_ pmanager	pmanager	PM	Über das Partitionieren und Löschen von Daten werden Tabellen mit schnell anwachsenden Datenmengen in festgelegten Intervallen geteilt. Sobald die definierte Zeitspanne verstrichen ist, kann auf Daten in einer Partition nicht mehr zugegriffen werden, um sie in APM-Reports zu verwenden. Nach einer weiteren, definierten Zeitspanne wird die Partition aus der Profildatenbank gelöscht.
hpbsm_pi_engine	pi_engine	PI_ENGINE	Die Service Health Analyzer Engine-Komponente sucht nach Anomalien im Hinblick auf das Baseline-Verhalten des Systems.
hpbsm_basel_engine	basel_engine	BASELVALIDATOR	Die Baseline-Prüfung validiert Baseline-Aufgaben im Hinblick auf Metadaten und fügt ggf. Aufgaben hinzu bzw. entfernt diese.

Konfigurieren des automatischen Failovers

Sie können die automatische Neuzuweisung von Diensten, die auf einem primären Server für die Datenverarbeitung ausgeführt werden, zu einem Sicherungsserver für die Datenverarbeitung konfigurieren. Um die automatische Neuzuweisung von Diensten, die auf einem primären Server für die Datenverarbeitung ausgeführt werden, zu einem Sicherungsserver für die Datenverarbeitung zu konfigurieren, müssen Sie folgendermaßen vorgehen:

- Definieren Sie einen Sicherungsserver für die Datenverarbeitung in der JMX-Konsole.
- Aktivieren Sie das automatische Failover.

Hinweis: Wenn Sie das automatische Failover konfigurieren und den Keep Alive-Zeitüberschreitungswert auf weniger als 10 Minuten festlegen, kann dies dazu führen, dass APM-Dienste nach einem Neustart auf den Sicherungsserver verschoben werden. Um dies zu vermeiden, sollten Sie beim Deaktivieren von APM den Sicherungsserver vor dem primären Server herunterfahren. Aktivieren Sie beim Aktivieren von APM den primären Server, und stellen Sie vor dem Aktivieren des Sicherungsservers sicher, dass alle Dienste gestartet wurden.

Definieren eines Sicherungsservers

Sie müssen die JMX-Konsole verwenden, um einen Sicherungsserver für die Datenverarbeitung zu definieren oder zu entfernen. Darüber hinaus können Sie die Konfigurationen für die hohe Verfügbarkeit anzeigen.

So verwenden Sie die JMX-Konsole zum Definieren eines Sicherungsservers:

1. Öffnen Sie in einem Webbrowser:
http://<Computernamen des Datenverarbeitungsservers>:29000
Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen zur Authentifizierung für die JMX-Konsole ein (wenden Sie sich an den Systemadministrator, falls Sie nicht über diese Anmeldeinformationen verfügen).
2. Wählen Sie im Abschnitt **Topaz** den Eintrag **service=hac-backup** aus.
3. Suchen Sie nach **addBackupServer** und geben Sie folgende Werte ein:
 - **primaryServerName**. Der Name des primären Servers.
 - **backupServerName**. Der Name des Sicherungsservers.

Verwenden Sie den Computernamen (nicht den FQDN) für diese beiden Parameter. Wenn Sie den Computernamen nicht genau kennen, können Sie mithilfe der unten beschriebenen **listservers**-Methode den Namen der bereits konfigurierten Computer ermitteln.

4. Klicken Sie auf **Aufrufen**.

So entfernen Sie einen Sicherungsserver:

1. Befolgen Sie die Anweisungen in Schritt 1 und 2, um auf JMX und den Dienst **hac-backup** zuzugreifen.
2. Suchen Sie nach **removeBackupServer** und geben Sie den folgenden Wert ein:
primaryServerName. Der Name des primären Diensts, für den Sie den Sicherungsserver entfernen.
3. Klicken Sie auf **Aufrufen**.

So zeigen Sie die Konfiguration für die hohe Verfügbarkeit an:

1. Befolgen Sie die Anweisungen in Schritt 1 und 2, um auf JMX und den Dienst **hac-backup** zuzugreifen.
2. Suchen Sie **listservers** und klicken Sie auf **Aufrufen**.

Das Ergebnis wird in einer Liste aus **Servern** und **Sicherungsservern** angezeigt. Sind keine Sicherungsserver definiert oder ist die hohe Verfügbarkeit nicht aktiviert, erhalten Sie eine Fehlermeldung mit dem Hinweis, dass das automatische Failover deaktiviert ist.

Aktivieren des automatischen Failovers

Verwenden Sie hierzu entweder die Infrastruktureinstellungen der APM-Benutzeroberfläche oder der JMX-Konsole. Mithilfe der JMX-Konsole können Sie auch überprüfen, ob die hohe Verfügbarkeit aktiviert ist.

So aktivieren Sie das automatische Failover in den Infrastruktureinstellungen:

1. Wählen Sie **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen**.
2. Wählen Sie **Foundation** und anschließend **Hochverfügbarkeitscontroller (HAC)** aus und suchen Sie den Eintrag **Automatische Ausfallsicherung (Failover) aktiviert** in der Tabelle **Allgemeine Eigenschaften**.
3. Ändern Sie den Wert auf **true**. Die Änderung wird sofort wirksam.
4. Geben Sie in der Tabelle die anderen Parameter entsprechend Ihren Anforderungen an. Die Details zu den einzelnen Parametern sind in der Tabelle enthalten.

So aktivieren Sie das automatische Failover in JMX:

1. Öffnen Sie in einem Webbrowser:
http://<Computername des Datenverarbeitungsservers>:29000
Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen zur Authentifizierung für die JMX-Konsole ein (wenden Sie sich an den Systemadministrator, falls Sie nicht über diese Anmeldeinformationen verfügen).
2. Wählen Sie im Abschnitt **Topaz** den Eintrag **service=hac-backup** aus.
3. Suchen Sie **void setAutomaticFailoverEnabled ()**, wählen sie **True** aus und klicken Sie auf **Aufrufen**.

So überprüfen Sie, ob das automatische Failover konfiguriert wurde:

1. Befolgen Sie die Anweisungen in Schritt 1 und 2, um auf JMX und den Dienst **hac-backup** zuzugreifen.
2. Suchen Sie **void getAutomaticFailoverEnabled ()** und klicken Sie auf **Aufrufen**.

Erneutes Zuweisen von Diensten mithilfe der JMX-Konsole

Sie können Dienste, je nach Verfügbarkeit von Servern und Ressourcen, zwischen Datenbearbeitungsservern verschieben. Das erneute Zuweisen von Diensten kann auch die Ausfallzeit während der Wartung von Servern für die Datenverarbeitung reduzieren.

Für dieses Verfahren ist es nicht erforderlich, die hohe Verfügbarkeit zu aktivieren, und die Quell- und Zielservers müssen keine Konfiguration für die hohe Verfügbarkeit aufweisen.

So verwenden Sie die JMX-Konsole zum erneuten Zuweisen von Diensten zwischen Servern für die Datenverarbeitung:

1. Öffnen Sie in einem Webbrowser:
http://<Computername des Datenverarbeitungsservers>:29000
Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen zur Authentifizierung für die JMX-Konsole ein (wenden Sie sich an den Systemadministrator, falls Sie nicht über diese Anmeldeinformationen verfügen).
2. Wählen Sie im Abschnitt **Topaz** den Eintrag **service=hac-backup** aus.
3. Suchen Sie nach **moveServices()** und geben Sie folgende Werte ein:
 - **customerId**. Die standardmäßige Kunden-ID für eine reguläre APM-Installation ist **1**. HPE Software-as-a-Service-Kunden müssen ihre Kunden-ID verwenden.
 - **srcServer**. Der Name des Quellservers, von dem aus Sie die Dienste verschieben.
 - **dstServer**. Der Name des Zielservers, auf den Sie die Dienste verschieben.

Verwenden Sie den Computernamen für diese beiden Parameter. Wenn Sie den Computernamen nicht genau kennen, können Sie mithilfe der oben beschriebenen **listservers**-Methode den Namen der bereits konfigurierten Computer ermitteln.

- **groupName**. Geben Sie keinen Wert für diesen Parameter ein.
4. Klicken Sie auf **Aufrufen**. Alle Dienste, die auf dem Quellserver ausgeführt werden, werden auf den Zielserver verschoben.
 5. Starten Sie die Online-Engine (MARBLE)-Prozesse, nachdem Sie diese auf den Zielserver verschoben haben, um sicherzustellen, dass das Modell synchronisiert bleibt.

Manuelles Neuzuweisen von Diensten

Achtung: Dieser Abschnitt richtet sich nur an erfahrene Benutzer.

Sie können ggf. Dienste, die auf einem primären Datenverarbeitungsserver ausgeführt werden, erneut manuell einem Sicherungsserver für die Datenverarbeitung zuweisen. Da ein Dienst immer nur auf einem Server für die Datenverarbeitung aktiv sein kann, müssen Sie entweder die bestehende Zuweisung entfernen oder deaktivieren, bevor Sie den Dienst einem anderen Server für die Datenverarbeitung neu zuweisen.

Um einen Dienst neu zuzuweisen, können Sie entweder eine neue Zuweisung hinzufügen oder eine bereits definierte, inaktive Zuweisung aktivieren.

Tipp: Sie können überprüfen, ob Dienste richtig neu zugewiesen, aktiviert oder deaktiviert wurden, indem Sie sich den Dienststatus in der JMX-Webkonsole ansehen. Details finden Sie unter "[Dienste, die dem Server zugewiesen werden](#)" auf Seite 90.

Entfernen der Zuweisung eines Diensts

Durch das Entfernen der Zuweisung eines Diensts wird der Eintrag aus der Tabelle HA_TASKS in der Verwaltungsdatenbank gelöscht. Er muss also als neue Zuweisung wieder hinzugefügt werden, wenn Sie den Dienst künftig verwenden möchten.

So entfernen Sie die aktuelle Zuweisung eines Diensts:

1. Öffnen Sie in einem Webbrowser:
http://<Computername des Datenverarbeitungsservers>:29000
Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen zur Authentifizierung für die JMX-Konsole ein (wenden Sie sich an den Systemadministrator, falls Sie nicht über diese Anmeldeinformationen verfügen).
2. Klicken Sie im Abschnitt **Topaz** auf **service=hac-manager**.
3. Geben Sie unter **removeAssignment()** die folgenden Daten ein:
 - **customer_id** Die standardmäßige Kunden-ID für ein einzelnes APM-System ist **1**. HPE Software-as-a-Service-Kunden sollten ihre Kunden-ID in diesem Feld verwenden.

Hinweis: Der Wert für **customer_id** für die Dienste PM und NOA ist immer **-1**, da diese Dienste dem System als Ganzes zugewiesen sind, und nicht einem bestimmten Kunden.

- **serviceName** Der Name der Diensts, für den Sie die aktuelle Zuweisung entfernen.

- **serverName** Der Name des Servers für die Datenverarbeitung, dem der Dienst gegenwärtig zugewiesen ist.
 - **processName** Der Name des Prozesses (z. B. **mercury_as**, **mercury_online_engine**, **mercury_offline_engine**, **topaz_pm**).
4. Klicken Sie auf **Aufrufen**. Die Zuweisung für den Dienst wird vom angegebenen Server für die Datenverarbeitung entfernt.

Ändern des Status eines zugewiesenen Diensts

Sie können die Zuweisung eines Diensts zu einem bestimmten Server für die Datenverarbeitung in der Tabelle HA_TASKS in der Verwaltungsdatenbank belassen, aktivieren oder deaktivieren Sie den Dienst jedoch, indem Sie den zugewiesenen Wert ändern.

Hinweis: Die Tabelle HA_TASK_ASSIGN früherer Versionen ist veraltet. Verwenden Sie die Tabelle HA_TASKS.

So ändern Sie den zugewiesenen Wert einer vorhandenen Zuweisung:

1. Öffnen Sie in einem Webbrowser:
http://<Computername des Datenverarbeitungsservers>:29000
Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen zur Authentifizierung für die JMX-Konsole ein (wenden Sie sich an den Systemadministrator, falls Sie nicht über diese Anmeldeinformationen verfügen).
2. Klicken Sie im Abschnitt **Topaz** auf **service=hac-manager**.
3. Geben Sie unter **changeAssignment()** die folgenden Daten ein:
 - **customerId**. Die standardmäßige Kunden-ID für eine reguläre APM-Installation ist **1**. HPE Software-as-a-Service-Kunden müssen ihre Kunden-ID verwenden.
Der Wert für **customer_id** für die Dienste PM und NOA ist immer **-1**, da diese Dienste dem System als Ganzes zugewiesen sind, und nicht einem bestimmten Kunden.
 - **serviceName** Der Name der Diensts, für den Sie den Zuweisungswert ändern.
 - **serverName** Der Name des Servers für die Datenverarbeitung, dem der Dienst zugewiesen ist.
 - **processName** Der Name des Prozesses.
 - **assignValue**. Der zugewiesene Wert für die Zuweisung. Jede Zahl zwischen -9 und 9 ist gültig. Mit dem Wert **1** wird die Zuweisung aktiviert. Jede andere Zahl deaktiviert die Zuweisung.
4. Klicken Sie auf **Aufrufen**. Die Zuweisung für den Dienst wurde entsprechend dem eingegebenen Wert für **assignValue** geändert.

Hinzufügen einer Zuweisung für einen Dienst

Sie können einem bestimmten Server für die Datenverarbeitung eine Zuweisung für einen Dienst hinzufügen und sie sofort aktivieren oder solange inaktiv belassen, bis sie benötigt wird. Dies ist nützlich, wenn Sie mit einem primären Server und einem Sicherungsserver für die Datenverarbeitung arbeiten. Zuweisungen für alle Dienste können für jeden Server erstellt werden, wobei die Zuweisungen zum primären Server für die

Datenverarbeitung aktiv sind, und die Zuweisungen zum Sicherungsserver für die Datenverarbeitung inaktiv sind.

So fügen Sie eine neue Zuweisung für einen Dienst hinzu:

1. Öffnen Sie in einem Webbrowser:
http://<Computernamen des Datenverarbeitungsservers>:29000
Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen zur Authentifizierung für die JMX-Konsole ein (wenden Sie sich an den Systemadministrator, falls Sie nicht über diese Anmeldeinformationen verfügen).
2. Klicken Sie im Abschnitt **Topaz** auf **service=hac-manager**.
3. Geben Sie unter **addAssignment()** die folgenden Daten ein:
 - **customer_id** Die ID des Kunden, dem der Dienst zugewiesen werden soll. Die standardmäßige Kunden-ID für ein einzelnes APM-System (also ein System, das nicht von HPE Software-as-a-Service verwaltet wird) ist **1**.

Hinweis: Der Wert für **customer_id** für die Dienste PM und NOA ist immer **-1**, da diese Dienste dem System als Ganzes zugewiesen sind, und nicht einem bestimmten Kunden.

 - **serviceName** Der Name des Diensts, den Sie zuweisen.
 - **serverName** Der Name des Servers für die Datenverarbeitung, dem der Dienst zugewiesen wird.
 - **processName** Der Name des Prozesses.
 - **assignValue**. Der zugewiesene Wert für die Zuweisung. Jede Zahl zwischen -9 und 9 ist gültig. Mit dem Wert **1** wird die Zuweisung aktiviert. Jede andere Zahl deaktiviert die Zuweisung.
4. Klicken Sie auf **Aufrufen**. Die Zuweisung für den Dienst wird dem angegebenen Server für die Datenverarbeitung hinzugefügt.

Manuelles Deaktivieren der Datenaggregatordienste

Der Datenaggregator kann in System Health deaktiviert werden (bevorzugte Methode). Wenn Sie jedoch Datenaggregatordienste deaktivieren müssen, aber entweder nicht über System Health verfügen oder die Applikation nicht verwenden können, können Sie dieses manuelle Verfahren ausführen.

So deaktivieren Sie die Dienste für die Offlineaggregation und die Engine für die Geschäftslogik auf dem Server für die Datenverarbeitung:

1. Wählen Sie **Admin > Plattform > Setup und Verwaltung > Infrastruktureinstellungen** und wählen Sie **Foundation** aus.
2. Wählen Sie **Offline-Aggregator** aus.
3. Bearbeiten Sie den Parameter **Aggregator ausführen**. Ändern Sie die Einstellung auf **False**. Die Änderung wird sofort wirksam.

Konfigurieren der APM-Daten-Collectoren in einer verteilten Umgebung

In diesem Abschnitt wird beschrieben, wie die HPE Application Performance Management-Daten-Collectoren für den Einsatz in einer verteilten Bereitstellung konfiguriert werden.

Business Process Monitor und Real User Monitor

Für die Funktionsfähigkeit von Business Process Monitor müssen Sie die URL des Gateway-Servers in der BPM Admin-Konsole-Applikation auf jedem Hostcomputer angeben, auf dem Business Process Monitor ausgeführt wird. Bearbeiten Sie den Eintrag für die URL des Gateway-Servers auf der Seite **Configure Instance** für jede Business Process Monitor-Instanz. Weitere Informationen finden Sie unter "Application Performance Management Registration Properties Area" im Business Process Monitor Administrator's Guide.

Für die Funktionsfähigkeit von Real User Monitor ist es für APM erforderlich, dass Sie die URL des Gateway-Servers in der Real User Monitor-Webkonsole angeben. Weitere Informationen hierzu finden Sie unter "APM Connection Settings" im Real User Monitor Administration Guide.

Geben Sie die Adresse des Gateway-Servers wie folgt an:

- Wenn Sie einen Gateway-Server installieren, geben Sie die URL dieses Computers an.
- Wenn Sie zwei oder mehr Gateway-Server in einem Cluster hinter einem Load Balancer installieren, geben Sie die URL des Load Balancer an.

Wenn Sie zwei Load Balancer für das Failover verwenden, geben Sie die URL von einem der Load Balancer an, und konfigurieren Sie die Hostnamen beider Load Balancer auf dem DNS-Servercomputer.

SiteScope

Für die Funktionsfähigkeit von SiteScope müssen Sie die URL des Gateway-Servers in jedem SiteScope-Profil angeben. Verwenden Sie dazu APM System Availability Management (**Admin > System Availability Management**). Weitere Informationen finden Sie unter "Konfigurieren der Verbindung" im SAM-Abschnitt im APM-Benutzerhandbuch.

Wenn Sie einen Load Balancer verwenden und virtuelle IPs oder URLs definiert haben, verwenden Sie die virtuellen IPs oder URLs für die Definition der URL des Gateway-Servers. Wenn Sie zwei Load Balancer für die Ausfallsicherung verwenden, geben Sie die URL von einem der Load Balancer an, und konfigurieren Sie die Hostnamen beider Load Balancer auf dem DNS-Servercomputer.

Weitere Informationen zur Konfiguration hoher Verfügbarkeit für SiteScope finden Sie im HPE SiteScope Failover Guide.

Anhang G: Deinstallation von APM 9.30

Verwenden Sie das folgende Verfahren, um APM vollständig zu deinstallieren.

Deinstallieren von APM-Servern in einer Windows-Umgebung

So deinstallieren Sie HPE Application Performance Management-Server in einer Windows-Umgebung vollständig:

1. Deinstallieren Sie APM über die Windows-Benutzeroberfläche oder unbeaufsichtigt.
 - a. Deinstallation von APM über die Windows-Benutzeroberfläche:
 - i. Wählen Sie auf dem Computer, von dem Sie HPE Application Performance Management deinstallieren, **Start > Einstellungen > Systemsteuerung > Programme und Funktionen** aus. Wählen Sie **HPE Application Performance Management**.
 - ii. Klicken Sie auf **Deinstallieren**, warten Sie, bis das APM-Deinstallationskript alle vorhandenen Updates entfernt hat, und befolgen Sie die Anweisungen auf dem Bildschirm.

Hinweis: In manchen Fällen kann dieser Vorgang einige Zeit in Anspruch nehmen (über 30 Minuten).
 - b. Unbeaufsichtigtes Deinstallieren von APM:
 - i. Beenden Sie alle APM-Server.
 - ii. Führen Sie den Befehl **<HPE APM-Installationsverzeichnis>\installation\bin\Uninstall.bat -i silent** aus.
2. Starten Sie den Servercomputer neu.
3. Wenn Sie APM mit Microsoft IIS verwenden, öffnen Sie den Internetdienste-Manager von IIS, und überprüfen Sie Folgendes:
 - a. Überprüfen Sie unter **Default Web Site**, ob die folgenden virtuellen Verzeichnisse entfernt wurden. Falls sie noch vorhanden sind, entfernen Sie sie:
 - o bpi
 - o bsm
 - o ext
 - o HPBSM
 - o jakarta
 - o mam_images
 - o mercuryam
 - o odb
 - o topaz
 - o tvb

- o ucmdb-ui
 - o uim
- b. Klicken Sie mit der rechten Maustaste in der Struktur auf den Servercomputernamen und wählen Sie **Properties** aus. Wenn im Dialogfeld **Properties** der Eintrag **WWW Service** in der Liste **Master Properties** angezeigt wird, klicken Sie auf **Edit**. Wählen Sie die Registerkarte **ISAPI Filters** aus. Wird der Filter **jakartaFilter** noch angezeigt, entfernen Sie ihn.

Hinweis: Wenn Sie APM deinstallieren und dann in einem anderen Verzeichnis auf dem Servercomputer neu installieren möchten, müssen Sie den Filter **jakartaFilter** nicht entfernen. Sie müssen jedoch den Pfad für den Filter aktualisieren. Details finden Sie unter "[Nach der Deinstallation von APM und einer Neuinstallation in einem anderen Verzeichnis funktioniert APM nicht](#)" auf Seite 115.

4. Rufen Sie den Windows-Registrierungs-Editor auf, indem Sie **Start > Ausführen** auswählen. Geben Sie **Regedit** ein.

Während der Installation wird der Wert für den Windows-Registrierungsschlüssel **HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ReservedPorts** so aktualisiert, dass er den folgenden Portbereich beinhaltet, der für APM erforderlich ist: 1098-1099, 8009-8009, 8080-8080, 4444-4444, 8083-8083, 8093-8093.

Diese Portbereiche werden während der Deinstallation nicht aus dem Registrierungsschlüssel entfernt. Sie sollten die Ports daher nach der Deinstallation von APM manuell aus dem Registrierungsschlüssel entfernen, wenn sie nicht mehr von einer anderen Applikation benötigt werden.

Tipp: Bei der Arbeit an der Registrierung empfiehlt es sich, sie zu sichern, bevor Sie Änderungen vornehmen.

Deinstallieren von APM-Servern in einer Linux-Umgebung

1. Melden Sie sich am Server als Benutzer **root** an.
2. Beenden Sie alle APM-Server.
3. Geben Sie für den Zugriff auf das Deinstallationsprogramm Folgendes ein: **cd /opt/HP/BSM/installation/bin**
4. Führen Sie das folgende Skript aus, um eine Deinstallation im UI-Modus auszuführen: **./uninstall.sh**. Zum Ausführen dieses Schritts im unbeaufsichtigten Modus verwenden Sie den Befehl **./uninstall.sh -i silent**.
5. Das APM-Deinstallationsprogramm beginnt. Folgen Sie den Anweisungen auf dem Bildschirm. Wenn das Deinstallationsprogramm abgeschlossen ist, wird eine Erfolgsmeldung angezeigt.
6. Klicken Sie auf **Finish**.

Hinweis: Wenn während der Deinstallation Probleme auftreten, wenden Sie sich an den HPE Support.

Deinstallieren von BSM-Servern vor der Installation von APM

Wenn Sie planen, APM 9.30 auf einem Computer zu installieren, auf dem eine BSM 9.2x-Version bereits vorhanden ist, müssen Sie die BSM 9.2x-Installation zuerst vollständig entfernen.

Hinweis: Die standardmäßige BSM-Deinstallation kann abhängig von der Anzahl der installierten Patches mehrere Stunden dauern. Um die Deinstallation zu beschleunigen, können Sie das BSM 9.2x Uninstall Tool ausführen. Dieses Tool verkürzt die Zeit der BSM-Deinstallation auf einige Minuten, da die vorhandene BSM-Installation mit Standardwerkzeugen des Betriebssystems entfernt wird.

So greifen Sie auf das BSM Uninstall Tool zu:

1. Wechseln Sie zur [HPE Software Support-Website](https://softwaresupport.hpe.com) (<https://softwaresupport.hpe.com>) und melden Sie sich an.
2. Klicken Sie auf **Patches**.
3. Suchen Sie nach **BSM 9.2x Uninstall Tool**.
4. Wählen Sie für Windows **BSM 9.2x Uninstall Tool for Windows**.
Wählen Sie für Linux **BSM 9.2x Uninstall Tool for Linux**.
5. Führen Sie nach Abschluss des BSM Uninstall Tools die Schritte 3 und 4 unter *Deinstallieren von BSM-Servern in einer Windows-Umgebung* unten aus. Diese Schritte enthalten Anweisungen zum IIS-Webserver und zur Windows-Registrierung.

Deinstallieren von BSM-Servern in einer Windows-Umgebung

So deinstallieren Sie HPE Business Service Management-Server in einer Windows-Umgebung vollständig:

1. Deinstallieren Sie BSM über die Windows-Benutzeroberfläche oder unbeaufsichtigt.
 - a. Deinstallation von BSM über die Windows-Benutzeroberfläche:
 - i. Wählen Sie auf dem Computer, von dem Sie HPE Business Service Management deinstallieren, **Start > Einstellungen > Systemsteuerung > Programme und Funktionen** aus. Wählen Sie **HPE Business Service Management** aus.
 - ii. Klicken Sie auf **Deinstallieren**, warten Sie, bis das BSM-Deinstallationskript alle vorhandenen Updates entfernt hat, und befolgen Sie die Anweisungen auf dem Bildschirm.

Hinweis: In manchen Fällen kann dieser Vorgang einige Zeit in Anspruch nehmen (über 30 Minuten).
 - iii. Wenn das Kontrollkästchen **Aktualisierungen anzeigen** aktiviert ist, werden alle über BSM installierten Aktualisierungen angezeigt. Wenn BSM entfernt wird, werden auch alle Aktualisierungen entfernt.
 - b. Unbeaufsichtigtes Deinstallieren von BSM:
 - i. Beenden Sie alle BSM-Server.

- ii. Führen Sie den Befehl **<HPBSM-Installationsverzeichnis>\installation\bin\Uninstall.bat -i silent** aus.
2. Starten Sie den Servercomputer neu.
3. Wenn Sie BSM mit Microsoft IIS verwenden, öffnen Sie den Internetdienste-Manager von IIS, und überprüfen Sie Folgendes:
 - a. Überprüfen Sie unter **Default Web Site**, ob die folgenden virtuellen Verzeichnisse entfernt wurden. Falls sie noch vorhanden sind, entfernen Sie sie:
 - o bpi
 - o bsm
 - o ext
 - o HPBSM
 - o jakarta
 - o mam_images
 - o mercuryam
 - o odb
 - o topaz
 - o tvb
 - o ucmdb-ui
 - o uim
 - b. Klicken Sie mit der rechten Maustaste in der Struktur auf den Servercomputernamen und wählen Sie **Properties** aus. Wenn im Dialogfeld **Properties** der Eintrag **WWW Service** in der Liste **Master Properties** angezeigt wird, klicken Sie auf **Edit**. Wählen Sie die Registerkarte **ISAPI Filters** aus. Wird der Filter **jakartaFilter** noch angezeigt, entfernen Sie ihn.

Hinweis: Wenn Sie BSM deinstallieren und dann in einem anderen Verzeichnis auf dem Servercomputer neu installieren möchten, müssen Sie den Filter **jakartaFilter** nicht entfernen. Sie müssen jedoch den Pfad für den Filter aktualisieren. Details finden Sie unter "[Nach der Deinstallation von APM und einer Neuinstallation in einem anderen Verzeichnis funktioniert APM nicht](#)" auf Seite 115.

4. Rufen Sie den Windows-Registrierungs-Editor auf, indem Sie **Start > Ausführen** auswählen. Geben Sie **Regedit** ein.

Während der Installation wird der Wert für den Windows-Registrierungsschlüssel **HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ReservedPorts** so aktualisiert, dass er den folgenden Portbereich beinhaltet, der für BSM erforderlich ist: 1098-1099, 8009-8009, 8080-8080, 4444-4444, 8083-8083, 8093-8093.

Diese Portbereiche werden während der Deinstallation nicht aus dem Registrierungsschlüssel entfernt. Sie sollten die Ports daher nach der Deinstallation von BSM manuell aus dem Registrierungsschlüssel entfernen, wenn sie nicht mehr von einer anderen Applikation benötigt werden.

Tipp: Bei der Arbeit an der Registrierung empfiehlt es sich, sie zu sichern, bevor Sie Änderungen vornehmen.

Deinstallieren von BSM-Servern in einer Linux-Umgebung

1. Melden Sie sich am Server als Benutzer **root** an.
2. Beenden Sie alle BSM-Server.
3. Geben Sie für den Zugriff auf das Deinstallationsprogramm Folgendes ein: **cd /opt/HP/BSM/installation/bin**
4. Führen Sie das folgende Skript aus, um eine Deinstallation im UI-Modus auszuführen: **./uninstall.sh**. Zum Ausführen dieses Schritts im unbeaufsichtigten Modus verwenden Sie den Befehl **./uninstall.sh -i silent**.
5. Das BSM-Deinstallationsprogramm beginnt. Folgen Sie den Anweisungen auf dem Bildschirm. Wenn das Deinstallationsprogramm abgeschlossen ist, wird eine Erfolgsmeldung angezeigt.
6. Klicken Sie auf **Finish**.
7. Überprüfen Sie die Protokolldatei **HPBsm_<Version>_HPOVInstaller.txt** im Verzeichnis **/tmp** auf Fehler. Dateien früherer Installationen befinden sich im Verzeichnis **/tmp/HPOVInstaller/HPBsm_<version>**.

Hinweis: Wenn während der Deinstallation Probleme auftreten, wenden Sie sich an den HPE Support.

Anhang H: Ändern von Benutzern des APM-Diensts

Dieser Anhang beschreibt das Verfahren zum Wechseln der mit APM verknüpften Benutzer unter Windows und Linux und enthält die folgenden Themen:

- ["Wechseln des Windows-Benutzers" auf Seite 108](#)
- ["Wechseln des Linux-Benutzers" auf Seite 109](#)

Wechseln des Windows-Benutzers

Der APM-Dienst zum Ausführen aller APM-Dienste und -Prozesse wird mithilfe des Dienstprogramms für das Setup und Datenbankkonfiguration installiert. Standardmäßig wird dieser Dienst mit dem lokalen Systembenutzer ausgeführt. Möglicherweise müssen Sie jedoch die Ausführung des Diensts einem anderen Benutzer zuweisen (wenn Sie z. B. die NTLM-Authentifizierung verwenden).

Der Benutzer, dem Sie die Ausführung des Diensts zuweisen, muss über die folgenden Berechtigungen verfügen:

- Ausreichende Datenbankberechtigungen (wie vom Datenbankadministrator definiert)
- Ausreichende Netzwerkberechtigungen
- Administratorberechtigungen auf dem lokalen Server

Hinweis: Der APM-Dienst wird als manueller Dienst installiert. Wenn Sie APM zum ersten Mal aktivieren, wird er zu einem automatischen Dienst.

So ändern Sie den Benutzer des APM-Dienstes:

1. Deaktivieren Sie APM (**Start > Alle Programme > HPE Application Performance Management > Verwaltung > HPE Application Performance Management deaktivieren**).
2. Doppelklicken Sie im Microsoft-Fenster **Dienste** auf **HP Bus Pro Mon**. Das Dialogfeld **Eigenschaften von HP BSM (Lokaler Computer)** wird geöffnet.
3. Klicken Sie auf die Registerkarte **Anmelden**.
4. Wählen Sie **Dieses Konto** aus und wählen Sie einen anderen Benutzer aus der Liste der gültigen Benutzer auf dem Computer aus.
5. Geben Sie das Windows-Kennwort des ausgewählten Benutzers ein und bestätigen Sie dieses Kennwort.
6. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern, und auf **OK**, um das Dialogfeld zu schließen.
7. Aktivieren Sie APM (**Start > Alle Programme > HPE Application Performance Management > Verwaltung > HPE Application Performance Management aktivieren**).

Hinweis: Dieser Vorgang muss wiederholt werden, wenn APM neu installieren oder aktualisieren.

Wechseln des Linux-Benutzers

APM muss so konfiguriert werden, dass es unter Linux mit einem bestimmten Benutzer ausgeführt wird. Dieser Benutzer kann entweder der root- oder ein anderer Benutzer sein. APM unterstützt immer nur einen Benutzer gleichzeitig. Der Benutzer wird mit dem Post-Installations-Assistenten definiert.

So wechseln Sie den Benutzer nach der APM-Installation:

1. Beenden Sie APM.
2. Starten Sie den Post-Installations-Assistenten erneut und geben Sie den neuen Benutzer an. Der Post-Installations-Assistent kann von folgendem Ort ausgeführt werden: **`/opt/HP/BSM/bin/postinstall.sh`**.
3. Melden Sie sich von Linux ab und melden Sie sich mit den neuen Benutzernamen an.
4. Führen Sie das Dienstprogramm für das Setup und die Datenbankkonfiguration aus.
Starten Sie das Dienstprogramm für das Setup und die Datenbankkonfiguration auf den Gateway- und den Datenverarbeitungsservern. Das Dienstprogramm für das Setup und die Datenbankkonfiguration kann im folgenden Speicherort ausgeführt werden: **`/opt/HP/BSM/bin/config-server-wizard.sh`**.
5. Starten Sie APM.

Anhang I: Wechseln von Webservern

Wenn Sie bereits APM installiert haben, und Ihren Webservertyp wechseln möchten, führen Sie die unten beschriebenen Schritte aus.

Hinweis: Wenn Sie die Smartcard-Authentifizierung aktiviert haben, und Ihren Webserver von Apache zu IIS oder umgekehrt wechseln möchten, müssen Sie zunächst die Smartcard-Authentifizierung deaktivieren. Sie können die Smartcard-Authentifizierung nach dem Wechseln des Webserver wieder aktivieren. Weitere Informationen zum Aktivieren und Deaktivieren der Smartcard-Authentifizierung finden Sie unter "Smartcard-Authentifizierung" im APM-Plattformverwaltungshandbuch.

1. Beenden Sie alle APM-Gateway- oder -Datenverarbeitungsserver. Details finden Sie unter "[Starten und Beenden von APM](#)" auf Seite 21.
2. Wenn Sie von IIS zu Apache wechseln, beenden Sie den IIS-Dienst oder wählen Sie im nächsten Schritt im Post-Installations-Assistenten einen anderen Port aus.
3. Wenn Sie von Apache zu IIS wechseln, konfigurieren Sie IIS. Weitere Informationen finden Sie unter:
 - Für Linux: "[Arbeiten mit dem Apache-Webserver](#)" auf Seite 51
 - Für Windows: "[Arbeiten mit dem IIS-Webserver](#)" auf Seite 44

4. Führen Sie den Post-Installations-Assistenten aus, und wählen Sie den neuen Typ des Webserver im entsprechenden Bildschirm aus.

Der Post-Installations-Assistent kann von folgendem Ort ausgeführt werden: **<HPE APM-Stammverzeichnis>\bin\postinstall.bat**. Wenn der Assistent jedoch vor Abschluss geschlossen wurde, verwenden Sie stattdessen die Datei **<HPE APM-Stammverzeichnis>/bin/ovii-postinstall.sh <TOPAZ_HOME>**, wobei **<TOPAZ_HOME>** das APM-Installationsverzeichnis (normalerweise **/opt/HP/BSM**) ist.

5. Starten Sie alle APM-Gateway- oder -Datenverarbeitungsserver.

Anhang J: Fehlerbehebung

Diese Anhang umfasst die folgenden Themen:

- [Ressourcen für die Fehlerbehebung](#) 112
- [Beheben von Installations- und Verbindungsproblemen](#) 113

Ressourcen für die Fehlerbehebung

- **Installationsprotokolldateien.** Details finden Sie unter "[Überprüfen der Installationsprotokolldateien](#)" auf [Seite 19](#).
- **Upgradeprotokollierungswerkzeug.** Führen Sie zum Anzeigen einer Übersicht über die Fehler, die während des Konfigurations-Upgrades im Upgrade-Assistenten aufgetreten sind, das Werkzeug zu Upgradeprotokollierung aus, das sich unter **<HPE APM-Stammverzeichnis>\tools\logTool\logTool.bat** befindet. Dadurch wird im selben Verzeichnis ein Report mit dem Namen **logTool.txt** generiert.
- **HPE-Wissensdatenbank zum Lösen von Softwareproblemen.** Weitere Informationen zur Fehlerbehebung finden Sie in der HPE-Wissensdatenbank zum Lösen von Softwareproblemen, über die Sie über die HPE Software Support-Website (<https://softwaresupport.hpe.com>) zugreifen können.
- **APM-Werkzeuge.** Sie können APM-Werkzeuge für die Fehlerbehebung in der HPE Application Performance Management-Umgebung verwenden. Die Werkzeuge befinden sich unter **<HPE APM-Stammverzeichnis>\tools**. Die meisten dieser Werkzeuge sollten nur in Abstimmung mit HPE-Mitarbeitern verwendet werden. Verwenden Sie das Programm zur Überprüfung des Datenbankschemas (**dbverify**) und das Dienstprogramm für Datenmarkierung entsprechend den Anweisungen in der jeweiligen Dokumentation.
- **APM Logging Administrator.** Dieses Werkzeug ermöglicht es Ihnen, den in APM-Protokollen angezeigten Detaillierungsgrad vorübergehend zu ändern und benutzerdefinierte Protokolle zu erstellen. Verwenden Sie zum Öffnen des APM Logging Administrator-Werkzeuges folgende URL:
http://<APM-Gateway-Server-FQDN>/topaz/logAdminBsm.jsp

Beheben von Installations- und Verbindungsproblemen

In diesem Abschnitt werden Probleme zusammen mit Lösungen beschrieben, die häufig bei der Installation von APM oder beim Herstellen einer Verbindung mit APM im Anschluss an die Installation auftreten können.

Der Zugriff auf APM unter Verwendung von Internet Explorer mit einem FQDN, der einen Domännennamen mit zwei Buchstaben enthält, ist nicht möglich

Internet Explorer unterstützt keine FQDNs mit Domännennamen, die nur zwei Buchstaben umfassen als standardmäßige virtuelle APM-URL (z. B. XXXX.aa).

Problemumgehung:

Wenn der FQDN einen Domännennamen mit nur zwei Buchstaben umfasst, verwenden Sie einen anderen Browser (nicht Internet Explorer) für den Zugriff auf APM.

Fehlermeldung beim Empfang: Zum Entpacken der Installationsdateien steht auf dem Laufwerk nicht ausreichend Speicherplatz zur Verfügung

Dies tritt während der Installation von Komponenten auf. Wenn Sie einen neuen Pfad für eine anderes Laufwerk mit ausreichend Speicherplatz angeben, wird die gleiche Fehlermeldung angezeigt.

Während die Dateien extrahiert werden, werden bestimmte Dateien immer im Verzeichnis **TEMP** auf dem Systemlaufwerk gespeichert, auch wenn Sie die Installationsdateien nicht im Standardpfad speichern.

Lösung:

- Schaffen Sie freien Speicherplatz auf dem Systemlaufwerk (wie in der Fehlermeldung angegeben). Setzen Sie dann die Installation fort.
- Wenn Sie auf dem Systemlaufwerk nicht für freien Speicherplatz sorgen können, ändern Sie den Pfad der Variablen **TEMP** des Systems.
 - **Windows:** Wählen Sie **Start > Einstellungen > Systemsteuerung > System**. Klicken Sie auf der Registerkarte **Erweitert** auf **Umgebungsvariablen** und bearbeiten Sie den Pfad für die Variable **TEMP** im Bereich der Benutzervariablen.
 - **Linux:** Führen Sie die folgenden Befehle aus:

```
export IATEMPDIR=/new/tmp
```

```
export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp
```

wobei /new/tmp das neue Arbeitsverzeichnis darstellt.

Die Installation schlägt aufgrund von Sicherheitsbeschränkungen des "/tmp"-Verzeichnisses unter Linux fehl

Wenn Sicherheitseinschränkungen des **/tmp**-Verzeichnisses die Skriptausführung verhindern, schlägt die Installation fehl.

Lösung:

Legen Sie durch Ausführen der folgenden Befehle ein neues **/tmp**-Verzeichnis fest, das nicht diesen Beschränkungen unterliegt:

```
export IATEMPDIR=/new/tmp  
export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp
```

wobei **/new/tmp** das neue Arbeitsverzeichnis darstellt.

Die Verbindung mit einer Microsoft SQL Server-Datenbank kann nicht hergestellt werden, wenn das Dienstprogramm für die Setup- und Datenbankkonfiguration ausgeführt wird

Überprüfen Sie, ob der Benutzer, mit dem der SQL Server-Dienst ausgeführt wird, über Schreibberechtigungen auf dem Datenträger verfügt, auf dem die Datenbank erstellt wird.

Eine Anmeldeaufforderung für das Netzwerk wird angezeigt, wenn eine APM-Serverinstallation abgeschlossen wird

Mögliche Ursache:

Dies kann eintreten, wenn als Authentifizierungsmethode für den IIS-Server nicht die Standardeinstellung **Anonymen Zugriff zulassen** festgelegt ist.

Lösung:

Setzen Sie die Authentifizierungsmethode des IIS-Servers auf die Standardeinstellung **Anonymen Zugriff zulassen** zurück und stellen Sie sicher, dass das Standardbenutzerkonto **IUSR_XXX** (wobei "XXX" für den Computernamen steht) ausgewählt ist (das Benutzerkonto **IUSR_XXX** wird während der IIS-Installation erzeugt). Deinstallieren Sie dann APM und installieren Sie das Programm anschließend erneut.

Servlet-Engine von Tomcat wird nicht gestartet und gibt einen Fehler aus

Die Fehlermeldung lautet wie folgt:

```
java.lang.reflect.InvocationTargetException: org.apache.tomcat.core.TomcatException: Root cause -  
Address in use: JVM_Bind
```

Mögliche Ursache:

Die Ausführung von Oracle HTTP-Server, der bei einer typischen Oracle-Installation installiert wird, auf demselben Computer wie die APM-Server führt zu einem Konflikt mit der Servlet-Engine von Tomcat.

Lösung:

Halten Sie den Oracle HTTP Server-Dienst an, deaktivieren und aktivieren Sie dann APM.

Damit das Problem nach einem Neustart nicht wieder auf dem Computer auftritt, ändern Sie die Starteinstellung für den Oracle HTTP Server-Dienst auf **Manuell**.

Aufgrund von Administratorbeschränkungen können APM-Komponenten nicht installiert werden

Mögliche Ursache:

Der Computer, auf dem Sie die Installation ausführen, verfügt über Software zur Richtlinienverwaltung, mit der der Zugriff auf Dateien, Verzeichnisse, die Windows-Registrierung usw. beschränkt wird.

Lösung:

Wenn diese Art von Software ausgeführt wird, wenden Sie sich an einen Mitarbeiter der Netzwerkadministration in Ihrem Unternehmen, um die erforderlichen Berechtigungen zum Installieren und Speichern von Dateien auf dem Computer zu bekommen.

Nach der Installation wird beim Zugriff auf APM der HTTP-Fehler 404 auf der Seite angezeigt

Führen Sie folgende Aktionen aus:

1. Überprüfen Sie, ob alle APM-Prozesse gestartet wurden, indem Sie die Statusseite aufrufen. Details finden Sie unter "How to View the Status of Processes and Services" im Handbuch APM-Plattformverwaltungshandbuch.
2. Wenn auf der Statusseite alle Services grün angezeigt werden, navigieren Sie über Port 29000 zu APM (<http://COMPUTERNAME:29000>).
Rufen Sie die JMX-Konsole auf. Wenn Sie die Konsole aufrufen können, fahren Sie mit Schritt 3 fort, um das Problem zu ermitteln.
3. Überprüfen Sie, ob der Webserver gestartet wurde (<http://COMPUTERNAME:8080>). Wenn der Webserver gestartet wurde, besteht wahrscheinlich ein Problem mit dem ISAPI-Filter.
4. Wenn das Problem beim ISAPI-Filter liegt und die Ausführung auf einem Server mit Microsoft Windows 2008 erfolgt, stellen Sie sicher, dass das Verfahren zum Erstellen einer Rolle ausgeführt wurde. Details finden Sie unter "[Arbeiten mit dem IIS-Webserver](#)" auf Seite 44.
5. Der Apache-Server kann möglicherweise aufgrund einer Portkollision nicht erfolgreich gestartet werden.

Nach der Deinstallation von APM und einer Neuinstallation in einem anderen Verzeichnis funktioniert APM nicht

Mögliche Ursache: Beim Deinstallieren und Neuinstallieren an einem anderen Speicherort wurde der ISAPI-Filter von IIS nicht mit dem neuen Pfad aktualisiert.

Lösung:

So aktualisieren Sie den ISAPI-Filter von IIS mit dem neuen Pfad:

1. Öffnen Sie den Internetdienste-Manager von IIS.
2. Klicken Sie mit der rechten Maustaste in der Struktur auf den Computernamen und wählen Sie **Properties** aus.

3. Wenn **WWW Service** in der Liste **Master Properties** angezeigt wird, klicken Sie auf **Edit**.
4. Wählen Sie die Registerkarte **ISAPI Filter** aus.
5. Stellen Sie sicher, dass **jakartaFilter** auf das richtige APM-Verzeichnis verweist.
6. Übernehmen Sie die Änderungen und beenden Sie den Internetdienste-Manager.
7. Starten Sie den IIS-Dienst neu.

Daten aus Business Process Monitor oder SiteScope werden nicht an APM gemeldet

Dieses Problem kann durch verschiedene Bedingungen verursacht werden. Details zu den Ursachen und den möglichen Lösungen finden Sie in der HPE-Wissensdatenbank zum Lösen von Softwareproblemen. Suchen Sie nach Artikelnummer KM438393. (<https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/KM438393>).

Business Process Monitor übermittelt keine Daten an den Gateway-Server mit IIS

Symptome/mögliche Ursachen:

- Keine Daten werden an Ladeprogramme übermittelt
- Website-Reports enthalten keine Daten
- Ein Fehler im Protokoll **data_deport.txt** auf dem Business Process Monitor-Computer, der wie folgt lautet:

```
Topaz returned an error (<html><head><title>Error Dispatching URL</title></head>
<body>
The URI:<br><b>api_reporttransactions_ex.asp</b><br/> is <b>not</b> mapped to an
API Adapter.<br>Either the URI is misspelled or the mapping file is incorrect
(the mapping file is located at:
D:\HPBAC\AppServer\TMC/resources/ServletDispatcher.xml)
</body>
</html>)
```

Das Problem kann überprüft werden, indem die folgende Seite `http://<Computername>/ext/mod_mdrv_wrap.dll?type=report_transaction` geöffnet wird. Liegt ein Problem vor, wird eine Meldung angezeigt, die besagt, dass ein Dienst vorübergehend nicht verfügbar ist.

Sie können auch die folgende URL übermitteln, um den Status der Webdatenerfassung zu überprüfen: `http://<Computername>/ext/mod_mdrv_wrap.dll?type=test`

Dieses Problem kann durch das Vorhandensein von **MercRedirectFilter** verursacht werden. Dies ist ein veralteter Filter, der für APM nicht mehr erforderlich ist und ein Überbleibsel früherer Versionen von APM sein kann.

Lösung:

Löschen Sie den Filter **MercRedirectFilter**, und stellen Sie sicher, dass **jakartaFilter** der einzige aktive ISAPI-Filter von IIS ist.

Business Process Monitor kann über das Internet keine Verbindung mit dem Gateway-Server herstellen, der mit Apache Web Server installiert ist

Mögliche Ursache:

Der Business Process Monitor-Computer kann den Namen des Gateway-Servers nicht richtig auflösen.

Lösung:

- Fügen Sie den Namen des Gateway-Servers zur Datei **<Stammverzeichnis des Windows-Systems>\system32\drivers\etc\hosts** auf dem Business Process Monitor-Computer hinzu.
- Ändern Sie den Namen des Gateway-Servers in der Datei **<HPE APM-Stammverzeichnis>\WebServer\conf\httpd.conf** auf dem Gateway-Server in einen Namen, der im DNS erkannt wird.

Beim Post-Installations-Assistenten tritt während der APM-Installation auf einem Linux-Computer ein Fehler auf

Dies kann auf einen Linux-Fehler zurückzuführen sein. Öffnen Sie die Datei **/etc/sysctl.conf**, und entfernen Sie die Zeile **vm.swappiness = 0**. Starten Sie den Post-Installations-Assistenten neu.

Adobe Flash Player kann nicht installiert werden

Adobe Flash Player wird mithilfe des Adobe Download Managers installiert, der keine Skripts für die automatische Proxy-Konfiguration verarbeiten kann. Wenn Internet Explorer für die Verwendung einer automatischen Proxy-Konfiguration konfiguriert ist, schlägt der Download Manager fehl, und es ist keine sichtbare Rückmeldung zu erkennen. Konfigurieren Sie einen Proxy-Host manuell, oder lesen Sie in der Flash Player-Dokumentation nach.

APM kann nicht gestartet werden bzw. der APM-Konfigurations-Assistent wird nicht geöffnet

Überprüfen Sie die Datei **supervisorwrapper.log** auf den folgenden Fehler:

<HPE APM-Stammverzeichnis>\conf\supervisor\manager\nannyManager.wrapper wrapper | OpenService fehlgeschlagen - Zugriff verweigert.

Wenn dieser Fehler vorliegt, kann das Problem möglicherweise darauf zurückgeführt werden, dass die Benutzerzugriffssteuerung (User Access Control, UAC) auf einem Windows-System aktiviert war. Deaktivieren Sie die UAC auf allen APM-Servern unter Windows.

Fehler bei der Anmeldung basierend auf FQDN

Wenn auf dem Anmeldebildschirm folgender Fehler angezeigt wird **Die HPE Application Performance Management-URL muss den vollqualifizierten Domänennamen (FQDN) enthalten. Geben Sie die HPE Application Performance Management-URL erneut in die Adressleiste ein** und Sie eine Verbindung über FQDN herstellen, überprüfen Sie, ob es eine DNS-Auflösung für virtuelle IP-Adressen mit Lastenausgleich von den APM-Gateways gibt. Möglicherweise müssen Sie der Hostdatei auf dem APM-

Gateway virtuelle IP-Adressen mit Lastenausgleich hinzufügen (ggf. für Applikationsbenutzer und für Daten-Collectoren).

Nach dem Klicken auf die Schaltfläche zum Anmelden passiert nichts, oder der Benutzer wird angemeldet, aber die Siteübersicht ist leer.

Mögliche Ursache:

Sie versuchen, sich bei APM über den Windows-Server statt den Clientcomputer anzumelden. Unter Windows Server ist die verstärkte Sicherheitskonfiguration für Internet Explorer normalerweise aktiviert. Mit dieser Konfiguration funktionieren einige APM-Benutzeroberflächenfunktionen, u. a. die APM-Anmeldeseite, möglicherweise nicht.

Lösung:

Überprüfen Sie, ob für Internet Explorer die verstärkte Sicherheitskonfiguration aktiviert ist. Wenn sie aktiviert ist, melden Sie sich über einen normalen Client an, nicht über den Windows-Server.

Wenn Sie die Anmeldung über den Server ausführen müssen, deaktivieren Sie die verstärkte Sicherheitskonfiguration für Internet Explorer (**Systemsteuerung > Windows-Komponenten hinzufügen/entfernen**), oder fügen Sie die APM-URL den vertrauenswürdigen Sites in den IE-Sicherheitseinstellungen hinzu.

Java-Applets werden nicht geöffnet

- Wählen Sie, wenn Sie Internet Explorer verwenden, **Extras > Internetoptionen > Verbindungen > LAN-Einstellungen** aus. Deaktivieren Sie die folgenden Optionen: **Automatische Suche der Einstellungen** und **Automatisches Konfigurationsskript verwenden**.
- Wählen Sie unter **Systemsteuerung > Java > Registerkarte Allgemein > Netzwerkeinstellungen** die Option **Direktverbindung** aus (und nicht die Standardoption **Browsereinstellungen verwenden**).

Bei der APM-Deinstallation treten Fehler auf

Wenn Fehler auftreten, die in etwa wie folgt lauten

Das Paket HPOv kann nicht deinstalliert werden.

können Sie diese Fehler ignorieren. APM wurde ordnungsgemäß deinstalliert.

Unleserliche ostasiatische Zeichen

Wenn Sie bei einigen RHEL6.x-Distributionen die APM-Installation in einem ostasiatischen Gebietschema (Koreanisch, Japanisch oder Vereinfachtes Chinesisch) ausführen, zeigt die Benutzeroberfläche der Installation unleserliche Zeichen an.

Probleumgehung:

Starten Sie das Installationsprogramm mit einer JRE, die ostasiatische Sprachen unterstützt.

```
setup.bin LAX_VM ${PATH_TO_JAVA}
```

Senden von Feedback zur Dokumentation

Wenn Sie Anmerkungen zu diesem Dokument haben, können Sie sich [per E-Mail an das Dokumentationsteam wenden](#). Ist auf Ihrem System ein E-Mail-Client installiert, klicken Sie auf den Link oben und ein E-Mail-Fenster mit folgendem Betreff wird geöffnet:

Feedback zu APM-Installationshandbuch (Application Performance Management 9.30)

Geben Sie Ihr Feedback ein und klicken Sie auf **Senden**.

Wenn kein E-Mail-Client verfügbar ist, kopieren Sie die oben genannten Informationen in eine neue Nachricht in einem Web-E-Mail-Client und senden Sie Ihr Feedback an Sw-doc@hpe.com.

Ihr Feedback ist willkommen!