Hewlett Packard
Enterprise

HPE Application Performance Management

Версия ПО: 9.30

Руководство по установке APM

Дата публикации: июль 2016 г.
Дата выпуска ПО: июль 2016 г.

Правовые уведомления

Гарантийные обязательства

Гарантии на продукты и услуги компании Hewlett Packard Enterprise формулируются только в заявлениях о прямой гарантии, сопровождающих эти продукты и услуги. Никакая часть настоящего документа не должна рассматриваться как дополнительные гарантийные обязательства. Компания HPE не несет ответственности за содержащиеся в них технические или редакционные ошибки.

Информация, содержащаяся в настоящем документе, может быть изменена без уведомления.

Пояснения в отношении ограниченных прав

Конфиденциальное компьютерное программное обеспечение. Для обладания, использования или копирования необходима действующая лицензия от компании HPE. В соответствии с положениями FAR 12.211 и 12.212 коммерческое программное обеспечение для компьютеров, документация программного обеспечения для компьютеров и технические данные коммерческих продуктов лицензируются государственным учреждениям США на условиях стандартной коммерческой лицензии поставщика.

Уведомление об авторских правах

Уведомление о товарных знаках

Adobe® и Acrobat® являются товарными знаками корпорации Adobe Systems Incorporated.

AMD и символ стрелки AMD являются товарными знаками Advanced Micro Devices, Inc.

Google™ и Google Maps™ являются товарными знаками корпорации Google Inc.

Intel®, Itanium®, Pentium® и Intel® Xeon® являются товарными знаками Intel Corporation в США и других странах.

iPod является товарным знаком корпорации Apple Computer, Inc.

Java является зарегистрированным товарным знаком корпорации Oracle и ее дочерних компаний.

Microsoft®, Windows®, Windows NT®, Windows Server® и Windows Vista™ являются товарными знаками или зарегистрированными товарными знаками корпорации Microsoft в США и других странах.

Oracle является зарегистрированным товарным знаком корпорации Oracle и ее дочерних компаний.

UNIX® является зарегистрированным торговым знаком The Open Group.

Обновление документации

На титульном листе этого документа приведена следующая информация:

- номер текущей версии программного обеспечения;
- дата публикации документа (изменяется при каждом обновлении документа);
- дата выпуска текущей версии программного обеспечения.

Чтобы проверить наличие обновлений или убедиться в том, что у вас последняя редакция документа, перейдите на сайт: https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=.

Для входа на этот сайт нужна учетная запись HPE Passport. Если у вас ее нет, нажмите кнопку **Create an account** на странице входа в HPE Passport.

Поддержка

Веб-сайт службы поддержки HPE Software находится по адресу: **https://softwaresupport.hpe.com**

Здесь вы найдете контактную информацию и подробные сведения о продуктах, услугах и поддержке, которые предоставляет HPE Software.

На веб-сайте службы поддержки HPE Software собраны ресурсы для самостоятельного решения проблем. Интерактивные инструменты технической поддержки помогут быстро и эффективно решать бизнес-задачи. На этом веб-сайте вы сможете:

- найти необходимые документы в базе знаний;
- подать и отследить заявку в службу технической поддержки, а также запросы на добавление функций;
- загрузить исправления программного обеспечения;
- управлять договорами поддержки;
- найти контактную информацию службы поддержки HPE;
- просмотреть сведения о доступных услугах;
- участвовать в обсуждениях с другими заказчиками;
- найти обучающие курсы по программному обеспечению и зарегистрироваться на них.

Чтобы получить доступ к большинству разделов поддержки, сначала необходимо зарегистрироваться в службе HPE Passport, а затем войти в свою учетную запись. Для ряда разделов также необходим договор на поддержку. Чтобы получить идентификатор HPE Passport, перейдите на страницу **https://softwaresupport.hpe.com** и щелкните **Register**.

Подробнее об уровнях доступа см. на странице:
https://softwaresupport.hpe.com/web/softwaresupport/access-levels

Решения, интеграции и практические рекомендации HPE Software

Посетите веб-сайт службы поддержки Hewlett Packard Enterprise Software (**https://softwaresupport.hpe.com/manuals**) и воспользуйтесь обширной подборкой практических рекомендаций.

Содержание

Введение

Добро пожаловать в руководство по установке APM. Данное руководство содержит подробные сведения о рабочем процессе установки APM

Это руководство предназначено для заказчиков, у которых не установлены предыдущие версии APM.

Если у вас установлена предыдущая версия APM, см. "Руководство по обновлению APM".

Структура руководства

Эта книга состоит из двух частей.

- Часть 1 содержит пошаговое описание процедуры установки APM.
- Часть 2 (приложение) содержит справочные данные и дополнительные процедуры.

Часть I: Процесс установки

Глава 1: Обзор установки APM 9.30

Установка APM 9.30 включает в себя следующие основные действия.

Глава 2: Общие предварительные требования

Перед началом установки выполните следующие действия:

1. Создание плана развертывания

Создайте полный план развертывания, включающий требования к программному обеспечению, оборудованию и список компонентов. Подробнее см. в руководстве по началу работы с APM и в документе "Требования к системе и таблицы поддержки APM".

2. Заказ и регистрация лицензий

Закажите у торгового представителя лицензии в соответствии с планом развертывания. Зарегистрируйте свою копию APM, чтобы получить доступ к службе технической поддержки и информации по всем продуктам HPE. Регистрация также дает право на обновление продукта. Зарегистрировать свою копию APM можно на сайте Служба поддержки HPE (https://softwaresupport.hpe.com).

3. Подготовка оборудования

Настройте серверы APM и сервер базы данных APM. Дополнительные сведения о настройке сервера базы данных см. в документе Руководство по базам данных APM.

4. Настройка веб-сервера (необязательно)

Во время установки APM устанавливает веб-сервер Apache на всех серверах шлюза APM. Если вы уже установили веб-сервер IIS и хотите использовать веб-сервер Apache, остановите службу **Веб-сервер IIS** перед установкой APM. Не изменяйте **Тип запуска** для этой службы. Не удаляйте роль **Веб-сервер IIS**. Чтобы использовать веб-сервер IIS, установите его на все серверы шлюза перед установкой APM.

Примечание. На компьютере может работать только один веб-сервер, использующий тот же порт, что и APM. Например, если во время установки сервера APM выбран HTTP-сервер Apache, а установка выполняется на компьютере, где уже работает сервер IIS, то перед началом установки нужно остановить службу IIS и установить для нее тип запуска **Вручную**. Подробнее см. в следующих разделах.

- Для Linux: Использование веб-сервера Apache на стр 51
- Для Windows: Использование веб-сервера IIS на стр 44

Требования к установке — Windows

Перед установкой серверов APM на платформе Windows следует обратить внимание на следующие условия.

- Рекомендуем устанавливать серверы APM на диск, имеющий не менее 40 ГБ свободного пространства. Подробнее о требованиях к системе см. в документе Системные требования и таблицы поддержки APM.
- Если серверы APM (в том числе серверы баз данных) устанавливаются в нескольких сегментах сети, настоятельно рекомендуем обеспечить минимальное число переходов между серверами и поддерживать минимально возможную задержку. Задержка в сети может негативно влиять на приложение APM и привести к проблемам с производительностью и стабильностью. Рекомендуем обеспечить задержку сети, не превышающую 5 миллисекунд независимо от числа переходов. Дополнительные сведения может предоставить Служба поддержки HPE.
- Серверы APM следует устанавливать на выделенных компьютерах, где не работают никакие другие приложения. Некоторые компоненты APM могут сосуществовать на серверах APM. Подробнее о поддержке сосуществования см. в документе Системные требования и таблицы поддержки APM.
- Чтобы использовать веб-сервер IIS, его нужно установить и включить на всех серверах шлюза перед установкой APM. Подробнее см. в разделе Использование веб-сервера IIS на стр 44.
- Серверы APM не следует устанавливать на диски, подключенные к локальным или сетевым ресурсам.
- В связи с определенными ограничениями веб-браузеров имена серверов шлюзов могут состоять только из букв или цифр (a–z, A–Z, 0–9), дефисов (-) и точек (.). Например, если имя сервера шлюза содержит знак подчеркивания, возможны проблемы с входом в систему APM через Microsoft Internet Explorer 7.0 или более поздних версий.
- При установке сервера APM можно задать другой путь к директории APM (по умолчанию это **C:\HPBSM**), при этом путь не должен содержать пробелов и не может быть длиннее 15 символов. Конечная папка должна называться **HPBSM**.
- Имя каталога установки может состоять только из букв и цифр (a–z, A–Z, 2–9).

  Примечание. Нельзя использовать цифры 0 и 1 в имени каталога установки

- Перед установкой APM необходимо отключить систему контроля доступа пользователей (UAC). Система контроля доступа включена по умолчанию в некоторых версиях Windows Server (например, 2008 SP2), поэтому ее нужно отключить вручную.
- Если планируется запуск серверов APM на платформе с повышенной безопасностью (в том числе с использованием протокола HTTPS), следует проанализировать процедуры безопасности, описанные в документе Руководство по повышению безопасности APM.
- В кластере APM откройте порт 21212 на сервере обработки данных.

Примечание. Во время установки обновляется параметр реестра Windows HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ReservedPorts — в него добавляются следующие диапазоны портов, необходимые для APM: 1098-1099, 2506-2507, 8009-8009, 29000-29000, 4444-4444, 8083-8083, 8093-8093.

Эти диапазоны портов не удаляются из реестра во время удаления APM. Их следует удалить из параметра реестра вручную после удаления APM, если они не нужны никаким другим приложениям.

Требования к установке — Linux

Перед установкой серверов APM на платформе Linux следует обратить внимание на следующие условия:

- Рекомендуем устанавливать серверы APM на диск, имеющий не менее 40 ГБ свободного пространства. Для каталога /tmp должно быть доступно как минимум 2,5 ГБ свободного пространства. Можно сменить каталог /tmp, выполнив следующую команду:

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

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

  Где `/new/tmp/dir` — это новый каталог /tmp.

  Подробнее о требованиях к системе см. в документе Системные требования и таблицы поддержки APM.

- Если серверы APM (в том числе серверы баз данных) устанавливаются в нескольких сегментах сети, настоятельно рекомендуем обеспечить минимальное число переходов между серверами и поддерживать минимально возможную задержку. Задержка в сети может негативно влиять на приложение APM и привести к проблемам с производительностью и стабильностью. Рекомендуем обеспечить задержку сети, не превышающую 5 миллисекунд независимо от числа переходов. Дополнительные сведения может предоставить Служба поддержки HPE.
- Серверы APM следует устанавливать на выделенных компьютерах, где не работают никакие другие приложения. Некоторые компоненты APM могут сосуществовать на серверах APM. Подробнее о поддержке сосуществования см. в документе Системные требования и таблицы поддержки APM.
- Перед установкой APM в системе Linux необходимо убедиться, что приложение SELinux его не заблокирует. Можно отключить SELinux либо настроить в нем запуск 32-битной версии java.

  Чтобы отключить SELinux, откройте файл **/etc/selinux/config**, задайте значение параметра **SELINUX=disabled** и перезапустите компьютер.

  На системах, где приложение SELinux отключено, параметр `SELINUX=disabled` настраивается в файле **/etc/selinux/config**:

  ```
  # Этот файл управляет работой SELinux в системе.
  # SELINUX= может принимать одно из трех следующих значений:
  #       enforcing – включена политика безопасности SELinux.
  #       permissive – SELinux вместо выполнения действия отображает предупреждения.
  #       disabled – полное отключение политик SELinux.
  SELINUX=disabled
  # SELINUXTYPE= может принимать одно из двух следующих значений:
  #       targeted – отслеживаемые процессы защищены.
  #       mls – многоуровневая система безопасности.
  SELINUXTYPE=targeted
  ```

  Кроме того, команда `getenforce` возвращает **Disabled**:

  ```
  ~]$ getenforce
  Отключено
  ```

  Чтобы гарантировать установку указанных выше пакетов, запустите программу rpm:

```
~]$ 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
```

До включения SELinux каждый файл файловой системы должен быть маркирован контекстом SELinux. До этого момента ограниченным доменам может быть отказано в доступе, что приведет к некорректной загрузке операционной системы.

Чтобы предотвратить такую ситуацию, задайте значение `SELINUX=permissive` в файле **/etc/selinux/config**:

```
# Этот файл управляет работой SELinux в системе.
# SELINUX= может принимать одно из трех следующих значений:
#       enforcing – включена политика безопасности SELinux.
#       permissive – SELinux вместо выполнения действия отображает предупреждения.
#       disabled – полное отключение политик SELinux.
SELINUX=permissive
# SELINUXTYPE= может принимать одно из двух следующих значений:
#       targeted – отслеживаемые процессы защищены.
#       mls – многоуровневая система безопасности.
SELINUXTYPE=targeted
```

Перезапустите систему от имени привилегированного пользователя. При следующей загрузке будут добавлены метки файловых систем. Метками контекста безопасности SELinux отмечаются все файлы:

```
~]# reboot
```

В режиме permissive политики безопасности SELinux отключены: информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не блокируются.

Прежде чем изменить режим на enforcing, выполните от имени привилегированного пользователя следующую команду, чтобы убедиться в том, что приложение SELinux не заблокировало никаких действий во время последней загрузки. Если SELinux не заблокировало действия во время последней загрузки, эта команда не возвращает никакого результата.

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

Если файл **/var/log/messages** не содержит никаких сообщений о заблокированных действиях, задайте значение `SELINUX=enforcing` в файле **/etc/selinux/config**:

```
# Этот файл управляет работой SELinux в системе.
# SELINUX= может принимать одно из трех следующих значений:
#       enforcing – включена политика безопасности SELinux.
#       permissive – SELinux вместо выполнения действия отображает предупреждения.
```

```
#       disabled – полное отключение политик SELinux.
SELINUX=enforcing
# SELINUXTYPE= может принимать одно из двух следующих значений:
#       targeted – отслеживаемые процессы защищены.
#       mls – многоуровневая система безопасности.
SELINUXTYPE=targeted
```

Перезагрузите систему. После перезагрузки убедитесь в том, что команда `getenforce` возвращает результат **Enforcing**:

```
~]$ 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
```

- Чтобы настроить запуск 32-битной версии java из SELinux, запустите команду **setsebool –P allow_execmod on**.
- Серверы APM не следует устанавливать на диски, подключенные к сетевым ресурсам.
- В связи с определенными ограничениями веб-браузеров имена серверов шлюзов могут состоять только из букв или цифр (a-z, A-Z, 0-9), дефисов (-) и точек(.). Например, если в имени сервера шлюза содержится знак подчеркивания, возможны проблемы с входом в систему APM. В этом случае для доступа к сайту BSM следует использовать IP-адрес, а не имя компьютера, содержащее знак подчеркивания.
- Если планируется запуск серверов APM на платформе с повышенной безопасностью (в том числе с использованием протокола HTTPS), следует проанализировать процедуры безопасности, описанные в документе Руководство по повышению безопасности APM.
- Чтобы установить APM на сервере, необходимы права привилегированного пользователя.
- Необходимо правильно настроить переменную среды **DISPLAY** на сервере APM. На компьютере, с которого происходит установка, должен быть включен X-Server, за исключением установки APM в автоматическом режиме. Подробнее см. в разделе Автоматическая установка APM на стр 64.
- В кластере APM откройте порт 21212 на сервере обработки данных.
- Прежде чем устанавливать APM 9.30 в операционных системах Oracle Linux (OEL) или Red Hat Enterprise Linux (поддерживаются версии 6.x и 7.x), нужно установить следующие пакеты RPM на всех компьютерах, где выполняется APM:

• glibc	• libXext
• glibc-common	• libXtst
• nss-softokn-freebl	• compat-libstdc++-33

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

Чтобы установить пакеты RPM, перечисленные в предыдущей таблице, запустите программу установки RPM на всех компьютерах, где выполняется APM:

<каталог_установки_APM>/rhel_oel_installation_fix/rpm_installer.sh.

- Если этот скрипт не может установит какой-либо из пакетов RPM, отображается следующее сообщение.

  ```
  !!! ERROR: package <имя пакета> has not been installed successfully

  In this case, refer the problem to your system administrator.
  ```

- Если пакет RPM уже установлен, скрипт пропускает этот пакет и устанавливает следующий.

  Однако можно попробовать принудительно повторно установить любой ранее установленный пакет, добавив параметр **f** в команду:

  <каталог_установки_APM>/rhel_oel_installation_fix/rpm_installer.sh

  Например:

  <каталог_установки_APM>/rhel_oel_installation_fix/rpm_installer.sh f

Если служба обновления Linux Yum не работает на вашем компьютере, нужно загрузить и установить необходимые пакеты RPM вручную с помощью следующей команды:

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

В различных системах используются разные версии этих пакетов. С сайта репозитория RPM можно загрузить пакеты RPM, которые соответствуют спецификациям версии вашей системы. Помочь в выполнении этой задачи может следующий инструмент поиска RPM (http://rpm.pbone.net/).

Чтобы определить версию пакета для загрузки, выполните следующую команду в окне терминала:

rpm –qa ${PACKAGE_NAME} (ex: rpm -qa glibc)

Результат выполнения команды выглядит следующим образом:

```
# rpm -qa glibc

glibc-2.12-1.132.el6.x86_64
```

В полученном результате указана версия пакета для установки на вашем компьютере.

В данном случае необходимо скачать и установить вручную пакет для архитектуры i686 версии glibc-2.12-1.132.el6.i686.

Глава 3: Установка APM 9.30

APM 9.30 устанавливается на наборе серверов. Этот набор может включать один сервер шлюза и один сервер обработки данных либо сервер на одном компьютере. В первом случае сначала запустите мастера на сервере обработки данных. Затем мастер сообщит, когда начинать установку на сервере шлюза.

Мастер установки сообщит, когда запускать мастер начальной настройки. После завершения работы мастера начальной настройки можно сразу автоматически запустить программу установки и настройки баз данных или отложить ее запуск.

Примечание. Если вы устанавливаете APM 9.30 на Windows Server 2008 R2 или 2012 R2:

1. В **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system** найдите параметр **Enable LUA** и смените его значение на **0**.
2. Перезагрузите компьютер.

Загрузите программное обеспечение

1. Перейдите на веб-сайт HPE SMTA (http://prssc.int.hpe.com/smta/smta.cgi) и войдите в учетную запись.
2. Рядом с пунктом **Release Name** выберите **APM0930** и нажмите кнопку **Search**.
3. Загрузите нужный ZIP-файл:
   - **HPE_APM_9.30_Windows_Setup.zip**
   - **HPE_APM_9.30_Linux_Setup.zip**
4. Распакуйте файл и запустите программу установки.

Запустите мастера установки и начальной настройки

- Установка APM на платформе Windows на стр 41
- Установка APM на платформе Linux на стр 49

Если доступно обновление, перейдите на веб-сайт службы поддержки HPE Software (https://softwaresupport.hpe.com) и загрузите нужное обновление.

Также можно запустить мастера установки и начальной настройки в автоматическом режиме. Подробнее см. в разделе Автоматическая установка APM на стр 64.

Примечание. Для мастеров обновления автоматический режим не поддерживается.

Глава 4: Процедуры, выполняемые после установки

В данной главе рассматриваются следующие темы:

Общая процедура, выполняемая после установки

Выполните эти задачи, чтобы завершить процесс установки.

- ## Обновление пользовательских KPI приложения Service Health

  В BSM изменился внутренний формат параметра KPI "KPI имеет критический статус, если". Поэтому, если вы создали пользовательские KPI, значение этого параметра после обновления может оказаться неправильным.

  Примечание. Для выполнения этого шага необходимо запустить APM.

  Чтобы решить эту проблему, выполните следующие действия.

  a. Откройте консоль JMX на сервере шлюза: http://<имя сервера шлюза>:29000/jmx-console, затем укажите имя пользователя и пароль.

  b. В разделе Topaz выберите **service=repositories_manager**.

  c. Найдите параметр **upgradeCriticalIf()** и введите в его поле значение **1** в качестве ID пользователя.

  d. Нажмите кнопку **Вызвать**.

- ## Удаление KPI OMi

  Если для бизнес-приложений, потоков бизнес-транзакций или бизнес-транзакций были назначены KPI, они будут повреждены, поскольку APM 9.30 не поддерживает OMi. Чтобы удалить поврежденные KPI, выполните следующие действия.

  a. Выполните синхронизацию для индикаторов работоспособности (**Администрирование > Service Health > Назначения > вкладка "Назначения индикаторов работоспособности"**).

  b. Выполните синхронизацию для KPI (**Администрирование > Service Health > Назначения > вкладка "Назначения KPI"**).

  c. В разделе "Типы КЕ" выберите **Корневой элемент** и нажмите кнопку **Синхронизировать тип КЕ** на каждой вкладке.

- ## Удаление временных файлов браузера

  При первом входе в систему APM после обновления следует удалить временные файлы браузера. Это касается всех браузеров, через которые осуществляется работа с APM.

- ## Отключение брандмауэра между серверами шлюза и обработки данных APM

  Размещение брандмауэров между серверами APM не поддерживается. Если на сервере APM (шлюза или обработки данных) включен брандмауэр операционной системы, необходимо оставить открытым канал для обмена данными между серверами шлюза и обработки данных APM.

  Кроме того, чтобы сборщики данных и пользователи APM могли взаимодействовать с серверами шлюза APM, следует оставить открытыми соответствующие порты в зависимости от вашей конфигурации APM. Как правило, это порты 443 (или 80) и 383. Подробнее см. в разделе "Использование портов" документа Руководство по администрированию платформы APM.

- ## Создание базы данных профилей

  После завершения работы мастеров установки создается схема базы данных профилей. Подробнее см. в разделе "Создание баз данных" документа Руководство по администрированию платформы APM.

- ## Загрузка дополнительных лицензий

  Главная лицензия APM вводится во время основного этапа установки APM, но для ряда приложений APM требуются дополнительные лицензии. Чтобы использовать эти приложения, необходимо получить лицензии от HPE. Подробнее см. на веб-сайте службы поддержки HPE Software (https://softwaresupport.hpe.com).

  Файлы лицензий передаются в диспетчер лицензий. Подробнее см. в разделе "Страница диспетчера лицензий" документа Руководство по администрированию платформы APM.

- ## Настройка LW-SSO, если балансировщик нагрузки размещается в отдельном домене

  Если используется балансировщик нагрузки, который находится в разных доменах с серверами, интегрируемыми с APM (например, NNMi, OO), необходимо изменить конфигурацию LW-SSO. Подробнее см. в разделе "Конфигурация LW-SSO для установки в нескольких доменах и вложенных доменах" документа Руководство по администрированию платформы APM.

- ## Выполнение процедур по повышению безопасности

  Чтобы защитить связь между серверами APM, выполните процедуру, описанную в разделе "Использование TLS в APM" документа Руководство по повышению безопасности APM.

- ## Проверка работы всех процессов

  Следует убедиться, что все процессы успешно запущены. Подробнее см. в разделе "Просмотр статуса процессов и служб" документа Руководство по администрированию платформы APM.

- ## Установка и настройка приложения "Работоспособность системы"

  System Health позволяет отслеживать производительность серверов, баз данных и сборщиков данных, работающих в системе APM, и контролировать их работоспособность. Рекомендуем устанавливать и настраивать System Health после развертывания серверов APM. Подробнее см. в разделе Руководство по приложению System Health.

- ## Проверка файлов журнала установки

  Чтобы просмотреть файл журнала установки, щелкните ссылку **Просмотреть файл журнала** в нижней части окна программы установки.

  В среде Windows этот файл вместе с другими файлами журнала для отдельных пакетов установки находится в каталоге **%temp%\..\HPOvInstaller\HPEApm_<версия>**.

  В среде Linux файлы журнала находятся в каталоге **/tmp/HPOvInstaller/HPEApm_<версия>**.

  Файл журнала программы установки имеет следующий формат:

HPEApm_<ВЕРСИЯ>_<ДАТА>_ HPOvInstallerLog.html или **HPEApm_<ВЕРСИЯ>_<ДАТА>_ HPOvInstallerLog.txt** (например, HPEApm_9.30_2016.05.23_15_48_HPOvInstallerLog.html).

Имена файлов журнала для отдельных пакетов установки имеют следующий формат:

Package_<ТИП_ПАКЕТА>_HPEApm_<ИМЯ_ПАКЕТА>_install.log (например, Package_msi_ HPEApm_BPMPkg_install.log).

Примечание. По умолчанию при перезагрузке сервера все файлы из папки **tmp** удаляются автоматически. Поэтому, установив APM, выполните резервное копирование всех файлов журналов перед перезагрузкой сервера

- ## Установка файлов для установки компонентов

Файлы установки компонентов служат для установки компонентов, используемых APM. Эти файлы не устанавливаются в процессе базовой установки APM. Их можно загрузить в отдельной области на веб-сайте и передать на страницу "Загружаемые компоненты APM" Затем файлы установки компонентов можно загружать из APM и использовать там, где они необходимы. Подробнее о работе со страницей "Загружаемые компоненты APM" см. в разделе "Загружаемые компоненты" документа Руководство по администрированию платформы APM.

Примечание.

- Компоненты на этой странице обновляются для каждого основной и вспомогательной версии (например, 9.00 и 9.20). Загрузить обновленные компоненты для вспомогательных версий и исправлений (например, 9.26) можно на веб-сайте службы поддержки HPE Software (https://softwaresupport.hpe.com).
- Чтобы установить компонент, можно запустить файл установки компонента непосредственно по сети. Подробнее об установке компонента см. в документации по нужному компоненту. Документация доступна на странице "Загружаемые компоненты" в APM после копирования файлов установки компонентов на эту страницу.

Чтобы установить файлы для установки компонентов, скопируйте файлы, которые должны быть доступны на странице "Загружаемые компоненты", из каталога в области загрузки версий в каталог **<корневой каталог HPE APM>\AppServer\webapps\site.war\admin\install** на сервере шлюза APM. При необходимости создайте структуру каталогов **admin\install**.

- ## Перезапуск APM

Перезапустите APM, отключив и включив все серверы. Подробнее см. в разделе Запуск и остановка APM на стр 21.

Запуск и остановка APM

Завершив установку сервера APM, перезагрузите компьютер. Рекомендуем сделать это как можно скорее. Обратите внимание: после перезагрузки компьютера необходимо войти в систему от имени того же пользователя, который был активен до перезагрузки.

Примечание. По умолчанию при перезагрузке сервера все файлы из папки **tmp** удаляются автоматически. Поэтому, установив APM, выполните резервное копирование всех файлов журналов перед перезагрузкой сервера.

После установки серверов APM (на одном компьютере или по одному экземпляру каждого типа сервера в распределенной среде) и подключения серверов к базам данных на каждом компьютере запускается APM.

Примечание. Чтобы проверить, какие серверы и компоненты APM установлены на компьютере APM, просмотрите раздел [INSTALLED_SERVERS] файла **<корневой каталог сервера APM>\conf\TopazSetup.ini**. Например, значение Data_Processing_Server=1 показывает, что на компьютере установлен сервер обработки данных.

Чтобы запустить или остановить APM в Windows, выполните следующие действия.

Выберите **Пуск > Все программы > HPE Application Performance Management > Администрирование > Включить | Отключить HPE Application Performance Management**. В распределенной среде сначала включите сервер обработки данных, а затем — сервер шлюза.

Чтобы запустить или остановить APM в Linux, выполните следующую команду:

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

Чтобы запустить, остановить или перезапустить APM с помощью скрипта демона, выполните команду:

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

Примечание. После остановки APM служба APM не удаляется из окна служб Microsoft. Эта служба удаляется только после удаления APM.

Вход и выход

Вход в APM выполняется со страницы входа в браузере на клиентском компьютере. По умолчанию в APM применяется стратегия проверки подлинности LW-SSO. Подробнее см. раздел "Вход в APM с LW-SSO" документа Руководство по администрированию платформы APM.

Можно полностью отключить проверку подлинности с единым входом или отключить LW-SSO и использовать другую поддерживаемую стратегию проверки подлинности. Сведения о выборе стратегии проверки подлинности см. в разделе "Установка стратегий проверки подлинности" документа Руководство по администрированию платформы APM.

Чтобы открыть страницу входа в APM и впервые войти в систему, выполните следующие действия.

1. В веб-браузере введите URL-адрес http://<имя_сервера>.<имя_домена>/HPBSM, где **имя_сервера** и **имя_домена** в совокупности представляют полное доменное имя сервера APM. Если используется несколько серверов или APM развернут в распределенной архитектуре, укажите соответственно URL-адрес балансировщика нагрузки или URL-адрес сервера шлюза.

   Примечание. Пользователи предыдущих версий BSM могут по-прежнему использовать созданные закладки для доступа по URL-адресу http://<имя_сервера>.<имя_домена>/mercuryam и http://<имя_сервера>.<имя_домена>/topaz

2. Введите имя администратора по умолчанию (admin) и пароль, указанный в программе установки и настройке базы данных, а затем нажмите кнопку **Вход**. После входа имя пользователя будет отображаться в правом верхнем углу экрана.
3. (Рекомендуем) Создайте несколько учетных записей для администраторов APM, чтобы они могли входить в систему. Подробнее о создании пользователей в системе APM см. в разделе "Управление пользователями" документа Руководство по администрированию платформы APM.

- Сведения об устранении проблем при входе в систему см. в разделе "Устранение неполадок и ограничения" документа Руководство по администрированию платформы APM.
- Сведения о различных стратегиях проверки подлинности при входе в APM см. в разделе "Стратегии проверки подлинности — обзор" документа Руководство по администрированию платформы APM.
- Подробнее о защищенном доступе к APM см. в документе Руководство по повышению безопасности APM.

После завершения сеанса рекомендуем выполнить выход с веб-сайта, чтобы предотвратить несанкционированное использование.

Чтобы выйти из системы, выполните следующие действия.

Нажмите кнопку **Выход** вверху страницы.

Добавление дополнительных серверов APM

Настроив рабочую среду APM 9.30, при необходимости можно добавить серверы шлюза и обработки данных.

Чтобы добавить новые серверы APM в существующую среду, выполните следующие действия.

1. Перейдите на веб-сайт HPE SMTA (http://prssc.int.hpe.com/smta/smta.cgi) и войдите в учетную запись.
2. Рядом с пунктом **Release Name** выберите **APM0930** нажмите кнопку **Search**.
3. Загрузите нужный ZIP-файл
   - **HPE_APM_9.30_Windows_Setup.zip**
   - **HPE_APM_9.30_Linux_Setup.zip**
4. Распакуйте файл и выполните программу установки на всех серверах APM (серверы шлюза и обработки данных).
5. Запустите программу установки и настройки базы данных.
   - **Windows:** на сервере APM выберите **Пуск > Все программы > HPE Application Performance Management > Администрирование > Настройка HPE Application Performance Management**. Также можно запустить файл непосредственно из расположения **<корневой каталог HPE APM>\bin\config-server-wizard.bat**.
   - **Linux:** на сервере APM откройте командную строку терминала и запустите сценарий **/opt/HP/BSM/bin/config-server-wizard.sh**.

   Подробнее об этой программе см. в разделе Развертывание сервера и настройка параметров базы данных на стр 54.
6. Перезапустите все серверы APM.

   После установки дополнительных серверов перезапустите все серверы APM и сборщики данных, чтобы они распознали новые серверы.

Глава 5: Настройка безопасного доступа к обратному прокси-серверу APM

В этом разделе описывается влияние прокси-серверов на обеспечение безопасности, а также предоставляются инструкции по их использованию с APM.

В данной главе рассматривается только аспекты безопасности использования прокси-серверов. Здесь не затрагиваются другие вопросы работы обратных прокси-серверов, например кэширование и балансировка нагрузки.

Обратный прокси-сервер — это промежуточный сервер, который размещается между клиентским компьютером и веб-сервером. Для клиентского компьютера обратный прокси-сервер выглядит как стандартный веб-сервер, который обслуживает запросы по протоколам HTTP и HTTPS и не требует особой настройки для каждого клиента.

Клиентский компьютер отправляет исходные запросы веб-содержимого, используя имя обратного прокси-сервера вместо имени веб-сервера. Затем обратный прокси-сервер отправляет запросы на один из веб-серверов. Веб-сервер отправляет ответы на клиентский компьютер через обратный прокси-сервер, однако для клиентского компьютера эти ответы выглядят так, будто были отправлены обратным прокси-сервером.

APM поддерживает работу с обратными прокси-серверами в архитектуре DMZ. Обратный прокси-сервер является HTTP или HTTPS-посредником между сборщиками данных и пользователями приложений APM и серверами APM.

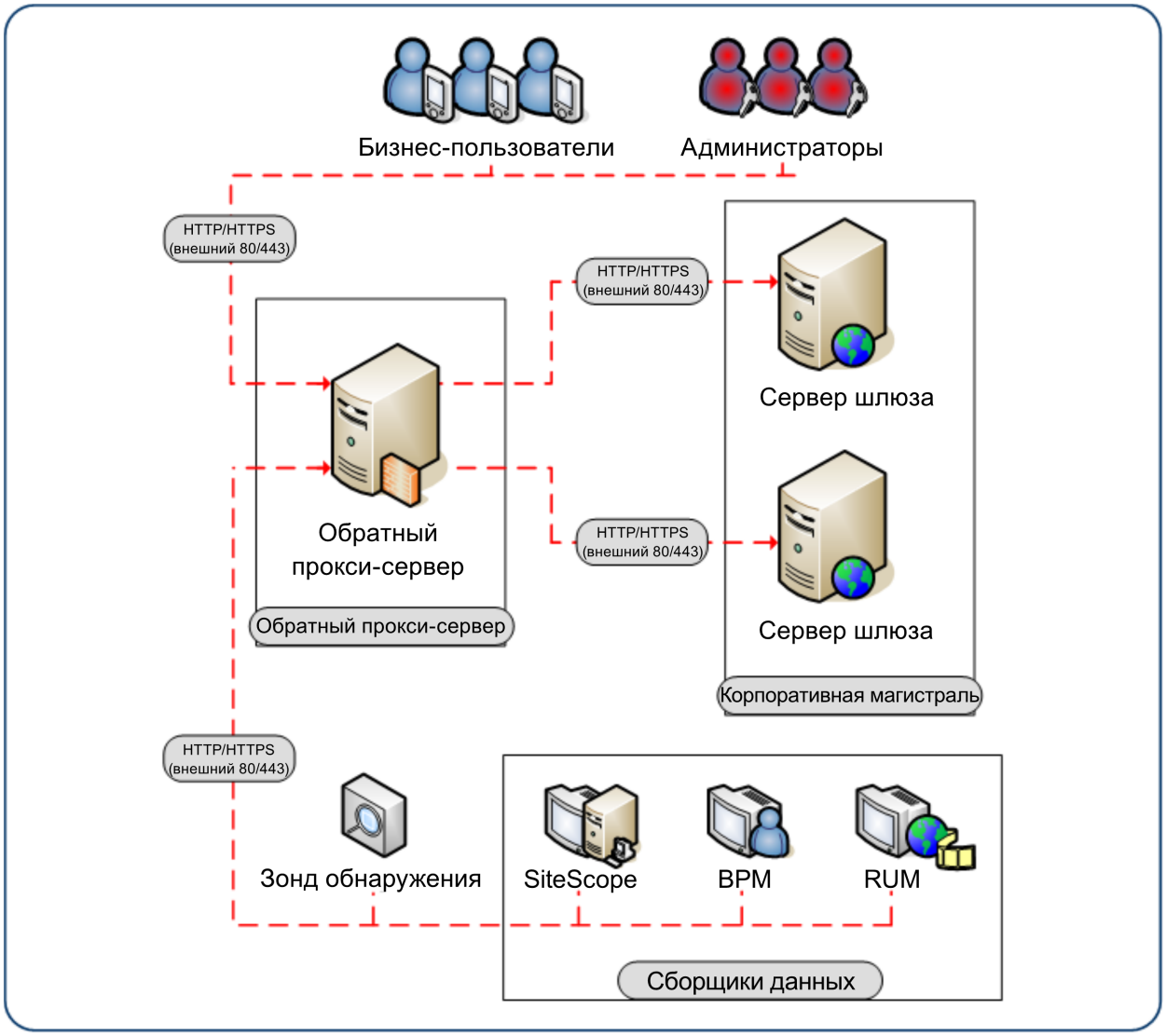
Сборщики данных могут получать доступ к APM через тот же или другой виртуальный хост, что и пользователи приложений.

Настройка обратного прокси-сервера

В этой топологии контекст обратного прокси-сервера состоит из двух разделов.

- Подключения, перенаправляемые на виртуальный хост для сборщиков данных.
- Подключения, перенаправляемые на виртуальный хост для пользователей приложений.

Использование обратного прокси-сервера показано на следующей схеме. Сборщики данных могут получать доступ к APM через тот же или другой виртуальный хост, что и пользователи приложений. Например, в среде используется один балансировщик нагрузки для пользователей приложений и еще один — для сборщиков данных.



Обратный прокси-сервер APM следует настраивать по разному в каждом из следующих случаев.

Сценарий №	Компоненты APM за обратным прокси-сервером
1	Сборщики данных (Business Process Monitor, Real User Monitor, SiteScope, зонд потока данных)
2	Пользователи приложений
3	Сборщики данных и пользователи приложений

Последовательность действий по настройке обратного прокси-сервера

В этом разделе рассмотрена общая последовательность действий по настройке обратного прокси-сервера на работу с серверами APM. Процедура отличается в зависимости от веб-сервера обратного прокси-сервера.

1. Если в качестве обратного прокси-сервера используется балансировщик нагрузки, то настраивать дополнительный обратный прокси-сервер не нужно. Подробнее см. в разделе Балансировка нагрузки для сервера шлюза на стр 87.
2. Выполните соответствующую процедуру в зависимости от того, какой веб-сервер использует ваш обратный прокси-сервер: Apache или IIS.

   Apache. Настройка обратного прокси-сервера — Apache на стр 27.

   IIS. Настройка обратного прокси-сервера — IIS на стр 32.
3. Настройте APM для поддержки обратного прокси-сервера. Подробнее см. в разделе Особая конфигурация HPE APM на стр 35.

Настройка обратного прокси-сервера — Apache

В этом разделе описывается, как настроить обратный прокси-сервер с помощью веб-сервера Apache версий 2.2.x.

Примечание. Настройка безопасного доступа к обратному прокси-серверу должна выполняться как часть рабочего процесса по повышению безопасности. Подробнее см. в разделе "Рабочий процесс по повышению безопасности" документа "Руководство по повышению безопасности".

В этом разделе рассматриваются следующие темы.

Настройка Apache для работы в качестве обратного прокси-сервера

Примечание. Настройка безопасного доступа к обратному прокси-серверу должна выполняться как часть рабочего процесса по повышению безопасности. Подробнее см. в разделе "Рабочий процесс по повышению безопасности" документа "Руководство по повышению безопасности".

1. Настройте Apache для работы в качестве обратного прокси-сервера.

   Чтобы Apache работал в качестве обратного прокси-сервера, его нужно настроить вручную.

   Например:

   a. Откройте файл <каталог установки Apache>\Webserver\conf\httpd.conf.

   b. Включите следующие модули:
      - LoadModule proxy_module modules/mod_proxy.so
      - LoadModule proxy_http_module modules/mod_proxy_http.so

   c. Добавьте следующие строки:

```
ProxyRequests off

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

2. Настройте поддержку для пользователей приложений и сборщиков данных, как показано в следующем примере. Подробнее см. Справочные материалы. Поддержка пользователей приложений APM на стр 29 и Справочные материалы. Поддержка сборщиков данных APM на стр 31.

Сборщики данных:

```
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
```

Пользователи приложений:

```
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
```

Примечание. При использовании IDM-SSO, возможно, потребуется добавить следующие строки (замените в строках ниже слово siteminderagent на имя вашего поставщика IDM-SSO):

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

3. Проверьте, что обратный прокси-сервер указывает на APM.
   - Перезапустите Apache
   - Перейдите по адресу http://<RP>/topaz, чтобы проверить видимость страницы входа APM. При вводе учетных данных отображается пустая страница, поскольку система APM еще не настроена на работу с обратным прокси-сервером.

Справочные материалы. Поддержка пользователей приложений APM

Следующую таблицу можно использовать как справочный материал для пользователей приложений, подключающихся через обратный прокси-сервер.

Запросы на... на обратном прокси-сервере	**Запрос к прокси-серверу выполняет:**
/hpbsm/*	http://[виртуальный хост для пользователей приложений]/hpbsm/* https://[виртуальный хост для пользователей приложений]/hpbsm/*
/excite/*	http://[виртуальный хост для пользователей приложений]/excite/* https://[виртуальный хост для пользователей приложений]/excite/*
/excite-runtime/*	http://[виртуальный хост для пользователей приложений]/excite-runtime/* https://[виртуальный хост для пользователей приложений]/excite-runtime/*
/filters/*	http://[виртуальный хост для пользователей приложений]/filters/* https://[виртуальный хост для пользователей приложений]/filters/*
/mam/*	http://[виртуальный хост для пользователей приложений]/mam/* https://[виртуальный хост для пользователей приложений]/mam/*
/mam_images/*	http://[виртуальный хост для пользователей приложений]/mam_images/* https://[виртуальный хост для пользователей приложений]/mam_images/*
/mcrs/*	http://[виртуальный хост для пользователей приложений]/mcrs/* https://[виртуальный хост для пользователей приложений]/mcrs/*
/mercuryam/*	http://[виртуальный хост для пользователей приложений]/mercuryam/* https://[виртуальный хост для пользователей приложений]/mercuryam/*

Запросы на... на обратном прокси-сервере	**Запрос к прокси-серверу выполняет:**
/odb/*	http://[виртуальный хост для пользователей приложений]/odb/* https://[виртуальный хост для пользователей приложений]/odb/*
/opal/*	http://[виртуальный хост для пользователей приложений]/opal/* https://[виртуальный хост для пользователей приложений]/opal/*
/OVPM/*	http://[виртуальный хост для пользователей приложений]/OVPM/* https://[виртуальный хост для пользователей приложений]/OVPM/*
/rumproxy/*	http://[виртуальный хост для пользователей приложений]/rumproxy/* https://[виртуальный хост для пользователей приложений]/rumproxy/*
/topaz/*	http://[виртуальный хост для пользователей приложений]/topaz/* https://[виртуальный хост для пользователей приложений]/topaz/*
/TopazSettings/*	http://[виртуальный хост для пользователей приложений]/TopazSettings/* https://[виртуальный хост для пользователей приложений]/TopazSettings/*
/ucmdb-api/*	http://[виртуальный хост для пользователей приложений]/ucmdb-api/* https://[виртуальный хост для пользователей приложений]/ucmdb-api/*
/ucmdb-ui/*	http://[виртуальный хост для пользователей приложений]/ucmdb-ui/* https://[виртуальный хост для пользователей приложений]/ucmdb-ui/* Примечание. Если используется обратный прокси-сервер и настроена интеграция с HPE Universal CMDB, значение таймаута для обратного прокси-сервера должно составлять не менее 1000 секунд. Например, в конфигурационном файле обратного прокси-сервера http.conf измените строку, которая задает значение параметра ProxyPass: ProxyPass /ucmdb-ui http://<сервер шлюза APM>/ucmdb-ui connectiontimeout=1000 timeout=1000
/uim/*	http://[виртуальный хост для пользователей приложений]/uim/* https://[виртуальный хост для пользователей приложений]/uim/*
/webinfra/*	http://[виртуальный хост для пользователей приложений]/webinfra/* https://[виртуальный хост для пользователей приложений]/webinfra/*

Справочные материалы. Поддержка сборщиков данных APM

Следующую таблицу можно использовать как справочный материал для сборщиков данных, подключающихся через обратный прокси-сервер.

Запрос на... на обратном прокси-сервере	**Запрос к прокси-серверу выполняет:**
/topaz/topaz_api/*	http://[виртуальный хост для пользователей приложений]/topaz_api/* https://[виртуальный хост для пользователей приложений]/topaz_api/*
/topaz/sitescope/*	http://[виртуальный хост для пользователей приложений]/topaz/sitescope/* https://[виртуальный хост для пользователей приложений]/topaz/sitescope/*
/ext/*	http://[виртуальный хост для пользователей приложений]/ext/* https://[виртуальный хост для пользователей приложений]/ext/*
/cm/*	http://[виртуальный хост для пользователей приложений]/cm/* https/[виртуальный хост для пользователей приложений]/cm/*
/mam-collectors/*	http://[виртуальный хост для пользователей приложений]/mam-collectors/* https/[виртуальный хост для пользователей приложений]/mam-collectors/*
/axis2/*	http://[виртуальный хост для пользователей приложений]/axis2/* https://[виртуальный хост для пользователей приложений]/axis2/* **Примечание.** Обязательно, если адаптер SOAP со встроенной моделью обслуживания во время выполнения (RTSM) используется для репликации через обратный прокси-сервер на защищенный сервер APM.

Примечание.

- Убедитесь в том, что ваш обратный прокси-сервер поддерживает логику обработки согласно приоритетам, когда при необходимости сначала обрабатывается более точное выражение, а потом более общее. Например, выражение **/topaz/topaz_api/*** должно быть обработано раньше выражения **/topaz/***.
- Для некоторых прокси-серверов также требуется указать обратный путь. При использовании обратного пути возвращаемые сервером заголовки HTTP и HTTPS меняются на относительные. Пример использования обратного пути см. в разделе Настройка Apache для работы в качестве обратного прокси-сервера на стр 27.

Настройка обратного прокси-сервера — IIS

В этом разделе рассматривается, как настроить обратный прокси-сервер с помощью веб-сервера IIS. Описания всех действий, которые выполняются в других программных продуктах кроме APM, предоставляются исключительно в ознакомительных целях.

Примечание. Настройка безопасного доступа к обратному прокси-серверу должна выполняться как часть рабочего процесса по повышению безопасности. Подробнее см. в разделе "Рабочий процесс по повышению безопасности" документа "Руководство по повышению безопасности".

В этом разделе рассматриваются следующие темы.

Настройка IIS для работы в качестве обратного прокси-сервера на стр 32

Настройте обратный прокси-сервер IIS на использование протокола SSL. на стр 33

Настройка IIS на проверку подлинности клиентов (необязательно) на стр 34

Настройка IIS для работы в качестве обратного прокси-сервера

Процедура может отличаться в зависимости от версии IIS.

Например:

1. Установите расширение маршрутизации запросов приложений (ARR). Подробнее см. по адресу http://www.iis.net/downloads/microsoft/application-request-routing.
2. Откройте диспетчер IIS.
3. Создайте новый веб-сайт IIS или используйте веб-сайт по умолчанию.
4. Создайте новую ферму сервера IIS и назовите ее APM.
   a. Добавьте в ферму новый сервер с IP-адресом вашего сервера шлюза APM.
   b. При появлении запроса разрешите создать правило переопределения URL-адресов.
5. Включите сервер IIS в качестве прокси-сервера.
   a. Выберите основной узел дерева (имя сервера), щелкните "Кэш маршрутизации запросов приложения" а затем выберите "Настройки прокси-сервера".
   b. Установите флажок **Включить прокси-сервер**.
   c. Установите для параметра **Версия HTTP** значение **Пропустить**.
   d. Установите флажок **Обратная перезапись хоста в заголовках ответов**.
   e. Нажмите кнопку **Применить**.
6. Проверьте, что обратный прокси-сервер указывает на APM.

   Перейдите по адресу http://<полное доменное имя хоста обратного прокси-сервера>/topaz, чтобы проверить видимость страницы входа APM. При вводе учетных данных отображается пустая страница, поскольку система APM еще не настроена на работу с обратным прокси-сервером.

Настройте обратный прокси-сервер IIS на использование протокола SSL.

Примечание. Настройка безопасного доступа к обратному прокси-серверу должна выполняться как часть рабочего процесса по повышению безопасности. Подробнее см. в разделе *Рабочий процесс по повышению безопасности* документа "Руководство по повышению безопасности".

1. На обратном прокси-сервере установите отношение доверия с ЦС, который выдал сертификат сервера.

   С помощью консоли управления Microsoft импортируйте корневой сертификат ЦС, выпустивший сертификат для данного сервера, в хранилище доверенных сертификатов.

   Например:

   a. На обратном прокси-сервере откройте консоль управления Microsoft (**Выполнить> mmc**).
   b. Добавьте оснастку (**Файл > Добавить/Удалить оснастку**).
   c. Выберите "Сертификаты" и щелкните **Добавить**.
   d. Выберите "Учетная запись компьютера" и нажмите **Далее**.
   e. Выберите "Локальный компьютер" и нажмите **Далее**.
   f. Нажмите кнопку **ОК**.
   g. Импортируйте сертификат.

      Импортируйте ca.cer в список доверенных центров сертификации.

2. Импортируйте сертификат сервера в консоль управления Microsoft.

   Импортируйте ранее полученный сертификат в "Личные > Сертификаты" в консоли управления Microsoft.

3. Включите протокол SSL на IIS.

   Например:

   a. В диспетчере IIS выберите свой веб-сайт.
   b. На панели действий выберите **Привязки**.
   c. Добавьте для HTTPS привязку к порту 443.
   d. Укажите сертификат вашего сервера в поле "SSL-сертификат".

4. Настройте обратный прокси-сервер на обязательное использование протокола SSL.

   Например:

   a. В диспетчере IIS выберите свой веб-сайт, а затем выберите **Настройки SSL**.
   b. Проверьте, что установлен флажок **Требовать SSL**.

5. Настройка SSL в SSL Offloading

   Если SSL-соединение прерывается на обратном прокси-сервере, выполните следующие действия.

a. Выполните следующую команду, чтобы разрешить IIS пропускать большие выборки данных (1 МБ).

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

b. В диспетчере IIS выберите основной узел дерева (имя сервера) > щелкните "Кэш маршрутизации запросов приложения" а затем выберите "Настройки прокси-сервера".

c. Проверьте, что установлен флажок **включить разгрузку SSL**.

Настройка IIS на проверку подлинности клиентов (необязательно)

1. Создайте заново привязку SSL, чтобы включить согласование клиента.

   Предыдущая привязка будет работать, но может вызвать проблемы производительности. Новая привязка включает согласование, что увеличивает производительность при проверке подлинности клиента.

   a. В пользовательском интерфейсе диспетчера IIS удалите текущую привязку.

   b. Выполните следующую команду на сервере IIS:

   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=<хэш сертификата сервера> appid={00112233-4455-6677-8899-AABBCCDDEEFF} clientcertnegotiation=enable

   > **Примечание.** Узнать хэш сертификата можно в консоли управления Microsoft, просмотрев отпечаток в сведениях о сертификате.

2. Настройте обратный прокси-сервер на обязательное использование сертфиката клиента.

   Например:

   a. В диспетчере IIS выберите свой веб-сайт, а затем выберите **Настройки SSL**.

   b. В **Сертификаты клиентов** выберите **Требовать**.

3. Укажите заголовок, который обратный прокси-сервер передает APM для проверки подлинности сертификата клиентов в кодировке Base64.

   Например:

   a. В диспетчере IIS выберите свою ферму, а затем выберите **Прокси-сервер**.

   b. Установите флажок **Обратная перезапись хоста в заголовках ответов**.

   c. В поле **передавать закодированные сертификаты клиентов в следующем заголовке**, введите имя заголовка **CLIENT_CERT_HEADER**.

   d. Нажмите **Применить**.

Особая конфигурация HPE APM

Кроме настройки обратного прокси-сервера на работу с APM необходимо настроить APM на работу с обратным прокси-сервером.

Примечание. APM следует настраивать только в том случае, если пользователи приложений подключаются к APM через обратный прокси-сервер. Если обратный прокси-сервер используется только для работы сборщиков данных, инструкции, приведенные в этом разделе, можно пропустить.

Настройка APM на работу с обратным прокси-сервером.

1. Выберите **Администрирование > Платформа > Установка и обслуживание > Настройки инфраструктуры**. Нажмите **Базовые настройки** и выберите контекст **Администрирование платформы** из раскрывающегося меню.
2. В области "Администрирование платформы — Конфигурация хостов" задайте следующие параметры.
   - **"URL-адрес виртуального сервера шлюза по умолчанию для пользователей приложений" и "URL-адрес локального виртуального сервера шлюза для сборщиков данных".** Проверьте, что данные URL-адреса принадлежат компьютеру (обратному прокси-серверу, балансировщику нагрузки или другому компьютеру), который используется для доступа к серверу шлюза. Пример:
     `http://my_reverse_proxy.example.com:80`.

     Если для доступа к серверу шлюза вы используете NAT-устройство, введите полный URL-адрес NAT-устройства. Пример:
     `http://nat_device.example.com:80`.

     "URL-адрес локального виртуального сервера шлюза для пользователей приложений" и "URL-адрес локального виртуального сервера шлюза для сборщиков данных" (необязательно). Если для доступа к компьютеру сервера шлюза необходимо использовать более одного URL-адреса (кроме указанных выше URL-адресов виртуального сервера шлюза), укажите локальный URL-адрес сервера для каждого компьютера, через которой вы хотите получать доступ к серверу шлюза. Пример:
     `http://my_specific_virtual_server.example.com:80`.

     Если значение параметра **URL-адрес локального виртуального сервера служб** определено для конкретного компьютера, то для этого компьютера используется этот URL-адрес вместо значения **URL-адрес по умолчанию виртуального сервера служб**.

   - **URL-адрес сервера шлюза прямого доступа для пользователей приложений**. Нажмите кнопку **Редактировать** и удалите URL-адрес в поле **значения**.

   - **URL-адрес сервера шлюза прямого доступа для сборщиков данных**. Нажмите кнопку **Редактировать** и удалите URL-адрес в поле **значения**.

3. В области "Конфигурация обратных прокси-серверов" задайте следующие параметры.
   - **Включить обратный прокси-сервер**. Установите для этого параметра значение true. Обратите внимание, что это нужно сделать после настройки предыдущих параметров.

   - **IP-адреса обратных прокси-серверов HTTP или HTTPS**. Введите внутренние IP-адреса

обратных прокси-серверов или устройств балансировки нагрузки, которые использовались для связи с сервером шлюза.

- Если указать IP-адрес обратного прокси-сервера, отправляющего запрос HTTP/HTTPS, то клиенту возвращается URL-адрес виртуального сервера по умолчанию или URL-адрес локального виртуального сервера (если он определен).
- Если в этом параметре не определены IP-адреса (не рекомендуем), то APM работает в общем режиме. То есть, возможен вход в систему APM только при помощи виртуального URL-адреса, а не напрямую через шлюз.

Примечание. Если используется обратный прокси-сервер, который находится в разных доменах с серверами шлюза APM, необходимо добавить IP -адрес обратного прокси-сервера в параметр **IP-адреса обратных прокси-серверов HTTP и HTTPS**. Подробнее см. раздел "Конфигурация LW-SSO для установки в нескольких доменах и вложенных доменах" документа "Руководство по администрированию платформы APM".

Чтобы узнать внутренний IP-адрес обратного прокси-сервера или балансировщика нагрузки, выполните следующие действия.

- Войдите в систему APM через обратный прокси-сервер или балансировщик нагрузки.
- Откройте журнал **<корневой каталог сервера шлюза HPE APM>\log\EJBContainer\UserActionsServlet.log**.
- IP-адрес, указанный в последней строке с записью о **входе в систему**, и есть IP-адрес обратного прокси-сервера или балансировщика нагрузки. В записи должно быть указано ваше имя пользователя.

4. Увеличьте таймаут для обратного прокси-сервера.
5. Перезапустите службу HPE APM на сервере шлюза APM и серверах обработки данных.

Примечание. После того как вы изменили базовый URL-адрес APM, считается, что клиент инициирует новые сеансы HTTP и HTTPS с использованием базового URL-адреса. Нужно убедиться в создании канала HTTP или HTTPS между клиентом и компьютером с новым URL-адресом.

Примечания и ограничения

Для работы APM нужно задать таймаут обратного прокси-сервера не менее 300 секунд. Это значение используется по умолчанию для некоторых версий Apache, но его можно уменьшить. Для выполнения некоторых операций, например установки пакета содержимого, следует увеличить значение таймаута до 1000 секунд (см. Настройка Apache для работы в качестве обратного прокси-сервера на стр 27).

Если APM работает в общем режиме, все клиенты APM должны получать доступ к компьютеру APM через обратный прокси-сервер.

Поддержка общего и особого режима обратного прокси-сервера для APM

Серверы APM отвечают на запросы пользователей приложений, отправляя базовый URL-адрес, который используется для определения правильных ссылок на запрошенные пользователем HTML-документы. Когда используется обратный прокси-сервер, APM в возвращаемой пользователю HTML-ссылке должен указывать базовый URL-адрес обратного прокси-сервера, а не базовый URL-адрес сервера APM.

Если обратный прокси-сервер используется только для сборщиков данных, то настройку следует выполнять только для сборщиков данных и обратного прокси-сервера. Она не требуется на серверах APM.

Существует два режима работы прокси-сервера, которые управляют доступом пользователей к серверам APM:

- Особый режим на стр 37.
- Общий режим на стр 37.

Особый режим

Этот режим используется для одновременного доступа к серверам APM напрямую и через конкретные обратные прокси-сервера. Доступ к серверу напрямую осуществляется в обход брандмауэра и прокси-сервера, поскольку вы работаете в локальной сети (интранет).

Когда в этом режиме HTTP- или HTTPS-запрос поступает от пользователя приложений через один из IP-адресов, определенных в параметре **IP-адреса обратных прокси-серверов HTTP** или **IP-адреса обратных прокси-серверов HTTPS**, то APM определяет базовый URL-адрес и заменяет его значением **URL-адрес виртуального сервера шлюза по умолчанию** или **URL-адрес локального виртуального сервера шлюза** (когда он определен). Если HTTP- или HTTPS-запрос поступает не через один из этих IP-адресов, то клиенту возвращается базовый URL-адрес, полученный APM в HTTP- или HTTPS-запросе.

Общий режим

Этот режим используется для доступа к серверу шлюза через обратный прокси-сервер. Все запрошенные URL-адреса изменяются и отправляются обратно с виртуальным IP-адресом сервера шлюза.

В этом режиме приложение APM при выполнении каждого HTTP- или HTTPS-запроса определяет базовый URL-адрес, который заменяется значением **URL-адрес виртуального сервера шлюза по умолчанию** или **URL-адрес локального виртуального сервера шлюза** (когда он определен).

При этом все клиенты APM обязательно должны получать доступ к серверам APM по URL-адресам, заданным с помощью параметра **URL-адрес виртуального сервера шлюза по умолчанию** или **URL-адрес локального виртуального сервера шлюза**.

Глава 6: Установка и настройка дополнительных компонентов

Подробные сведения о полноценном рабочем процессе настройки APM, а также о понятиях и компонентах APM, см. в руководстве по началу работы с APM, которое входит в справку APM.

При установке и настройке дополнительных компонентов используйте следующие материалы:

Элемент	Ресурс
Платформа APM	Сведения о том, как настраивать платформу APM, см. в документе Руководство по администрированию платформы APM, доступном в справке APM.
Интеграции с APM	Сведения о различных типах интеграции с APM см. на портале с решениями и интеграциями HPESW https://hpenterprise.sharepoint.com/teams/aztec/
Компоненты APM	• **Real User Monitor:** см. Руководство по установке и обновлению Real User Monitor. • **Business Process Monitor:** см. Руководство по развертыванию Business Process Monitor. • **SiteScope:** см. Руководство по развертыванию HPE SiteScope. • **Diagnostics:** см. Руководство по установке и настройке Diagnostics. • **System Health:** см. Руководство по приложению System Health. • **Зонд потока данных:** см. руководство по установке зонда потока данных.

Указанные ресурсы можно найти по следующим адресам:

- Страница с руководствами по планированию и развертыванию: корневой каталог установки APM (**Get_documentation.htm**), или в APM в меню **Справка > Руководства по планированию и развертыванию**.
- Страница загружаемых компонентов: Выберите **Администрирование > Платформа > Установка и обслуживание > Загружаемые компоненты**.
- Посетите веб-сайт службы поддержки HPE Software по адресу https://softwaresupport.hpe.com.

Часть II: Приложения

Приложение A: Установка APM на платформе Windows

В этом приложении рассматриваются следующие темы.

Подготовка информации, необходимой для установки

Перед установкой следует подготовить следующие сведения.

- **Имена целевых каталогов**. Во время установки APM устанавливаются пакеты HPE L-Core. Если уже установлена более ранняя версия этих пакетов, то они автоматически обновляются. В противном случае установленная версия не перезаписывается. Это изменение нельзя отменить.
- Во время установки необходимо выбрать каталоги для установки следующих общих пакетов.
  - 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
- **Ключ лицензии**. Можно использовать оценочную лицензию (60 дней) или импортировать бессрочную лицензию. Файл .DAT с лицензией может находиться в локальной или сетевой папке.

  Если в дальнейшем понадобится обновить ключ лицензии (например, в случае приобретения лицензии на один или несколько новых компонентов APM), это можно сделать на сайте APM: выберите **Администрирование > Платформа > Установка и обслуживание > Управление лицензиями** и нажмите кнопку **Добавить лицензию из файла**. Сведения об обновлении ключа лицензии см. в разделе "Лицензии" документа Руководство по администрированию платформы APM.
- **Номер для обслуживания** Номер для обслуживания предоставляется вместе с пакетом APM.
- **Электронный адрес администратора.**
- **Номер порта, используемый веб-сервером.** Этот порт служит для доступа к APM. Порт по умолчанию — 80.
- **Имя компьютера с сервером шлюза.** Имя должно указываться вместе с доменом.

- **Имя балансировщика нагрузки** (если он используется)**.** Этот балансировщик нагрузки используется для доступа к сайту APM.
- **Имя почтового SMTP-сервера.**
- **Имя отправителя SMTP.** Это имя появляется в уведомлениях, отправляемых из APM. Это имя не может содержать пробелы. Если введенное имя содержит пробелы, то отчеты не будут доставляться.

  Примечание. После запуска APM можно настроить альтернативный SMTP-сервер в разделе **Администрирование > Платформа > Установка и обслуживание > Настройки инфраструктуры**.

Использование веб-сервера IIS

APM, установленный на платформе Windows, работает с HTTP-сервером Apache или сервером Microsoft Internet Information Server (IIS). Тип веб-сервера указывается в мастере начальной настройки. Чтобы изменить эти настройки, можно повторно запустить мастер начальной настройки.

Примечание. На компьютере должен работать только один веб-сервер, использующий тот же порт, что и APM. Например, если во время установки сервера APM выбран HTTP-сервер Apache, а установка выполняется на компьютере, где уже работает сервер IIS, то перед началом установки нужно остановить службу IIS и установить для нее режим запуска **Вручную**.

HTTP-сервер Apache

APM использует версию HTTP-сервера Apache, адаптированную компанией HPE для APM. Она устанавливается во время установки сервера.

По умолчанию для HTTP-сервера Apache не включено использование SSL. Сведения о настройке веб-сервера для использования SSL см. на сайте http://httpd.apache.org/docs/2.2/ssl/. SSL следует включить для всех каталогов, используемых в APM, в соответствии с файлом конфигурации Apache (**httpd.conf** и **httpd-ssl.conf**).

Microsoft Internet Information Server (IIS)

- Для ОС Microsoft Windows Server 2008, где используется веб-сервер IIS 7.X, см. ОС Microsoft Windows Server 2008 с веб-сервером IIS 7.X на стр 44.
- Для ОС Microsoft Windows Server 2012, где используется веб-сервер IIS 8, см. ОС Microsoft Windows Server 2012 с веб-сервером IIS 8 на стр 44.

ОС Microsoft Windows Server 2008 с веб-сервером IIS 7.X

Если установка выполняется в ОС Microsoft Windows Server 2008 и используется веб-сервер IIS 7.X, необходимо выполнить следующую процедуру.

1. На **панели управления** выберите пункты **Администрирование** > **Диспетчер серверов**.
2. Щелкните правой кнопкой элемент **Роли** и выберите команду **Добавить роль сервера**, чтобы запустить мастер добавления ролей.
3. На странице "Выбор служб ролей" выберите **роль веб-сервера (IIS)** для установки.

   Если откроется всплывающее окно с вопросом **Добавить компоненты, необходимые для веб-сервера (IIS)?**, нажмите кнопку **Добавить необходимые компоненты**.
4. Дважды нажмите кнопку **Далее**.
5. На панели "Выбор служб ролей" выберите следующие роли.
   a. В разделе **Основные функции HTTP**: **Статическое содержимое** (обычно включена по умолчанию)
   b. В разделе **Разработка приложений**: **Расширения ISAPI** и **Фильтры ISAPI**.
   c. В разделе **Средства управления**: **Скрипты и средства управления IIS**
6. Нажмите кнопку **Установить**.

ОС Microsoft Windows Server 2012 с веб-сервером IIS 8

Если установка выполняется в ОС Microsoft Windows Server 2012 и используется веб-сервер IIS 8, необходимо выполнить следующую процедуру.

1. На **панели управления** выберите пункты **Администрирование** > **Диспетчер серверов**.
2. Выберите **Управление** > **Добавить роли и компоненты**.
3. Щелкните **Далее**.
4. Выберите **Установка ролей или компонентов**.
5. Щелкните **Далее**.
6. Выберите **Выбрать сервер из пула серверов**
7. Щелкните **Далее**.
8. На странице "Выбор служб ролей" выберите **роль веб-сервера (IIS)** для установки.

   Если откроется всплывающее окно с вопросом **Добавить компоненты, необходимые для веб-сервера (IIS)?**, нажмите кнопку **Добавить необходимые компоненты**.
9. Дважды нажмите кнопку **Далее**.
10. На панели "Выбор служб ролей" выберите следующие роли.
    a. В разделе **Основные функции HTTP**:
       - **Статическое содержимое** (обычно включена по умолчанию)
       - **Перенаправление HTTP**
    b. В разделе **Разработка приложений**: **Расширения ISAPI** и **Фильтры ISAPI**.
    c. В разделе **Средства управления**: **Скрипты и средства управления IIS**
11. Щелкните **Далее**.
12. Нажмите кнопку **Установить**.

Установка APM на платформе Windows

Серверы APM (сервер шлюза и сервер обработки данных) устанавливаются из пакета распространения APM. Если установка выполняется на компьютере, где не работает сервер IIS, то в ходе установки APM устанавливается HTTP-сервер Apache.

На компьютерах, где устанавливаются серверы APM, необходимы права администратора.

Примечание. Убедитесь, что никакие другие программы установки и процессы не используют установщик Windows. Если установщик Windows занят другими процессами, то продолжение установки APM невозможно. Необходимо остановить другие задачи установки, остановить установку APM, нажав кнопку **Отмена** в мастере установки, а затем снова запустить установку APM.

Первый мастер установки копирует файлы и пакеты на компьютер. Мастер начальной настройки выполняет регистрацию, настройку подключения, веб-сервера и настроек SMTP.

Также можно установить APM в автоматическом режиме. Подробнее см. в разделе Автоматическая установка APM на стр 64.

Чтобы установить серверы APM, выполните следующие действия.

1. Перейдите на веб-сайт HPE SMTA (http://prssc.int.hpe.com/smta/smta.cgi) и войдите в учетную запись.
2. Рядом с пунктом **Release Name** выберите **APM0930** нажмите кнопку **Search**.
3. Загрузите файл **HPE_APM_9.30_Windows_Setup.zip**.
4. Распакуйте файл в локальный каталог.
5. В меню **Пуск** выберите пункт **Выполнить**.
6. Введите расположение, из которого выполняется установка, и имя файла **HPApm_9.30_setup.exe**. Файл установки для серверов APM находится в каталоге **Windows_Setup**. Например, введите d:\Windows_Setup\HPApm_9.30_setup.exe

   Примечание. Если установка выполняется на виртуальной машине, то необходимо скопировать exe-файл и каталог пакетов на локальный компьютер. Установка по сети на виртуальную машину завершается ошибкой.
7. Нажмите кнопку **ОК**. Начнется установка.
8. Следуйте указаниям на экране, чтобы установить сервер.
   - **Язык**. Если программа установки переведена на другие языки, выберите язык из доступных вариантов.

     Возможно предупреждение от антивирусной программы. Установку можно продолжать, не выполняя никаких действий и не останавливая антивирусные программы, работающие на компьютере.

   - **Тип установки:**

- Выберите тип установки **Шлюз**, чтобы установить на текущем компьютере сервер шлюза.
- Выберите тип установки **Обработка данных**, чтобы установить на текущем компьютере сервер обработки данных.
- Выберите тип установки **Типично**, чтобы установить на одном компьютере сервер шлюза и сервер обработки данных.

Примечание. Если установка выполняется на компьютере с Windows 2008 R2 Server, то может появиться следующее сообщение: Недопустимая папка установки для общего содержимого. Эта проблема может быть связана с отсутствием прав администратора для установки APM на компьютере. Обратитесь к системному администратору.

- **Каталоги установки**. Для установки необходимо выбрать следующие каталоги.
  - Выберите каталог установки для общего содержимого HPE. В каталоге **%ALLUSERSPROFILE%\HP\BSM** содержатся дополнительные общие данные.
  - Выберите каталог установки для содержимого, привязанного к продукту. В среде Microsoft Windows этот путь должен иметь длину не более 15 символов и не может содержать пробелы. Если длина имени превышает 15 символов или оно не оканчивается на **HPBSM**, то на следующем этапе установки будет предложено задать другое имя.

Примечание. Во время установки может появляться следующее сообщение: Необходимые порты заняты. Если при установке оказывается, что порты заняты, то установка не завершается ошибкой, но рекомендуем освободить необходимые порты. В противном случае понадобится изменить конфигурацию APM для использования другого набора портов.

Этот этап установки в виртуальной среде может занять приблизительно полчаса-час.

После завершения процесса рядом с каждым успешно развернутым пакетом и приложением появляются отметки о выполнении. Если происходят ошибки, то открывается окно "Ошибка" с указанием возможных причин для ошибок скриптов установки.

9. Затем открывается мастер начальной настройки. Выполните следующие действия.
   - **Зарегистрируйте продукт.**
   - **Настройте настройки подключения.**
     i. **HTTP-сервер Apache.** Если порт 80, используемый по умолчанию, уже используется существующим веб-сервером, APM уведомляет пользователя о конфликте и предлагает способы разрешения. Если выбран сервер Apache, необходимо также ввести адрес электронной почты администратора APM.
     ii. **Microsoft IIS.** Если сервер IIS использует порт, отличный от 80, введите порт IIS. Если выбран сервер IIS, необходимо также ввести адрес веб-сайта IIS для использования в APM.
   - **Выберите тип веб-сервера.**
     - Если APM не обнаружил на компьютере экземпляр Microsoft IIS, то предлагается только вариант **HTTP-сервер Apache**. Если APM должен работать с сервером Microsoft IIS, нажмите кнопку **Отмена**, чтобы выйти из мастера. Установите сервер IIS и перезапустите мастер после установки.

- **Укажите почтовый сервер SMTP.**
  - Рекомендуем указывать полный интернет-адрес SMTP-сервера. Используйте только буквы и цифры.
  - В поле **Имя отправителя** укажите имя, которое будет отображаться в плановых отчетах и в оповещениях, отправляемых APM. Если на данном компьютере когда-либо устанавливался APM, то может отображаться имя по умолчанию: **HP_BSM_Notification_Manager**. Можно принять это имя или ввести другое.
  - После запуска APM можно настроить альтернативный SMTP-сервер в разделе **Администрирование платформы > Администрирование > Платформа > Установка и обслуживание > Настройки инфраструктуры**.

Если развертывание выполняется на нескольких серверах, установите дополнительные серверы APM, выполнив описанные выше шаги.

Примечание. Чтобы изменить настройки, можно повторно запустить мастер начальной настройки. Мастер начальной настройки можно запустить из следующей папки: **<корневой каталог HPE APM>\bin\postinstall.bat**. Однако если он запускается в первый раз или был закрыт до завершения работы, используйте другой файл: **<корневой каталог HPE APM>\bin\ovii-postinstall.bat <TOPAZ_HOME>**, где **<TOPAZ_HOME>** — каталог установки APM (обычно C:\HPBSM).

Приложение B: Установка APM на платформе Linux

В этом приложении рассматриваются следующие темы.

Подготовка информации, необходимой для установки

Перед установкой следует подготовить следующие сведения.

- **Номер для обслуживания.** Этот номер предоставляется вместе с пакетом APM.
- **Имя веб-сервера.** Имя должно указываться вместе с доменом.

  Примечание. При установке в Linux имя домена необходимо вводить вручную.

- **Электронный адрес администратора.**
- **Имя почтового SMTP-сервера.**
- **Имя отправителя SMTP.** Это имя появляется в уведомлениях, отправляемых из APM.
- **Имя компьютера с сервером шлюза.**
- **Имя балансировщика нагрузки** (если он используется). Этот балансировщик нагрузки используется для доступа к сайту APM.
- **Номер порта, используемый веб-сервером**. Номер порта по умолчанию — 80.

Использование веб-сервера Apache

Сервер APM на платформе Linux работает с HTTP-сервером Apache.

Примечание. На компьютере с APM должен работать только один веб-сервер.

HTTP-сервер Apache

APM использует версию HTTP-сервера Apache, адаптированную компанией HPE для APM. Она устанавливается во время установки сервера.

По умолчанию APM работает с HTTP-сервером Apache через порт 80. Если порт 80 уже используется, то конфликт портов можно разрешить двумя способами.

- Перед началом установки APM измените конфигурацию службы, использующей этот порт, и задайте другой порт.
- Во время установки APM выберите другой порт для HTTP-сервера Apache.

По умолчанию для HTTP-сервера Apache не включено использование SSL. Сведения о настройке веб-сервера для использования SSL см. на сайте http://httpd.apache.org/docs/2.2/ssl/. SSL следует включить для всех каталогов, используемых в APM, в соответствии с файлом конфигурации Apache (**httpd.conf** и **httpd-ssl.conf**).

Установка серверов APM на платформе Linux

Серверы APM (сервер шлюза и сервер обработки данных) устанавливаются из установочного пакета APM 9.30.

Чтобы подтвердить, что файлы установки содержат код, разработанный HPE, и не подвергались стороннему вмешательству, можно использовать открытый ключ HPE и выполнить инструкции по проверке, приведенные на веб-сайте HPE: https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning.

Также можно установить APM в автоматическом режиме. Подробнее см. в разделе Автоматическая установка APM на стр 64.

Примечание. Не рекомендуем устанавливать APM с помощью эмулятора, например Exceed. Установка через эмулятор может замедлить ход установки и негативно сказаться на внешнем виде и функциональных возможностях пользовательского интерфейса.

Чтобы установить серверы APM, выполните следующие действия.

1. Войдите на сервер от имени привилегированного пользователя (**root**).
2. Перейдите на веб-сайт HPE SMTA (http://prssc.int.hpe.com/smta/smta.cgi) и войдите в учетную запись.
3. Рядом с пунктом **Release Name** выберите **APM0930** и нажмите кнопку **Search**.
4. Загрузите файл **HPE_APM_9.30_Linux_Setup.zip**.
5. Распакуйте файл в локальный каталог.
6. (Необязательно) Чтобы подтвердить, что файлы установки содержат код, разработанный HPE, и не подвергались стороннему вмешательству, можно использовать открытый ключ HPE и выполнить инструкции по проверке, приведенные на веб-сайте https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning.
7. Запустите скрипт:

   /HPApm_9.30_setup.bin
8. Следуйте указаниям на экране, чтобы установить сервер.

   Примечание. Если APM обнаруживает на компьютере предыдущую установку, отображается предупреждение о перезаписи всех измененных данных конфигурации.

   - Выберите тип установки.
     - Выберите тип установки **Шлюз**, чтобы установить на текущем компьютере сервер шлюза.
     - Выберите тип установки **Обработка данных**, чтобы установить на текущем компьютере сервер обработки данных.
     - Выберите тип установки **Типично**, чтобы установить на одном компьютере сервер шлюза и сервер обработки данных.
   - Файлы APM копируются в каталог **/opt/HP/BSM**.

- Данные для общего содержимого HPE размещаются в каталоге **/var/opt/OV**.

Примечание. Во время установки может появляться следующее сообщение:

Необходимые порты заняты. Если при установке оказывается, что порты заняты, то установка не завершается ошибкой, но рекомендуем освободить необходимые порты.

Этот этап установки в виртуальной среде может занять приблизительно полчаса-час.

После завершения процесса рядом с каждым успешно развернутым пакетом и приложением появляются отметки о выполнении. При обнаружении ошибок открывается вкладка **Ошибки** с описанием возможных ошибок.

9. Затем открывается мастер начальной настройки. Выполните следующие действия.
   - **Зарегистрируйте продукт.** Введите значения **Имя, Компания** и **Номер для обслуживания**.
   - **Настройте настройки подключения.**
     - Хост. Необходимо указывать полное доменное имя. Имя сервера может уже отображаться по умолчанию, но необходимо вручную добавить имя домена. Если используется балансировщик нагрузки, здесь необходимо ввести имя компьютера для этого устройства.
     - Порт. Если порт 80, используемый по умолчанию, уже используется существующим веб-сервером, APM уведомляет пользователя о конфликте и предлагает способы разрешения..
   - **Просмотрите тип веб-сервера и введите адрес электронной почты администратора APM.** APM устанавливает HTTP-сервер Apache. Этот веб-сервер необходимо использовать в среде Linux.
   - **Укажите почтовый сервер SMTP.**
     - Рекомендуем указывать полный интернет-адрес SMTP-сервера. Используйте только буквы и цифры.
     - В поле "Имя отправителя" укажите имя, которое будет отображаться в плановых отчетах и в оповещениях, отправляемых APM.

Примечание. Чтобы изменить настройки, можно повторно запустить мастер начальной настройки. Мастер начальной настройки можно запустить из следующей папки: **<корневой каталог HPE APM>/bin/postinstall.sh**. Однако если он запускается в первый раз или был закрыт до завершения работы, используйте другой файл: **<корневой каталог HPE APM>/bin/ovii-postinstall.sh <TOPAZ_HOME>**, где **<TOPAZ_HOME>** — каталог установки APM (обычно /opt/HP/BSM).

Приложение C: Развертывание сервера и настройка параметров базы данных

В этом приложении рассматриваются следующие темы.

Примечание. Если используется Oracle Server, то далее под термином **схема пользователя** следует понимать термин **база данных**.

Обзор программы установки и настройки баз данных

Для настройки развертывания сервера, создания баз данных и схем пользователей используется программа установки и настройки баз данных.

Программу установки и настройки баз данных можно запустить во время установки сервера APM или выбрать ее на последней странице мастера начальной настройки. Эту программу также можно запустить после установки сервера независимо от процедуры установки. В обоих случаях выполняются одинаковые действия.

При установке в распределенной среде сначала запустите программу на сервере обработки данных, а потом — на сервере шлюза.

Если позднее понадобится изменить типы баз данных или параметры подключения, можно снова запустить программу установки и настройки баз данных. Следует отключить сервер APM, на котором запущена программа. Подробнее см. в разделе Запуск и остановка APM на стр 21.

После изменения типа базы данных или параметров подключения перезапустите все серверы APM и сборщики данных.

Примечание. Если изменить параметры подключения для БД управления после запуска APM, может быть нарушена целостность БД RTSM и утеряно много данных.

Перед началом этой процедуры рекомендуем просмотреть разделы Настройка параметров базы данных на стр 56 и Информация, необходимая для настройки параметров базы данных на стр 58.

Дополнительные сведения о подготовке MS SQL Server или Oracle Server в системе для использования с APM см. в документе Руководство по базам данных APM.

Примечание. Не используйте программу установки и настройки баз данных вместо или до мастера обновления. Используйте ее, только если процесс обновления завершен и среда назначения — производственная.

Настройка параметров базы данных

Необходимо задать параметры подключения для следующих баз данных:

- БД управления
- RTSM

Чтобы настроить подключение к этим базам данных, выполните следующие действия.

- Выберите планируемый тип базы данных: MS SQL Server или Oracle Server
- Выберите создание или повторное использование базы данных в MS SQL Server или схемы пользователя в Oracle Server. См. Создание баз данных на стр 56.
- Укажите параметры подключения к базе данных или схеме пользователя. См. Подключение к существующим базам данных на стр 56.

Примечание. Если необходимо изменить активную базу данных управления для APM, обратитесь в службу Служба поддержки HPE.

Создание баз данных

Базы данных на сервере MS SQL Server или Oracle Server можно создавать в программе установки и настройки баз данных или вручную непосредственно на сервере БД (например, если в организации запрещено использовать учетные данные администратора во время установки). Если базы данных созданы вручную, то все равно нужно запустить программу установки и настройки баз данных для подключения к базам.

Инструкции по созданию баз данных вручную на MS SQL Server см. в разделе "Создание и настройка баз данных Microsoft SQL Server" документа Руководство по базам данных APM. Инструкции по созданию схем пользователей вручную на Oracle Server см. в разделе "Создание схем пользователей Oracle Server вручную" документа Руководство по базам данных APM.

Примечание. Каждая база данных или схема пользователя, создаваемая в APM (на одном сервере БД или на разных серверах), должна иметь уникальное имя.

Подключение к существующим базам данных

При работе с программой установки и настройки баз данных выбирается, будет ли создаваться новая база данных (схема пользователя) или устанавливаться подключение к существующей базе (схеме).

Вариант **Подключиться к существующей схеме** обычно выбирается в следующих сценариях.

- При подключении к базе данных или схеме пользователя, созданной вручную непосредственно в MS SQL Server/Oracle Server.
- При установке APM в распределенной среде и запуске программы на серверах, устанавливаемых после первого. В этом случае сначала нужно запустить мастер на сервере обработки данных, а затем — на серверах шлюза.

Выполняется подключение к базам данных и схемам пользователей, созданным во время установки сервера обработки данных. После подключения к базе данных управления с использованием параметров подключения, заданных во время установки первого сервера, параметры подключения

для других баз данных будут по умолчанию отображаться на соответствующих экранах. При работе на сервере шлюза отображаются не все базы данных.

Сведения о реализации распределенного развертывания APM см. в разделе "Конфигурации развертывания" руководства по началу работы с APM.

Информация, необходимая для настройки параметров базы данных

Перед настройкой параметров баз данных необходимо подготовить сведения, описанные в следующих разделах.

Настройка параметров подключения для MS SQL Server

Для создания новых баз данных и подключения к уже существующим необходимы следующие сведения.

- **Имя хоста.**Имя компьютера, на котором установлен MS SQL Server. Если подключение выполняется в динамическом режиме не к экземпляру MS SQL Server по умолчанию, введите следующие данные: <имя_хоста>\<имя_экземпляра>

  Внимание! Поле **Имя хоста** в программе может содержать не более 26 (двадцати шести) символов. Если в среде не допускается использование имени хоста без имени домена, воспользуйтесь одним из следующих обходных решений.

  - Укажите IP-адрес вместо имени хоста в поле **Имя хоста**.
  - Сопоставьте имя хоста с IP-адресом в файле hosts в Windows. Укажите сопоставленное имя в поле **Имя хоста**.

- **Порт.** Порт TCP/IP MS SQL Server. APM автоматически отображает порт по умолчанию: **1433**.
  - Если подключение к именованному экземпляру выполняется в статическом режиме, введите номер порта.
  - Если подключение к именованному экземпляру выполняется в динамическом режиме, измените номер порта на **1434**. Этот порт может динамически прослушивать и определять правильный порт базы данных.

- **Имя базы данных.** Имя существующей созданной вручную базы данных или имя, которое получит новая база данных (например, APM_Management).

  Примечание. Не поддерживаются имена баз данных, которые начинаются с цифр.

- **Имя пользователя и пароль** (если используется проверка подлинности MS SQL Server). Имя и пароль пользователя с правами администратора в MS SQL Server. Обратите внимание на необходимость ввода пароля.

  Совет. Мы рекомендуем не входить под именем пользователя по умолчанию **sa** по соображениям безопасности.

Для создания баз данных и подключения к ним можно использовать проверку подлинности Windows (а не MS SQL Server). Для этого необходимо удостовериться, что пользователь Windows, запускающий службу APM, имеет необходимые права для доступа к базе данных MS SQL Server. Сведения о том, как назначить пользователя Windows, который будет запускать службу APM, см. в разделе Смена пользователей службы APM на стр 105. Сведения о том, как добавить пользователя Windows в MS SQL Server, см. в разделе "Использование проверки подлинности Windows для доступа к базе данных Microsoft SQL Server" документа Руководство по базам данных APM.

Примечание. В среде Linux проверка подлинности Windows не поддерживается.

Настройка параметров подключения для Oracle Server

Примечание. Если сервер Oracle Server размещается в Real Application Cluster (Oracle RAC), то для некоторых параметров, описанных в этом разделе, следует задать другие значения. Подробнее см. в разделе, посвященном поддержке Oracle Real Application Cluster, в документе Руководство по базам данных APM.

Перед настройкой параметров базы данных убедитесь, что для каждой схемы пользователя создано хотя бы одно табличное пространство для сохранения данных приложений, а также задано хотя бы одно временное табличное пространство в соответствии с требованиями. Подробнее о создании табличных пространств и определении их размера для схем пользователей BSM см. в разделе "Инструкции по настройке и масштабированию Oracle" документа Руководство по базам данных APM.

Для создания новой схемы пользователя и для подключения к уже существующей необходимы следующие сведения.

- **Имя хоста.** Имя компьютера, на котором установлен Oracle Server.

  Внимание! Поле **Имя хоста** в программе может содержать не более 26 (двадцати шести) символов. Если в среде не допускается использование имени хоста без имени домена, воспользуйтесь одним из следующих обходных решений.

  - Укажите IP-адрес вместо имени хоста в поле **Имя хоста**.
  - Сопоставьте имя хоста с IP-адресом в файле hosts в Windows. Укажите сопоставленное имя в поле **Имя хоста**.

- **Порт.** Порт прослушивателя Oracle. APM автоматически отображает порт по умолчанию: **1521**.
- **SID.** Имя экземпляра Oracle, служащее уникальным идентификатором экземпляра базы данных Oracle, используемого APM.
- **Имя схемы и пароль.** Имя и пароль для существующей схемы пользователя или имя, которое получит новая схема пользователя (например, APM_MANAGEMENT).

Для создания новой схемы пользователя необходимы следующие дополнительные сведения.

- **Имя пользователя и пароль администратора** (для подключения от имени администратора). Имя и пароль пользователя с правами доступа администратора в Oracle Server (например, системного пользователя).
- **Табличное пространство по умолчанию.** Имя выделенного табличного пространства по умолчанию, используемого для создания схемы пользователя.
- **Временное табличное пространство.** Имя временного табличного пространства, назначенного схеме пользователя. Табличное пространство Oracle по умолчанию — **temp**.

Примечание. Чтобы создать новую схему пользователя APM, необходимы разрешения администратора и права на выполнение CREATE USER, CONNECT, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, UNLIMITED TABLESPACE, CREATE VIEW и CREATE PROCEDURE в Oracle Server.

Запуск программы установки и настройки базы данных.

Программу установки и настройки баз данных можно запустить во время установки APM или отдельно. Если программа установки и настройки баз данных запускается отдельно от установки APM, следует учесть следующие важные замечания.

- Если на компьютере APM открыто окно командной строки, перед продолжением работы с программой установки и настройки баз данных его необходимо закрыть.
- Если этот мастер запускается не во время начальной установки, а после установки для изменения существующей конфигурации, необходимо отключить APM перед запуском программы установки и настройки баз данных (выберите **Пуск > Программы > HPE Business Service Management > Администрирование > Отключить HPE Business Service Management**).
- При задании параметров базы данных используйте только буквы латинского алфавита.

Примечание. Эту программу также можно запустить в автоматическом режиме. Подробнее см. в разделе Автоматическая установка APM на стр 64.

Чтобы задать параметры базы данных и настроить развертывание сервера, выполните следующие действия.

1. Запустите программу установки и настройки баз данных одним из следующих способов.
   - При завершении работы с мастером начальной настройки запустите программу установки и настройки базы данных.
   - **Windows:** на сервере APM выберите **Пуск > Программы > HPE Application Performance Management > Администрирование > Настройка HPE Application Performance Management**. APM запускает программу установки и настройки базы данных. Также можно запустить файл непосредственно из расположения **<корневой каталог HPE APM>\bin\config-server-wizard.bat**.
   - **Linux:** на сервере APM откройте командную строку терминала и запустите сценарий **/opt/HP/BSM/bin/config-server-wizard.sh**.
2. Следуйте указаниям на экране, чтобы настроить базы данных.
   a. **Лицензия**. Если эта программа запускается в первый раз, можно выбрать использование оценочной лицензии или загрузить новые лицензии. Если программа запускается не в первый раз, то можно пропустить этот этап или загрузить дополнительные лицензии. Файл лицензии имеет расширение .DAT и должен располагаться на сервере, где работает программа, или быть доступным по сети.

      После установки APM можно обновить лицензии на странице "Управление лицензиями" в разделе администрирования платформы. Подробнее см. в разделе "Лицензии" документа Руководство по администрированию платформы APM.

   b. **Развертывание сервера**. Рекомендуем сначала ввести сведения о развертывании в калькулятор емкости, чтобы определить область развертывания, а также приложения и компоненты, которые будут работать. Сохраненный файл Excel с калькулятором емкости можно загрузить на эту страницу программы. Обязательные поля автоматически заполняются данными из калькулятора емкости в зависимости от сведений, введенных на

листе Excel. Подробнее см. в руководстве по началу работы с APM.

- **Пользователи**. Число пользователей, одновременно находящихся в системе, определяет уровень нагрузки: **малая**, **средняя** или **большая**.
- **Модель**. Число конфигурационных единиц в модели определяет ее размер: **малая**, **средняя**, **большая** или **очень большая**.
- **Данные метрик**. Число отслеживаемых приложений, транзакций, расположений и хостов определяет объем данных метрик: **малый**, **средний** или **большой**.
- **<Список приложений>**. Установите или снимите флажки для приложений, чтобы активировать или деактивировать их для этого развертывания. Отключите неиспользуемые приложения, чтобы освободить память и ресурсы процессора для используемых приложений.

  Примечание. Если какая-либо функция не включена в этой программе, то она не будет доступна ни одному пользователю. Подробности о всех параметрах приложений приводятся в подсказках в калькуляторе емкости.

  Если после завершения установки нужно изменить развертывание, можно подобрать уровни емкости и включить или отключить приложения и функции на странице "Развертывание сервера" в разделе администрирования платформы.

Также можно ввести данные на этой странице вручную, но настоятельно рекомендуем использовать калькулятор емкости для определения области и емкости развертывания.

c. **Настройки входа**. Введите пароли для администратора (пользователь admin), чтобы получить доступ к APM и консоли JMX.

Также можно задать поле **Пароль для доступа к RTSM**, чтобы защитить данные, передаваемые в Модель обслуживания во время выполнения из RUM.

Примечание. Если во время установки APM вы изменили пароль **Доступ к RTSM**, следует также сменить этот пароль в Diagnostics и RUM.

d. **Конфигурация IIS**. Если используется Microsoft Internet Information Server (IIS) версии 7.X в ОС Microsoft Windows Server 2008, то для APM необходимо включить следующие роли IIS.

- Расширения ISAPI
- Фильтры ISAPI
- Скрипты и средства управления IIS
- Статическое содержимое

Если эти роли уже включены, но экран настройки IIS не открывается.

Если какие-либо из ролей не включены, то для них можно запросить автоматическую настройку: выбрать **Включить роли IIS автоматически** и нажать кнопку **Далее**.

Чтобы настроить роли вручную, выберите вариант **Включить роли IIS вручную** и нажмите кнопку **Далее**.

e. **Настройка брандмауэра**. Если APM располагается за брандмауэром, то при запуске программы на сервере шлюза можно настроить брандмауэр вручную или автоматически.

- Если на этом сервере включен брандмауэр, может понадобиться открыть дополнительные порты. Подробнее см. в разделе "Использование портов" документа Руководство по администрированию платформы APM.

- Если выбрана настройка вручную, настройка портов не выполняется, и необходимо вручную настроить порты на сервере шлюза и сервере обработки данных.

f. Чтобы включить подключения к базе данных, необходимо нажать кнопку **Готово** на последнем экране программы.

3. Если программа установки и настройки баз данных запускалась в рамках установки сервера APM, то APM можно запускать на всех серверах только после успешной настройки всех параметров для всех баз данных. Подробнее см. в разделе Запуск и остановка APM на стр 21.

   Если программа установки и настройки баз данных запускалась для добавления нового сервера шлюза или для изменения ранее определенных типов базы данных или параметров подключения, то после успешного изменения параметров следует перезапустить все серверы APM и сборщики данных.

   Примечание. Если эта программа использовалась для изменения любых баз данных в рабочей среде APM, то из приложений MyBSM и Service Health будут удалены страницы и компоненты. Чтобы восстановить страницы и компоненты приложений MyBSM и Service Health, выполните следующие действия.

   - Откройте следующий каталог: **<корневой каталог сервера шлюза>\conf\uimashup\import**. Он содержит два каталога: **\loaded** и **\toload**.
   - Скопируйте содержимое каталога **\loaded** в каталог **\toload**. Перезапустите APM.

Приложение D: Автоматическая установка APM

Мастера для установки и настройки APM можно запустить в автоматическом режиме. В автоматическом режиме мастера запускаются из командной строки без отображения пользовательского интерфейса. Это позволяет пользователям Linux запускать эти мастера без использования X-окон (автоматический режим можно применять и в Windows).

Инструкции написаны для пользователей LInux. Чтобы выполнить файлы в среде Windows, замените все расширения файлов .bin на .exe и все расширения .sh на .bat.

Примечание. Для мастеров обновления автоматический режим не поддерживается.

В этом приложении рассматриваются следующие темы.

Как выполнить полную установку APM 9.30 автоматически

Эта процедура описывает полную установку APM в автоматическом режиме, включая использование мастера установки, мастера начальной настройки и установку последних вспомогательных версий.

Примечание. Для мастеров обновления автоматический режим не поддерживается.

1. Запустите мастер установки APM 9.30 в автоматическом режиме, запустив файл установки из командной строки с помощью параметра **-i silent**. Установочный файл хранится в корневом каталоге **<установочного носителя APM>**.
   - Чтобы установить серверы обработки данных и шлюза на один компьютер (стандартная установка) в каталог установки по умолчанию, выполните следующую команду:

     HPApm_9.30_setup.bin -i silent

   - Чтобы установить сервера обработки данных и шлюзов на разные компьютеры, используйте следующую процедуру.
     i. Создайте пустой файл **ovinstallparams.ini** в том же каталоге, где хранится исполняемый файл установки на обоих серверах.
     ii. Скопируйте следующий раздел в INI-файл на сервере шлюза.

     [installer.properties]

     setup=HPBsm

     group=**gateway**

     iii. Запустите мастер установки на сервере шлюза в автоматическом режиме:

     HPApm_9.30_setup.bin -i silent

     iv. Скопируйте следующий раздел в INI-файл на сервере обработки данных.

     [installer.properties]

     setup=HPBsm

     group=**process**

     v. Запустите мастер установки на сервере обработки данных в автоматическом режиме:

     HPApm_9.30_setup.bin -i silent

2. Откройте файл ответов в **<корневой каталог HPE APM>\Temp\emptyRspFile.xml** и добавьте значения в разделе Post Install.
3. Если вы планируете работать с APM от имени другого пользователя (не root), создайте нужного пользователя.
4. Запустите мастер начальной настройки.

   silentConfigureBSM.sh <корневой каталог HPE APM>\temp\emptyRspFile.xml postinstall
5. Выйдите из Linux и снова войдите (необязательно). Если при установке APM в среде Linux в мастере начальной настройки вы указали обычного пользователя (не root), необходимо выйти из системы и снова войти в нее под именем этого пользователя.
6. Запустите программу установки и настройки базы данных.

<корневой каталог HPE APM>\bin\silentConfigureBSM.<корневой каталог HPE APM>\temp\emptyRspFile. xml postinstall

7. Включите APM. Подробнее см. в разделе Запуск и остановка APM на стр 21.
8. Первое включение APM может занять около часа. Чтобы проверить статус APM, используйте следующий URL-адрес:

   http://localhost:11021/invoke?operation=showServiceInfoAsHTML&objectname=Foundations%3Atype%3DNannyManager
9. Мастер обновления хранится на серверах шлюза, обработки данных и серверах APM на одном компьютере в следующих расположениях.
   - В Windows:
     - Обновление с версии BSM 9.25: **<корневой каталог HPE APM>\bin\upgrade_wizard_run_from925.bat**
     - Обновление с версии BSM 9.26: **<корневой каталог HPE APM>\bin\upgrade_wizard_run_from926.bat**
   - В Linux:
     - Обновление с версии BSM 9.25: **/opt/HP/BSM/bin/upgrade_wizard_run_from925.sh**
     - Обновление с версии BSM 9.26: **/opt/HP/BSM/bin/upgrade_wizard_run_from926.sh**
10. В APM выберите **Администрирование платформы > Установка и обслуживание > Развертывание серверов**, чтобы включить приложения APM.

Как создать файл ответов, чтобы автоматически перезапустить мастер начальной настройки и программу установки и настройки базы данных.

При выполнении программы установки и настройки базы данных можно создать XML-файл, сохранив в нем использованные значения. Этот файл можно использовать для выполнения мастера на различных компьютерах.

1. Запустите программу установки и настройки базы данных в существующей системе APM.
2. Файл ответов создается и сохраняется в каталоге **<корневой каталог HPE APM>/temp** или в указанном расположении. В этом файле автоматически сохраняются значения, заданные при выполнении мастера начальной настройки, а также программы установки и настройки базы данных.
3. Можно запустить мастер начальной настройки и программу установки и настройки базы данных на любом компьютере в автоматическом режиме, использовав файл ответов со следующим синтаксисом:

   silentConfigureBSM.sh <путь к файлу ответов>/<имя файла ответов>.xml

   Примечание. Можно отдельно запустить два мастера с помощью следующей команды:

   silentConfigureBSM.sh <путь к файлу ответов>/<имя файла ответов>.xml [postinstall | configserver]

   Файл silentConfigureBSM.sh хранится в каталоге **<корневой каталог HPE APM>/bin**.

Как настроить проверку подлинности Windows при автоматическом запуске программы установки и настройки базы данных.

Программа установки и настройки базы данных позволяет настроить APM так, чтобы использовать учетные данные проверки подлинности Windows для подключения к схеме базы данных. Чтобы включить эту функцию при создании файла ответов вручную, оставьте пустыми ключи UserName и Password для каждой соответствующей схемы. В следующем примере показан пример раздела схемы базы управления в файле ответов, который позволяет использовать проверку подлинности Windows.

```
        <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>
```

Как зашифровать пароли в файле ответов

Пароли, которые хранятся в файле ответов, можно зашифровать для дополнительной безопасности. Для этого запустите программу шифрования паролей:

<корневой каталог HPE APM>/bin/postinstall.sh.

Введите свой пароль и программа шифрования вернет зашифрованную строку. Скопируйте строку в файл ответов, где должен был храниться пароль.

Ограничение. Зашифрованные пароли можно использовать только на компьютере, где выполняется программа шифрования.

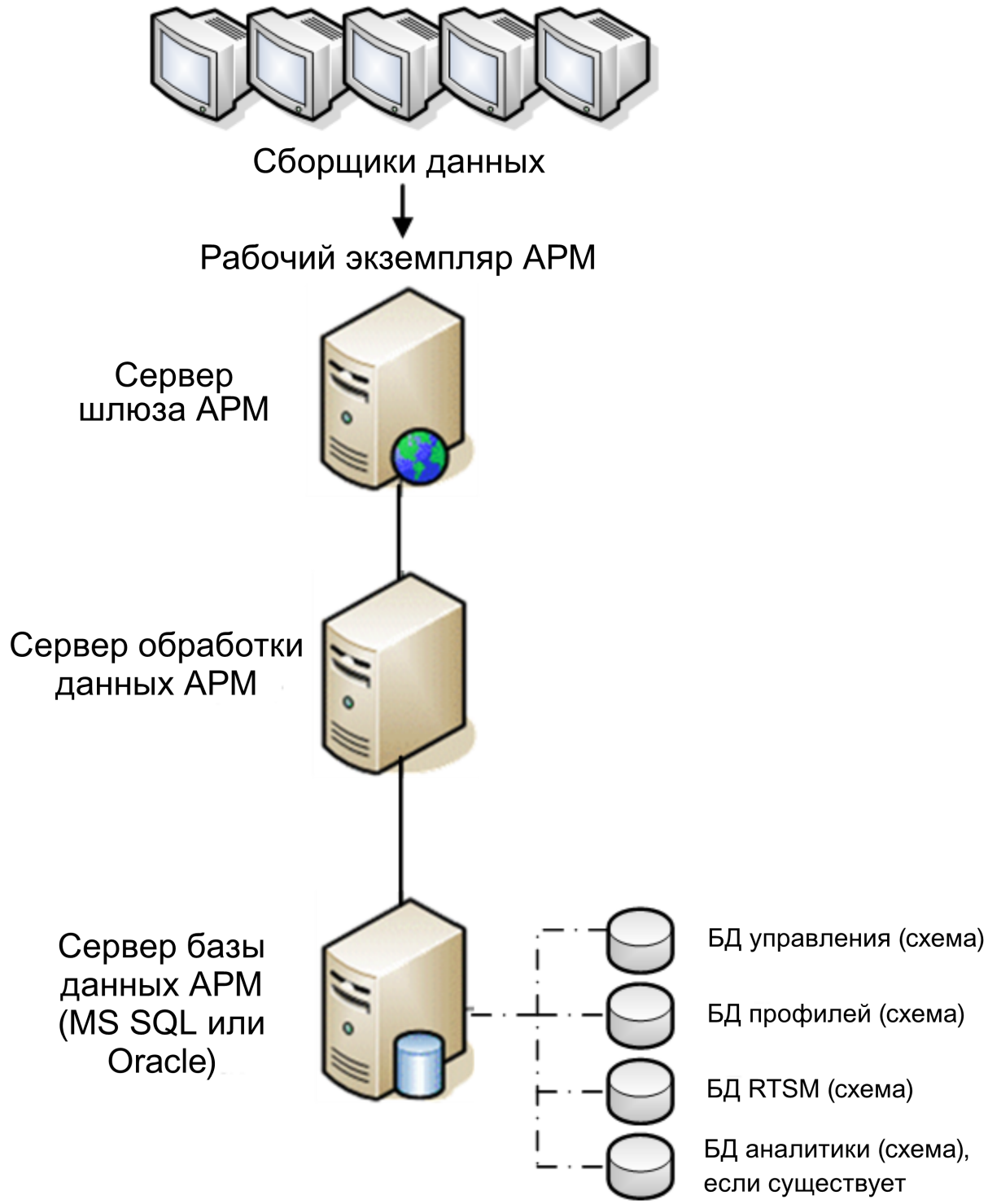
Чтобы отказаться от шифрования паролей, введите обычные пароли в файл ответов и задайте значение **IsEncrypted="false"**.

Приложение E: Аварийное восстановление APM

Общие сведения об аварийном восстановлении APM

Для системы APM можно настроить и активировать (в случае необходимости) систему аварийного восстановления.

В данной главе описываются основные принципы и даются указания по настройке системы аварийного восстановления, а также действия по переводу вторичной системы APM в режим основной системы APM.



Примечание.

- Для аварийного восстановления требуется вручную переносить различные файлы конфигурации и обновлять схемы баз данных APM. Чтобы выполнять эту процедуру,

необходим хотя бы один администратор APM и администратор базы данных, знакомый с базами данных и схемами APM.

- APM может развертываться в нескольких вариантах и конфигурациях. Для проверки работы сценария аварийного восстановления в конкретной среде необходимо тщательное тестирование и документирование. Обратитесь в HPE Professional Services, чтобы при проектировании аварийного восстановления и процедуры резервного переключения использовать рекомендованные методики.
- В среде аварийного восстановления должна быть установлена такая же операционная система, а каталог установки должен соответствовать каталогу в исходной среде.

Подготовка среды аварийного восстановления

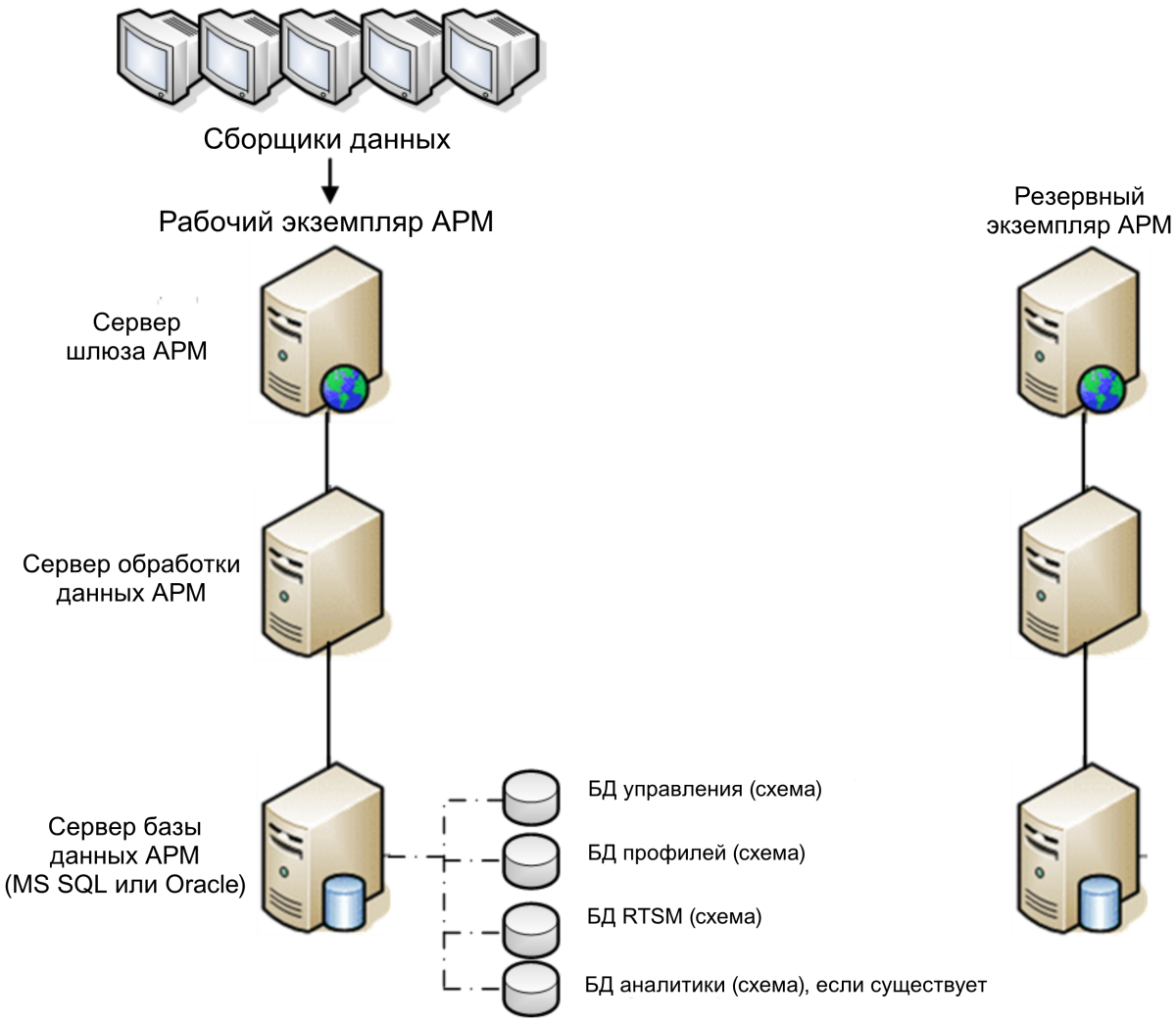
Подготовка среды аварийного восстановления

1. Установка набора серверов APM

Установите второй экземпляр APM в конфигурации, аналогичной конфигурации производственной среды.

- Установите в резервной среде точно такую же версию BSM, как в производственной среде.
- Резервная среда должна быть аналогична производственной (например, развертывание на одном или на двух компьютерах, аналогичное оборудование и т. д.), за исключением ситуаций, когда в производственной среде установлено более одного сервера шлюза или обработки данных. В последнем случае нужно создать только один набор серверов APM (один сервер шлюза и один сервер обработки данных либо сервер на одном компьютере) в качестве среды аварийного восстановления.
- В резервной среде должна быть установлена такая же операционная система, а каталог установки должен соответствовать каталогу в исходной среде.
- Не запускайте программу настройки сервера и базы данных, не создавайте базы данных и не включайте серверы.

На следующем рисунке показана типичная среда APM с установленной резервной системой.



2. Копирование файлов конфигурации из исходной системы

Скопируйте файлы, которые изменялись вручную, из следующих каталогов производственного экземпляра APM в тот же тип сервера в резервном экземпляре:

- odb/conf
- odb/content/
- BLE/rules/<пользовательские правила>.jar

Если создавались пользовательские отчеты в формате Excel, то их необходимо вручную скопировать в резервный экземпляр. Эти отчеты хранятся в каталоге **<корневой каталог HPE APM>\AppServer\webapps\site.war\openapi\excels** в отдельных папках для каждого ID заказчика.

Также скопируйте все остальные файлы и каталоги, в которые вносились изменения.

Примечание. Рекомендуем создавать резервные копии серверов APM ежедневно. В зависимости от объема и периодичности изменений конфигурации может потребоваться

более частое создание резервных копий, чтобы при отказе производственного экземпляра не были потеряны изменения конфигурации.

3. Настройка резервной базы данных

Создайте копию исходной базы данных. Теперь исходная база данных может служить резервной, а копия базы данных будет основной базой данных.

Примечание. HPE рекомендует выполнять этот этап сценария аварийного восстановления только опытному администратору базы данных.

- **Microsoft SQL — настройка доставки файлов журнала БД**

  Доставка файлов журнала позволяет свести к минимуму пропуски в данных мониторинга и конфигурации. При доставке файлов журнала создается точный дубликат исходной базы данных, отстающий от оригинала только на время, ушедшее на копирование и загрузку. После этого резервный сервер базы данных можно сделать рабочим в случае отказа последнего. После восстановления работоспособности основного сервера можно сделать его резервным, т.е. поменять серверы местами.

  Доставку файлов журнала необходимо настроить для следующих баз данных APM.

  - БД управления
  - RTSM
  - БД профилей (все базы данных)
  - БД Analytics (если есть)

  Сведения о настройке доставки для файлов журнала в Microsoft SQL Server см. в документации по Microsoft SQL Server.

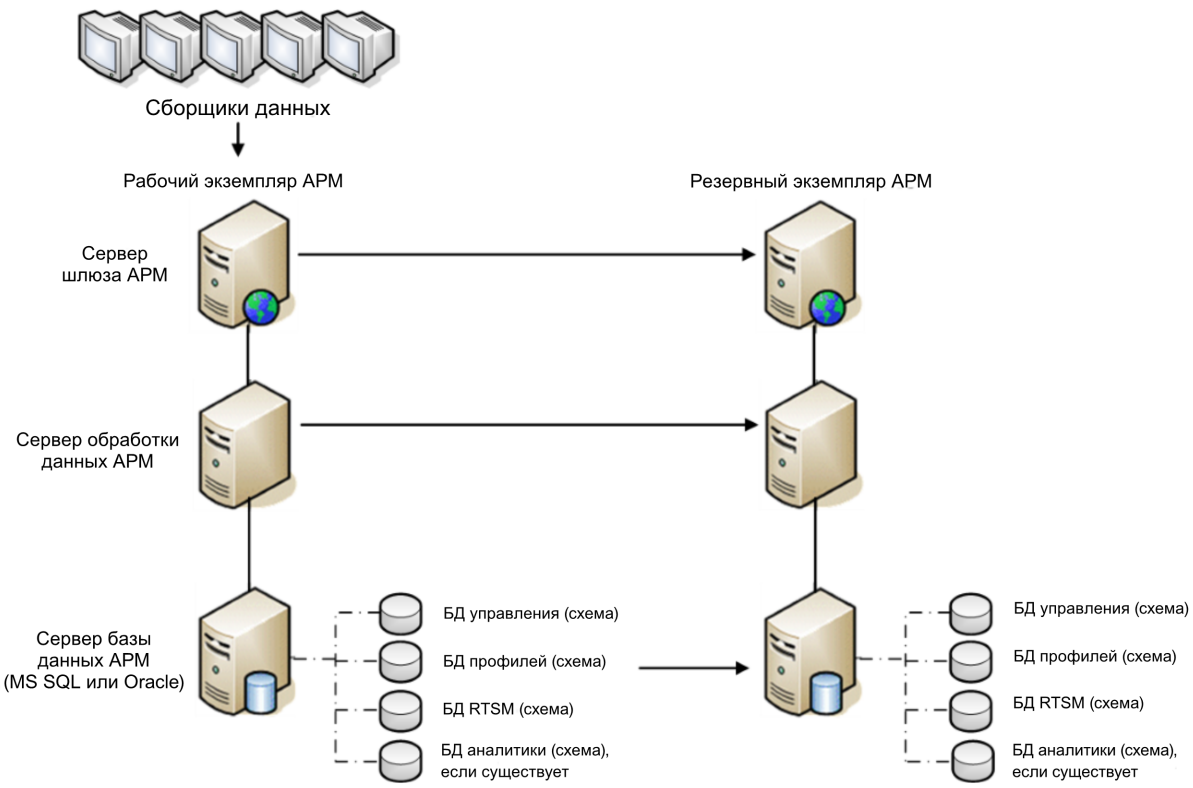
- **Oracle — настройка резервной базы данных (Data Guard)**

  Oracle ведет журналы не для каждой схемы, а только на уровне базы данных. Это значит, что нельзя создать резервную базу данных на уровне схемы, и необходимо создавать копии баз данных производственной системы в резервной системе.

  Сведения о настройке резервной базы данных см. в документации Oracle.

После успешного завершения настройки резервной базы данных необходимо синхронизировать резервную базу данных APM с производственной.

На следующем рисунке показаны производственная и резервная системы с включенной доставкой файлов журнала:


Сборщики данных
Рабочий экземпляр APM
Резервный экземпляр APM
Сервер шлюза APM
Сервер обработки данных APM
Сервер базы данных APM (MS SQL или Oracle)
БД управления (схема)
БД профилей (схема)
БД RTSM (схема)
БД аналитики (схема), если существует
БД управления (схема)
БД профилей (схема)
БД RTSM (схема)
БД аналитики (схема), если существует

Процедура очистки

После создания копии исходной среды необходимо вручную изменить некоторые настройки, чтобы не перепутать исходную среду с новой. Данная процедура удаляет из файлов конфигурации производственного экземпляра все ссылки, касающиеся конкретного компьютера.

Примечание.

- Перед началом процедуры активации администратор APM должен убедиться, что установлена необходимая лицензия для резервного экземпляра, а все доступные сборщики данных могут связываться с резервным экземпляром.
- HPE рекомендует, чтобы инструкции SQL в рамках данной процедуры выполнял опытный администратор базы данных.
- Приведенные ниже инструкции SQL должны выполняться в базе данных управления, за исключением последнего шага. Инструкции SQL из последнего шага должны выполняться в базе данных RTSM.

1. Удалите старые данные из таблиц высокой доступности (HA).

   В базе данных управления среды аварийного восстановления выполните следующие запросы:

   - **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. В базе данных управления среды аварийного восстановления выполните следующий запрос:

   Delete from PROPERTIES where NAME = 'HAServiceControllerUpgrade'

3. В таблице Sessions замените ссылки на базы данных управления среды аварийного восстановления ссылками на резервные базы данных.

   a. Выполните следующий запрос, чтобы получите имена всех баз данных:

      SELECT * FROM SESSIONS

      where SESSION_NAME like '%Unassigned%'

   b. Обновите следующие столбцы в каждой полученной строке указанными значениями:

- **SESSION_NAME:** замените именем новой восстановленной базы данных (только если SESSION_NAME имеет вид '%Unassigned%'). Используйте следующий скрипт:

  UPDATE SESSIONS set SESSION_NAME='Unassigned<имя_НОВОГО_сервера_БД><имя_НОВОЙ_схемы><имя_пользователя_БД>'

  WHERE SESSION_NAME='Unassigned<имя_СТАРОГО_сервера_БД><имя_СТАРОЙ_схемы><имя_пользователя_старой_БД>'
- **SESSION_DB_NAME:** замените именем новой восстановленной схемы. Используйте следующий скрипт:

  UPDATE SESSIONS set SESSION_DB_NAME='<имя_НОВОЙ_схемы>'

  WHERE SESSION_DB_NAME='<имя_СТАРОЙ_схемы>'
- **SESSION_DB_HOST:** замените именем хоста новой восстановленной базы данных. Используйте следующий скрипт:

  UPDATE SESSIONS set SESSION_DB_NAME='<имя_НОВОГО_хоста>'

  WHERE SESSION_DB_HOST='<имя_СТАРОГО_хоста>'
- **SESSION_DB_PORT:** замените именем порта новой восстановленной схемы. Используйте следующий скрипт:

  UPDATE SESSIONS set SESSION_DB_PORT='<имя_порта_НОВОЙ_схемы>'

  WHERE SESSION_DB_PORT='<имя_порта_СТАРОЙ_схемы>'
- **SESSION_DB_SID:** замените именем нового восстановленного ID сеанса. Используйте следующий скрипт:

  UPDATE SESSIONS set SESSION_DB_SID='<имя_нового_SID>'

  WHERE SESSION_DB_SID='<имя_старого_SID>'
- **SESSION_DB_UID:** замените новым восстановленным именем. Используйте следующий скрипт:

  UPDATE SESSIONS set SESSION_DB_UID='<имя_нового_UID>'

  WHERE SESSION_DB_UID='<имя_старого_UID>'
- **SESSION_DB_SERVER:** замените именем нового восстановленного сервера. Используйте следующий скрипт:

  UPDATE SESSIONS set SESSION_DB_SERVER='<имя_НОВОГО_сервера>'

  WHERE SESSION_DB_SERVER='<имя_СТАРОГО_сервера>'

4. В таблице Analytics замените ссылки на базы данных управления ссылками на резервные базы данных.
   a. Выполните следующий запрос, чтобы получите имена всех баз данных:

      SELECT * FROM ANALYTICS_DATABASES
   b. Обновите следующие столбцы в каждой полученной строке указанными значениями:
      - **DB_HOST:** замените именем хоста новой восстановленной базы данных. Используйте следующий скрипт:

        update ANALYTICS_DATABASES set DB_HOST='NEWDatabasehostname' where DB_HOST='OLDDatabasehostname';
      - **DB_SERVER:** замените именем нового восстановленного сервера. Используйте следующий скрипт:

update ANALYTICS_DATABASES set DB_SERVER='NEWDatabaseServerName' where DB_SERVER='OLDDatabaseServerName'

- **DB_NAME:** замените именем нового восстановленного сервера. Используйте следующий скрипт:

  update ANALYTICS_DATABASES set DB_NAME='NEWDatabaseName' where DB_NAME='OLDDatabaseName'

- **DB_SID:** замените именем нового восстановленного ID сеанса. Используйте следующий скрипт:

  update ANALYTICS_DATABASES set DB_SID ='NEWSID' where DB_SID='OLDSID';

- **DB_PORT:** замените именем порта новой восстановленной схемы. Используйте следующий скрипт:

  update ANALYTICS_DATABASES set DB_PORT= 'NewPort' where DB_PORT='OldPort'

5. Удалите данные о кластере шины из таблицы PROPERTIES в базе данных управления.

   Выполните следующий запрос:

   Delete from PROPERTIES where

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

6. Удалите компьютеры из таблицы Deployment в базе данных управления.

   Выполните следующий запрос:

   DELETE from DEPLOY_HW

7. Значения диспетчера настроек в таблице **SETTING_PARAMETERS** в базе данных управления.

   Обновите URL-адреса и сервер LDAP в таблице SETTING_PARAMETERS.

   В следующей таблице показаны ключи из таблицы диспетчера настроек, которые нужно обновить:

SP_CONTEXT	SP_NAME	Описание
platform	settings.smtp.server	Имя SMTP-сервера, используемого для модуля оповещений
scheduledreports	settings.smtp.server	Имя SMTP-сервера, используемого для плановых отчетов
platform	default.core.server.url	URL-адрес для доступа сборщиков данных к серверу шлюза в APM
platform	default.centers.server.url	URL-адрес для доступа пользователей к APM
platform	virtual.centers.server.url	
platform	virtual.core.server.url	

   Измените следующий запрос для каждого ключа в таблице и выполните его:

   update SETTING_PARAMETERS set SP_VALUE='<новое значение>'

   where SP_CONTEXT='<значение контекста>' and SP_NAME='<значение имени>'

   Выполните следующие команды:

- update SETTING_PARAMETERS set SP_VALUE='<новое_имя_компьютера>', где SP_CONTEXT='platform' и SP_NAME='settings.smtp.server'
- update SETTING_PARAMETERS set SP_VALUE='<новое_имя_компьютера>', где SP_CONTEXT='scheduledreports' и SP_NAME='settings.smtp.server'
- update SETTING_PARAMETERS set SP_VALUE='http://<новое_имя_компьютера>:80', где SP_CONTEXT='platform' и SP_NAME='default.core.server.url'
- update SETTING_PARAMETERS set SP_VALUE='http://<новое_имя_компьютера>:80', где SP_CONTEXT='platform' и SP_NAME='default.centers.server.url'

Две последних настройки в таблице не требуют обновления, если не используется балансировщик нагрузки или обратный прокси-сервер. В таком случае обновите настройки следующим-образом:

- update SETTING_PARAMETERS set SP_VALUE='http://<балансировщик нагрузки или обратный прокси-сервер>:80', где SP_CONTEXT='platform' и SP_NAME='virtual.centers.server.url'
- update SETTING_PARAMETERS set SP_VALUE='http://<балансировщик нагрузки или обратный прокси-сервер>:80', где SP_CONTEXT='platform' и SP_NAME='virtual.core.server.url'

8. Обновите ключи SYSTEM.

   Обновите следующие ключи в таблице SYSTEM в базе данных управления:

AdminServerURL	http://<DPS1>:port	По умолчанию номер порта не задается.
GraphServerURL	http://<GW1>/topaz/	
GraphServerURL4.5.0.0	http://<GW1>/topaz/	
application.tac.path	http://<GW1>:port/AdminCenter	По умолчанию используется порт 80.
application.flipper.path	http://<GW1>:port/monitoring	По умолчанию используется порт 80.

   Измените следующий запрос для каждого значения в таблице и выполните его:

   update SYSTEM set SYS_VALUE='<новое значение>' where SYS_NAME='<ключ>',

   где **<новое значение>** это новый URL-адрес в формате исходного URL-адреса.

   Пример.

   update SYSTEM set SYS_VALUE='http://<новое имя компьютера>:port', где SYS_NAME='AdminServerURL'

   Примечание. По умолчанию используется порт 80.

9. Очистите и обновите таблицы в базе данных RTSM.

   Данная процедура удаляет из таблиц конфигурации RTSM все ссылки, касающиеся конкретного компьютера.

   Выполните следующие инструкции SQL в базе данных RTSM:

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

Настройка новой среды

1. Запуск программы настройки сервера и базы данных

   Запустите программу настройки сервера и базы данных на каждом компьютере, чтобы повторно инициализировать необходимые таблицы в базе данных. Чтобы запустить эту программу, выберите **Пуск > Все программы > HPE Application Performance Management > Администрирование > Настройка HPE Application Performance Management**.

   Примечание. При работе с программой настройки сервера и базы данных необходимо подключиться к базам данных, созданным для резервной среды (т.е. к тем, в которые были отправлены резервные данные). Запуск этой программы в производственном экземпляре может привести к полной потере данных конфигурации.

   Запускайте программу настройки сервера и базы данных на компьютерах в том же порядке, в котором выполнялась установка APM в резервной среде.

2. Включите APM

   Включите APM на новых серверах.

3. Выполните процедуру очистки после запуска, чтобы отключить устаревшие хосты, не входящие в резервный экземпляр.

   Чтобы отключить устаревшие хосты, выполните следующие действия.

   a. В APM откройте раздел **Администрирование > Платформа > Установка и обслуживание > Развертывание серверов** и выберите пункт **Отключить компьютер**.
   b. Отключите все устаревшие хосты.

4. Повторите процедуры по повышению безопасности (не обязательно)

   Если вы повысили безопасность исходной среды, следует повторить процедуры по повышению безопасности в новой среде.

   Процедуры настройки обратного прокси-сервера повторять не требуется.

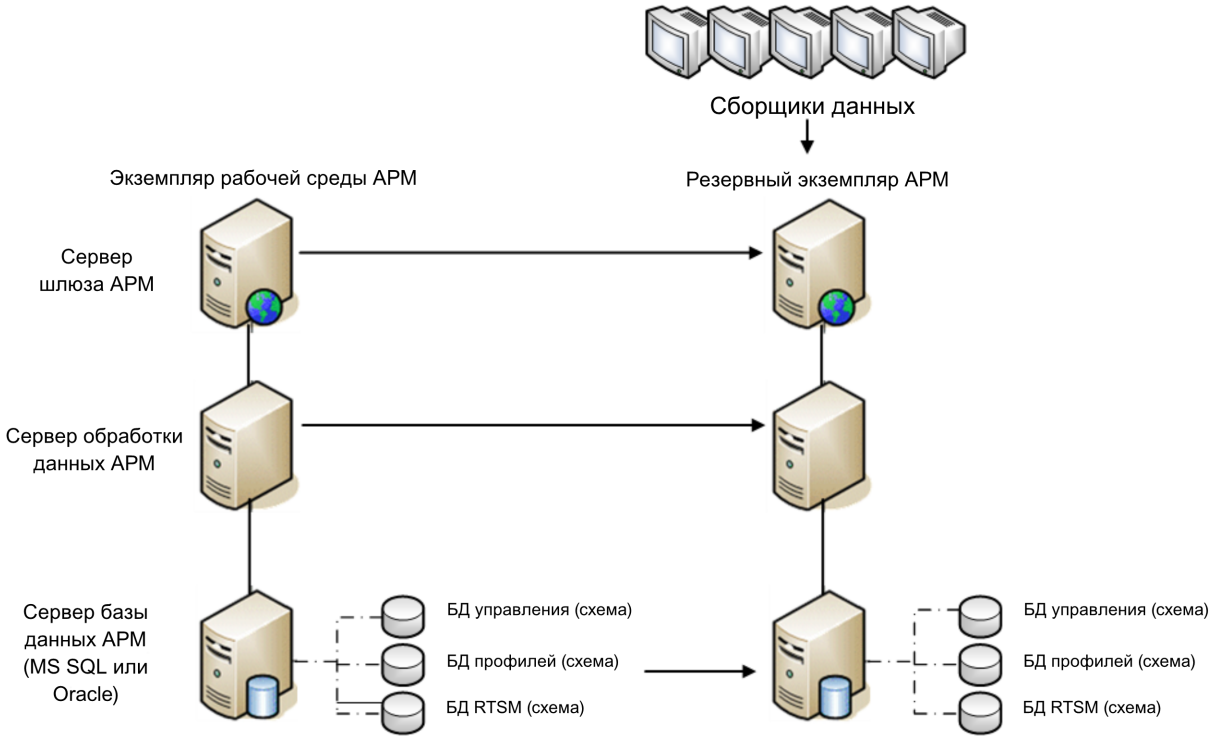
   Подробнее см. в руководстве по повышению безопасности APM.

Настройка сборщиков данных

1. Настройте сборщики данных.

   Настройте все сборщики данных, включая агенты Business Process Monitor, платформы Real User Monitor, экземпляры SiteScope, HPOM, Service Manager, Operations Orchestration (если он установлен на отдельном сервере), для работы с резервным экземпляром. Подробнее см. в документации по каждому сборщику данных.

   На следующем рисунке показан резервный экземпляр, полностью прошедший активацию:



2. Настройка подключений к резервным сборщикам данных.

   Если в каких-либо сборщиках данных произошла ошибка, и они перемещены на другие компьютеры, то необходимо передать новые URL-адреса на серверы APM. Это выполняется в различных приложениях APM. Пример.

Сборщик данных	**Процедура**
SiteScope	Повторно подключите серверы SiteScope к серверу APM из консоли SiteScope.
Business Process Monitor	Повторно подключите серверы BPM к серверу APM из консоли BPM.

Сборщик данных	Процедура
Real User Monitor	Повторно подключите серверы RUM к серверу APM из консоли RUM.
HP Operations Orchestration	На сервере HP Operations Orchestration измените конфигурацию в соответствии с данными нового сервера APM, выполнив процедуру, описанную в руководстве "Решения и интеграции".
HPE Service Manager	На сервере HPE Service Manager измените конфигурацию в соответствии с данными нового сервера APM, выполнив процедуру, описанную в руководстве "Решения и интеграции".
Сборщик данных SHA PA	Повторно подключите сборщик данных SHA PA, запустив еще раз мастер настройки.

Приложение F: Высокая доступность для APM

В этом приложении рассматриваются следующие темы.

Обзор параметров высокой доступности

Доступность и надежность системы можно повысить различными способами, в которых сочетаются применение нескольких серверов, внешние средства балансировки нагрузки и процедуры резервного переключения.

При конфигурации высокой доступности сервера APM настроены таким образом, что обслуживание будет продолжаться несмотря на перебои электропитания, простой компьютера и высокую нагрузку.

Балансировку нагрузки и высокий уровень доступности можно реализовать при развертывании на одном компьютере и в распределенном развертывании. Для балансировки нагрузки добавляется дополнительный сервер шлюза, а для обеспечения высокой доступности добавляется резервный сервер обработки данных.

Высокая доступность реализуется на двух уровнях.

- **Аппаратная инфраструктура.** К этому уровню относятся резервные серверы, сети, источники питания и другие элементы.
- **Приложение.** Этот уровень состоит из двух компонентов.
  - **Балансировка нагрузки.** Балансировка нагрузки распределяет рабочую нагрузку по нескольким компьютерам. В результате производительность и доступность системы увеличиваются.

    Внешнее устройство балансировки нагрузки — это аппаратно-программный модуль, предоставляемый внешним поставщиком. Необходимо установить этот модуль и настроить его для работы с приложениями APM.

  - **Резервное переключение.** Если основной сервер отказывает или становится временно недоступным, то работу, выполняемую сервером обработки данных, принимает на себя резервный сервер.

    В этой главе подробно описывается реализация балансировки нагрузки и резервного переключения.

Примечание. Подразделение HPE Software Professional Services предоставляет консультационные услуги для заказчиков по стратегическому планированию и развертыванию APM. За подробными сведениями обращайтесь к представителю компании HPE.

Балансировка нагрузки для сервера шлюза

Если установлено несколько серверов шлюза APM, то APM может использовать внешние механизмы балансировки нагрузки, чтобы равномерно распределять операции обработки и передачи данных по сети. Это особенно важно в случаях высокой нагрузки, чтобы исключить чрезмерную загрузку отдельно взятого сервера.

Примечание. Рекомендуем устанавливать APM за балансировщиком нагрузки или обратным прокси-сервером. Это обеспечивает дополнительную безопасность и может упростить процедуры обновления и аварийного восстановления.

В этом разделе рассматриваются следующие темы.

Настройка балансировки нагрузки на стр 87

Примечания и ограничения на стр 89

Настройка балансировки нагрузки

1. Создайте два виртуальных имени хоста. Виртуальное имя хоста должно быть полным доменным именем в формате **<имя_сервера>.<имя_домена>**. Это требование необходимо для поддержки проверки подлинности упрощенного единого входа, которая включена по умолчанию.

   Первое имя хоста предназначено для доступа к веб-сайту APM на сервере шлюза. Этот URL-адрес можно передавать пользователям APM. Второе имя хоста предназначено для доступа сборщиков данных к серверу шлюза. Этот URL-адрес должен использоваться при настройке сборщиков данных для связи с APM.
2. Введите имена хоста для балансировщика нагрузки в настройках инфраструктуры для виртуальных серверов. Для этого выберите **Администрирование > Платформа > Установка и обслуживание > Настройки инфраструктуры**, а затем **Базовые настройки** > **Администрирование платформы – Конфигурация хостов**:
   - **URL-адрес виртуального сервера шлюза по умолчанию для пользователей приложений.** Виртуальное имя хоста для веб-сайта APM. Сервер шлюза, на котором идет работа, должен иметь возможность разрешить этот виртуальный IP-адрес. Это значит, что команда **nslookup** для **виртуального имени хоста для пользователей приложений**, запущенная на этом сервере шлюза, должна возвращать имя и IP-адрес.
   - **URL-адрес виртуального сервера шлюза по умолчанию для сборщиков данных.** Виртуальное имя хоста для сборщиков данных. Все сборщики данных должны иметь возможность разрешить этот виртуальный IP-адрес. Это значит, что команда **nslookup** для **виртуального имени хоста для сборщиков данных**, запущенная на сервере сборщика данных, должна возвращать имя и IP-адрес.
3. В области "Конфигурация обратных прокси-серверов" задайте следующие параметры.
   - **Параметр "Разрешить использование обратного прокси-сервера" = true.**
   - **IP-адреса обратных прокси-серверов HTTP**

     Добавьте в это поле внутренние IP-адреса устройств балансировки нагрузки.

- Если указать IP-адрес балансировщика нагрузки, отправляющего запрос HTTP/HTTPS, то клиенту возвращается URL-адрес виртуального сервера по умолчанию или URL-адрес локального виртуального сервера (если он определен).
- Если в этом параметре не определены IP-адреса (не рекомендуем), то APM работает в общем режиме. возможен вход в систему APM только при помощи виртуального URL-адреса, а не напрямую через шлюз.

Примечание. Если используется балансировщик нагрузки, которое не находится в одном домене с серверами шлюза APM, необходимо добавить IP-адрес обратного прокси-сервера в параметр **IP-адреса обратных прокси-серверов HTTP и HTTPS**. Подробнее см. раздел "Конфигурация LW-SSO для установки в нескольких доменах и вложенных доменах" документа "Руководство по администрированию платформы APM".

Чтобы узнать IP-адрес балансировщика нагрузки, выполните следующие действия.

a. Войдите в систему APM через балансировщик нагрузки.
b. Откройте журнал **<корневой каталог сервера шлюза HPE APM>\log\EJBContainer\UserActionsServlet.log**.
c. IP-адрес, указанный в последней строке с записью о входе в систему, и есть IP-адрес балансировщика нагрузки. В записи должно быть указано ваше имя пользователя.

4. После изменения настроек обратного прокси-сервера перезапустите службу HPE APM на сервере шлюза APM и сервере обработки данных.

Примечание. Если ваш балансировщик нагрузки позволяет выбирать топологию Full-NAT или Half-NAT, выберите **Full-NAT**.

5. Настройте балансировщик нагрузки для доступа сборщиков данных. Все сборщики данных должны иметь доступ к виртуальному IP-адресу балансировщика нагрузки. Используйте стандартные настройки для балансировщика нагрузки и дополнительно задайте следующие значения.
   - Мы рекомендуем использовать алгоритм циклического перебора, чтобы сбалансировать нагрузку на серверы шлюза APM.
   - Используйте следующий URI проверки активности.
     - Строка отправки: **GET /ext/mod_mdrv_wrap.dll?type=test**
     - Строка приема: **Система Web Data Entry доступна**
6. Настройте балансировщик нагрузки для доступа пользователей.
   - Используйте стандартные настройки для балансировщика нагрузки и дополнительно установите режим сохранения **включено закрепление по сеансам** или **привязка к адресу назначения** (в зависимости от устройства балансировки). Если эти параметры недоступны, и можно выбрать закрепление **по файлам cookie** или **по IP-адресу**, то рекомендуем режим закрепления **по IP-адресу**. Если этот параметр настроен неправильно, то возможны периодические проблемы с пользовательским интерфейсом.
   - Используйте следующий URI проверки активности.
     - Строка отправки: **GET /topaz/topaz_api/loadBalancerVerify_centers.jsp**
     - Строка приема: **Успешно**

Примечания и ограничения

- APM поддерживает аппаратные и виртуальные балансировщики нагрузки. С точки зрения безопасности лучше использовать аппаратный балансировщик нагрузки. Все балансировщики нагрузки должны позволять настройку закрепленных сеансов для пользователей и мониторов работоспособности на основе URL-адреса.
- Если используются два балансировщика нагрузки (для поддержки резервного переключения), то убедитесь, что на компьютере с DNS-сервером настроены имена хостов для обоих устройств балансировки. Затем можно указать имя компьютера, полное доменное имя хоста или URL-адрес любого балансировщика нагрузки, когда это будет необходимо для сборщиков данных или в браузере, чтобы открыть сайт APM.
- Если два сервера шлюза установлены на разных логических дисках, например один на диске C:\, а другой на диске E:\, то доступ к APM может оказаться невозможен.

  Обходное решение. Создайте дубликат пути на диске **C:\, скопировав E:\<корневой каталог HPE APM>\conf\settings** в **C:\<корневой каталог HPE APM>\conf\settings**.
- Если используются два балансировщика нагрузки (для поддержки резервного переключения), каждое из которых работает с несколькими типами серверов, то следует определить на каждом устройстве балансировки уникальное виртуальное имя хоста для каждого типа сервера, сопоставить виртуальные имена хоста с фактическими именами хоста соответствующих серверов и убедиться, что все виртуальные имена хоста настроены на компьютере с DNS-сервером. Затем можно указать любое из доступных виртуальных имен хоста для каждого сборщика данных или в браузере, чтобы открыть сайт APM.
- Настроив балансировщик нагрузки, убедитесь в его доступности со всех серверов APM (серверов шлюзов и обработки данных) по виртуальным адресам, указанным для подключений.

Высокая доступность для сервера шлюза

HPE Application Performance Management предоставляет функции обеспечения высокой доступности для серверов шлюза, чтобы гарантировать доставку данных в назначение и возможность использования приложений APM в случае отказа сервера.

Защищенная доставка входящих данных

APM обеспечивает защищенную доставку данных мониторинга. Защищенная доставка означает, что данные не удаляются из одного хранилища, пока они не будут направлены в следующее хранилище и сохранены в нем.

Примечание. HPE Professional Services предлагает консультации по оптимальным методам работы. Чтобы узнать, как получить эти услуги, обратитесь к представителю HPE.

APM поддерживает следующие механизмы, обеспечивающие высокую доступность необработанных данных.

- Если отказывает компьютер, на котором располагается веб-сервер или сервер шлюза, то данные направляются балансировщиком нагрузки на другой сервер шлюза или помещаются в очереди сборщика данных, пока веб-сервер не станет доступен.
- Если компьютер с веб-сервером или сервером шлюза получает данные, но шина недоступна, то данные хранятся в сборщике данных, пока шина вновь не станет доступной.
- Если шина принимает данные, но недоступен загрузчик данных мониторинга, то данные хранятся в шине, пока загрузчик снова не станет доступен. Затем данные отправляются в базу данных.

Высокая доступность для приложения Service Health

HPE Application Performance Management предоставляет функции обеспечения высокой доступности для приложения Service Health на сервере шлюза, чтобы пользователи могли продолжать работу с приложением Service Health даже при отказе сервера шлюза во время пользовательского сеанса.

Когда пользователь входит в APM и начинает работу с приложением Service Health, сведения о сеансе регистрируются на определенном сервере шлюза, а балансировщик нагрузки направляет все данные, передаваемые в рамках данного сеанса, на этот же сервер шлюза. Если этот сервер шлюза отказывает, то балансировщик нагрузки перенаправляет сеанс на другой сервер шлюза, и сеанс повторно регистрируется на новом сервере шлюза. Пользователь продолжает работу без перерыва в обслуживании и без необходимости повторно входить в APM.

Для балансировщика нагрузки на сервере шлюза должен быть задан режим **включено закрепление по сеансам**. Подробнее см. в разделе Настройка балансировки нагрузки на стр 87.

Внимание! В некоторых ситуациях может оказаться, что переход с одного сервера шлюза на другой займет несколько секунд. До завершения такого перехода некоторые действия пользователя могут завершаться ошибками.

Высокая доступность для сервера обработки данных

Для обеспечения высокой доступности следует установить резервный сервер обработки данных. В случае отказа основного сервера обработки данных APM продолжает работу, используя резервный сервер.

Совет. Рекомендуем устанавливать основной и резервный серверы обработки данных, обладающих сравнимыми характеристиками оборудования, объемом памяти и производительностью.

Если для сервера обработки данных включена высокая доступность и определен резервный сервер, то в случае, когда одна или несколько служб становятся недоступными, контроллер высокой доступности выполняет автоматическое резервное переключение и переносит службы на резервный сервер. Сервер получает текущую конфигурацию из базы данных управления и продолжает обслуживание в качестве нового активного сервера обработки данных.

Службы можно вручную перенести на резервный сервер с помощью консоли JMX. Например, это может понадобиться в случае, когда планируется техническое обслуживание одного из серверов обработки данных. Перенос служб вручную может сократить время простоя APM.

Примечание. При развертывании нового экземпляра APM первый запущенный сервер обработки данных становится сервером по умолчанию для служб, назначенных этому серверу, то есть становится основным сервером обработки данных. Когда запускается второй сервер обработки данных, ему можно назначить роль резервного сервера. Подробнее см. в разделе "Общие сведения о переназначении служб" документа Руководство по администрированию платформы APM.

В этом разделе рассматриваются следующие темы.

Службы, назначенные серверу

Серверам шлюза и серверам обработки данных назначаются разнообразные процессы. Каждый процесс отвечает за работу определенных служб. В консоли JMX можно просмотреть службы, работающие на серверах APM или на определенном сервере, например, на сервере обработки данных.

Просмотр служб через веб-консоль JMX.

1. В веб-браузере откройте адрес

   http://<имя компьютера сервера обработки данных>:29000
2. Введите учетные данные для проверки подлинности консоли JMX, когда они будут запрошены (если эти данные отсутствуют, обратитесь к системному администратору).
3. В разделе **Topaz** выберите значение **service=hac-manager**.
4. Для метода **java.lang.String listAllAssignments()** нажмите кнопку **Вызвать**.

   Чтобы просмотреть службы на определенном сервере, например сервере обработки данных, введите имя этого сервера в качестве значения параметра. Чтобы просмотреть все службы, оставьте параметр имени сервера пустым.

Процессы, работающие на сервере, отображаются в таблице. Оперативная таблица JMX содержит следующие столбцы:

Имя столбца	Описание
Услуга	Имя назначенной услуги
Заказчик	ID заказчика, которому назначена услуга. По умолчанию для отдельной системы APM (которая не управляется с помощью HPE Software-as-a-Service) ID заказчика имеет значение 1. Услуга с ID заказчика -1 является глобальной услугой, которая используется всеми заказчиками в среде SaaS.
Процесс	Имя сервера обработки данных и имя процесса JVM, отвечающего за услугу. Также отображается продолжительность работы сервера и время последней проверки связи с сервером.
Назначено	Показывается, активно ли в данный момент назначение услуги, дата назначения услуги и время, в течение которого служба была назначена.
Состояние	Текущее состояние службы. Допустимые состояния: 1 – остановлен 2 – запускается 3 – останавливается 4 – выполняется -1 – ошибка -2 – не удалось остановить -3 – не удалось запустить Указывается дата перехода услуги в текущее состояние и продолжительность пребывания в этом состоянии.
Подп. сервера	Сигнатура сервера.
Подп. состояния	Сигнатура состояния (должна совпадать с сигнатурой сервера).

Службы, управляемые контроллером высокой доступности (HAC)

В следующей таблице описываются службы сервера обработки данных, которыми может управлять контроллер высокой доступности (HAC). Также указываются:

- Имя процесса в JVM
- Имя, используемое контроллером высокой доступности (HAC) для процесса
- Службы, работающие в процессе
- Описание процесса

Имя процесса JVM	**Имя процесса HAC**	**Имя услуги**	**Описание услуги** **Расположение файла журнала**
Mercury AS	mercury _as	KPI_ ENRICHMENT	Служба KPI_Enrichment отвечает за добавление KPI на панели мониторинга в КЕ, добавленные в модель внешними системами мониторинга. Добавляемые KPI и КЕ, в которые они добавляются, можно настраивать.
		BSM_DT	BSM_DT обрабатывает значения времени простоя, заданные в системе. Значения времени простоя можно задавать в КЕ. Они влияют на оповещения, события, отчеты, вычисление KPI и мониторинг.
		VERTICALS	Служба Verticals предназначена для SAP и обеспечивает совместимость с APM. Служба SAP связывает данные, полученные от серверов SiteScope и Business Process Monitor, с объектами SAP, полученными из RTSM.
		EUM_ADMIN	EUM_ADMIN отвечает за администрирование End User Management, если серверы Business Process Monitor и Real User Monitor настроены для мониторинга.
mercury_odb	odb	BSM_ODB	RTSM — это центральный репозиторий данных о конфигурации, собранных различными приложениями и инструментами (APM и сторонних разработчиков). Данная информация используется для создания представлений APM.

Имя процесса JVM	Имя процесса HAC	Имя услуги	Описание услуги Расположение файла журнала
hpbsm_ bizImpact	businessimpact_ service	BIZ_IMPACT	Компонент "Влияние на бизнес" позволяет просматривать бизнес-КЕ и SLA, на которые влияет другой КЕ в приложении Service Health.
		LIV_SERVICE	Локальное представление влияния также позволяет создавать локальные представления влияния в приложении Service Health. Они не зависят от других представлений. Когда изменяются определения индикаторов в КЕ в пределах локального представления влияния, это изменение никак не затрагивает данную КЕ в других представлениях.
hpbsm _offline _engine	offline_ engine	NOA	Служба нового автономного агрегатора проверяет и синхронизирует (ежечасно или ежедневно) новые задачи для автономного агрегатора.
hpbsm _marble _supervisor	marble_ supervisor	DASHBOARD	Служба панели мониторинга на сервере обработки данных отвечает за расчеты оперативной бизнес-логики для приложения Service Health.
hpbsm_ pmanager	pmanager	PM	Диспетчер секционирования и очистки разделяет быстро растущие таблицы на секции с определенным интервалом времени. После истечения определенного времени данные, находящиеся в секции, становятся недоступными для отчетов APM. Когда истекает другой определенный период времени, эта секция удаляется из базы данных профилей.
hpbsm_pi_ engine	pi_engine	PI_ENGINE	Модуль Service Health Analyzer отслеживает отклонения от нормы для базовых показателей системы.
hpbsm_basel_ engine	basel_engine	BASELVALIDATOR	Средство проверки базовых задач проверяет выполнение базовых задач по набору метаданных и добавляет или удаляет задачи по мере необходимости.

Настройка автоматического резервного переключения

Можно настроить для служб, работающих на основном сервере обработки данных, автоматическое переназначение на резервный сервер обработки данных. Чтобы настроить для служб, работающих на основном сервере обработки данных, автоматическое переназначение на резервный сервер обработки данных, выполните следующие действия.

- Определите резервный сервер обработки данных на консоли JMX.
- Включите автоматическое резервное переключение.

Примечание. Если включить автоматическое резервное переключение и задать таймаут проверки активности менее десяти минут, службы APM могут переключиться на резервный сервер после перезапуска. Чтобы исключить такую ситуацию, при отключении APM сначала завершайте работу резервного сервера, а затем — основного. При включении APM сначала включите основной сервер и убедитесь, что запущены все службы, а затем включите резервный сервер.

Определение резервного сервера

Для определения или удаления резервного сервера обработки данных необходимо использовать консоль JMX. Также можно просмотреть конфигурации высокой доступности.

Чтобы определить резервный сервер на консоли JMX, выполните следующие действия.

1. В веб-браузере откройте адрес
   http://<имя компьютера сервера обработки данных>:29000

   Введите учетные данные для проверки подлинности консоли JMX, когда они будут запрошены (если эти данные отсутствуют, обратитесь к системному администратору).
2. В разделе **Topaz** выберите значение **service=hac-backup**.
3. Найдите метод **addBackupServer** и введите следующие значения:
   - **primaryServerName**. Имя основного сервера.
   - **backupServerName**. Имя резервного сервера.

   В обоих параметрах следует задавать имя компьютера, а не полное доменное имя (FQDN). Если имя компьютера точно не известно, можно использовать метод **listservers**, описанный далее, чтобы получить список имен уже настроенных компьютеров.
4. Нажмите кнопку **Вызвать**.

Чтобы удалить резервный сервер, выполните следующие действия.

1. Выполните шаги 1 и 2, описанные выше, чтобы открыть консоль JMX и службу **hac-backup**.
2. Найдите метод removeBackupServer и введите следующее значение:

   primaryServerName. Имя основного сервера, для которого удаляется резервный сервер.
3. Нажмите кнопку **Вызвать**.

Чтобы просмотреть конфигурацию высокой доступности, выполните следующие действия.

1. Выполните шаги 1 и 2, описанные выше, чтобы открыть консоль JMX и службу **hac-backup**.
2. Найдите метод **listservers** и нажмите кнопку **Вызвать**.

Появится список **Серверы** и список **Резервные серверы**. Если резервные серверы не определены или не включена высокая доступность, то появится сообщение о том, что автоматическое резервное переключение отключено.

Включение автоматического резервного переключения

Его можно включить в разделе "Настройки инфраструктуры" в интерфейсе APM или в консоли JMX. В консоли JMX также можно проверить, включена ли высокая доступность.

Чтобы включить автоматическое резервное переключение в настройках инфраструктуры, выполните следующие действия.

1. Выберите **Администрирование > Платформа > Установка и обслуживание > Настройки инфраструктуры**.
2. Выберите пункты **Базовые настройки** и **Контроллер высокой доступности**, а затем найдите запись **Автоматическое резервное переключение включено** в таблице "Общие свойства".
3. Измените значение на **true**. Изменение вступает в силу немедленно.
4. Укажите другие параметры в таблице согласно своим требованиям. В таблице содержатся подробные описания всех параметров.

Чтобы включить автоматическое резервное переключение на консоли JMX, выполните следующие действия.

1. В веб-браузере откройте адрес
   http://<имя компьютера сервера обработки данных>:29000

   Введите учетные данные для проверки подлинности консоли JMX, когда они будут запрошены (если эти данные отсутствуют, обратитесь к системному администратору).
2. В разделе **Topaz** выберите значение **service=hac-backup**.
3. Найдите метод **void setAutomaticFailoverEnabled ()**, выберите значение **True** и нажмите кнопку **Вызвать**.

Чтобы проверить, настроено ли автоматическое резервное переключение, выполните следующие действия.

1. Выполните шаги 1 и 2, описанные выше, чтобы открыть консоль JMX и службу **hac-backup**.
2. Найдите метод **void getAutomaticFailoverEnabled()** и нажмите кнопку **Вызвать**.

Переназначение служб с помощью консоли JMX

Если возникают проблемы с доступностью сервера и с ресурсами, можно перемещать службы между серверами обработки данных. Переназначение служб также позволяет ограничить простой, вызванный техническим обслуживанием серверов обработки данных.

Для выполнения этой процедуры не обязательно включать высокую доступность и не обязательно настраивать исходный сервер и сервер назначения для высокой доступности.

Чтобы переназначить службы между серверами обработки данных с помощью консоли JMX, выполните следующие действия.

1. В веб-браузере откройте адрес
   http://<имя компьютера сервера обработки данных>:29000

   Введите учетные данные для проверки подлинности консоли JMX, когда они будут запрошены (если эти данные отсутствуют, обратитесь к системному администратору).

2. В разделе **Topaz** выберите значение **service=hac-backup**.
3. Найдите метод **moveServices()** и введите следующие значения:
   - **customerId.** По умолчанию ID заказчика для обычной установки APM имеет значение **1**. Заказчики HPE Software-as-a-Service должны указывать свой ID.
   - **srcServer**. Имя исходного сервера, с которого перемещаются службы.
   - **dstServer**. Имя сервера назначения, на который перемещаются службы.

     В обоих параметрах следует задавать имя компьютера. Если имя компьютера точно не известно, можно использовать метод **listservers**, описанный далее, чтобы получить список имен уже настроенных компьютеров.
   - **groupName**. Оставьте значение этого параметра пустым.
4. Нажмите кнопку **Вызвать**. Все службы, работающие на исходном сервере, будут перенесены на сервер назначения.
5. Переместив процессы оперативного модуля (MARBLE) на сервер назначения, перезапустите их, чтобы гарантировать синхронизацию.

Службы, переназначаемые вручную

Внимание! Этот раздел предназначен только для опытных пользователей.

В случае необходимости можно вручную переназначить службы, работающие на основном сервере обработки данных, на резервный сервер обработки данных. Поскольку служба может быть активна только на одном сервере обработки данных, необходимо либо удалить существующее назначение, либо сделать его неактивным перед переназначением службы на другой сервер обработки данных.

Чтобы переназначить службу, можно добавить новое назначение или активировать ранее определенное, но в данный момент неактивное назначение.

Совет. Чтобы проверить, какие службы были успешно переназначены, активированы или деактивированы, можно просмотреть статус службы на веб-консоли JMX. Подробнее см. в разделе Службы, назначенные серверу на стр 91.

Удаление назначения службы

При удалении назначения службы удаляется запись из таблицы HA_TASKS в базе данных управления, и чтобы вновь использовать службу в дальнейшем, необходимо добавить ее в виде нового назначения.

Чтобы удалить текущее назначение службы, выполните следующие действия.

1. В веб-браузере откройте адрес
   http://<имя компьютера сервера обработки данных>:29000

   Введите учетные данные для проверки подлинности консоли JMX, когда они будут запрошены (если эти данные отсутствуют, обратитесь к системному администратору).
2. В разделе **Topaz** выберите значение **service=hac-manager**.
3. В методе **removeAssignment()** введите следующие данные.

- **customer_id.** По умолчанию ID заказчика для отдельной системы APM имеет значение **1**. Заказчики HPE Software-as-a-Service должны указывать в этом поле свой ID.

  Примечание. Для служб PM и NOA customer_id всегда имеет значение -1, потому что эти службы назначены всей системе, а не отдельному заказчику.

- **serviceName.** Имя службы, для которой удаляется текущее назначение.
- **serverName.** Имя сервера обработки данных, которому служба назначена в данный момент.
- **processName.** Имя процесса (например, **mercury_as**, **mercury_online_engine**, **mercury_offline_engine**, **topaz_pm**).

4. Нажмите кнопку **Вызвать**. Назначение для службы будет удалено с указанного сервера обработки данных.

Изменение статуса назначенной службы

Можно оставить назначение службы для определенного сервера обработки данных в таблице HA_TASKS в базе данных управления, но сделать его активным или неактивным, изменив его значение.

Примечание. Таблица HA_TASK_ASSIGN из предыдущих версий устарела. Используйте таблицу HA_TASKS.

Чтобы изменить значение существующего назначения, выполните следующие действия.

1. В веб-браузере откройте адрес
   http://<имя компьютера сервера обработки данных>:29000

   Введите учетные данные для проверки подлинности консоли JMX, когда они будут запрошены (если эти данные отсутствуют, обратитесь к системному администратору).
2. В разделе Topaz выберите значение **service=hac-manager**.
3. В методе **removeAssignment()** введите следующие данные.
   - **customerId.** По умолчанию ID заказчика для обычной установки APM имеет значение **1**. Заказчики HPE Software-as-a-Service должны указывать свой ID.

     Для служб PM и NOA customer_id всегда имеет значение -1, потому что эти службы назначены всей системе, а не отдельному заказчику.

   - **serviceName.** Имя службы, для которой изменяется значение назначения.
   - **serverName.** Имя сервера обработки данных, которому служба назначена.
   - **processName.** Имя процесса.
   - **assignValue.** Значение для назначения. Допускаются любые числа от –9 до 9. Значение **1** делает назначение активным, а любое другое число — неактивным.

4. Нажмите кнопку **Вызвать**. Назначение службы будет изменено в соответствии с введенным значением **assignValue**.

Добавление назначения для службы

Можно добавить назначение службы для определенного сервера обработки данных и активировать его сразу или оставить неактивным, пока оно не понадобится. Это удобно при работе с основным и резервным сервером обработки данных. Всем службам можно создать назначения для каждого сервера и сделать назначения для основного сервера обработки данных активными, а для резервного сервера — неактивными.

Чтобы добавить новое назначение для службы, выполните следующие действия.

1. В веб-браузере откройте адрес
   http://<имя компьютера сервера обработки данных>:29000

   Введите учетные данные для проверки подлинности консоли JMX, когда они будут запрошены (если эти данные отсутствуют, обратитесь к системному администратору).
2. В разделе Topaz выберите значение **service=hac-manager**.
3. В методе **removeAssignment()** введите следующие данные.
   - **customer_id.** ID заказчика, которому назначается служба. По умолчанию для отдельной системы APM (которая не управляется с помощью HPE Software-as-a-Service) ID заказчика имеет значение **1**.

     Примечание. Для служб PM и NOA customer_id всегда имеет значение -1, потому что эти службы назначены всей системе, а не отдельному заказчику.
   - **serviceName.** Имя назначаемой службы.
   - **serverName.** Имя нового сервера обработки данных, которому назначается служба.
   - **processName.** Имя процесса.
   - **assignValue.** Значение для назначения. Допускаются любые числа от –9 до 9. Значение **1** делает назначение активным, а любое другое число — неактивным.
4. Нажмите кнопку **Вызвать**. Назначение для службы будет добавлено на указанный сервер обработки данных.

Отключение служб агрегатора данных вручную

Агрегатор данных можно отключить в приложении Service Health (это предпочтительный метод). Если же нужно отключить службы агрегатора данных, но приложение System Health отсутствует или недоступно для использования, эту процедуру можно выполнить вручную.

Чтобы отключить службы автономного агрегирования и модуля бизнес-логики на сервере обработки данных, выполните следующие действия.

1. Перейдите в меню **Администрирование > Платформа > Установка и обслуживание > Настройки инфраструктуры** и выберите **Базовые настройки**.
2. Выберите пункт **Автономный агрегатор**.
3. Для параметра **Запускать агрегатор** измените значение на **False**. Изменение вступает в силу немедленно.

Настройка сборщиков данных APM в распределенной среде

В этом разделе описывается настройка сборщиков данных HPE Application Performance Management для работы в распределенной среде.

Business Process Monitor и Real User Monitor

Для работы экземпляров Business Process Monitor необходимо указать URL-адрес сервера шлюза в приложении Консоль администрирования BPM на каждом хосте, где работает Business Process Monitor. Измените запись URL-адреса сервера шлюза на странице "Настройка экземпляра" для каждого экземпляра Business Process Monitor. Подробнее см. раздел "Область свойств регистрации Application Performance Management" документа Руководство администратора Business Process Monitor.

Для работы экземпляров Real User Monitor в APM необходимо задать URL-адрес сервера шлюза в веб-консоли Real User Monitor. Подробнее см. в разделе "Настройки подключения APM" документа Руководство по администрированию Real User Monitor.

Адрес сервера шлюза указывается следующим образом.

- Если устанавливается один сервер шлюза, укажите URL-адрес этого компьютера.
- Если несколько серверов шлюза объединяются в кластер и располагаются за балансировщиком нагрузки, укажите URL-адрес устройства балансировки.

Если используются два балансировщика нагрузки (для поддержки резервного переключения), укажите URL-адрес любого устройства и убедитесь, что на компьютере с DNS-сервером настроены имена хостов для обоих устройств балансировки.

SiteScope

Для работы экземпляров SiteScope необходимо указать URL-адрес сервера шлюза в каждом профиле SiteScope, используя APM System Availability Management (**Администрирование > System Availability Management**). Подробнее см. в разделе "Настройка подключения" в главе, посвященной SAM, документа Руководство пользователя APM.

Если используется балансировщик нагрузки и определены виртуальные IP-адреса или URL-адреса, то их можно использовать при определении URL-адреса сервера шлюза. Если используются два балансировщика нагрузки (для поддержки резервного переключения), укажите URL-адрес любого устройства и убедитесь, что на компьютере с DNS-сервером настроены имена хостов для обоих устройств балансировки.

Подробнее о настройке высокой доступности для SiteScope см. в документе Руководство по HPE SiteScope Failover.

Приложение G: Удаление APM 9.30

Чтобы полностью удалить APM, выполните следующее.

Удаление серверов APM в среде Windows

Чтобы полностью удалить серверы HPE Application Performance Management в среде Windows, выполните следующие действия.

1. Удалите APM через пользовательский интерфейс Windows или автоматически.
   a. Чтобы удалить APM через пользовательский интерфейс Windows, выполните следующие действия.
      i. На компьютере, с которого удаляется HPE Application Performance Management, выберите **Пуск > Параметры > Панель управления > Программы и компоненты**. Выберите **HPE Application Performance Management**.
      ii. Нажмите кнопку **Удалить**, подождите, пока скрипт удаления APM удалит все установленные обновления, и следуйте указаниям на экране.

      Примечание. Этот процесс может занять много времени (дольше 30 минут).

   b. Чтобы удалить APM автоматически, выполните следующие действия.
      i. Остановите все серверы APM.
      ii. Выполните команду **<корневой каталог установки HPE APM>\installation\bin\uninstall.bat -i silent**
2. Перезагрузите сервер.
3. Если APM работает с Microsoft IIS, откройте диспетчер служб Интернета IIS и проверьте следующие условия.
   a. В разделе **Веб-сайт по умолчанию** убедитесь, что удалены следующие виртуальные каталоги (удалите их, если они все еще отображаются):
      - bpi
      - bsm
      - ext
      - HPBSM
      - jakarta
      - mam_images
      - mercuryam
      - odb
      - topaz
      - tvb
      - ucmdb-ui
      - uim

b. Щелкните правой кнопкой имя компьютера сервера в дереве и выберите пункт **Свойства**. В диалоговом окне "Свойства" в списке "Основные свойства" выберите **Служба веб-публикаций** и нажмите кнопку **Изменить**. Перейдите на вкладку **Фильтры ISAPI**. Если отображается фильтр **jakartaFilter**, удалите его.

Примечание. Если после удаления APM планируется повторная установка в другой каталог на компьютере, не следует удалять фильтр **jakartaFilter**, но понадобится обновить путь к фильтру. Подробнее см. в разделе После удаления APM и повторной установки в другой каталог APM не работает на стр 112.

4. Откройте редактор реестра Windows: выберите **Пуск > Выполнить**. Введите команду **Regedit**.

   Во время установки обновлен параметр реестра Windows **HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ReservedPorts** — в него добавлены следующие диапазоны портов, необходимые для APM: 1098-1099, 8009-8009, 8080-8080, 4444-4444, 8083-8083, 8093-8093.

   Эти диапазоны портов не удаляются из реестра во время удаления сервера. Их следует удалить из параметра реестра вручную после удаления APM, если они не нужны никаким другим приложениям.

   Совет. Перед внесением изменений в реестр рекомендуем создать его резервную копию.

Удаление серверов APM в среде Linux

1. Войдите на сервер от имени привилегированного пользователя (**root**).
2. Остановите все серверы APM.
3. Чтобы открыть программу удаления, введите: **cd /opt/HP/BSM/installation/bin**
4. Запустите следующий скрипт для удаления в режиме с пользовательским интерфейсом: **./uninstall.sh**. Чтобы выполнить этот шаг в автоматическом режиме, воспользуйтесь командой **./uninstall.sh -i silent**.
5. Запустится программа удаления APM. Следуйте указаниям на экране. После завершения программы появится сообщение, подтверждающее успешное удаление.
6. Нажмите кнопку **Готово**.

Примечание. Если во время удаления обнаруживаются проблемы, обратитесь в службу Служба поддержки HPE.

Удаление серверов BSM перед установкой APM

Прежде чем устанавливать APM 9.30 на компьютер с установленной версией BSM 9.2x, полностью удалите BSM 9.2x.

Примечание. Стандартный процесс удаления BSM может занять несколько часов в зависимости от количества установленных исправлений. Чтобы ускорить процесс, можно запустить инструмент удаления BSM 9.2x. Этот инструмент сокращает время на удаление BSM до нескольких минут, используя стандартные инструменты операционной системы.

Чтобы использовать инструмент удаления BSM, выполните следующие действия.

1. Перейдите на веб-сайт службы поддержки HPE Software (https://softwaresupport.hpe.com) и войдите в учетную запись.
2. Щелкните **Patches**.
3. Найдите **BSM 9.2x Uninstall Tool.**
4. Для Windows выберите **BSM 9.2x Uninstall Tool for Windows**.

   Для Linux выберите **BSM 9.2x Uninstall Tool for Linux**.
5. После завершения работы инструмента удаления BSM выполните шаги 3 и 4 процедуры *Удаление серверов BSM в среде Windows*, которая приведена ниже. В этих шагах предоставляются инструкции о веб-сервере IIS и реестре Windows.

Удаление серверов BSM в среде Windows

Чтобы полностью удалить серверы HPE Business Service Management в среде Windows, выполните следующие действия.

1. Удалите BSM через пользовательский интерфейс Windows или автоматически.
   a. Чтобы удалить BSM через пользовательский интерфейс Windows, выполните следующие действия.
      i. На компьютере, с которого удаляется HPE Business Service Management, выберите **Пуск > Параметры > Панель управления > Программы и компоненты**. Выберите **HPE Business Service Management**.
      ii. Нажмите кнопку **Удалить**, подождите, пока скрипт удаления BSM удалит все установленные обновления, и следуйте указаниям на экране.

      Примечание. Этот процесс может занять много времени (дольше 30 минут).

      iii. Если установлен флажок **Показывать обновления**, то отображаются все обновления, установленные для BSM. Вместе с BSM удаляются все обновления.
   b. Чтобы удалить BSM автоматически, выполните следующие действия.
      i. Остановите все серверы BSM.
      ii. Выполните команду **<каталог установки HPBSM>\installation\bin\uninstall.bat -i silent**
2. Перезагрузите сервер.
3. Если BSM работает с Microsoft IIS, откройте диспетчер служб Интернета IIS и проверьте следующие условия.
   a. В разделе **Веб-сайт по умолчанию** убедитесь, что удалены следующие виртуальные каталоги (удалите их, если они все еще отображаются):
      - bpi
      - bsm
      - ext
      - HPBSM
      - jakarta
      - mam_images

- mercuryam
- odb
- topaz
- tvb
- ucmdb-ui
- uim

b. Щелкните правой кнопкой имя компьютера сервера в дереве и выберите пункт **Свойства**. В диалоговом окне "Свойства" в списке "Основные свойства" выберите **Служба веб-публикаций** и нажмите кнопку **Изменить**. Перейдите на вкладку **Фильтры ISAPI**. Если отображается фильтр **jakartaFilter**, удалите его.

Примечание. Если после удаления BSM планируется повторная установка в другой каталог на компьютере, не следует удалять фильтр **jakartaFilter**. но понадобится обновить путь к фильтру. Подробнее см. в разделе После удаления APM и повторной установки в другой каталог APM не работает на стр 112.

4. Откройте редактор реестра Windows: выберите **Пуск > Выполнить**. Введите команду **Regedit**.

   Во время установки обновлен параметр реестра Windows **HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ReservedPorts** — в него добавлены следующие диапазоны портов, необходимые для BSM: 1098-1099, 8009-8009, 8080-8080, 4444-4444, 8083-8083, 8093-8093.

   Эти диапазоны портов не удаляются из реестра во время удаления сервера. Их следует удалить из параметра реестра вручную после удаления BSM, если они не нужны никаким другим приложениям.

   Совет. Перед внесением изменений в реестр рекомендуем создать его резервную копию.

Удаление серверов BSM в среде Linux

1. Войдите на сервер от имени привилегированного пользователя (**root**).
2. Остановите все серверы BSM.
3. Чтобы открыть программу удаления, введите: **cd /opt/HP/BSM/installation/bin**
4. Запустите следующий скрипт для удаления в режиме с пользовательским интерфейсом: **./uninstall.sh**. Чтобы выполнить этот шаг в автоматическом режиме, воспользуйтесь командой **./uninstall.sh -i silent**.
5. Запустится программа удаления BSM. Следуйте указаниям на экране. После завершения программы появится сообщение, подтверждающее успешное удаление.
6. Нажмите кнопку **Готово**.
7. Проверьте наличие ошибок в файле журнала **HPB_<номер версии>_HPOvInstaller.txt**, расположенном в каталоге **/tmp**. Файлы предыдущей установки находятся в каталоге **/tmp/HPOvInstaller/HPBsm_<номер версии>**.

Примечание. Если во время удаления обнаруживаются проблемы, обратитесь в службу Служба поддержки HPE.

Приложение H: Смена пользователей службы APM

В этом приложении описывается процедура смены пользователей службы APM в системах Windows и Linux. В приложении рассмотрены следующие вопросы.

Смена пользователя Windows

Служба APM, которая запускает все службы и процессы APM, устанавливается программой установки и настройки баз данных. По умолчанию данная служба запускается от имени пользователя локальной системы. Однако запуск службы может понадобиться поручить другому пользователю (например, при использовании проверки подлинности NTLM).

Пользователь, которому это поручено, должен иметь следующие разрешения:

- достаточные права доступа к базе данных (как установлено администратором базы данных);
- достаточные права доступа к сети;
- права администратора на локальном сервере.

Примечание. Служба APM устанавливается как запускаемая вручную, а после первого включения APM она становится автоматической.

Чтобы сменить пользователя службы APM, выполните следующие действия.

1. Отключите APM (**Пуск > Программы > HPE Application Performance Management > Администрирование > Отключить HPE Application Performance Management**).
2. В окне служб Microsoft дважды щелкните **HP Bus Pro Mon**. Откроется диалоговое окно "Свойства HP BSM (локальный компьютер)".
3. Щелкните вкладку **Вход в систему**.
4. Выберите пункт **С учетной записью** и просмотрите список допустимых пользователей на компьютере, чтобы выбрать нужного.
5. Введите и подтвердите пароль данного пользователя для входа в Windows.
6. Нажмите кнопку **Применить**, чтобы сохранить настройки, а затем кнопку **ОК**, чтобы закрыть диалоговое окно.
7. Включите APM (**Пуск > Программы > HPE Application Performance Management > Администрирование > Включить HPE Application Performance Management**).

Примечание. Эту процедуру необходимо выполнять после переустановки или обновления APM.

Смена пользователя Linux

В системах Linux APM следует выполнять от имени определенного пользователя: привилегированного или какого-либо другого. APM поддерживает работу только одно пользователя в определенный момент времени. Этого пользователя можно определить с помощью мастера начальной настройки.

Чтобы сменить пользователя после установки APM, выполните следующие действия.

1. Остановите APM.
2. Перезапустите мастер начальной настройки и укажите нового пользователя. Мастер начальной настройки можно запустить из следующей папки: **/opt/HP/BSM/bin/postinstall.sh**.
3. Выйдите из системы Linux и войдите под именем нового пользователя.
4. Запустите программу установки и настройки базы данных.

   Запустите программу установки и настройки базы данных на серверах шлюза и обработки данных. Программу установки и настройки базы данных можно запустить из следующей папки **/opt/HP/BSM/bin/config-server-wizard.sh**.
5. Запустите APM.

Приложение I: Смена веб-сервера

Чтобы сменить веб-сервер после установки APM, выполните следующую процедуру.

Примечание. Если включена проверка подлинности по смарт-карте и нужно сменить веб-сервер Apache на IIS или наоборот, сначала необходимо отключить эту проверку подлинности. Восстановить проверку подлинности по смарт-карте можно после смены веб-сервера. Подробнее о том, как включать и отключать проверку подлинности по смарт-карте, см. в разделе "Проверка подлинности по смарт-карте" документа Руководство по администрированию платформы APM.

1. Отключите все серверы шлюза и обработки данных APM. Подробнее см. в разделе Запуск и остановка APM на стр 21.
2. Если выполняется смена веб-сервера IIS на Apache, остановите службу IIS или выберите другой порт в мастере начальной настройки в следующем шаге.
3. Если выполняется смена веб-сервера Apache на IIS, настройте IIS. Подробнее см. в следующих разделах.
   - Для Linux: Использование веб-сервера Apache на стр 51
   - Для Windows: Использование веб-сервера IIS на стр 44
4. Запустите мастер начальной настройки и выберите новый тип веб-сервера в соответствующем окне.

   Мастер начальной настройки можно запустить из следующей папки: **<корневой каталог HPE APM>\bin\postinstall.bat**. Однако если мастер закрылся до завершения работы, используйте другой файл: **<корневой каталог HPE APM>/bin/ovii-postinstall.sh <TOPAZ_HOME>**, где **<TOPAZ_HOME>** — каталог установки APM (обычно /opt/HP/BSM).
5. Запустите все серверы шлюза и обработки данных APM.

Приложение J: Устранение неполадок

В этом приложении рассматриваются следующие темы.

Ресурсы по устранению неполадок

- **Файлы журнала установки.** Подробнее см. в разделе Проверка файлов журнала установки на стр 19.
- **Средство журнала обновления.** Чтобы просмотреть сводку ошибок, произошедших во время обновления конфигурации с помощью мастера обновления, запустите средство журнала обновления: **<корневой каталог HPE APM>\tools\logTool\logTool.bat**. Составленный отчет располагается в том же каталоге и получает имя **logTool.txt**.
- **База знаний HPE для самостоятельного решения проблем.** Дополнительные сведения по устранению неполадок см. в базе знаний HPE для самостоятельного решения проблем, доступной на веб-сайте службы поддержки HPE Software (https://softwaresupport.hpe.com).
- **Инструменты APM.** Можно устранять неполадки в среде HPE Application Performance Management с помощью инструментов APM. Они доступны в каталоге **<корневой каталог HPE APM>\tools**. Большинство инструментов следует использовать только по согласованию с сотрудниками HPE. Программу проверки схемы БД (dbverify) и программу пометки данных следует использовать согласно инструкциям, приведенным в документации.
- **Администратор ведения журналов APM.** Этот инструмент позволяет временно изменять уровень детализации для журналов APM, а также создавать пользовательские журналы. Чтобы открыть администратор ведения журналов APM, откройте следующий URL-адрес:

  http://<полное доменное имя сервера шлюза APM>/topaz/logAdminBsm.jsp

Устранение неполадок установки и подключения

В этом разделе описываются распространенные проблемы, которые могут возникать при установке APM или при подключении к APM после установки, а также решения этих проблем.

Не удается подключиться к APM через Internet Explorer по полному доменному имени, если домен состоит из двух букв

Internet Explorer не поддерживает работу с полными доменными именами, где в URL-адресе виртуального APM сервера по умолчанию домен состоит из двух букв (например, XXXX.aa).

Обходное решение

Если в URL-адресе домен состоит из двух букв, для доступа к APM используйте другой браузер (не Internet Explorer).

Получено сообщение об ошибке: недостаточно места на диске для извлечения файлов установки

Такое случается при установке компонентов. Если ввести новый путь на другом диске, где достаточно места, снова появляется то же сообщение об ошибке.

В процессе извлечения файлов некоторые данные всегда сохраняются в каталог TEMP на системном диске, даже если для файлов установки выбрано сохранение в расположении, отличном от пути по умолчанию.

Решение

- Освободите достаточно места на системном диске (как указано в сообщении об ошибке), а затем продолжайте процедуру установки.
- Если невозможно освободить достаточно места на системном диске, измените путь в системной переменной TEMP.
  - **Windows.** Выберите пункты **Пуск > Параметры > Панель управления > Система > Вкладка "Дополнительно" > Переменные среды**, а затем измените путь для переменной **TEMP** в области "Переменные среды пользователя".
  - **Linux.** Выполните следующие команды:

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

    Где `/new/tmp/dir` — это новый рабочий каталог.

Не удалось выполнить установку из-за ограничений безопасности для каталога /tmp в Linux

Если для каталога /tmp установлены ограничения безопасности, которые не разрешают выполнение скрипта из этого каталога, установка завершится сбоем.

Решение

Задайте новый каталог /tmp, для которого не задано этих ограничений, выполнив следующие команды:

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

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

Где `/new/tmp/dir` — это новый рабочий каталог.

Подключение к базе данных Microsoft SQL Server в программе установки и настройки баз данных завершается ошибкой

Убедитесь, что пользователь, от имени которого работает служба SQL Server, обладает разрешениями для записи на диск, на котором создается база данных.

После завершения установки сервера APM появляется приглашение для входа в сеть.

Возможная причина

Такое может происходить, если для метода проверки подлинности на сервере IIS не задано значение по умолчанию — **Разрешить анонимный доступ**.

Решение

Верните для метода проверки подлинности на сервере IIS значение по умолчанию (**Разрешить анонимный доступ**) и убедитесь, что выбрана учетная запись пользователя по умолчанию **IUSR_XXX** (здесь XXX обозначает имя компьютера). Учетная запись пользователя **IUSR_XXX** создается во время установки IIS. Затем удалите и снова установите APM.

Модуль сервлетов Tomcat не запускается и выдает ошибку

Сообщение об ошибке выглядит так:

java.lang.reflect.InvocationTargetException: org.apache.tomcat.core.TomcatException: Основная причина — используется адрес: JVM_Bind

Возможная причина

Работа HTTP-сервера Oracle, который входит в состав типичной установки Oracle, на одном компьютере с серверами APM вызывает конфликт с модулем сервлетов Tomcat.

Решение

Остановите службу HTTP-сервера Oracle, отключите и заново включите APM.

Чтобы избежать повторения проблемы после перезагрузки компьютера, задайте для службы HTTP-сервера Oracle режим запуска **Вручную**.

Не удается установить компоненты APM из-за административных ограничений.

Возможная причина

На компьютере, где выполняется установка, работает ПО управления на основе политик, которое ограничивает доступ к файлам, каталогам, реестру Windows и т. д.

Решение

Если работает подобная программа, обратитесь к администратору сети организации, чтобы получить разрешения, необходимые для установки и сохранения файлов на компьютере.

После установки при попытке доступа к APM на странице появляется сообщение об ошибке HTTP 404

Выполните следующие задачи.

1. Откройте страницу статуса и убедитесь, что запущены все процессы APM. Подробнее см. в разделе "Просмотр статуса процессов и служб" документа Руководство по администрированию платформы APM.
2. Если на странице статуса все службы отмечены зеленым цветом, откройте APM через порт 29000 (http://ИМЯ_КОМПЬЮТЕРА:29000).

   Проверьте доступ к консоли JMX. Если консоль доступна, перейдите к шагу 3 и постарайтесь обнаружить проблему.
3. Проверьте, запущен ли веб-сервер (http://ИМЯ_КОМПЬЮТЕРА). Если веб-сервер запущен, то возможно, имеется проблема с фильтром ISAPI.
4. Если имеется проблема с фильтром ISAPI в Microsoft Windows 2008 Server, проверьте, выполнена ли процедура по созданию роли. Подробнее см. в разделе Использование веб-сервера IIS на стр 44.
5. Не удается запустить сервер Apache из-за конфликта портов.

После удаления APM и повторной установки в другой каталог APM не работает

Возможная причина Во время удаления и повторной установки в другое место фильтр ISAPI для IIS не был обновлен с указанием нового пути.

Решение

Чтобы обновить путь для фильтра ISAPI IIS, выполните следующие действия.

1. Откройте диспетчер служб Интернета IIS.
2. Щелкните правой кнопкой имя компьютера в дереве и выберите пункт **Свойства**.
3. В списке "Основные свойства" выберите **Служба веб-публикаций** и нажмите кнопку **Изменить**.
4. Перейдите на вкладку **Фильтр ISAPI**.
5. Убедитесь, что в фильтре **jakartaFilter** правильно задан каталог APM.
6. Примените изменения и закройте диспетчер служб Интернета.
7. Перезапустите службу IIS.

Данные Business Process Monitor или SiteScope не передаются в APM

Эта проблема может возникать в различных ситуациях. Подробнее о причинах и возможных решениях см. на сайте База знаний HPE для самостоятельного решения проблем в статье номер KM438393 (https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/KM438393).

Мониторы Business Process Monitor не передают данные на сервер шлюза (IIS)

Симптомы и возможные причины

- Загрузчики не получают данные
- Отсутствуют данные в отчетах веб-сайта
- В журнале **data_deport.txt** на компьютере Business Process Monitor присутствует ошибка следующего вида:

```
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>)
```

Чтобы подтвердить наличие этой проблемы, откройте страницу http://<имя компьютера>/ext/mod_mdrv_wrap.dll?type=report_transaction. Если проблема присутствует, то отображается сообщение "Служба временно недоступна".

Также можно отправить следующий URL-адрес, чтобы проверить статус Web Data Entry: http://<имя компьютера>/ext/mod_mdrv_wrap.dll?type=test

Эта проблема может вызываться фильтром **MercRedirectFilter**, который устарел и больше не нужен для APM. Он мог остаться от предыдущих версий APM.

Решение

Удалите фильтр **MercRedirectFilter** и убедитесь, что для IIS работает только фильтр ISAPI **jakartaFilter**.

Business Process Monitor не удается подключиться через Интернет к серверу шлюза (Apache)

Возможная причина

Компьютеру Business Process Monitor не удается правильно разрешить имя сервера шлюза.

Решение

- Добавьте имя сервера шлюза в файл **<корневой каталог системы Windows>\system32\drivers\etc\hosts** на компьютере Business Process Monitor.
- Измените имя сервера шлюза в файле **<корневой каталог HPE APM>\WebServer\conf\httpd.conf** на сервере шлюза на имя, известное в службе DNS.

Мастер начальной настройки завершается с ошибкой во время установки APM на компьютере Linux

Это может вызываться ошибкой в Linux. Откройте файл **/etc/sysctl.conf** и удалите строку **vm.swapiness = 0**. Перезагрузите мастер, запускаемый после установки.

Не удалось установить Adobe Flash Player

Adobe Flash Player устанавливается с помощью приложения Adobe Download Manager, которое не поддерживает скрипты автоматической настройки прокси-сервера. Если в Internet Explorer настроена автоматическая настройка прокси-сервера, то приложение загрузки прекращает работу, не отвечая на запросы ("зависает"). Настройте хост прокси-сервера вручную или изучите документацию по Flash Player.

Не удалось запустить APM или не открывается мастер настройки APM

Проверьте наличие следующей ошибки в файле supervisorwrapper.log:

<корневой каталог HPE APM>\conf\supervisor\manager\nannyManager.wrapper wrapper | OpenService failed - Access is denied.

Если присутствует эта ошибка, то проблему может вызывать контроль учетных записей, включенный в системе Windows. Отключите контроль учетных записей на всех Windows-серверах APM.

Не удается войти по полному доменному имени

На экране входа появляется следующая ошибка: **URL-адрес HPE Application Performance Management должен содержать полное доменное имя. Снова введите URL-адрес HPE Application Performance Management в адресную строку** и проверьте, есть ли разрешение DNS для виртуальных IP-адресов устройства балансировки нагрузки с шлюзов APM. Может понадобиться добавить виртуальные IP-адреса средства балансировки нагрузки (для пользователей и приложений и в случае необходимости для сборщиков данных) в файл hosts на сервере шлюза APM.

После нажатия кнопки "Вход" ничего не происходит или пользователь выполняет вход, но карта сайта пуста.

Возможная причина

Вход в APM выполняется не с клиентского компьютера, а с Windows Server. В Windows Server обычно включена конфигурация усиленной безопасности Internet Explorer. В этой конфигурации не работают некоторые функции пользовательского интерфейса APM, в том числе страница входа в APM.

Решение.

Проверьте, включена ли конфигурация усиленной безопасности Internet Explorer. Если она включена, то используйте для входа обычный клиент, а не сервер Windows.

Если необходимо выполнять вход с сервера, то отключите конфигурацию усиленной безопасности Internet Explorer (**Панель управления > Установка и удаление компонентов Windows**) или добавьте URL-адрес APM в список доверенных сайтов в настройках безопасности Internet Explorer.

Не открываются апплеты Java

- Если используется Internet Explorer, выберите пункты **Сервис** > **Свойства браузера** > **Подключения** > **Настройка сети**. Снимите флажки **Автоматическое определение настроек** и **Использовать скрипт автоматической настройки**.
- Выберите **Панель управления** > **Java** > вкладка **Общие** > **Настройки сети** и выберите вариант **Прямое подключение**, а не вариант по умолчанию **Использовать настройки браузера**.

Удаление APM завершается ошибкой

Возможно получение ошибок примерно следующего содержания:

The package HPOv….can not be uninstalled.

Такие ошибки можно игнорировать. Система APM была успешно удалена.

Нечитаемые символы восточноазиатских языков

В некоторых пакетах распространения RHEL6.x при выборе варианта установки APM на восточноазиатском языке (корейском, японском или китайском упрощенном) интерфейс установки отображает нечитаемые символы.

Обходное решение

Запустите программу установки с JRE, которая поддерживает восточноазиатские языки.

setup.bin LAX_VM ${PATH_TO_JAVA}

Отправить отзыв о документации

Если у вас есть комментарии к этому документу, напишите в отдел документации. Если в системе настроен почтовый клиент, по нажатию этой ссылки откроется окно электронного письма с темой:

Отзыв о документе Руководство по установке APM (Application Performance Management 9.30)

Напишите в письме свой отзыв и отправьте его нам.

Если вы работаете с электронной почтой через браузер, скопируйте указанную выше информацию в новое письмо и отправьте его по адресу Sw-doc@hpe.com.

Благодарим за отзыв!