

HP Service Health Reporter

Версия ПО: 9.40

Операционные системы Windows® и Linux

Руководство по настройке

Дата выпуска документа: Январь 2015 г.

Дата выпуска программного обеспечения: Январь 2015 г.



Официальное уведомление

Гарантийные обязательства

Гарантии на продукты и услуги компании HP формулируются только в заявлениях о прямой гарантии, сопровождающих эти продукты и услуги. В них нет ничего, что может быть истолковано как дополнительная гарантия. Компания HP не несет ответственности за технические или редакторские ошибки и неточности, содержащиеся в данном документе.

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

Пояснения в отношении ограниченных прав

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

Заявление об авторских правах

© Copyright 2015 Hewlett-Packard Development Company, L.P.

Уведомление о товарных знаках

Adobe® является товарным знаком корпорации Adobe Systems Incorporated.

Microsoft® и Windows® — товарные знаки корпорации Майкрософт, зарегистрированные в США.

UNIX® является зарегистрированным товарным знаком консорциума The Open Group.

Обновление документации

На титульной странице настоящего документа представлены следующие идентификационные данные.

- Номер версии программного обеспечения.
- Дата выпуска документа, которая изменяется при каждом его обновлении.
- Дата выпуска программы, которая указывает дату выпуска данной версии ПО.

Чтобы проверить наличие обновлений или убедиться в том, что используется последняя редакция документа, откройте вебсайт

<http://h20230.www2.hp.com/selfsolve/manuals>

Для доступа к этому сайту необходимо зарегистрироваться в службе HP Passport и войти в систему. Регистрация HP Passport ID производится на сайте:

<http://h20229.www2.hp.com/passport-registration.html>

Также можно перейти по ссылке **New users - please register** на странице входа в службу HP Passport.

Оформление подписки в службе поддержки соответствующего продукта также позволит получать обновленные и новые редакции. Подробные сведения можно получить у торгового представителя компании HP.

Поддержка

Используйте веб-сайт технической поддержки программного обеспечения компании HP по адресу <http://www.hp.com/go/hpsoftwaresupport>

На этом веб-сайте приведена контактная информация и подробные сведения о продуктах, услугах и поддержке, предоставляемых компанией HP в сфере программного обеспечения.

Служба поддержки программного обеспечения компании HP в Интернете предоставляет заказчикам возможности для самостоятельного устранения неполадок. Она обеспечивает быстрый и эффективный доступ к интерактивным средствам технической поддержки, которые необходимы для управления бизнесом. Клиенты службы поддержки могут использовать этот веб-сайт для решения следующих задач.

- Поиск необходимых документов в базе знаний.
- Подача и отслеживание заявок в службу технической поддержки и запросов на расширение функциональных возможностей.
- Загрузка исправлений программного обеспечения.
- Управление договорами и на оказание поддержки.
- Поиск контактной информации службы поддержки компании HP.
- Просмотр сведений о доступных услугах.
- Участие в обсуждениях с другими пользователями программного обеспечения.
- Поиск курсов обучения по программному обеспечению и регистрация для участия в них.

Для получения доступа к большинству разделов поддержки сначала необходимо зарегистрироваться в качестве пользователя службы HP Passport, а затем войти в систему. Для ряда разделов поддержки также необходимо наличие договора на оказание поддержки. Чтобы зарегистрировать учетную запись HP Passport, перейдите по адресу

<http://h20229.www2.hp.com/passport-registration.html>

Получить более подробные сведения об уровнях доступа можно по адресу

http://h20230.www2.hp.com/new_access_levels.jsp

Веб-сайт портала **HP Software Solutions Now** содержит сведения о решениях и интеграциях HPSW. Этот сайт позволяет изучить продукты HP на предмет соответствия бизнес-потребностям, содержит полный список интеграций между продуктами HP, а также список процессов ITIL. URL-адрес этого веб-сайта: <http://h20230.www2.hp.com/sc/solutions/index.jsp>

Информация о PDF-версии интерактивной справки

Этот документ представляет собой PDF-версию интерактивной справки. Этот PDF-файл предоставляется для удобной печати нескольких разделов справки или ознакомления с ней в формате PDF. Поскольку содержимое справки создано для просмотра в браузере, некоторые разделы могут быть не отформатированы должным образом. Некоторые интерактивные разделы могут отсутствовать в PDF-версии. Эти разделы можно напечатать из интерактивной справки.

Содержание

Часть I: Настройка SHR	7
Глава 1: Сценарии развертывания, поддерживаемые SHR	8
HP Operations Manager;	8
Business Service Management/Operations Manager i	9
VMware vCenter	11
Другие источники данных	12
Глава 2: Планирование настройки SHR с использованием BSM/OMi	14
Настройка источника топологии RTSM для SHR	14
Включение атрибутов ЭК для пакета содержимого	20
Глава 2: Планирование настройки SHR с использованием HPOM	24
Глава 3: Основная конфигурация	35
Задача 1. Запустите административную консоль	37
Задача 2. Настройте подключение к базе данных	38
Задача 3. Создайте схему базы данных	40
Задача 4. Создайте учетную запись пользователя для базы данных управления	46
Задача 5. Настройте сборщики, установленные в удаленных системах	47
Задача 6: Выберите источник данных	48
Источники данных для сценария BSM или OMi	49
Источники данных для сценария развертывания HPOM	51
Источник данных VMware vCenter	52
Задача 7. Настройка источника топологии	52
Настройка источника определения службы RTSM	52
Настройка источника определения службы HPOM	54
Настройка определения службы vCenter	56
Задача 8. сетевого устройства	57
Глава 4: Настройка источника данных	58
Настройка источника данных баз данных управления и профилей	58
Настройка источника данных HP OMi	62
Настройка источника данных HP Operations Manager	64
Настройка источника данных для агента HP Operations Agent	65
Настройка источника данных сети (с помощью универсальной базы данных)	65
Настройка источника данных VMware vCenter	66
Настройка источника данных SiteScope	68
Глава 5: Установка пакетов содержимого	71

Перед началом работы	71
Проверьте источники данных	71
Выбор компонентов пакетов содержимого	72
Установка компонентов пакетов содержимого	73
Часть II: Лицензирование	77
Глава 6: Лицензирование SHR	78
Используемые лицензии (LTU)	78
Получение ключа бессрочной лицензии	80
Установка ключа бессрочной лицензии	82
Повторная активация лицензии SAP BusinessObjects	83
Часть III: Переход к среде Windows 2012	85
Глава 7: Параллельный перенос	86
Часть IV: Дополнительная настройка	92
Глава 8: Настройка защищенного подключения для SHR (HTTPS)	93
Создание файла хранилища ключей	93
Настройка защищенного подключения (HTTPS)	93
Для административной консоли SHR	94
Для консоли InfoView SHR	96
Глава 9: Сертификат проверки подлинности клиента для SHR	98
Проверка подлинности и авторизация	98
Предварительные условия проверки подлинности на основе сертификатов	98
Настройка метода извлечения имени пользователя	102
Настройка административной консоли SHR	102
Настройка SAP BusinessObjects InfoView	106
Глава 10: Резервное копирование и восстановление базы данных	111
Создание резервной копии баз данных SHR в Windows	112
Для базы данных Sybase IQ	112
Для базы данных и хранилища файлов SAP BusinessObjects	125
Для таблицы базы данных управления	131
Создание резервной копии баз данных SHR в Linux	135
Для базы данных Sybase IQ	135
Для базы данных и хранилища файлов SAP BusinessObjects	138
Для таблиц базы данных управления	140
Восстановление баз данных SHR	141
Восстановление SHR в Windows	141
Для базы данных Sybase IQ	141

Для базы данных и хранилища файлов SAP BusinessObjects	144
Для таблицы базы данных управления	150
Восстановление SHR в Linux	151
Для базы данных Sybase IQ	151
Для базы данных и хранилища файлов SAP BusinessObjects	153
Для таблицы базы данных управления	162
Часть V: Справочник	164
Приложение A: Мониторы SiteScope дляSHR	165
Приложение B: Установка Xcelsius	172
Требования к оборудованию и программному обеспечению	172
Установка Xcelsius (необязательно)	172
Отправить отзыв о документации	173

Часть I: Настройка SHR

В этом разделе представлены сведения о различных сценариях развертывания, поддерживаемых SHR для создания отчетов, соответствующих этой среде.

Service Health Reporter (SHR) — это междоменное решение по составлению хронологических отчетов о производительности инфраструктуры. С помощью сведений о топологии в отчетах показано, как работоспособность, производительность и доступность базовой инфраструктуры влияет на бизнес-службы и бизнес-приложения в долгосрочной перспективе. SHR в реальном времени отслеживает связи элементов инфраструктуры с бизнес-службами, используя те же службы топологии, которые задействуются в продуктах, собирающих данные о производительности в управляемых узлах.

Service Health Reporter выполняет сбор данных в различных источниках данных и составляет отчеты с обработанными данными. Компоненты Service Health Reporter используются следующим образом: в базе данных Sybase IQ хранятся данные о производительности, SAP BusinessObjects используется для составления отчетов, в базе данных PostgreSQL хранятся данные управления. Компонент сборщика SHR выполняет сбор данных в RTSM, HP OM, базе данных профилей BSM, базе данных управления BSM, Operations Manager i (OMi), HP SiteScope, HP Network Node Manager i (NNMi) через NNM iSPI Performance for Metrics, Network Performance Server (NPS) и HP Operations agent.

Все компоненты Service Health Reporter можно установить в одной системе. Если ресурсов одной системы недостаточно для выполнения всех компонентов Service Health Reporter, компоненты сборщика данных, SAP BusinessObjects и СУБД Sybase IQ можно установить в отдельных системах. Если источники данных распределены на большой территории, можно развернуть сборщик Service Health Reporter в нескольких различных системах. Это позволит снизить нагрузку на сеть и обеспечить связь с источниками данных.

Модель топологии или представления логически сопоставляют и связывают бизнес-службы с элементами ИТ-среды. SHR позволяет определить службу топологии и собирать данные об инфраструктуре в узлах, входящих в топологию. Таким образом каждое изменение данных о топологии автоматически отражается в отчетах во время выполнения.

SHR поддерживает следующие источники топологии:

- BSM/OMi
- HP Operations Manager (HPOM)
- VMware vCenter

SHR может подключаться только к одному источнику топологии за раз.

Глава 1: Сценарии развертывания, поддерживаемые SHR

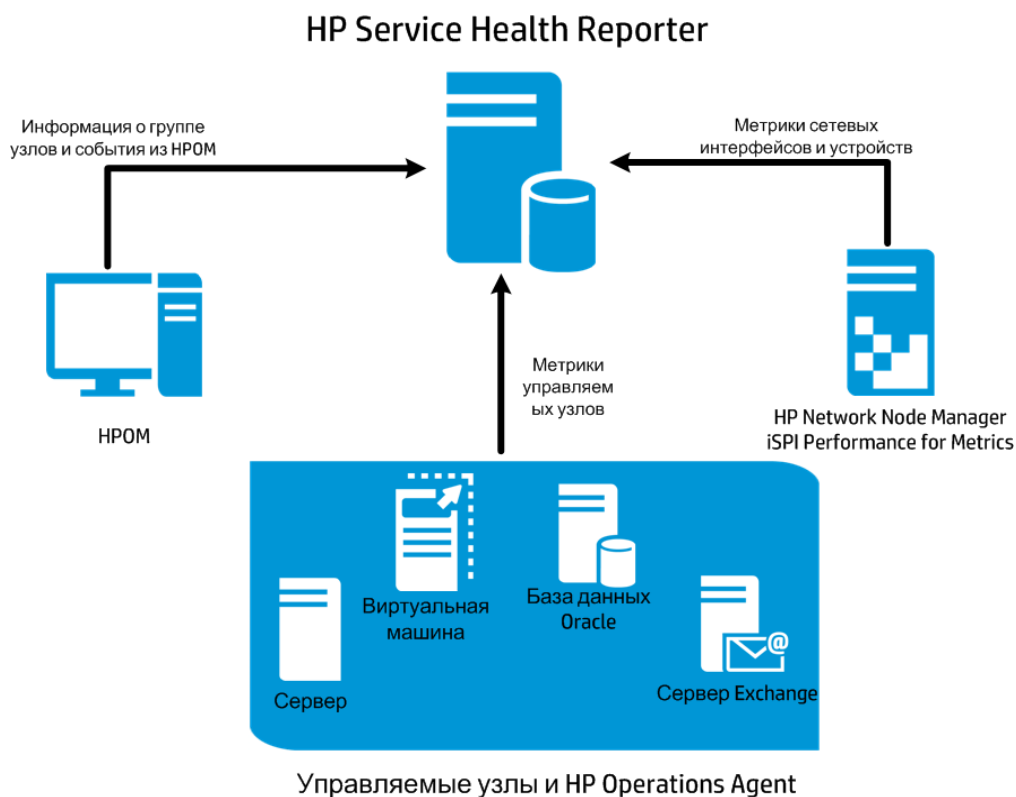
Ниже представлены сценарии развертывания, поддерживаемые SHR:

- [Развертывание с BSM/OMi](#)
- [Развертывание с HP Operations Manager](#)
- [Развертывание с VMware vCenter](#)
- [Другие варианты развертывания](#)

HP Operations Manager;

В этом варианте развертывания источником данных о топологии является группа управляемых узлов, определенных в HPOM и логически сгруппированных для мониторинга операций. Эти логические группы узлов создаются пользователями HPOM для классификации узлов в качестве отдельных организаций или органов, входящих в предприятие. Например, в HPOM можно создать группу Exchange Servers и поместить в нее серверы Exchange и узлы Active Directory, относящиеся к APJ. Группы узлов HPOM используются в SHR для получения данных о топологии.

SHR собирает данные топологии только из HPOM в этой среде, однако вы можете использовать VMware vCenter как источник данных для создания отчетов.



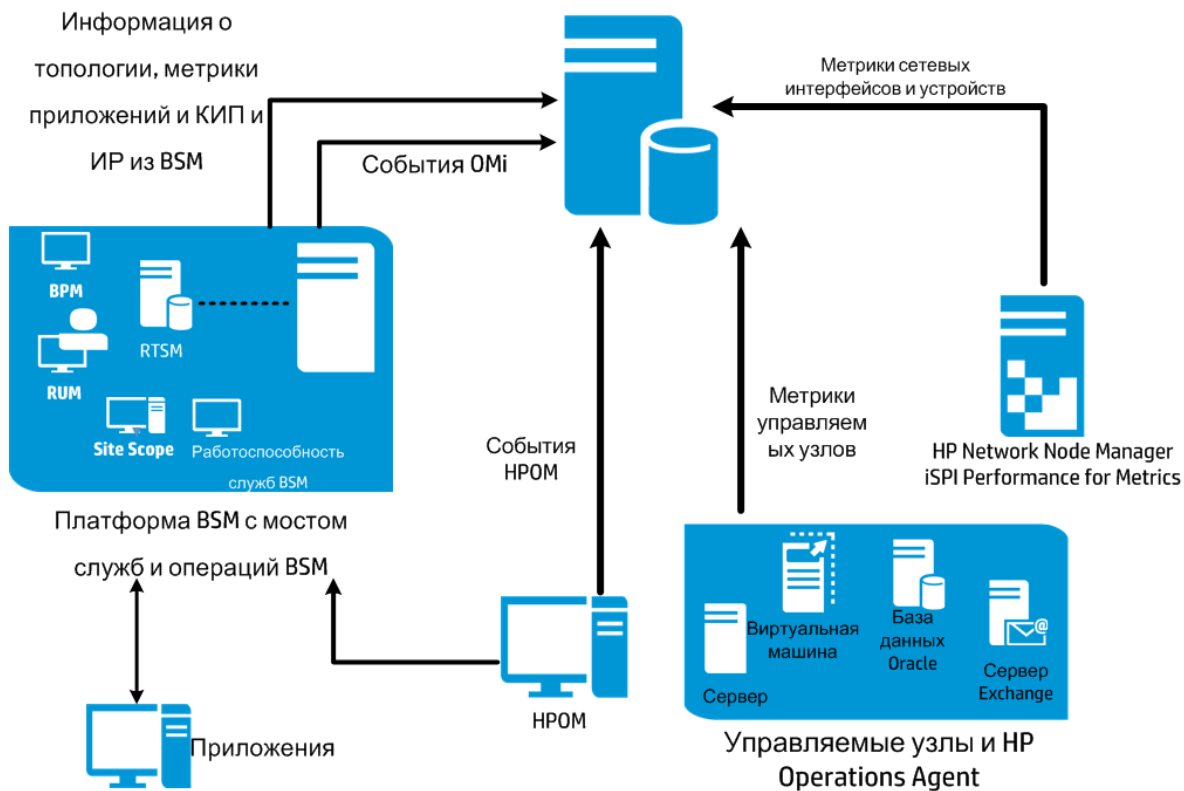
Business Service Management/Operations Manager i

В этом варианте развертывания источником данных о топологии является Run-time Service Model (RTSM). SHR обнаруживает и синхронизирует данные топологии из OMi. В среде BSM с базовыми серверами HPOM при использовании этого метода синхронизации обнаруженные данные топологии принимаются из нескольких систем HPOM, и сразу после обнаружения изменений обновляются элементы конфигурации (ЭК) и связи ЭК в модели RTSM. Для обнаружения и синхронизации данных о топологии в RTSM также можно использовать метод динамической синхронизации топологии HPOM D-MoM. В среде с OMi 10.00 SHR использует RTSM для получения данных топологии и метрик из систем HP Operations Agent или HP SiteScope, настроенных с OMi.

Кроме того, можно настроить NPS совместно с SHR для создания отчетов с данными, собранными NNMi.

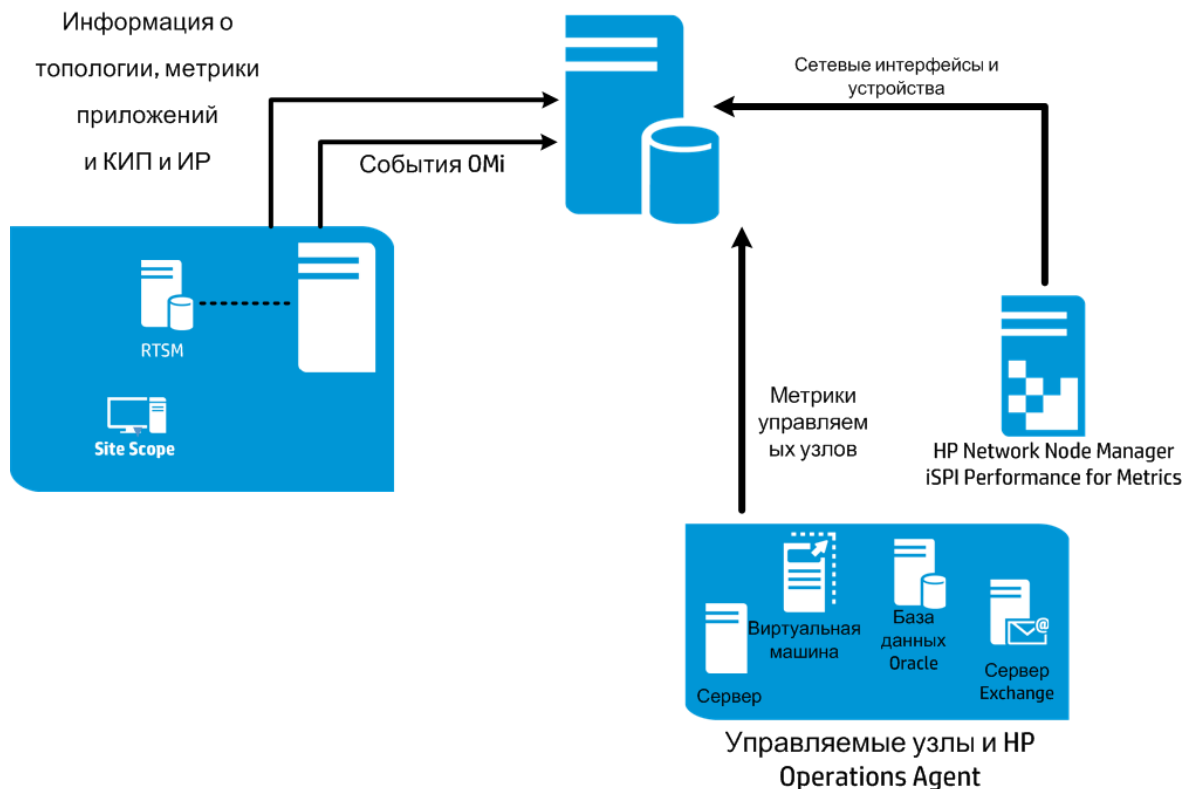
На схеме ниже изображен поток данных от HP Operations agent, HPOM, NNM iSPI Performance for Metrics и данных топологии из RTSM в среде BSM среде с базовыми серверами HPOM.

HP Service Health Reporter



На схеме ниже изображен поток данных от HP Operations agent, HPOM, NNM iSPI Performance for Metrics и данных топологии из RTSM в среде BSM OMi 10.00.

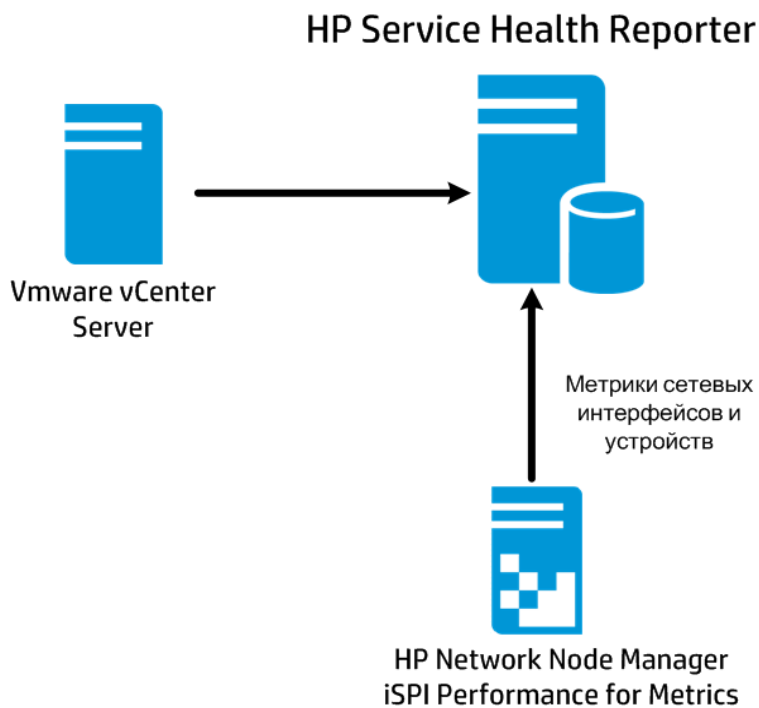
HP Service Health Reporter с Omi 10.00



VMware vCenter

VMware vCenter — это распределенное клиент-серверное программное решение, обеспечивающее централизованную и гибкую платформу управления виртуальной инфраструктурой важнейших корпоративных систем. VMware vCenter осуществляет централизованный мониторинг производительности и событий и обеспечивает повышенный уровень видимости виртуальной среды, тем самым помогая ИТ-администраторам без труда управлять средой.

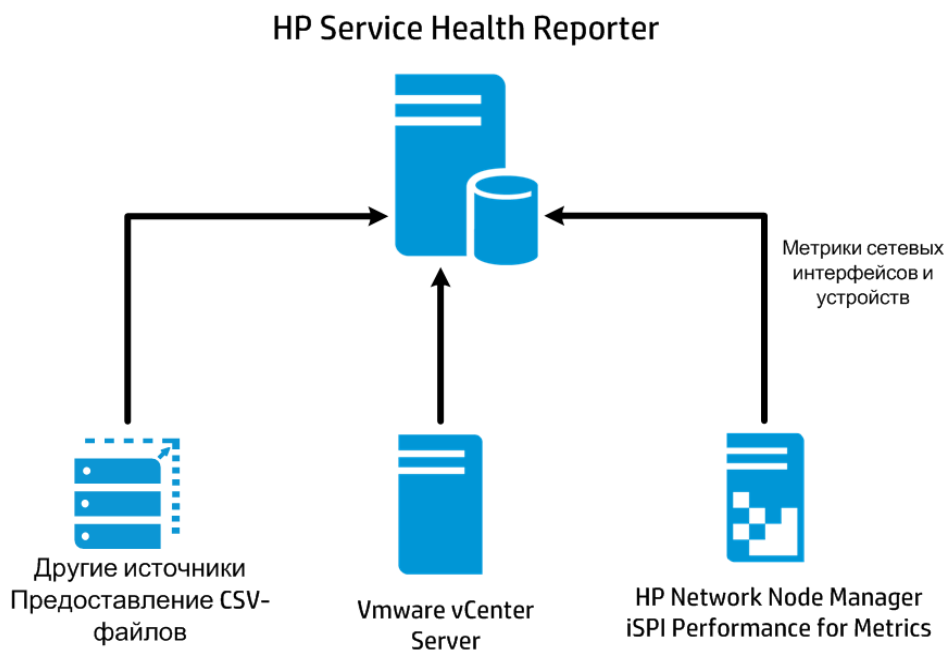
В сценарии развертывания VMware vCenter сервер VMware vCenter является источником данных о топологии для SHR.



Другие источники данных

В дополнение к базовым сценариям развертывания возможен независимый сбор данных из следующих источников:

- Развертывание с NNMi
- Развертывание с универсальной базой данных
- Развертывание с другими приложениями с использованием CSV



Глава 2: Планирование настройки SHR с использованием BSM/OMi

Если вы планируете настроить SHR для работы с установкой BSM или OMi, убедитесь, что выполняются следующие условия:

- ПО BSM/OMi установлено и настроено должным образом.
- Если вы отслеживаете системы и приложения с помощью компонента Monitoring Automation OMi и пакетов управления, убедитесь, что соответствующие политики пакетов управления развернуты.
- Если вы отслеживаете системы с помощью базовых серверов HPOM и интеллектуальных подключаемых модулей (SPI), убедитесь, что развернуты соответствующие политики SPI.
- Обязательно разверните необходимые представления OMi (см. раздел "[Настройка источника топологии RTSM для SHR](#)" ниже)

Настройка источника топологии RTSM для SHR

RTSM является источником данных о топологии для SHR. В данные о топологии входят все ЭК, моделируемые и обнаруживаемые в RTSM. Информация о ресурсах узлов непосредственно извлекается из приложений HP Operations Agent и HP SiteScope.

Примечание. Информация о ресурсах узлов является локальным измерением в приложениях HP Operations Agent и HP SiteScope.

Предварительные условия для пакетов управления

Для просмотра отчетов о пакетах содержимого SHR, которые осуществляют сбор данных из источников OMi10, необходимо установить соответствующие пакеты управления:

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SQL Server
- Oracle
- Oracle WebLogic
- IBM WebSphere

Установка этих пакетов управления также обязательна для просмотра отчетов SHR о Service Health и OMi.

Чтобы настроить источник топологии RTSM в SHR, необходимо выполнить описанные ниже задачи.

Задача 1: Развертывание представлений топологии

В среде HP BSM RTSM служит для обнаружения ЭК и создания представлений топологии. Чтобы настроить SHR для сбора данных в доменах, сначала нужно развернуть эти представления топологии для каждого пакета содержимого.

Представления топологии содержат атрибуты ЭК, с помощью которых пакеты содержимого собирают нужные данные. Набор представлений топологий различен для разных пакетов содержимого.

Например, для пакета содержимого Exchange Server может потребоваться представление топологии, в котором перечислены серверы Exchange, серверы почтовых ящиков, хранилища почтовых ящиков и общих папок и т.д. При этом для пакета содержимого System Management может потребоваться другое представление топологии, в котором перечислены все бизнес-приложения, бизнес-службы и ресурсы системы (ЦП, память, диски) в пределах инфраструктуры. В зависимости от представлений могут меняться атрибуты ЭК для каждого пакета содержимого.

Чтобы развернуть представления модели топологии для пакетов содержимого на сервере HP BSM, выполните следующие действия.

1. Выполните вход в систему HP BSM от имени администратора.
2. Выполните вход в систему, где установлен SHR, от имени администратора посредством удаленного доступа из системы HP BSM.

Перейдите в папку %PMDB_Home%\packages (для Windows) или \$PMDB_HOME/packages (для Linux) и скопируйте следующие представления топологии.

Пакет содержимого	Имя представления	Расположение
BPM (Synthetic Transaction Monitoring)	EUM_BSMR.zip	<p>Для Windows</p> <p>%PMDB_HOME%\packages\EndUserManagement\ETL_BPM.ap\source\cmdb_views</p> <p>Для Linux</p> <p>\$PMDB_HOME/packages\EndUserManagement\ETL_BPM.ap\source\cmdb_views</p>

Пакет содержимого	Имя представления	Расположение
Real User Transaction Monitoring	EUM_BSMR.zip	<p>Для Windows</p> <p>%PMDB_HOME%\packages\EndUserManagement\ETL_RUM.ap\source\cldb_views</p> <p>Для Linux</p> <p>\$PMDB_HOME\packages\EndUserManagement\ETL_RUM.ap\source\cldb_views</p>
Сеть	SHR_Network_Views.zip	<p>Для Windows</p> <p>%PMDB_HOME%\packages\Network\ETL_Network_NPS.ap\source\cldb_views</p> <p>Для Linux</p> <p>\$PMDB_HOME\packages\Network\ETL_Network_NPS.ap\source\cldb_views</p>
System Management	SM_BSM9_Views.zip	<p>Для Windows</p> <p>%PMDB_HOME%\packages\SystemManagement\ETL_SystemManagement_PA.ap\source\cldb_views</p> <p>Для Linux</p> <p>\$PMDB_HOME\packages\SystemManagement\ETL_SystemManagement_PA.ap\source\cldb_views</p>

Пакет содержимого	Имя представления	Расположение
Oracle	SHR_DBOracle_Views.zip	<p>Для Windows</p> <p>%PMDB_ HOME%\Packages\DatabaseOracle\ETL_ DBOracle_DBSPI.ap\source\cldb_ views\SHR_DBOracle_Views.zip</p> <p>Для Linux</p> <p>\$PMDB_HOME\Packages\DatabaseOracle\ETL_ DBOracle_DBSPI.ap\source\cldb_ views\SHR_DBOracle_Views.zip</p>
Oracle WebLogic Server	J2EEApplication.zip	<p>Для Windows</p> <p>%PMDB_ HOME%\packages\ApplicationServer\ETL_ AppSrvrWLS_WLSSPI.ap\source\cldb_views</p> <p>Для Linux</p> <p>\$PMDB_ HOME\packages\ApplicationServer\ETL_ AppSrvrWLS_WLSSPI.ap\source\cldb_views</p>
IBM WebSphere Application Server	J2EEApplication.zip	<p>Для Windows</p> <p>%PMDB_HOME%\ packages\ApplicationServer\ETL_ AppSrvrWBS_WBSSPI.ap\source\cldb_views</p> <p>Для Linux</p> <p>\$PMDB_HOME\ packages\ApplicationServer\ETL_ AppSrvrWBS_WBSSPI.ap\source\cldb_views</p>

Пакет содержимого	Имя представления	Расположение
Microsoft SQL Server	SHR_DBMSSQL_Views.zip	<p>Для Windows</p> <p>%PMDB_HOME%\packages\DatabaseMSSQL\ETL_DBMSSQL_DBSPI.ap\source\cmdb_views</p> <p>Для Linux</p> <p>\$PMDB_HOME\packages\DatabaseMSSQL\ETL_DBMSSQL_DBSPI.ap\source\cmdb_views</p>
Microsoft Exchange Server	SHR_Exchange_Business_View.zip	<p>Для Windows</p> <p>%PMDB_HOME%\packages\ExchangeServer\ETL_Exchange_Server2007.ap\source\cmdb_views</p> <p>Для Linux</p> <p>\$PMDB_HOME\packages\ExchangeServer\ETL_Exchange_Server2007.ap\source\cmdb_views</p>
Microsoft Active Directory	SHR_AD_Business_View.zip	<p>Для Windows</p> <p>%PMDB_HOME%\packages\ActiveDirectory\ETL_AD_ADSPI.ap\source\cmdb_views</p> <p>Для Linux</p> <p>\$PMDB_HOME\packages\ActiveDirectory\ETL_AD_ADSPI.ap\source\cmdb_views</p>

Например, чтобы скопировать zip-файлы для System Management, перейдите в папку %pmdb_home%\packages\System_Management\System_Management.ap\CMDb_View\SM_BSM9_Views.zip и скопируйте файл SM_BSM9_Views.zip в систему хоста HP BSM.

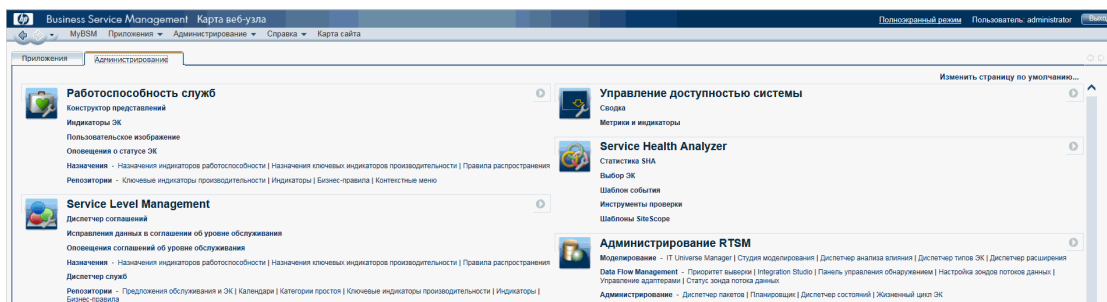
3. В веб-браузере введите следующий URL-адрес:

http://<имя_сервера>.<имя_домена>/HPBSM

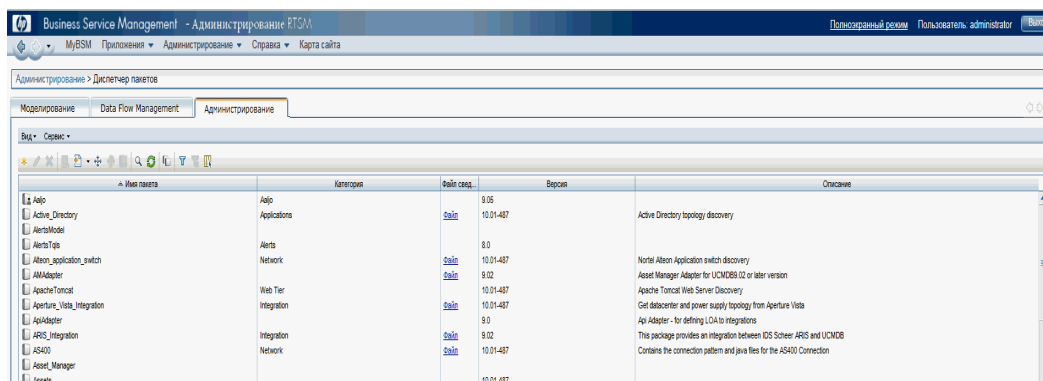
Здесь <имя_сервера> — это имя сервера HP BSM, а <имя_домена> — имя домена пользователя, соответствующее конфигурации сети пользователя.

Откроется страница входа в Business Service Management.

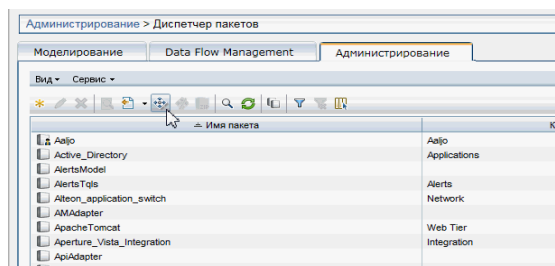
4. Введите имя пользователя и пароль и нажмите кнопку **Войти**. Откроется карта сайта Business Service Management.
5. Выберите **Администрирование->Администрирование RTSM**. Откроется страница «Администрирование RTSM».



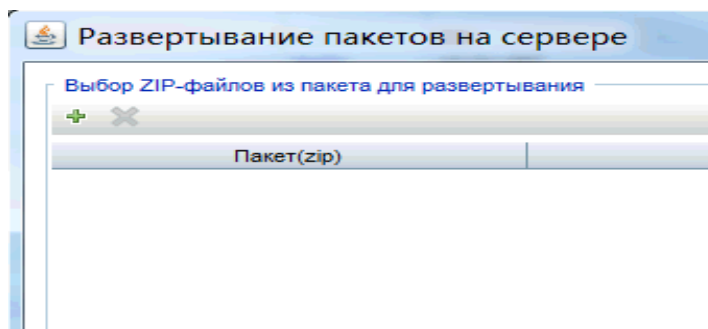
6. Выберите **Администрирование->Диспетчер пакетов**. Откроется страница «Диспетчер пакетов».



7. Щелкните значок **Развернуть пакеты на сервере (с локального диска)**. Откроется диалоговое окно «Развертывание пакета на сервере».



8. Щелкните значок **Добавить**.



Откроется диалоговое окно «Развертывание пакета на сервере (с локального диска)».

9. Перейдите к расположению zip-файлов пакета содержимого, выберите нужные файлы и нажмите кнопку **Открыть**.

Представления TQL и ODB для развертывания можно просмотреть и выбрать в разделе «Выберите ресурсы для развертывания» в диалоговом окне «Развертывание пакета на сервере (с локального диска)». Проверьте, что выбраны все файлы.

10. Нажмите кнопку **Развернуть**, чтобы развернуть представления пакета содержимого.

Включение атрибутов ЭК для пакета содержимого

Примечание. Ознакомьтесь с этим разделом, даже если вы не используете OMi 10.00. В среде OMi 10.00 используйте данные сервера OMi вместо сервера BSM (в следующих действиях по настройке).

Представление каждого пакета содержимого содержит список атрибутов ЭК, относящихся к этому пакету содержимого. Атрибуты ЭК, необходимые для сбора данных, автоматически включаются в каждом представлении пакета содержимого после развертывания.

Чтобы включить дополнительные атрибуты ЭК для сбора дополнительных данных, важны для бизнеса, выполните следующие действия.

1. В веб-браузере введите следующий URL-адрес:

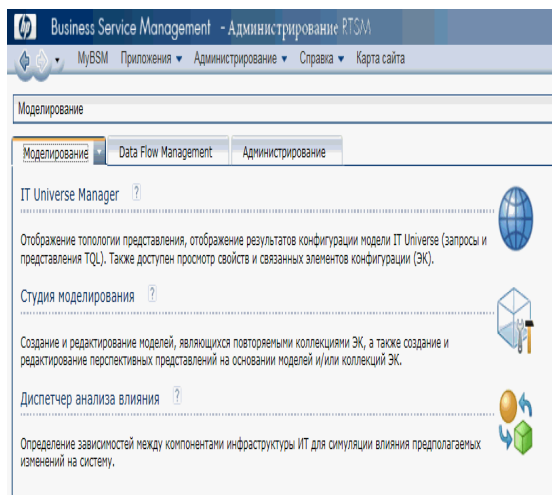
`http://<имя_сервера>.<имя_домена>/HPBSM`

Здесь *<имя_сервера>* — это имя сервера HP BSM, а *<имя_домена>* — имя домена пользователя, соответствующее конфигурации сети пользователя.

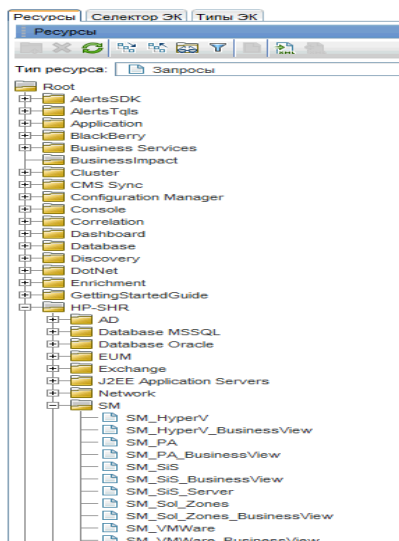
Откроется страница входа в Business Service Management.

2. Введите имя пользователя и пароль и нажмите кнопку **Войти**. Откроется карта сайта Business Service Management.

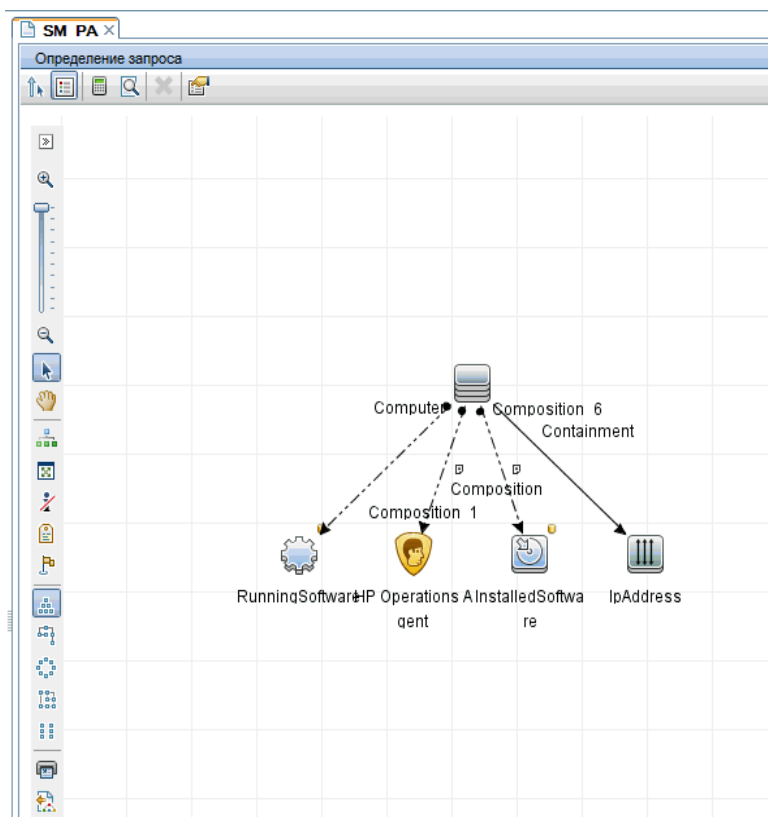
3. Выберите **Администрирование** -> **Администрирование RTSM**. Откроется страница «Администрирование RTSM».
4. Выберите **Моделирование** -> **Modeling Studio**. Откроется страница Modeling Studio.



5. В области «Ресурсы» разверните элемент HP-SHR, разверните папку пакета содержимого и дважды щелкните представление топологии, чтобы открыть его.

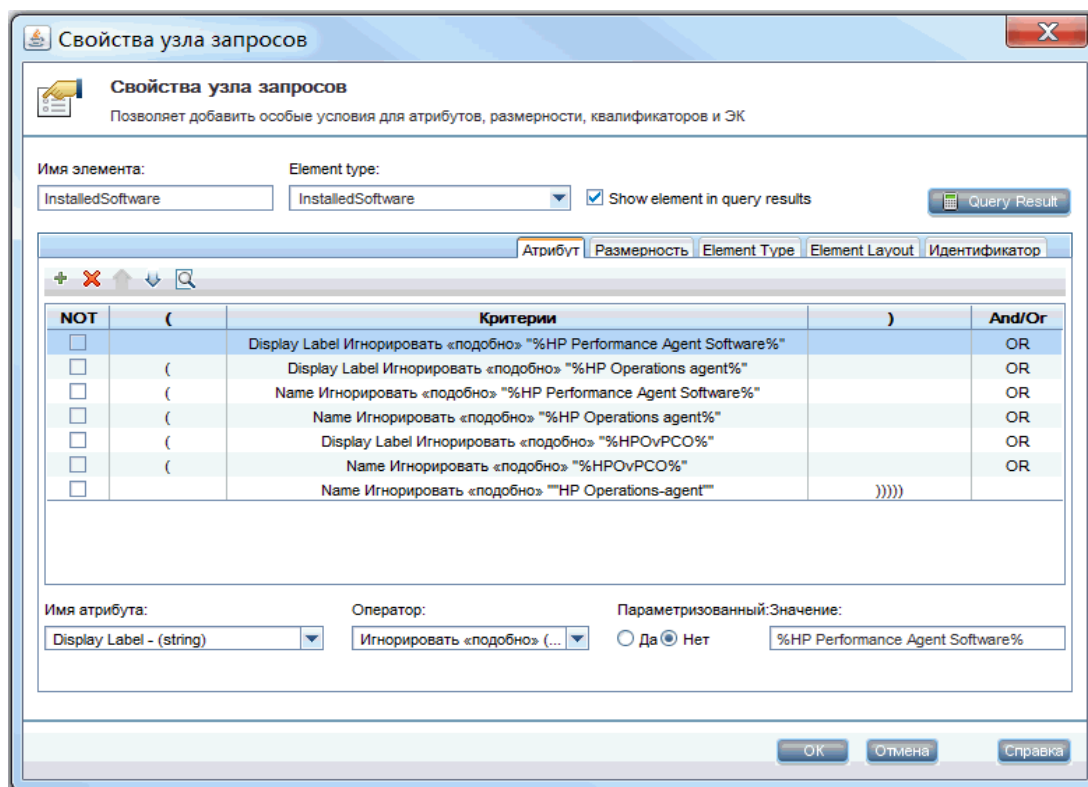


6. В области «Топология» щелкните правой кнопкой мыши любой узел на диаграмме топологии и нажмите кнопку **Свойства узла запроса**, чтобы просмотреть список атрибутов ЭК для выбранного узла.



Откроется диалоговое окно «Свойства узла запроса».

7. Выберите **Атрибуты**. Выберите атрибуты для включения и нажмите кнопку **ОК**.



Представления пакетов содержимого успешно развернуты в зависимости от типа сценария развертывания, выбранного для SHR.

Настройка SiteScore для интеграции с SHR

HP SiteScore — это решение для безагентного мониторинга, которое позволяет следить за доступностью и производительностью распределенных ИТ-инфраструктур, например серверов, операционных систем, сетевых устройств, сетевых служб, приложений и их компонентов.

Чтобы SHR собирал данные для физических узлов из SiteScore, необходимо создать мониторы в SiteScore. Мониторы — это средства для автоматического подключения к различным системам и приложениям, используемым в корпоративных бизнес-системах, и для запроса этих систем и приложений. Эти мониторы собирают данные о различных ИТ-компонентах среды и сопоставляются с метриками, используемыми в SHR (загрузка ЦП, использование памяти и т.п.). После создания мониторов также необходимо включить в SiteScore регистрацию данных в агенте HP Operations Agent или базе данных профилей BSM, чтобы SHR смог получать необходимые данные от агента. Выполняйте эту задачу только если в системе установлен SiteScore. В противном случае перейдите к следующей задаче.

См. список мониторов (включая счетчики и показатели), которые нужно создать в SiteScore, в разделе ["Мониторы SiteScore для SHR" на странице 165](#).

Дополнительные сведения о создании мониторов в SiteScore см. в руководствах *Использование SiteScore* и *Справочник по мониторам*. Эти документы доступны по следующему URL-адресу:

<http://h20230.www2.hp.com/selfsolve/manuals>

Включите интеграцию между SiteScope и BSM для передачи платформе BSM собранных мониторами SiteScope данных о топологии. Дополнительные сведения об интеграции SiteScope с BSM см. в *работа с Business Service Management (BSM)* руководства *Использование SiteScope*.

Чтобы включить интеграцию SiteScope с SHR, выполните следующие действия.

1. Выполните от имени администратора вход в систему, где установлен SHR.
2. Откройте SiteScope, введя адрес SiteScope в веб-браузере. По умолчанию используется адрес `http://<SiteScope host name>:<port number>/SiteScope`.
3. Включите интеграцию SiteScope с агентом HP Operations Agent для регистрации данных. Необходимые действия описаны в *работа с Operations Manager и BSM с помощью агента HP Operations Agent* руководства *Использование SiteScope*.
4. Задайте число мониторов и периодичность подачи данных в рамках интеграции с агентом HP Operations Agent. Конфигурация SiteScope по умолчанию позволяет запускать несколько тысяч мониторов, важно правильно определить масштаб при планировании максимального числа мониторов, метрик и типов мониторов, хранящихся в рамках интеграции метрик SiteScope-HPOM. Дополнительные сведения см. в разделе *Рекомендации по масштабированию для интеграции метрик SiteScope-Operations Manager* руководства *Использование SiteScope*.

Если вы настроили удаленный сборщик с помощью определения службы, обязательно перезапустите службу сборщика на системе сборщика после установки пакетов содержимого.

Чтобы вручную перезапустить службу в Windows, откройте окно служб, щелкните службу HP_PMDB_Platform_Collection правой кнопкой и выберите **Перезапустить**.

Чтобы вручную перезапустить службу в Linux, перейдите в каталог `/etc/init.d` и выполните следующую команду:

```
service HP_PMDB_Platform_Collection --full-restart
```

Глава 2: Планирование настройки SHR с использованием HPOM

Если вы планируете настроить SHR для работы с установкой HPOM, убедитесь, что выполняются следующие условия:

- ПО HPOM установлено и настроено должным образом.
- Убедитесь, что развернуты необходимые политики SPI.
- Обязательно разверните необходимые представления OMi (см. раздел ["Настройка источника топологии RTSM для SHR"](#) на странице 14

Настройка служб SHR, когда приложение SHR установлено в домене

Если приложение SHR установлено в системе, входящей в домен (например, DOMAIN\Administrator), запустите службы *HP PMDB Platform Administrator* и *HP PMDB Platform Collection*. Необходимо настроить службы для пользователя домена перед настройкой подключения к источнику определения службы HPOM.

Задача 1: Настройка службы администратора платформы HP PMDB для домена

1. Для настройки выполните следующие действия.
2. Выберите **Пуск > Выполнить**. Откроется диалоговое окно «Выполнить».
3. Введите `services.msc` в поле Открыть и нажмите клавишу **ВВОД**. Откроется окно «Службы».
4. В правой части окна щелкните правой кнопкой мыши элемент `HP_PMDB_Platform_Administrator` и выберите команду **Остановить**.
5. Щелкните правой кнопкой мыши службу `HP_PMDB_Platform_Administrator` и выберите **Свойства**. Откроется диалоговое окно свойств службы SHR.
6. На вкладке «Вход в систему» выберите вариант **С учетной записью**.
7. Введите `DOMAIN\Administrator` в поле (где Administrator — локальный пользователь с привилегиями администратора).
8. Введите пароль пользователя в поле «Пароль».
9. Снова введите пароль в поле «Подтверждение».
10. Нажмите кнопку **Применить**, а затем **ОК**.
11. В правой части окна щелкните правой кнопкой мыши элемент `HP_PMDB_Platform_Administrator` и выберите команду **Запустить**.

Задача 2. Настройка службы HP PMDB Platform Collection Service для домена

Выполните следующие действия.

1. Выберите **Пуск > Выполнить**. Откроется диалоговое окно «Выполнить».
2. Введите `services.msc` в поле Открыть и нажмите клавишу **ВВОД**. Откроется окно «Службы».
3. В правой части окна щелкните правой кнопкой мыши элемент `HP_PMDB_Platform_Collection_Service` и выберите команду **Остановить**.

4. Щелкните правой кнопкой мыши службу `HP_PMDB_Platform_Collection_Service` и выберите **Свойства**. Откроется диалоговое окно со свойствами службы сбора данных SHR.
5. На вкладке «Вход в систему» выберите вариант **С учетной записью**.
6. Введите `DOMAIN\Administrator` в поле (где `Administrator` — локальный пользователь с привилегиями администратора).
7. Введите пароль пользователя в поле «Пароль».
8. Снова введите пароль в поле «Подтверждение».
9. Нажмите кнопку **Применить**, а затем **ОК**.
10. В правой части окна щелкните правой кнопкой мыши элемент `HP_PMDB_Platform_Collection_Service` и выберите команду **Запустить**.

Эти действия обязательны только в случае, когда продукт устанавливается в домене.

После выполнения действий по настройке переходите к настройке подключения к определению службы HPOM.

Создание учетной записи пользователя базы данных на сервере базы данных HPOM

Выполнение этой задачи зависит от способа установки Microsoft SQL Server в среде HPOM и от возможностей по настройке SHR для обмена данными с сервером базы данных HPOM. Возможны два сценария.

- **Сценарий 1:** HPOM для Windows 8.x/9.x установлен в одной системе, а Microsoft SQL Server 2005 или Microsoft SQL Server 2008 установлен в той же системе или в удаленной системе. SHR, установленный в другой системе, можно настроить для подключения к SQL Server с использованием проверки подлинности Windows или проверки подлинности SQL Server (смешанный режим). Метод проверки подлинности, определенный в SQL Server, может использоваться в SHR для настройки подключения к базе данных HPOM.
- **Сценарий 2:** HPOM для Windows 8.x использует выпуск Microsoft SQL Server 2005 Express Edition, который встроен в систему по умолчанию. Аналогично, в HPOM для Windows 9.x по умолчанию используется встроенный выпуск Microsoft SQL Server 2008 Express Edition. В этом сценарии используется режим проверки подлинности Windows NT. Однако в этом случае невозможно удаленное соединение между SQL Server и SHR. Поэтому необходимо создать для SHR учетную запись пользователя для поддержки смешанного режима проверки подлинности в этом сценарии.

Перед созданием учетной записи пользователя необходимо включить смешанный режим проверки подлинности. См. указания по следующему URL-адресу:

<http://support.microsoft.com>

Чтобы создать имя пользователя и пароль для проверки подлинности, выполните следующие действия. Действия для Microsoft SQL Server 2008 аналогично действиям, выполняемым в SQL Server 2005.

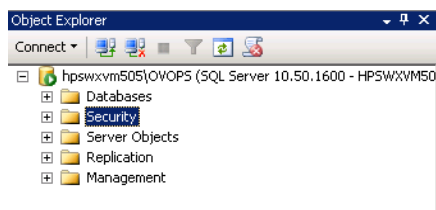
1. Создайте имя пользователя и пароль:
 - a. Выполните вход в систему HPOM с встроенным Microsoft SQL Server 2005.
 - b. Выберите **Пуск->Программы -> Microsoft SQL Server 2005->SQL Server Management Studio**. Откроется окно Microsoft SQL Server Management Studio.

Примечание. Если в системе не установлена среда SQL Server Management Studio, ее можно загрузить в соответствующем разделе веб-сайта Microsoft по следующему URL-адресу: <http://www.microsoft.com>

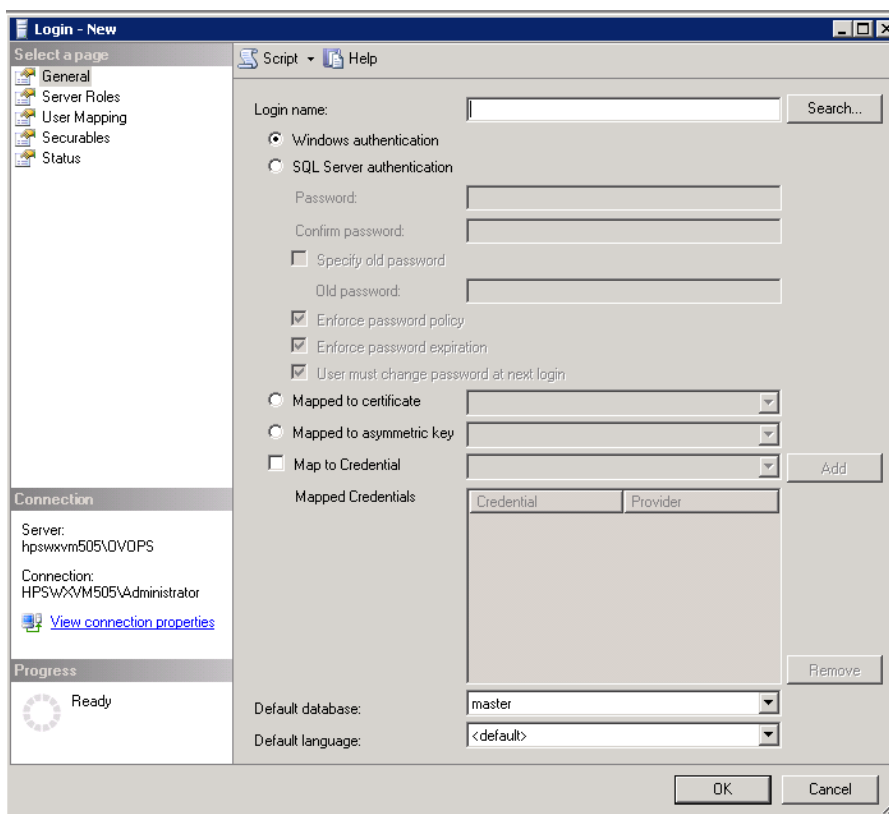
- c. В диалоговом окне «Подключение к серверу» выберите режим **Проверка подлинности NT** в списке «Проверка подлинности» и нажмите кнопку **Соединить**.



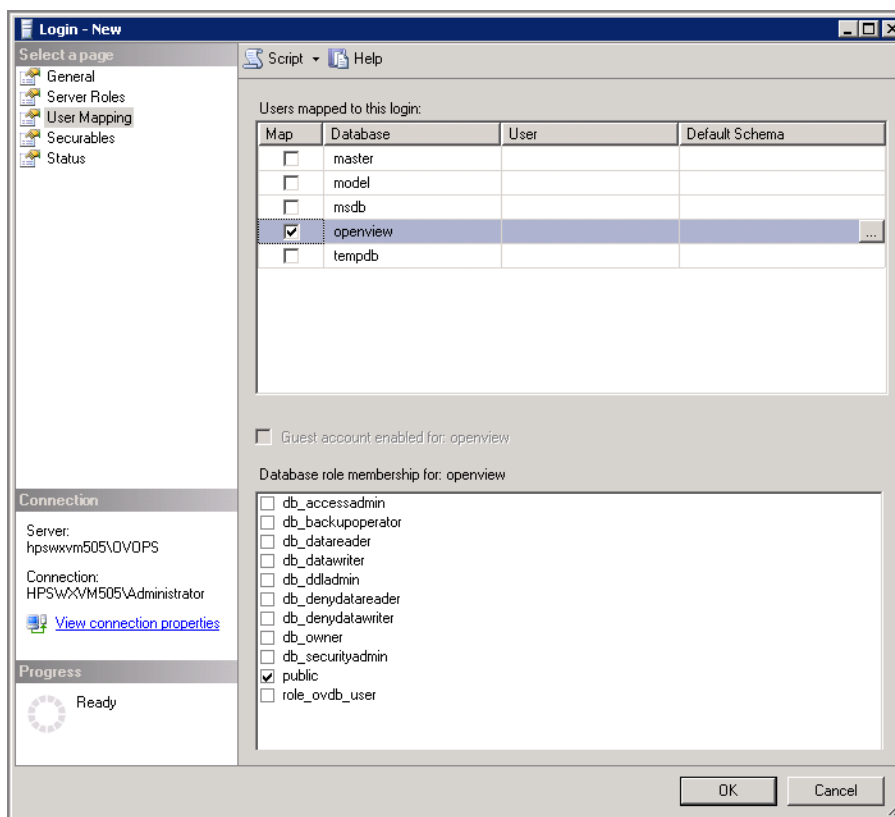
- d. В области «Обозреватель объектов» разверните папку «Безопасность».



- e. Щелкните правой кнопкой мыши папку «Имена входа» и выберите команду **Создать имя входа**. Откроется диалоговое окно «Имя входа - создание».

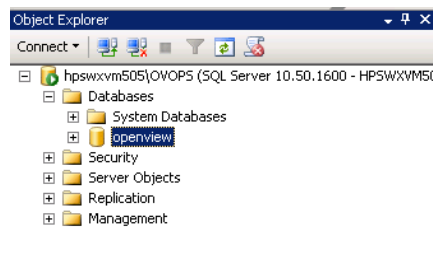


- f. В поле «Имя входа» введите имя пользователя. Укажите другие необходимые данные.
- g. Выберите вариант **Проверка подлинности SQL Server**.
- h. В поле «Пароль» введите пароль.
- i. В поле «Подтверждение» снова введите пароль. Можно отключить правила проверки паролей, чтобы создать простой пароль.
- j. Нажмите кнопку **Сопоставление пользователей**.
- k. В разделе «Пользователи, сопоставленные с этим именем входа», установите флажок **openview**.

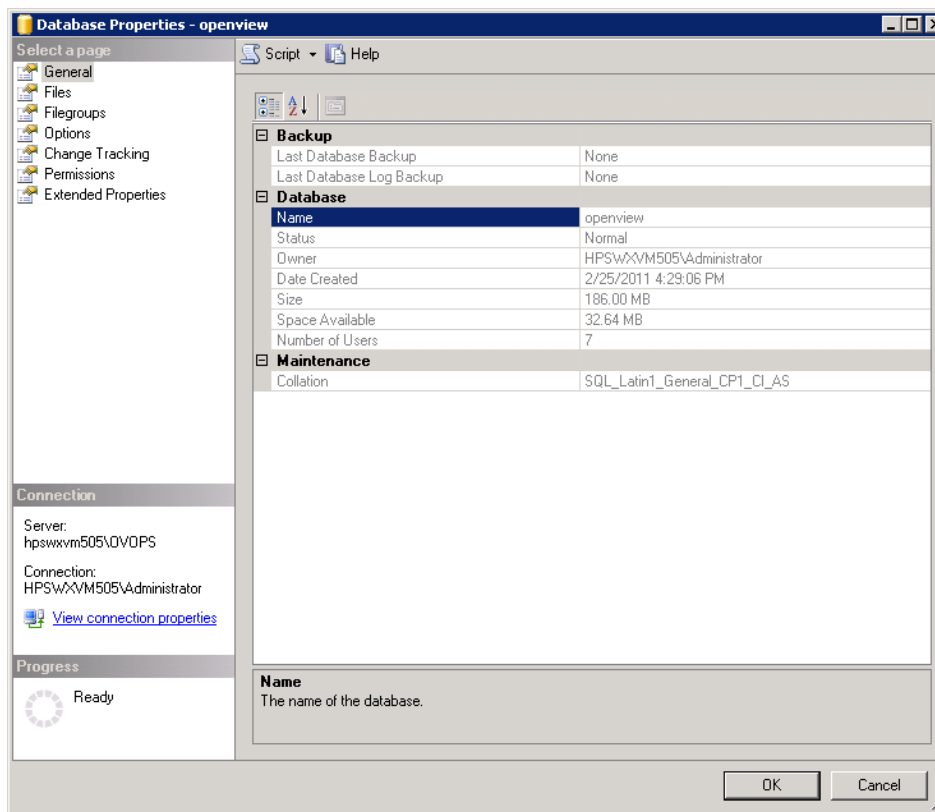


Нажмите кнопку **OK**, чтобы создать имя пользователя и пароль.

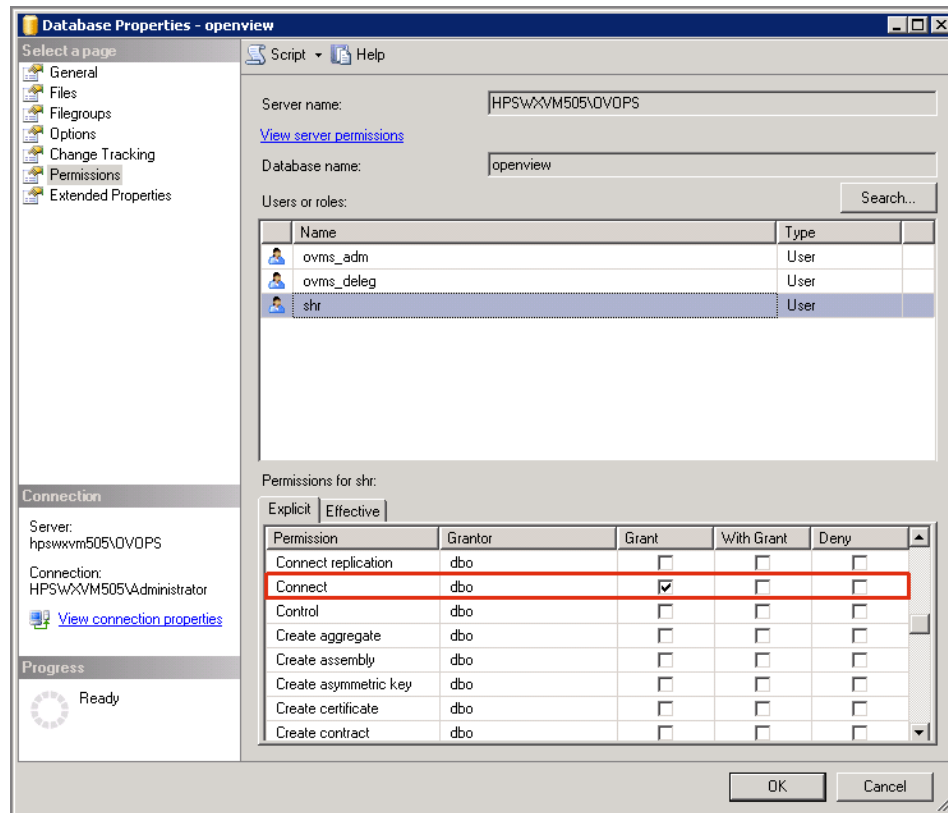
2. Пользователь базы данных должен иметь по крайней мере разрешения **CONNECT** и **SELECT**. Чтобы включить разрешения **CONNECT** и **SELECT** для созданной учетной записи пользователя, выполните следующие действия.
 - a. В области «Обозреватель объектов» разверните папку «Базы данных».



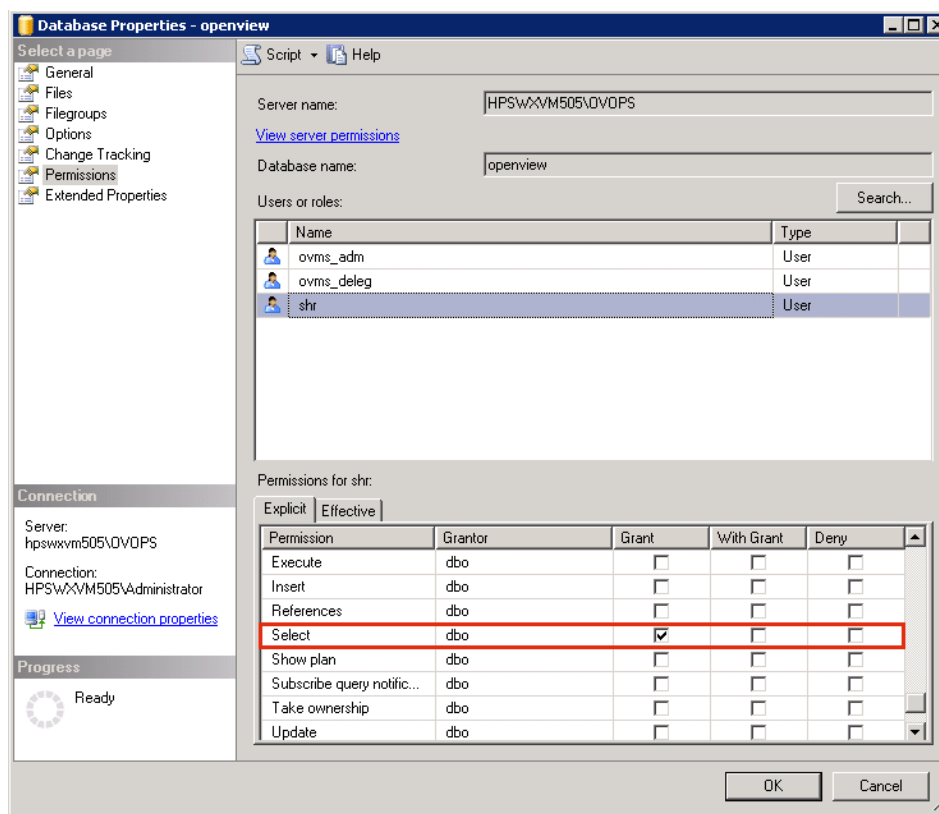
- b. Щелкните правой кнопкой мыши пункт **openview** и выберите **Свойства**. Откроется диалоговое окно «Свойства базы данных - openview».



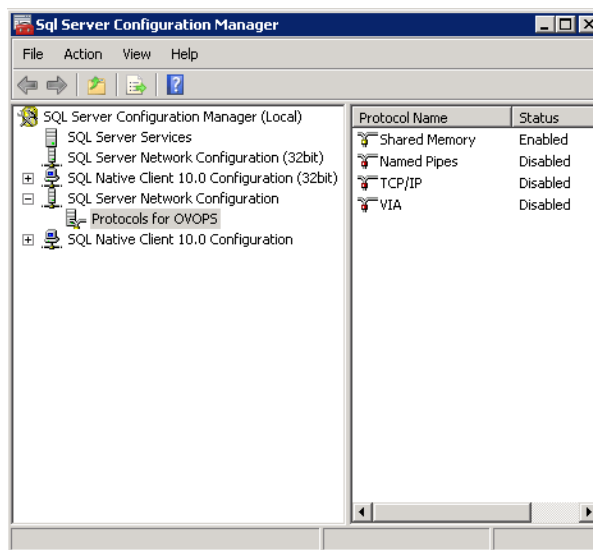
- c. В области «Выберите страницу» нажмите кнопку **Разрешения**.
- d. В разделе «Пользователи или роли» щелкните созданную учетную запись пользователя.
- e. Прокрутите список «Явные разрешения для проверки» до разрешения CONNECT и установите для него флажок **Предоставить**.



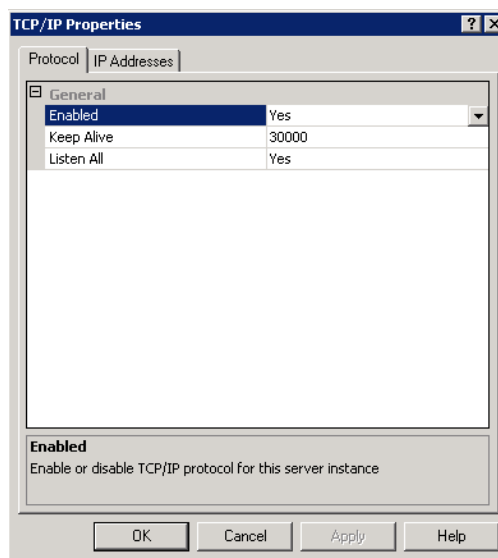
- f. Прокрутите список «Явные разрешения для проверки» до разрешения SELECT и установите для него флажок **Предоставить**.



- g. Нажмите кнопку **OK**.
3. Проверьте номер порта сервера HPOM.
 - a. Выберите **Пуск->Программы -> Microsoft SQL Server 2005->Configuration Tools -> SQL Server Configuration Manager**. Откроется окно диспетчера конфигурации SQL Server.
 - b. Разверните папку «Конфигурация сети SQL Server» и выберите пункт **Протоколы для OVOPS**. Если имя экземпляра изменилось, выберите нужное имя экземпляра.



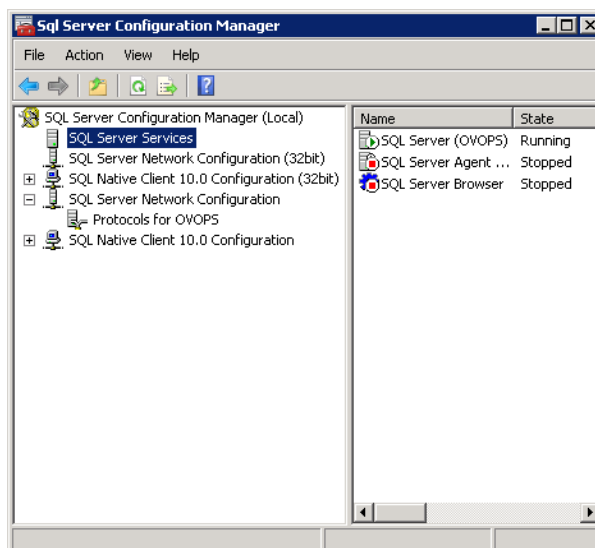
- c. В правой части окна щелкните правой кнопкой мыши элемент **TCP/IP** и выберите команду **Включить**.
- d. Щелкните правой кнопкой мыши пункт **TCP/IP** и выберите **Свойства**. Откроется диалоговое окно «Свойства TCP/IP».



На вкладке **IP-адреса** в разделе IPAll запишите номер порта.

- 4. Перезапустите сервер базы данных HPOM.

- а. В окне диспетчера конфигурации SQL Server щелкните ссылку **Службы SQL Server**.



- б. В правой части окна щелкните правой кнопкой мыши элемент **SQL Server (OVOPS)** и выберите команду **Перезапустить**.

Во время настройки подключения к источнику данных HPOM с помощью компонента Административная консоль можно использовать вновь созданные имя пользователя и пароль, а также имеющиеся имя экземпляра и номер порта.

Примечание. Эти действия можно выполнить с помощью программы командной строки `osql`. Дополнительные сведения см. на веб-сайте Microsoft по следующему URL-адресу:

<http://support.microsoft.com>

Проверка номера порта сервера HPOM

Если в HPOM используется база данных типа Oracle, выполните следующие действия, чтобы проверить номер порта.

1. Выполните вход на сервер Oracle.
2. Перейдите в папку `$ORACLE_HOME/network/admin` или `%ORACLE_HOME%\NET80\Admin`.
3. Откройте файл `listener.ora`. В этом файле указан номер порта для сервера HPOM.

Глава 3: Основная конфигурация

Этот раздел содержит три подраздела, в которых представлены подробные процедуры первичной настройки. После установки SHR и запуска административной консоли откроется мастер настройки, который поможет настроить базы данных, сборщики и источник топологии SHR. Во время настройки вы можете настроить только локальный сборщик или выполнить настройку позднее с помощью страницы конфигурации сборщика. После выполнения задач в мастере настройки откроется окно мастер развертывания. Вы можете настроить или установить оставшиеся пакеты с помощью страницы «Ожидающая конфигурация».

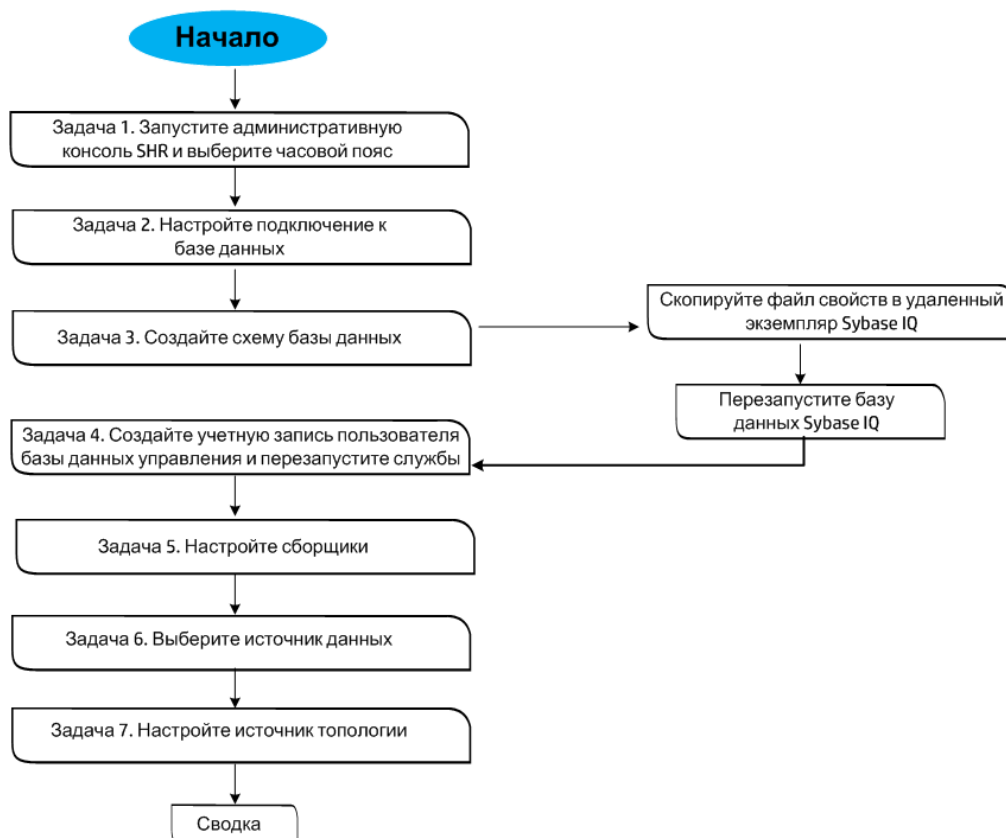
Если вы не настроили источники данных с помощью мастера настройки на этом этапе, их можно настроить позднее с помощью страницы конфигурации сборщика в административной консоли.

Все задачи настройки, описанные в этой главе, необходимо выполнить сразу после установки или обновления SHR, но до установки пакетов содержимого посредством диспетчера развертывания.

На следующей схеме показаны задачи, выполняемые после установки, если база данных Sybase IQ находится на сервере SHR в той же системе.



На следующей схеме показаны задачи, выполняемые после установки или обновления SHR с удаленной базой данных.



Задача 1. Запустите административную консоль

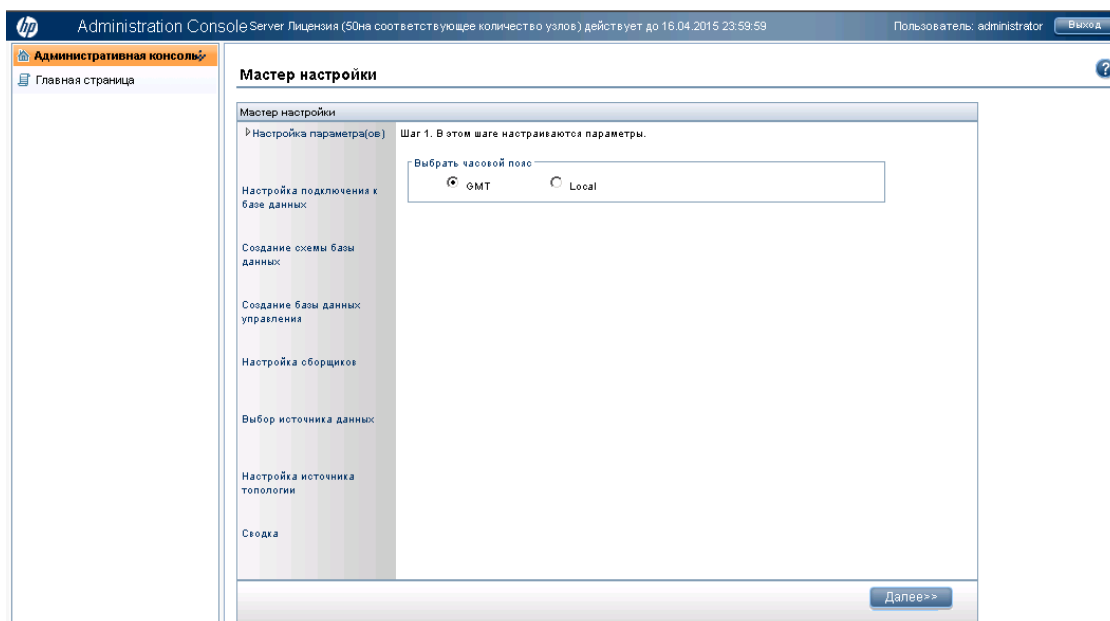
1. Запустите административную консоль в веб-браузере по следующему URL-адресу.

`http://<SHR_Server_FQDN>:21411`

2. Введите слово **administrator** в поле «Имя для входа» и нажмите кнопку **Войти**, чтобы продолжить. Откроется главная страница.

Примечание. Если для доступа к административной консоли используется другая учетная запись пользователя, убедитесь, что она имеет права администратора.

Мастер настройки SHR после установки открывается только в том случае, если не выполнены задачи настройки после установки. Мастер сохраняет состояние сеансов, что позволяет продолжить ранее прерванный сеанс настройки.



3. На странице «Настройте параметры SHR» выберите часовой пояс (GMT или локальный), в котором будет работать SHR.

В разделе «Выберите часовой пояс HP SH Reporter» выполните одно из следующих действий.

- Чтобы в SHR действовало время GMT, выберите вариант **GMT**.
- Чтобы SHR действовало время локальной системы, выберите вариант **Локальный**.

Примечание. Выбранный на этой странице часовой пояс применяется к системе и отчетам SHR, при этом информация о времени выполнения процессов, таких как сбор данных и потоки рабочих процессов, всегда регистрируется по местному времени независимо от выбранного параметра.

4. Нажмите кнопку **Далее**. Откроется страница «Настройка подключения к базе данных».

Задача 2. Настройте подключение к базе данных

На странице «Настройка подключения к базе данных» укажите сведения о сервере базы данных, на котором создается база данных для SHR.

Чтобы настроить подключение к базе данных, выполните следующие действия.

1. На странице «Настройка подключения к базе данных» выберите вариант **Удаленная база данных**, если приложение SHR установлено с удаленной базой Sybase IQ. В противном

случае переходите к следующему шагу.

2. В разделе **Введите параметры подключения к базе данных** введите следующие значения:

Поле	Описание
Имя хоста	Имя или IP-адрес хоста, где работает сервер базы данных Sybase IQ.
Порт	Номер порта для запроса сервера базы данных. По умолчанию используется порт 21424.
Имя сервера	Имя сервера Sybase IQ. Имя сервера Sybase IQ должно быть уникальным в пределах подсети. Имя сервера отображается в этом поле только в информационных целях. Его никогда не следует изменять.

3. В разделе **Введите пользователя базы данных управления (с правами DBA) и пароль** введите следующие значения:

Поле	Описание
Имя пользователя	Имя пользователя базы данных Sybase IQ. Этот пользователь должен иметь права DBA. По умолчанию используется имя пользователя <code>dba</code> .
Пароль	Пароль пользователя базы данных. По умолчанию используется пароль <code>sql</code> . Рекомендуется сменить пароль по умолчанию перед переходом к задачам настройки после установки. См. сведения о смене пароля в документации по SAP Sybase IQ на веб-сайте URL: http://infocenter.sybase.com

4. В разделе **Выберите пароль для пользователя базы данных PMDB (PMDB_ADMIN)** введите следующие значения:

Поле	Описание
Пароль администратора	Пароль администратора базы данных PMDB.
Подтверждение пароля администратора	Снова введите тот же пароль для подтверждения.

5. Нажмите кнопку **Далее**. Откроется страница «Создание схемы базы данных».

Задача 3. Создайте схему базы данных

На странице «Создание схемы базы данных» укажите размер развертывания базы данных, то есть число узлов, в которых SHR будет собирать данные. В зависимости от выбранного значения SHR вычисляет и отображает рекомендуемый размер базы данных.

Если база данных Sybase IQ встроена в SHR, выполните задачу, описанную в разделе [Создание схемы для локальной базы данных Sybase](#).

Если база данных Sybase IQ размещена в удаленной системе, выполните задачу, описанную в разделе [Создание схемы для удаленной базы данных Sybase](#).

Создание схемы для локальной базы данных Sybase

Чтобы создать схему для локальной базы данных Sybase IQ, установленной на сервере SHR, выполните следующие действия:

1. В разделе «Выберите размер развертывания» выберите один из следующих объемов данных в зависимости от потребностей.

Поле	Описание
Низкий	В этом варианте SHR поддерживает сбор данных менее чем из 500 узлов.
Средний объем	В этом варианте SHR поддерживает сбор данных от 500 до 5000 узлов.
Высокий	В этом варианте SHR поддерживает сбор данных от 5000 до 20000 узлов.

2. В разделе «Рекомендуемая конфигурация IQ» введите следующие значения:

Поле	Описание
Главный кэш IQ (Мбайт)	Рекомендуемый размер главного буферного кэша для главного хранилища Sybase IQ. Это значение устанавливается по умолчанию.
Временный кэш IQ (Мбайт)	Рекомендуемый размер временного буферного кэша для временного хранилища Sybase IQ. Это значение устанавливается по умолчанию.
Размер DBSpace в IQ (Мбайт)	Рекомендуемый размер для dbspace IQ_System_Main, где хранятся главные файлы базы данных. Этот размер можно изменять.

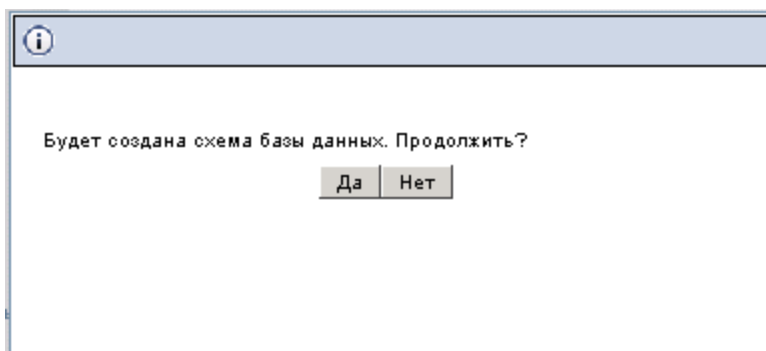
Поле	Описание
Размер временного DBSpace в IQ (Мбайт)	Рекомендуемый размер для dbspace IQ_System_Temp, где хранятся временные файлы базы данных. Этот размер можно изменять.

3. В поле «Расположение файла база данных» введите расположение, где будут храниться файлы базы данных.

Пример для Windows C:\HP-SHR\Sybase\db, для Linux: /opt/HP/BSM/Sybase/db.

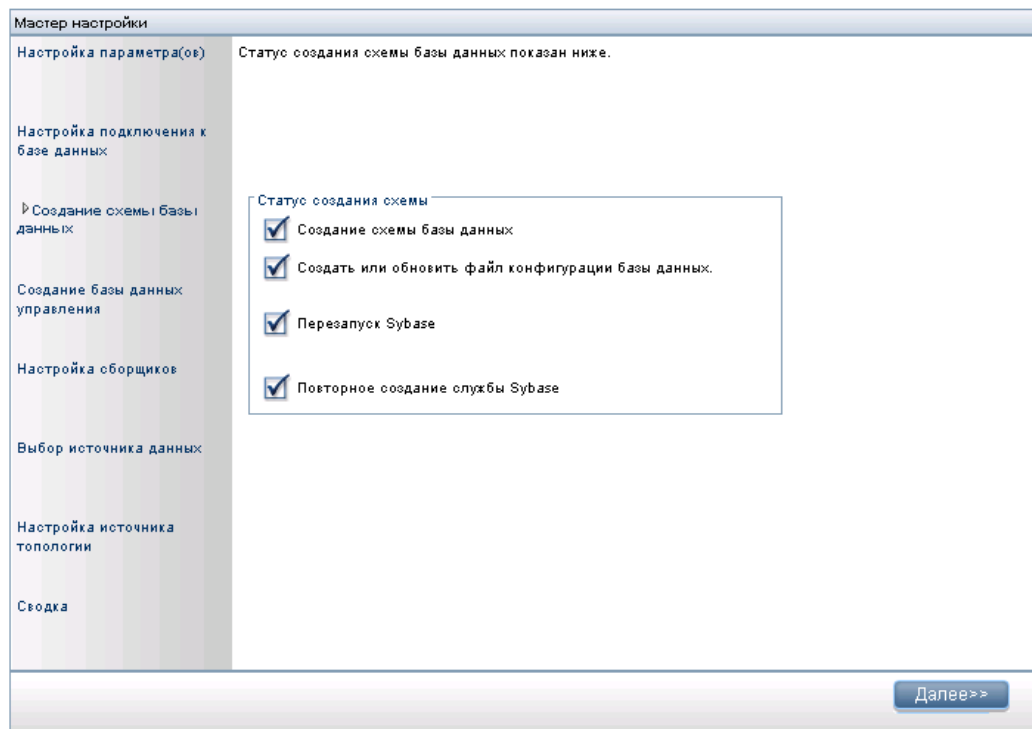
Внимание. Убедитесь, что ресурсов системы достаточно для обеспечения выбранного объема данных, собираемых SHR. См. информацию о требованиях к ресурсам для выбранного объема в *матрице поддержки HP Service Health Reporter*.

- a. Нажмите кнопку **Далее**. Откроется диалоговое окно подтверждения.



- b. Нажмите **Yes**. Если подключение к базе данных установлено успешно и создана схема, то откроется страница подтверждения со статусом создания схемы.

Мастер настройки



- c. Для продолжения нажмите кнопку **Далее**.
- d. Если не удалось установить подключение к базе данных и создать схему, нажмите кнопку **Назад**, чтобы проверить указанные значения.

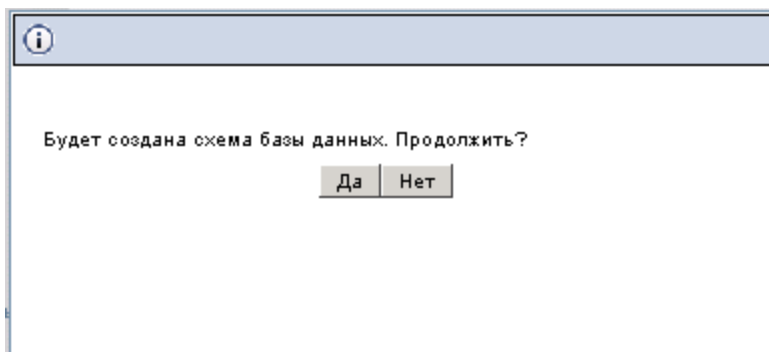
Создание схемы для удаленной базы данных Sybase

Если SHR установлен с удаленной БД Sybase IQ, выполните следующие действия.

1. Выполните шаги 1 и 2, описанные в разделе "[Создание схемы для локальной базы данных Sybase](#)" на [странице 40](#).
2. В поле «Расположение файла база данных» введите расположение, где будут храниться файлы базы данных. Пример для Windows C:\HP-SHR\Sybase\db, для Linux: /opt/HP/BSM/Sybase/db. Создайте папку базы данных перед тем как вводить путь в поле «Расположение файла базы данных».

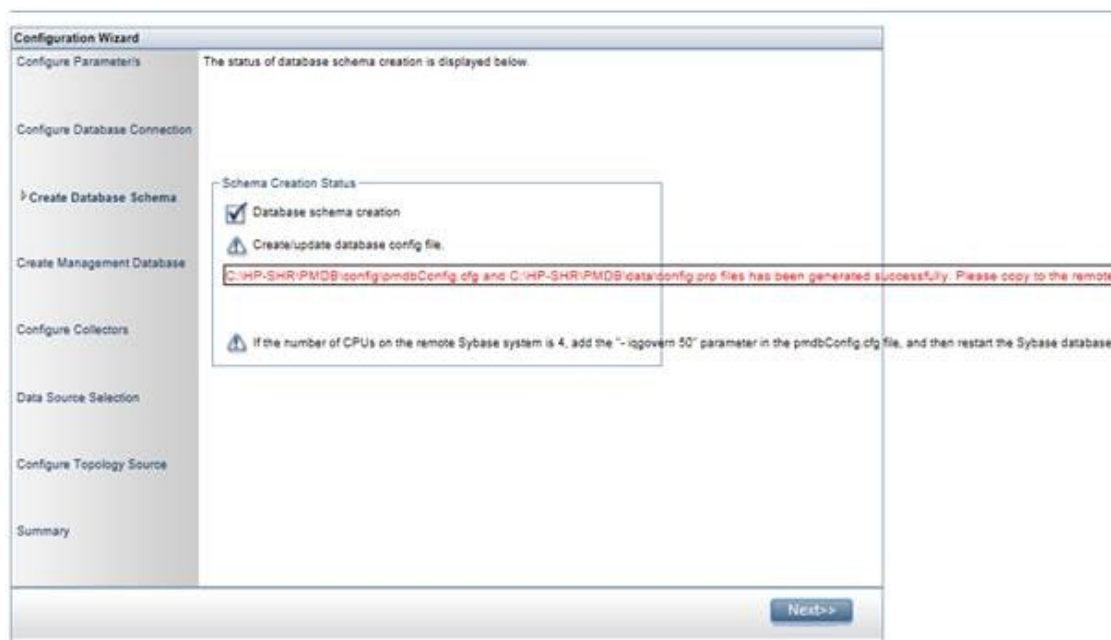
Внимание. Убедитесь, что ресурсов системы достаточно для обеспечения выбранного объема данных, собираемых SHR. См. информацию о требованиях к ресурсам для выбранного объема в *матрице поддержки HP Service Health Reporter*.

3. Нажмите кнопку **Далее**. Откроется диалоговое окно подтверждения.



Проверьте наличие папки с базой данных на удаленном компьютере.

4. Нажмите **Yes**. Если подключение к базе данных установлено успешно и создана схема, то откроется страница подтверждения со статусом создания схемы.



Скопируйте созданный файл `pmdbConfig.cfg` и файл `config.prpv` в удаленную систему и перезапустите базу данных. Чтобы скопировать файлы в удаленную систему, следуйте инструкциям в мастере настройки.

Примечание. Если SHR и SAP BusinessObjects установлены в ОС Windows, и приложение SAP Sybase IQ установлено в Linux, выполните следующие команды в консоли командной строки в системе Sybase IQ после создания схемы базы данных Sybase:

- dos2unix \$PMDB_HOME/data/config.prp
- dos2unix \$IQDIR15/scripts/pmdbConfig.cfg

5. В системах с 4 или менее ЦП выполните следующие действия:
- a. Войдите в систему, в которой установлено приложение Sybase.
 - b. Откройте следующий файл в текстовом редакторе.

В Windows:

```
%PMDB_HOME%\config\pmdbConfig.cfg
```

В Linux:

```
$PMDB_HOME/config/pmdbConfig.cfg
```

- c. Добавьте следующую строку в конец файла.

```
-iqgovern 50
```

- d. Перезапустите службу HP_PMDB_Platform_Sybase.

6. Для продолжения нажмите кнопку **Далее**.

Примечание. Если не удалось установить подключение к базе данных и создать схему, нажмите кнопку **Назад**, чтобы проверить указанные значения.

Проверка создания схемы удаленной базы данных Sybase

Вы должны проверить следующее после успешного создания схемы базы данных Sybase:

- Убедитесь, что база данных Sybase IQ создана.

Убедитесь, что следующие файлы присутствуют в папке базы данных (указанной в поле «Расположение файла базы данных»).

- pmdb.db
- pmdb.iq
- pmdb.iqmsg
- pmdb.iqtmp
- pmdb.lmp

- `pmdb.log`
- `pmdb_user_main01.iq`
- Убедитесь, что база данных Sybase IQ запущена.
 - Windows: Убедитесь, что на вкладке **Процессы** в **Диспетчере задач** отображается процесс `IQSRV15.exe`.
 - Linux: Выполните команду `ps -ef|grep iqsrv15` и убедитесь, что возвращается значение `<process_id>`.
- Проверьте подключение к серверу Sybase IQ.
 - Windows:
 - В системе SHR выберите **Пуск > Выполнить**. Откроется диалоговое окно «Выполнить».
 - Введите `dbisql` в поле «Открыть» и нажмите клавишу **ВВОД**. Откроется диалоговое окно **Connect** программы Interactive SQL.
 - Введите следующее:
 - В поле User ID введите `pmdb_admin`
 - В поле «Password» введите пароль, указанный при создании базы данных Sybase IQ после установки.
 - В поле **Action** выберите **Connect to a running database on this computer** в раскрывающемся списке.
 - В поле Server Name введите имя сервера, на котором установлена база данных SHR SybaseIQ.

Совет. Имя сервера можно найти в файле `pmdbConfig.cfg`. Откройте файл, имя сервера — это текст после `-n`.

- Linux: Выполните следующую команду:

```
dbisql -nogui -c "uid=dba;pwd=sql;dbn=utility_db;eng=<server_name>;commlinks=tcip(host=<host_name>;port=21424)"
```

Пример

```
dbisql -nogui -c "uid=dba;pwd=sql;dbn=utility_db;eng=abc;commlinks=tcip(host=abc.com;port=21424)"
```

Задача 4. Создайте учетную запись пользователя для базы данных управления

Базой данных управления называется хранилище оперативной обработки транзакций (OLTP), используемое SHR для хранения данных времени выполнения, таких как статус потока заданий по обработке данных, статус измененных таблиц и сведения об источниках данных.

На странице «Создание базы данных управления» введите сведения о пользователе для базы данных управления.

Чтобы создать учетную запись пользователя для базы данных управления, выполните следующие действия.

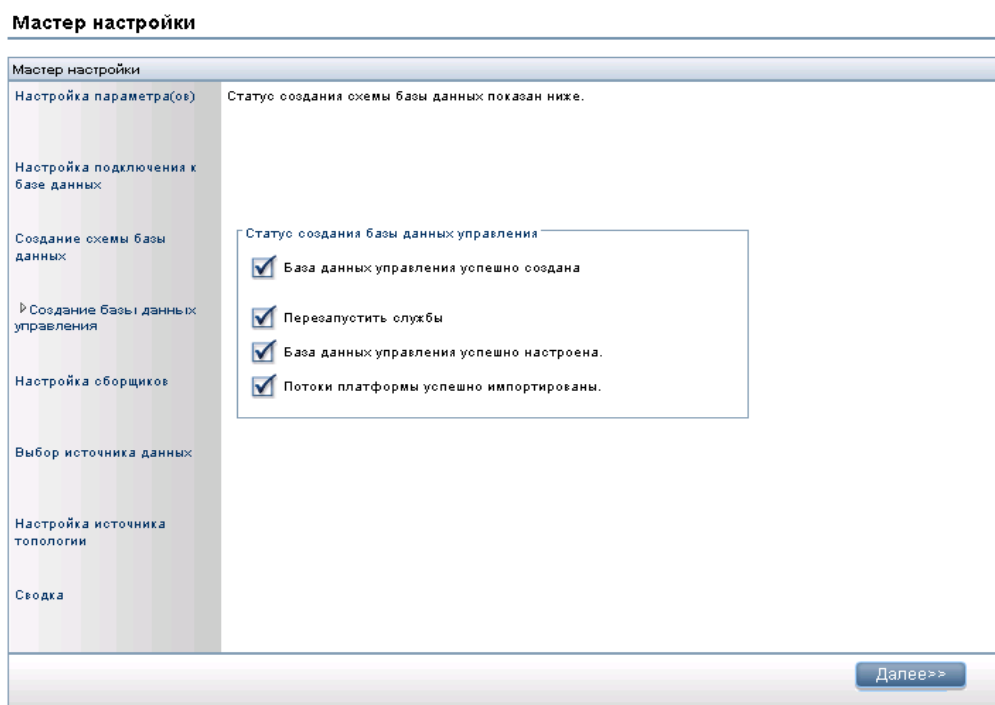
1. В разделе «Введите пользователя базы данных управления (с правами DBA) и пароль» введите следующие значения:

Поле	Описание
Имя пользователя	Имя администратора базы данных PostgreSQL. По умолчанию используется имя <i>postgres</i> .
Пароль	Пароль администратора базы данных PostgreSQL. Значение по умолчанию: <i>PMDB92_admin@hp</i> .

2. Чтобы изменить пароль для пользователя БД управления, введите в разделе «Введите сведения о пользователе базы данных управления HP SH Reporter» следующие значения:

Поле	Описание
Имя пользователя	Имя для пользователя базы данных управления. По умолчанию используется имя <i>pmdb_admin</i> .
Новый пароль	Пароль для пользователя базы данных управления.
Подтверждение нового пароля	Снова введите тот же пароль для подтверждения.

3. Нажмите кнопку **Далее**. Откроется страница «Статус создания базы данных управления».
4. Ознакомьтесь с задачами, выполненными в рамках подключения к базе данных, и сведениями о базе данных управления и нажмите кнопку **Далее**. Откроется страница настройки сборщиков.



Задача 5. Настройте сборщики, установленные в удаленных системах

Перед настройкой сборщика необходимо выполнить следующую команду на удаленной системе:

В Windows:

```
"perl %PMDb_HOME%\bin\scripts\configurePoller.pl <полное доменное имя системы SHR>"
```

В Linux:

```
"perl $PMDb_HOME/bin/scripts/configurePoller.pl <полное доменное имя системы SHR>"
```

Примечание. Эта команда выполняет обмен сертификатами между системой SHR и системой сборщика, в результате чего между SHR и сборщиком устанавливается канал связи. Один экземпляр сборщика может использовать только один экземпляр SHR. Настройка нескольких экземпляров SHR для одного сборщика не поддерживается.

На странице настройки сборщика можно создать новый сборщик, удалить существующий сборщик и привязать приложение к существующим сборщикам.

1. На странице настройки сборщика нажмите **Создать**.

Откроется раздел параметров конфигурации, в котором следует ввести следующие значения:

Поле	Описание
Name	Имя сборщика, установленного в удаленной системе. Имя не может содержать следующие специальные знаки:
Имя хоста	Имя хоста сборщика
HTTP/HTTPS	Сделайте выбор в зависимости от используемого протокола.

2. Нажмите **ОК**, чтобы завершить создание сборщика, а затем кнопку **Сохранить**.
3. Нажмите кнопку **Проверить подключение**, чтобы проверить статус подключения.

Если отчет о статусе содержит сообщение «Проверка подключения - неудача», выполните следующие действия:

- a. Выполните вход в систему сборщика.
- b. Убедитесь, что служба `HP_PMDB_Platform_Collection` запущена.

Если служба не запущена, запустите ее вручную.

- c. Чтобы запустить службу вручную:

В Windows:

- Откройте окно служб, щелкните службу `HP_PMDB_Platform_Collection` правой кнопкой и выберите **Запустить**.

В Linux:

- Перейдите в каталог `/etc/init.d` и выполните следующую команду:

```
service HP_PMDB_Platform_Collection start
```

Задача 6: Выберите источник данных

На странице выбора источника данных укажите сценарий развертывания, для которого выбраны источники данных и другие параметры. В следующей таблице перечислены области, которые можно отслеживать в каждом сценарии развертывания.

Сценарий развертывания	Области мониторинга
BSM 9.2x	<ul style="list-style-type: none"> • Мониторинг системы • Virtual Environment Performance • Network Performance • События операций и ключевой индикатор производительности • HP End User Monitoring • Производительность корпоративных приложений
OMi 10	<ul style="list-style-type: none"> • Мониторинг системы • Virtual Environment Performance • Network Performance • События операций и ключевой индикатор производительности • Производительность корпоративных приложений
HPOM	<ul style="list-style-type: none"> • Мониторинг системы • Virtual Environment Performance • Network Performance • Событие операций • Производительность корпоративных приложений
Только VMware vCenter	<ul style="list-style-type: none"> • Virtual Environment Performance • Network Performance
Другое	Network Performance

Источники данных для сценария BSM или OMi

Необходимо настроить следующие сборщики данных в SHR.

- Сборщик данных для сбора хронологических данных мониторинга искусственных транзакций (BPM) и мониторинга реальных пользователей (RUM) из базы данных профилей и базы данных управления. Он также собирает события, сообщения, данные о доступности и ключевые индикаторы производительности из баз данных источников данных, таких как

база данных профилей, база данных управления, базы данных HPOM и HP OMi.

- Сборщик агента HP Operations Agent для сбора метрик производительности системы и данных, относящихся к приложениям, базам данных и ресурсам системы. Данные собираются агентами HP Operations Agent, которые установлены на управляемых узлах.

Выполните следующие действия.

1. В разделе **Сценарий развертывания** выберите **BSM/OMi**.
2. В разделе **Версия BSM/OMi** выберите версию приложения.
3. В разделе **Производительность системы** выберите источник данных для системы.
 - a. Если вы выберете SiteScope для производительности системы, появится раздел **Канал метрик SiteScope**.
 - b. Вы должны выбрать базу данных профилей или API для прямого доступа в качестве канала метрик для SiteScope.

Примечание. Если SiteScope используется для мониторинга производительности системы или виртуальной среды в OMi 10.x, канал метрики для SiteScope направляется через API для прямого доступа.

4. *(Необязательно)*. В разделе **Virtual Environment Performance** выберите источник данных для виртуальной среды. Выберите технологию для источника данных.

Источник данных	Выберите технологию
HP Operations Agent	VMware IBM LPAR Microsoft Hyper-V Solaris Zones
SiteScope	VMware Примечание. Для производительности виртуальной среды необходимо также выбрать канал метрик. При использовании OMi 10.x данные для SiteScope можно собирать только через API прямого доступа.
VMware vCenter	VMware

5. *(Необязательно)*. В разделе **Производительность сети** выберите **NNMi, интегрированный с BSM/OMi**, если компоненты NNMi и NNMi SPI Performance доступны в среде.
6. В разделе **События операций и ключевой индикатор производительности** выберите источники данных для необходимых событий.
7. В разделе **HP End User Monitoring** выберите источник данных для компонентов, отслеживаемых BSM.

Примечание. В случае развертывания для OMi 10.x этот параметр отключен.

8. В разделе **Производительность корпоративных приложений** выберите источник данных для пакетов управления, отслеживаемых OMi.
9. Раздел **Выберите технологию** открывается после выбора необходимого пакета управления, установите флажок **Пакет управления**.

Примечание. Если вы выберете пакет управления Microsoft Exchange Server, откроется раздел **Выберите версию MS Exchange Server**. Кроме того, выберите версию Exchange Server.

10. Нажмите кнопку **Сохранить**. Откроется сводка выбранных элементов.
11. Нажмите кнопку **Далее**. Откроется страница «Настройка источника топологии».

Источники данных для сценария развертывания HPOM

Выполните следующие действия.

1. В разделе **Сценарий развертывания** выберите **HPOM**.
2. В разделе **Производительность системы** выберите **HP Operations Agent**.
3. *(Необязательно)*. В разделе **Производительность виртуальной среды** выберите источник данных для виртуальной среды.
4. *(Необязательно)*. В разделе **Производительность сети** выберите **NNMi, интегрированный с BSM/OMi**, если компоненты NNMi и NNMi SPI Performance доступны в среде.
5. В разделе **Событие операций** выберите **События HPOM** для событий.
6. В разделе **Производительность корпоративных приложений** выберите источники данных для интеллектуального подключаемого модуля, отслеживаемого HPOM.

Примечание. Если вы выберете Microsoft Exchange Server, откроется раздел **Выберите версию MS Exchange Server**. Выберите версию Exchange Server.

7. Нажмите кнопку **Сохранить**. Откроется сводка выбранных элементов.
8. Нажмите кнопку **Далее**. Откроется страница «Настройка источника топологии».

Источник данных VMware vCenter

Для сбора данных выполните следующие действия:

1. В разделе «Сценарий развертывания» выберите **Только VMware vCenter**.
2. В разделе «Производительность виртуальной среды» выберите **VMware**.
3. *(Необязательно)*. В разделе «Производительность сети» выберите **Производительность сети**, если компоненты NNMi и NNMi SPI Performance доступны в среде.
4. Нажмите кнопку **Сохранить**. Появится следующее сообщение: Сохранение выполнено.
5. Нажмите кнопку **Далее**. Открывается страница «Настройка источника топологии».

Задача 7. Настройка источника топологии

Перед настройкой SHR для сбора данных необходимо настроить источник топологии. Задачи по настройке источника топологии подразделяются на следующие категории.

- Если приложение SHR развернуто в среде BSM Service and Operations Bridge или Application Performance Management, см. раздел ["Настройка источника определения службы RTSM" ниже](#).
- Если приложение SHR развернуто в среде HPOM, см. раздел ["Настройка источника определения службы HPOM" на странице 54](#).
- Если приложение SHR развернуто в среде VMware vCenter, см. раздел ["Настройка определения службы vCenter" на странице 56](#).

Примечание. После настройки источника топологии (RTSM, HPOM или VMware vCenter) вы не сможете изменить его.

Настройка источника определения службы RTSM

На странице «Настройка источника топологии»:

1. В разделе **Источник определения службы** щелкните **RTSM**.
2. Нажмите кнопку **Создать**. Откроется диалоговое окно «Параметр подключения».
3. В разделе «Параметр подключения» введите следующие значения:

Поле	Описание
Имя хоста	IP-адрес или полное доменное имя сервера BSM или OMi. Для распределенной установки HP BSM введите имя сервера шлюза в это поле.
Порт	Номер порта для запроса веб-службы RTSM. По умолчанию используется порт 80. Если номер порта изменился, обратитесь к администратору BSM.
Имя пользователя	Имя пользователя веб-службы RTSM. По умолчанию используется имя пользователя admin.
Пароль	Пароль пользователя веб-службы RTSM. По умолчанию используется пароль admin.
Станция сбора данных	Если вы установили сборщики данных на удаленных системах, вы можете выбрать локальный сборщик или удаленный сборщик. Чтобы настроить удаленный сборщик с помощью этого источника определения службы, выберите одну из доступных удаленных систем в раскрывающемся списке. Чтобы использовать сборщик, установленный в системе SHR по умолчанию, выберите локальный сборщик.

4. Нажмите кнопку **ОК**.
5. Нажмите кнопку **Сохранить**, чтобы сохранить добавленную информацию.
6. Нажмите кнопку **Проверить подключение**.
7. В окне подтверждения нажмите кнопку **Да**. На панели информационных сообщений появится сообщение **Сохранение выполнено**.

Можно настроить дополнительные источники данных HPOM, выполнив шаги 2–7.

См. дополнительные сведения о настройке источников определения службы HPOM в разделе *Управление корпоративной топологией интерактивной справки HP Service Health Reporter для администраторов*.

8. Для продолжения нажмите кнопку **Далее**. Откроется сводная страница.
9. Нажмите кнопку **Готово**, чтобы завершить задачи настройки после установки. Откроется страница «Диспетчер развертывания».

Настройка источника определения службы HPOM

На странице «Настройка источника топологии»:

1. В разделе **Источник определения службы** щелкните **HP OM**.
2. Нажмите кнопку **Создать**. Откроется диалоговое окно «Параметр подключения».
3. В разделе «Параметр подключения» введите следующие значения:

Внимание. Если для подключения к серверу базы данных HPOM используется метод проверки подлинности в базе данных, то здесь необходимо указать данные пользователя, имеющего разрешения SELECT и CONNECT для базы данных openview.

Поле	Описание
Тип источника данных	Выберите версию HPOM, настроенную в вашей среде. Возможные варианты: HPOM для Windows. HPOM для Unix; HPOM для Linux; HPOM для Solaris.
Тип базы данных	Тип базы данных выбирается автоматически в зависимости от выбранного типа источника данных. Типу источника данных HPOM для Windows соответствует тип базы данных MSSQL. Источникам HPOM для Unix, HPOM для Linux и HPOM для Solaris соответствует тип базы данных Oracle.
Имя хоста	IP-адрес или полное доменное имя сервера BSM или OMi. Для распределенной установки HP BSM введите имя сервера шлюза в это поле.

Поле	Описание
Экземпляр базы данных	Системный идентификатор (SID) экземпляра базы данных в источнике данных. По умолчанию экземпляр базы данных имеет идентификатор OVOPS. Если приложение MSSQL Server настроено для использования экземпляра базы данных по умолчанию (неименованного), оставьте это поле пустым.
Порт	Номер порта для запроса сервера базы данных HPOM. Сведения о проверке номера порта для экземпляра базы данных (например, OVOPS) см. в разделе "Проверка номера порта сервера HPOM" на странице 34.
Проверка подлинности Windows	Параметр, включающий проверку подлинности Windows для доступа к базе данных HPOM. Пользователь может использовать для доступа к HPOM те же учетные данные, которые действуют в системе Windows, где размещается база данных. Этот параметр отображается только если выбран тип источника данных HPOM для Windows.
Имя пользователя	Имя пользователя базы данных HPOM. Если для типа источника данных HPOM для Windows выбран параметр проверки подлинности Windows, то это поле отключено и выводится пустым.
Пароль	Пароль пользователя базы данных HPOM. Если для типа источника данных HPOM для Windows выбран параметр проверки подлинности Windows, то это поле отключено и выводится пустым.
Станция сбора данных	Если вы установили сборщики данных на удаленных системах, вы можете выбрать локальный сборщик или удаленный сборщик. Чтобы настроить удаленный сборщик с помощью этого источника определения службы, выберите одну из доступных удаленных систем в раскрывающемся списке. Чтобы использовать сборщик, установленный в системе SHR по умолчанию, выберите локальный сборщик.

4. Нажмите кнопку **ОК**.
5. Нажмите кнопку **Сохранить**, чтобы сохранить добавленную информацию.
6. Нажмите кнопку **Проверить подключение**.

7. В окне подтверждения нажмите кнопку **Да**. На панели информационных сообщений появится сообщение **Сохранение выполнено**.

Можно настроить дополнительные источники данных НРОМ, выполнив шаги 2–7.

См. дополнительные сведения о настройке источников определения службы НРОМ в разделе *Управление корпоративной топологией интерактивной справки HP Service Health Reporter для администраторов*.

Примечание. Чтобы собирать данные с хостов, не входящих в домен, администратор НРОМ должен выполнить разрешение DNS для этих хостов, чтобы они были доступны для SHR, установленного в домене.

8. Для продолжения нажмите кнопку **Далее**. Откроется сводная страница.
9. Нажмите кнопку **Готово**, чтобы завершить задачи настройки после установки. Откроется страница «Диспетчер развертывания».

Настройка определения службы vCenter

На странице «Настройка источника топологии»:

1. В разделе **Источник определения службы** щелкните **VMware vCenter**.
2. Нажмите кнопку **Создать**. Откроется диалоговое окно «Параметр подключения».
3. В разделе «Параметр подключения» введите следующие значения:

Поле	Описание
Имя хоста	IP-адрес или полное доменное имя сервера vCenter.
Имя пользователя	Имя пользователя веб-службы vCenter. administration@vsphere.local — это имя пользователя по умолчанию.
Пароль	Пароль пользователя веб-службы vCenter.

Поле	Описание
Станция сбора данных	<p>Если вы установили сборщики данных на удаленных системах, вы можете выбрать локальный сборщик или удаленный сборщик.</p> <p>Чтобы настроить удаленный сборщик с помощью этого источника определения службы, выберите одну из доступных удаленных систем в раскрывающемся списке.</p> <p>Чтобы использовать сборщик, установленный в системе SHR по умолчанию, выберите локальный сборщик.</p>

4. Нажмите кнопку **ОК**.
5. Нажмите кнопку **Сохранить**, чтобы сохранить добавленную информацию.
6. Нажмите кнопку **Проверить подключение**.
7. В окне подтверждения нажмите кнопку **Да**. На панели информационных сообщений появится сообщение **Сохранение выполнено**.

Можно настроить дополнительные источники данных vCenter, выполнив шаги 2–7.

8. Для продолжения нажмите кнопку **Далее**. Откроется сводная страница.
9. Нажмите кнопку **Готово**, чтобы завершить задачи настройки после установки. Откроется страница «Диспетчер развертывания».

Если вы настроили удаленный сборщик с помощью определения службы, обязательно перезапустите службу сборщика на системе сборщика после установки пакетов содержимого.

Для перезапуска службы вручную выполните следующие действия:

В Windows:

- Откройте окно служб, щелкните службу HP_PMDB_Platform_Collection правой кнопкой и выберите **Запустить**.

В Linux:

- Перейдите в каталог `/etc/init.d` и выполните следующую команду:

```
service HP_PMDB_Platform_Collection --full-restart
```

Задача 8. сетевого устройства

Страница сводки содержит сводку всех разделов.

Глава 4: Настройка источника данных

Перед установкой пакетов содержимого необходимо настроить SHR на подключение к источникам данных.

Настройка источника данных баз данных управления и профилей

В среде HP BSM можно установить несколько баз данных профилей для масштабирования, поскольку одной базы данных может оказаться недостаточно для хранения всех данных. Кроме того, могут потребоваться разные базы данных профилей для хранения важных и прочих данных. Сведения о различных базах данных профилей, развернутых в среде, хранятся в базе данных управления.

Чтобы настроить подключения к нескольким базам данных профилей, нужно также настроить базу данных управления на странице BSM/OMi.

Чтобы настроить базы данных управления, выполните следующие действия.

1. В административной консоли выберите пункты **Конфигурация сбора данных > BSM/OMi > База данных управления**.
2. Нажмите кнопку **Создать**. Откроется диалоговое окно «Параметры подключения».
3. Введите следующие значения в диалоговом окне «Параметры подключения»:

Поле	Описание
Источник данных	Выбрать источник данных: BSM или OMi.
Имя хоста	IP-адрес или полное доменное имя сервера БД управления. Данное поле не отображается, если выбран параметр База данных в Oracle RAC .
Порт	Номер порта для запроса сервера БД управления. Данное поле не отображается, если выбран параметр База данных в Oracle RAC .
Тип базы данных	Тип СУБД, в которой создается база данных управления. Возможные значения: Oracle, MSSQL или PostgreSQL.

Поле	Описание
Проверка подлинности Windows	Если выбран тип базы данных MSSQL, то можно включить проверку подлинности Windows для MSSQL. В этом случае пользователь может использовать для доступа к SQL Server те же учетные данные, которые действуют в системе Windows, где размещается база данных.
Экземпляр базы данных	Системный идентификатор (SID) экземпляра БД управления. Данное поле не отображается, если выбран параметр База данных в Oracle RAC . Примечание. Чтобы узнать имя хоста, номер порта и идентификатор SID для базы данных, обратитесь к администратору <i>HP Business Service Management</i> .
Имя базы данных	Имя базы данных. Это поле отображается только если выбран тип базы данных MSSQL.
База данных в Oracle RAC	Этот параметр отображается, только если выбран тип базы данных Oracle.
Имя службы	Имя службы. Этот параметр отображается, только если выбран параметр База данных в Oracle RAC .
Имя ORA-файла	ORA-файл, который содержит сведения о подключении к Oracle Real Application Cluster. Этот параметр отображается, только если выбран параметр База данных в Oracle RAC .
Имя пользователя	Имя пользователя БД управления, которое указывается в мастере настройки BSM во время установки БД управления. Примечание. Если выбрана проверка подлинности Windows, то это поле отключено.
Пароль	Пароль пользователя БД управления, который указывается в мастере настройки BSM во время установки БД управления. Примечание. Если выбрана проверка подлинности Windows, то это поле отключено.

4. Нажмите кнопку **ОК**.
5. Нажмите кнопку **Проверить подключение**, чтобы проверить подключение.
6. Нажмите кнопку **Сохранить**, чтобы сохранить изменения, внесенные на этой странице. На панели информационных сообщений появится сообщение **Сохранение выполнено**.

Чтобы настроить базу данных профилей, выполните следующие действия.

1. В административной консоли выберите пункты **Конфигурация сбора данных > BSM/OMi > База данных профилей**.
2. Нажмите кнопку **Создать**. Откроется диалоговое окно «Параметры подключения».
3. Введите следующие значения в диалоговом окне «Параметры подключения»:

Поле	Описание
Имя хоста	IP-адрес или полное доменное имя сервера БД профилей. Данное поле не отображается, если выбран параметр База данных в Oracle RAC .
Порт	Номер порта для запроса сервера БД профилей. Данное поле не отображается, если выбран параметр База данных в Oracle RAC .
Тип базы данных	Тип СУБД, в которой создается база данных профилей. Возможные значения: Oracle, MSSQL или PostgreSQL.
База данных управления	Привязка базы данных профилей к базе данных управления. Если сбор данных осуществляется только с SiteScope, выбирать базу данных управления не требуется.
Домены	Выберите домены, для которых требуется собирать данные. Примечание. Необходимо выбрать домены, для которых требуется собирать данные. Если настройка топологий непосредственно после установки была пропущена, следует вернуться к ней сейчас для выбора доменов сбора данных. <ul style="list-style-type: none">■ HP Operations Manager;■ OMi■ RUM■ BPM■ Service Health

Поле	Описание
Экземпляр базы данных	Системный идентификатор (SID) экземпляра БД профилей. Данное поле не отображается, если выбран параметр База данных в Oracle RAC . Примечание. Чтобы узнать имя хоста, номер порта и идентификатор SID для базы данных, обратитесь к администратору <i>HP Business Service Management</i> .
Проверка подлинности Windows	Если выбран тип базы данных MSSQL, то можно включить проверку подлинности Windows для MSSQL. В этом случае пользователь может использовать для доступа к SQL Server те же учетные данные, которые действуют в системе Windows, где размещается база данных.
Имя базы данных	Имя базы данных. Это поле отображается только если выбран тип базы данных MSSQL.
База данных в Oracle RAC	Этот параметр отображается, только если выбран тип базы данных Oracle.
Имя службы	Имя службы. Этот параметр отображается, только если выбран параметр База данных в Oracle RAC .
Имя ORA-файла	ORA-файл, который содержит сведения о подключении к Oracle Real Application Cluster. Этот параметр отображается, только если выбран параметр База данных в Oracle RAC .
Имя пользователя	Имя пользователя БД профилей, которое указывается в мастере настройки BSM во время установки БД профилей. Примечание. Если выбрана проверка подлинности Windows, то это поле отключено.
Пароль	Пароль пользователя БД профилей, которое указывается в мастере настройки BSM во время установки БД профилей. Примечание. Если выбрана проверка подлинности Windows, то это поле отключено.
Станция сбора данных	Этот параметр используется для сборщика, установленного в удаленной системе.

4. Нажмите кнопку **ОК**.
5. Нажмите кнопку **Проверить подключение**, чтобы проверить подключение.
6. Нажмите кнопку **Сохранить**, чтобы сохранить изменения, внесенные на этой странице. На панели информационных сообщений появится сообщение **Сохранение выполнено**.

После сохранения созданного подключения к базе данных управления SHR (локальный или удаленный сборщик) получает сведения о базе данных профилей из источника данных БД управления и выводит все существующие источники данных БД профилей в разделе «База данных профилей» на странице.

Для источника данных БД профилей по умолчанию включен сбор данных. Кроме того, задается периодичность сбора данных каждый час.

При использовании удаленного сборщика необходимо выбрать станцию сбора данных в раскрывающемся списке «Тип базы данных» в разделе «База данных профилей» на этой странице.

См. дополнительные сведения о настройке подключений к источнику данных БД профилей в разделе «Управление сбором данных БД управления / БД профилей» *интерактивной справки Service Health Reporter для администраторов*.

Включение сбора данных ключевых индикаторов производительности для ЭК работоспособности служб

Ключевые индикаторы производительности отражают производительность и доступность ЭК на высоком уровне. Данные ключевых индикаторов производительности, принадлежащие определенным логическим ЭК работоспособности служб, таким как бизнес-служба, бизнес-приложение, бизнес-процесс и хост, по умолчанию заносятся в базу данных профилей. SHR собирает эти данные в базе для составления отчетов.

Однако данные ключевых индикаторов производительности для других типов ЭК не заносятся в базу данных профилей автоматически. Чтобы включить регистрацию данных ключевых индикаторов производительности для этих типов ЭК, необходимо настроить эти ЭК в HP BSM. Дополнительные сведения см. в разделе *Постоянные данные и хронологические данные руководства HP Business Service Management - использование приложения «Работоспособность служб»*. Это руководство доступно по следующему URL-адресу для продукта *Application Performance Management (BAC)*:

<http://h20230.www2.hp.com/selfsolve/manuals>

Настройка источника данных HP OMi

Если установлен пакет содержимого HP OMi, необходимо настроить подключение к базе данных HP OMi для сбора данных.

Перед созданием нового подключения к источнику данных HP OMi убедитесь, что на странице «БД управления/БД профилей» существует подключение к источнику данных для базы данных управления. Это подключение необходимо для извлечения данных о назначенном пользователе/группе для HP OMi, которые хранятся в базе данных управления.

Если в среде установлен один или несколько экземпляров OMi, то необходимо настроить источник данных OMi, принадлежащий модели HP BSM RTSM, которая была настроена в качестве источника топологии.

Чтобы настроить подключения к источнику данных HP OMi, выполните следующие действия.

1. В административной консоли выберите пункты **Конфигурация сбора данных > BSM/OMi > OMi**.
2. Нажмите кнопку **Создать**, чтобы создать подключение к источнику данных HP OMi. Откроется диалоговое окно «Параметры подключения».
3. Выберите или введите следующие значения в диалоговом окне **Параметры подключения**:

Имя хоста	IP-адрес или полное доменное имя сервера базы данных HP OMi.
Порт	Номер порта для запроса сервера базы данных HP OMi.
Экземпляр базы данных	Системный идентификатор (SID) экземпляра базы данных HP OMi. Если приложение MSSQL Server настроено для использования экземпляра базы данных по умолчанию (неименованного), оставьте это поле пустым. Чтобы узнать имя хоста, номер порта и идентификатор SID для базы данных, обратитесь к администратору базы данных HP OMi.
Тип базы данных	Тип СУБД, в которой создается база данных HP OMi. Возможные значения: Oracle или MSSQL.
Проверка подлинности Windows	Если выбран тип базы данных MSSQL, то можно включить проверку подлинности Windows для MSSQL. В этом случае пользователь может использовать для доступа к SQL Server те же учетные данные, которые действуют в системе Windows, где размещается база данных.
Имя базы данных	Имя базы данных. Это поле отображается только если выбран тип базы данных MSSQL.
Имя пользователя	Имя пользователя базы данных HP OMi. Если выбрана проверка подлинности Windows, то это поле отключено и отображается пустым.
Пароль	Пароль пользователя базы данных HP OMi. Если выбрана проверка подлинности Windows, то это поле отключено и отображается пустым.
Станция сбора данных	Определяет, какой сборщик используется, — локальный или удаленный.

4. Нажмите кнопку **OK**.

Примечание. Можно создать только одно подключение к источнику данных HP OMi. После создания подключения кнопка «Создать» по умолчанию отключена. Убедитесь, что значения введены правильно.

5. Нажмите кнопку **Проверить подключение**, чтобы проверить подключение.
6. Нажмите кнопку **Сохранить**, чтобы сохранить изменения. На панели информационных сообщений появится сообщение Сохранение выполнено.
7. Чтобы изменить расписание сбора данных HP OMi для одного или нескольких хостов, в столбце «Периодичность расписания» укажите время сбора от 1 до 24 часов в поле «Ч».
8. Нажмите кнопку **Сохранить**, чтобы сохранить изменения. На панели информационных сообщений появится сообщение Сохранение выполнено.

Настройка источника данных HP Operations Manager

Если установлен пакет содержимого HP Operations Manager (HPOM) и создано подключение к источнику топологии для HPOM на странице «Определение службы», то на странице HP Operations Manager появляется то же подключение к источнику данных. Новое подключение создавать не нужно. Можно проверить существующее подключение и сохранить его.

Важно заметить, что при обновлении подключения к источнику данных на странице «Определение службы» сведения о подключениях на странице Operations Manager не обновляются.

Чтобы настроить подключение к базе данных, выполните следующие действия.

1. В административной консоли выберите пункты **Конфигурация сбора данных** -> **HP Operations Manager**. Откроется страница HP Operations Manager.
2. Установите флажок рядом с именем хоста и нажмите кнопку **Проверить подключение**, чтобы проверить подключение.
3. Нажмите кнопку **Сохранить**, чтобы сохранить изменения. На панели информационных сообщений появится сообщение Сохранение выполнено.

Можно настроить дополнительные источники данных HPOM, нажав кнопку «Создать». Чтобы изменить определенное подключение к источнику данных, нажмите кнопку **Настроить**.

4. Чтобы изменить расписание сбора данных HPOM для одного или нескольких хостов, в столбце **Периодичность расписания** укажите время сбора от 1 до 24 часов в поле Ч.
5. Нажмите кнопку **Сохранить**, чтобы сохранить изменения. На панели информационных сообщений появится сообщение Сохранение выполнено.

Настройка источника данных для агента HP Operations Agent

В сценарии развертывания RTSM не нужно создавать новые подключения к источнику данных агента HP Operations Agent, поскольку по умолчанию все узлы, на которых устанавливается агент HP Operations Agent, автоматически обнаруживаются при сборе сведений о топологии. Эти источники данных или узлы агентов HP Performance Agent указываются на странице «Источники данных РА» административной консоли.

Чтобы просмотреть список источников данных агентов HP Operations Agent, выполните следующие действия.

1. В административной консоли выберите пункты **Конфигурация сбора данных >- HP Operations Manager**. Откроется страница «Источник данных HP Operations Agent».
2. Чтобы просмотреть подробные сведения об источниках данных агентов HP Operations Agent, щелкните имя представления или число в сводной таблице источников данных HP Operations Agent. Откроется таблица сведений об источнике данных HP Operations Agent.
3. Чтобы изменить расписание сбора данных для одного или нескольких хостов, укажите в столбце **Периодичность опроса** время опроса от 1 до 24 часов в поле **Ч**.
4. Нажмите кнопку **Сохранить**, чтобы сохранить изменения. На панели информационных сообщений появится сообщение Сохранение выполнено.

См. дополнительные сведения о настройке подключений к источнику данных агента HP Operations Agent в *интерактивной справке Service Health Reporter для администраторов*.

Настройка источника данных сети (с помощью универсальной базы данных)

Если установлен пакет содержимого Network, то необходимо настроить SHR (локальный сборщик данных) или удаленный сборщик данных для сбора данных о сети в NNMI. NNMI использует NPS в качестве репозитория для данных о производительности сети. На странице «Универсальная база данных» административной консоли можно настроить SHR для сбора необходимых данных в NPS. На этой странице также можно настроить подключения к универсальным базам данных, использующим СУБД Sybase, Oracle или SQL Server.

Чтобы настроить подключение к источнику данных NPS, выполните следующие действия.

1. В административной консоли выберите пункты **Конфигурация сбора данных >Универсальная база данных**. Откроется страница «Универсальная база данных».
2. Нажмите кнопку **Создать**, чтобы создать подключение к источнику данных NPS. Откроется диалоговое окно «Параметры подключения».

3. Выберите или введите следующие значения в диалоговом окне **Параметры подключения**:

Имя хоста	IP-адрес или полное доменное имя сервера базы данных NPS.
Порт	Номер порта для запроса сервера базы данных NPS.
Часовой пояс	Часовой пояс, настраиваемый в экземпляре базы данных.
Тип базы данных	Тип СУБД, в которой создается база данных NPS.
Домен	Выберите сферы деятельности, о которых SHR будет собирать данные из базы данных выбранного типа.
URL-адрес	URL-адрес экземпляра базы данных.
Имя пользователя	Имя пользователя базы данных NPS.
Пароль	Пароль пользователя базы данных NPS.
Станция сбора данных	Определяет, какой сборщик используется, — локальный или удаленный.

Параметр **Сфера деятельности** появляется только после установки пакета содержимого NetworkPerf_ETL_PerfSPI9.10 или NetworkPerf_ETL_PerfSPI9.20. Версия пакета содержимого зависит от версии ПО **HP Network Node Manager iSPI Performance for Metrics**, установленного в вашей среде.

4. Нажмите кнопку **ОК**.
5. Нажмите кнопку **Проверить подключение**, чтобы проверить подключение.
6. Нажмите кнопку **Сохранить**, чтобы сохранить изменения. На панели информационных сообщений появится сообщение Сохранение выполнено.
7. Чтобы изменить расписание сбора данных HP OMi для одного или нескольких хостов, в столбце **Периодичность расписания** укажите время сбора от 1 до 24 часов в поле **Ч**.
8. Нажмите кнопку **Сохранить**, чтобы сохранить изменения. На панели информационных сообщений появится сообщение Сохранение выполнено.

Для всех создаваемых подключений к источнику данных сбор данных включается по умолчанию. См. дополнительные сведения о настройке подключений к источнику данных сети в *интерактивной справке Service Health Reporter для администраторов*.

Настройка источника данных VMware vCenter

VMware vCenter можно настроить в качестве источника сбора метрик виртуализации в сценарии развертывания HPOM.

Выполните следующие действия.

1. В административной консоли выберите пункты **Конфигурация сбора данных ->VMware vCenter**. Откроется страница «Источник данных VMware vCenter».
2. Нажмите кнопку **Создать**, чтобы проверить подключение. Откроется диалоговое окно «Параметры подключения».
3. Введите следующие значения в диалоговом окне «Параметры подключения»:

Имя хоста	IP-адрес или полное доменное имя сервера базы данных VMware vCenter.
Имя пользователя	Имя пользователя базы данных VMware vCenter.
Пароль	Пароль пользователя базы данных VMware vCenter.
Станция сбора данных	Определяет, какой сборщик используется, — локальный или удаленный.

Примечание. Если для сбора данных о топологии используется несколько источников данных VMware vCenter, повторите [шаг 2 на стр. 109](#) для каждого подключения к VMware vCenter, которое вы хотите создать.

4. Чтобы изменить расписание сбора данных VMware vCenter для одного или нескольких хостов, в столбце «Периодичность расписания» укажите время сбора от 5 до 60 минут в поле «Мин».
5. Нажмите кнопку **Сохранить**, чтобы сохранить изменения. На панели информационных сообщений появится сообщение Сохранение выполнено.
6. На сервере VMware vCenter предоставьте пользователю следующие разрешения:
 - Установите для разрешения datastore значение «Browse Datastore».
 - Установите для разрешения datastore значение «Low Level File Operations».
 - Установите для разрешения sessions значение «Validate session».
7. На сервере VMware vCenter установите уровень статистики:
 - a. В клиенте vSphere выберите пункты **Administration -> vCenter Server Settings**.
 - b. В окне vCenter Server Settings нажмите элемент **Statistics**. На странице Statistics Interval отображаются временной интервал, по прошествии которого будет сохраняться статистика vCenter Server, продолжительность сохранения статистики и уровень статистики.
 - c. Нажмите кнопку **Edit**.

- d. В окне Edit Statistics Interval выберите уровень статистики Statistics Interval из раскрывающегося списка. В окне Edit Statistics Interval отображается тип собираемых статистических данных, соответствующий выбранному уровню статистики. Необходимо установить уровень статистики не ниже 2.

Настройка источника данных SiteScope

На странице SiteScope можно настроить источник данных SiteScope, который собирает данные с нескольких мониторов SiteScope в среде. На этой странице можно включать и отключать сбор данных, добавлять и удалять подключение к источнику данных в зависимости от требований организации. Если база данных профиля выбрана в качестве канала для метрик в мастере настройки, вы должны создать сборщик для источника данных SiteScope.

Чтобы создать новое подключение к источнику данных SiteScope:

1. В административной консоли выберите пункты **Конфигурация сбора данных > SiteScope**. Откроется страница SiteScope.
2. Нажмите кнопку **Создать**. Откроется диалоговое окно «Параметры подключения».
3. Введите следующие значения в диалоговом окне «Параметры подключения»:

Поле	Описание
Параметры подключения	
Имя хоста	IP-адрес или полное доменное имя сервера SiteScope.
Порт	Номер порта для запроса сервера SiteScope
Использовать SSL	<i>(Необязательно.)</i> Если выбран этот параметр, необходимо также включить на сервере SiteScope поддержку связи по протоколу SSL.
Имя пользователя	Имя пользователя SiteScope.
Пароль	Пароль пользователя SiteScope.
Строка инициализации	Общий ключ, используемый для установки подключения к серверу SiteScope.
Станция сбора данных	Этот параметр используется для сборщика, установленного в удаленной системе.

Поле	Описание
<p>Общие параметры интеграции данных Эти параметры обеспечивают интеграцию общих данных между сервером SiteScore и сервером SHR. После успешной установки подключения сервера SiteScore отправляют данные на сервер SHR.</p> <p>Кроме того, в SHR необходимо создать тег и применить его вручную к мониторам SiteScore, по которым требуется составлять отчеты. Подробнее о применении тега см. в документации по SiteScore.</p>	
Имя интеграции	<p>Укажите имя интеграции.</p> <p>Примечание. Заданное имя впоследствии нельзя изменить.</p>
Кодировка	Тип кодирования для связи между SHR и SiteScore.
Использовать SSL	<i>(Необязательно.)</i> Если выбран этот параметр, необходимо также включить на сервере SiteScore поддержку связи по протоколу SSL.
Интервал передачи данных (секунды)	Частота, с которой SiteScore отправляет данные в SHR. Это настраиваемый параметр.
Таймаут запроса (секунды)	Время, по истечении которого подключение прекращается. Если задан ноль (0), время ожидания не ограничено. Это настраиваемый параметр.
Таймаут подключения (секунды)	Время ожидания повторной установки подключения. Если задан ноль (0), время ожидания не используется. Это настраиваемый параметр.
Число повторных попыток	Число попыток подключения, предпринимаемых сервером SiteScore при ошибке подключения к SHR.
Проверка подлинности при необходимости	<i>(Необязательно.)</i> Если выбран этот параметр, при проверке подлинности используется имя пользователя и пароль веб-сервера.
Имя пользователя для проверки подлинности	Если в SHR настроено использование обычной проверки подлинности, укажите имя пользователя для доступа к серверу.
Пароль для проверки подлинности	Если в SHR настроено использование обычной проверки подлинности, укажите пароль для доступа к серверу.
Адрес прокси-сервера	Если на SiteScore включен прокси-сервер, укажите адрес прокси-сервера.

Поле	Описание
Имя пользователя прокси-сервера	Укажите имя пользователя для прокси-сервера.
Пароль прокси-сервера	Укажите пароль для прокси-сервера.
Создать тег	Выберите эту команду, если требуется создать тег для мониторов SiteScore, который необходимо применить с сервера SiteScore вручную.
Имя тега	Пользовательское имя тега.

4. Нажмите кнопку ОК.
5. Нажмем кнопку Save («Сохранить»).

На панели информационных сообщений появится сообщение Сохранение выполнено.

Для созданного подключения к источнику данных SiteScore по умолчанию включен сбор данных. Кроме того, задается периодичность сбора данных каждые 15 минут.

Глава 5: Установка пакетов содержимого

Для установки необходимых пакетов содержимого в SHR используется служебная программа «Диспетчер развертывания», доступная посредством административной консоли. Эта программа с веб-интерфейсом упрощает процедуру установки, структурируя пакеты содержимого по домену, по приложениям источников данных, из которых будут собираться данные, и по отдельным компонентам пакетов содержимого, которые будут устанавливаться для сбора данных.

Примечание. Остановите службу HP PMDB Platform Timer Service перед обновлением пакетов содержимого в рамках обновления SHR до последней версии. Если при обновлении пакетов содержимого возникнет сбой, будет выполнен откат к предыдущему состоянию.

Сохранение настроенных готовых отчетов не поддерживается; после обновления пакетов содержимого такие отчеты перезаписываются отчетами по умолчанию.

Создание отчетов путем изменения системы Universe для пакета содержимого также не поддерживается, и такие отчеты не будут работать после обновления пакета содержимого.

Перед началом работы

Прежде чем начинать установку пакетов содержимого проверьте следующее:

- Задачи настройки после установки и выбор источников данных выполнены.
- Задачи настройки сбора данных выполнены.

Проверьте источники данных

SHR позволяет проверить доступность и целостность источников данных перед установкой пакетов содержимого.

1. Откройте следующую страницу:

`http://<SHR Server FQDN>:<port>/BSMRApp/dscheck.jsf`

2. Чтобы проверить источники данных, связанные с RTSM, щелкните **RTSM**.

Щелкните **Просмотр** для просмотра результатов Результаты включают список отсутствующих обязательных типов и атрибутов ЭК.

3. Чтобы проверить источники данных, связанные с HP Operations Agent, щелкните **PA**.

Щелкните **Просмотр** для просмотра результатов Результаты включают сводку статуса узлов и отсутствующих политик.

Выбор компонентов пакетов содержимого

Пакет содержимого — это киоск данных, хранящий данные, собираемые из различных источников. Данные относятся к определенной области (производительность системы, производительность виртуальной среды и т.п.) и отвечают требованиям определенной группы пользователей для анализа, представления содержимого и удобства использования. Например, пакет содержимого System Performance предоставляет данные о доступности и производительности систем в ИТ-инфраструктуре. В пакеты содержимого также входит реляционная модель, которая определяет тип данных, собираемых для анализа заданного аспекта, и набор отчетов для отображения собранных данных.

Структура пакетов содержимого состоит из следующих уровней или компонентов.

- **Компонент «Сфера деятельности»:** В компоненте Domain или Core Domain определяется модель данных для каждого пакета содержимого. Он содержит правила для создания реляционной схемы, а также правил обработки данных, включая набор стандартных правил предварительной агрегации, для обработки данных в базе данных. Компонент Domain может включать часто используемые измерения и кубы, которые могут использоваться в компонентах пакета содержимого Report. Компонент пакета содержимого Domain не зависит от настроенного источника топологии и от источника данных, из которого собираются данные.
- **Компонент ETL («Извлечение, преобразование и загрузка»).** В компоненте пакета содержимого ETL определяются политики сбора данных и правила преобразования, выверки и промежуточного хранения. Также включены правила обработки данных, которые определяют порядок выполнения действий по обработке данных.
- Компонент пакета содержимого ETL зависит от источника данных. Поэтому в каждой области анализа для каждого приложения источника данных используется отдельный компонент ETL пакета содержимого. Например, для сбора данных о производительности системы из агента HP Operations Agent необходимо установить компонент SysPerf_ETL_PerformanceAgent. Для сбора данных о производительности системы из HP SiteScope необходимо установить компонент SysPerf_ETL_SiS (получающий данные, записанные в CODA) или SysPerf_ETL_SiS_DB (получающий данные, записанные в базу данных профилей BSM).
- С одним приложением источника данных могут работать несколько компонентов ETL. Например, можно использовать отдельный компонент ETL для каждой технологии виртуализации, поддерживаемой в агенте Performance Agent (зоны Oracle Solaris, VMware, IBM LPAR и Microsoft HyperV). Компонент ETL может зависеть от одного или нескольких компонентов Domain. Кроме того, несколько компонентов ETL могут передавать данные в один компонент Domain.
- **Компонент «Отчеты»:** В компоненте пакета содержимого Report определяются зависящие от приложения правила агрегирования, бизнес-представления, системы SAP BOBJ Universe и отчеты для заданного домена. Компоненты Report могут зависеть от одного или нескольких компонентов Domain. Этот компонент обеспечивает гибкие возможности расширения модели данных, определенной в одном или нескольких компонентах Domain.

Список компонентов пакетов содержимого, доступных для установки, зависит от источника топологии, настроенного на этапе настройки после установки. После настройки источника топологии диспетчер развертывания фильтрует список компонентов пакета содержимого, показывая только компоненты, которые можно установить в поддерживаемом сценарии развертывания. Например, если настроен источник топологии RTSM, то в диспетчере развертывания показываются только компоненты, которые можно устанавливать в сценариях развертывания SaOB и APM.

См. дополнительные сведения о каждом пакете содержимого и содержащихся в нем отчетах в *интерактивной справке Service Health Reporter для пользователей*.

Установка компонентов пакетов содержимого

Для установки компонента пакетов содержимого используется программа «Диспетчер развертывания».

Чтобы установить пакеты содержимого, выполните следующие действия.

1. Запустите административную консоль в веб-браузере.
 - a. Откройте следующий URL-адрес:

`http://<SHR_Server_FQDN>:21411`
 - b. Введите слово *administrator* в поле «Имя для входа» и нажмите кнопку **Войти**, чтобы продолжить. Откроется главная страница.

Примечание. Если для доступа к административной консоли используется другая учетная запись пользователя, убедитесь, что она имеет права администратора.

2. В левой части окна нажмите **Администрирование**, затем выберите пункт **Диспетчер развертывания**. Откроется диспетчер развертывания.

В диспетчере развертывания показываются компоненты пакета содержимого, которые могут устанавливаться в поддерживаемом сценарии развертывания. По умолчанию для установки выбираются все компоненты пакетов содержимого, соответствующие данному сценарию развертывания. Можно изменить выбор, сняв флажки для выбранного содержимого, приложения источника данных и компонентов пакета содержимого в списке. В приведенной ниже таблице указано содержимое, относящееся к каждому сценарию развертывания.

Список пакетов содержимого

Содержимое	BSM/OMi	HP Operations Manager;	Application Performance Management	VMware vCenter
Default	✓	✓	✓	✓
Cross-Domain Operations Events	✓			
Health and Key Performance Indicators	✓		✓	
IBM WebSphere Application Server	✓	✓		
Microsoft Active Directory	✓	✓		
Microsoft Exchange Server	✓	✓		
Microsoft SQL Server	✓	✓		
MSAppCore	✓	✓		
Network Performance ^a	✓	✓		
События операций	✓	✓		
Oracle	✓	✓		
Oracle WebLogic Server	✓	✓		
Real User Transaction Monitoring	✓		✓	

^aНеобходимо использовать содержимое NetworkPerf_ETL_PerfiSPI9.20_NonRTSM ETL в среде RTSM SHR, в которой Network Mode Manager i (NNMi) не интегрирован с BSM.

Содержимое	BSM/OMi	HP Operations Manager;	Application Performance Management	VMware vCenter
Synthetic Transaction Monitoring	✓		✓	
System Performance	✓	✓		✓
Virtual Environment Performance	✓	✓		✓

3. Нажмите **Установить/Обновить**.

Диспетчер развертывания начнет установку выбранных компонентов пакета содержимого.

Ход установки отображается в столбце «Статус». Страница «Диспетчер развертывания» автоматически обновляется, чтобы показать обновленный статус.

После завершения установки в столбце «Статус» для каждого компонента пакета содержимого появляется сообщение Успешная установка.

Примечание. Если запущены какие-либо потоки рабочих процессов, диспетчер развертывания выводит на экран следующее сообщение:

Все необходимые службы остановлены, но несколько заданий по-прежнему активны. Повторите попытку позже.

Если вы увидите на экране это сообщение, подождите, пока не будут завершены все потоки рабочих процессов.

После установки пакетов содержимого для просмотра подробного сопоставления отслеживаемых объектов со столбцами таблицы базы данных SHR выполните следующие действия:

1. Перейдите в следующий каталог на сервере SHR.

B Windows: %PMDB_HOME%\bin

B Linux: \$PMDB_HOME/bin

2. Выполните следующую команду:

shr_utility -flow -l <location>

В этом случае *<location>* — это локальный каталог в системе SHR.

Эта команда создает другие файлы .xls в *<location>* — по одному для каждого пакета содержимого. Каждый файл .xls описывает сопоставление отслеживаемых объектов со столбцами таблицы базы данных SHR для определенного пакета содержимого.

Часть II: Лицензирование

Глава 6: Лицензирование SHR

По умолчанию SHR включает временную лицензию Instant-on, которая действует в течение 60 дней. Чтобы продолжить использование SHR по истечении этого срока, необходимо установить бессрочную лицензию.

В лицензию на SHR входят следующие компоненты.

- **ПО HP Service Health Reporter**

Эта лицензия распространяется на платформу сбора данных, SAP BusinessObjects Enterprise, высокопроизводительную базу данных управления производительностью для хранения и обработки собранных метрик и готовые пакеты содержимого. Также предоставляется право на сбор метрик и составление отчетов по метрикам для 50 узлов.

- **Дополнительные пакеты масштабирования по 50 узлов**

Можно добавить дополнительные разрешения на сбор данных и составление отчетов для наращивания решения в соответствии с размером среды.

Для обработки лицензий SHR интегрируется с пакетом лицензирования диспетчера лицензий HP. Диспетчер лицензий HP предоставляет платформу лицензий SHR и возможности установки временной или бессрочной лицензии.

Получить бессрочную лицензию можно посредством диспетчера лицензий HP или непосредственно из HP Password Center на веб-сайте HP Webware.

Используемые лицензии (LTU)

[Таблица 1](#) содержит информацию обо всех лицензиях LTU, доступных для SHR.

Таблица 1. ^aИспользуемые лицензии (LTU)

LTU	Товарная позиция (SKU)	Описание
HP Service Health Reporter Standard Edition 50 Service Health Nodes SW E-LTU	TD905AAE	<p>Эта лицензия LTU включает в себя следующие пакеты содержимого:</p> <ul style="list-style-type: none"> • Пакет содержимого System Management и Virtualization • Пакеты содержимого SPI • Пакеты содержимого событий (OM, OMi) <p>В этой лицензии LTU отсутствуют пакеты содержимого BSM EUM и Network.</p>
HP Service Health Reporter Advanced 50 Service Health Nodes SW E-LTU	TJ756AAE	<p>Эта лицензия LTU предоставляет права на использование всех готовых пакетов содержимого, доступных в SHR.</p>
HP Service Health Reporter Upgrade from Standard to Advanced 50 Service Health Nodes SW E-LTU	TD906AAE	<p>Эта лицензия LTU предоставляет права на обновление SHR с версии Standard Edition до версии Advanced Edition.</p>
HP Service Health Reporter add 50 Nodes for Standard or Advanced Service Health Nodes SW E-LTU	TJ757AAE	<p>Это дополнительный пакет, добавляющий права на 50 дополнительных узлов SHR.</p>
Performance Insight to Service Health Reporter Advanced Core for Migration Software E-LTU	TJ773AAE	<p>Это пакет переноса для пользователей Performance Insight, позволяющий перейти на лицензию HP Service Health Reporter Advanced Core LTU (50 узлов).</p>

^aУзел представляет собой реальную или виртуальную компьютерную систему или устройство (например, принтер, маршрутизатор или мост) в сети.

Таблица 1. Узел представляет собой реальную или виртуальную компьютерную систему или устройство (например, принтер, маршрутизатор или мост) в сети.Используемые лицензии (LTU), continued

LTU	Товарная позиция (SKU)	Описание
Performance Insight to Service Health Reporter Advanced Migration 250 Service Health Software E-LTU	TJ774AAE	Это пакет переноса для пользователей Performance Insight, позволяющий перейти на лицензию HP Service Health Reporter Advanced 250 Nodes LTU.
Performance Insight to Service Health Reporter Advanced Migration 1000 Service Health Software E-LTU	TJ775AAE	Это пакет переноса для пользователей Performance Insight, позволяющий перейти на лицензию HP Service Health Reporter Advanced 1000 Nodes LTU.
Performance Insight to Service Health Reporter Advanced Migration 5000 Service Health Software E-LTU	TJ776AAE	Это пакет переноса для пользователей Performance Insight, позволяющий перейти на лицензию HP Service Health Reporter Advanced 5000 Nodes LTU.
Performance Insight to Service Health Reporter Advanced Migration Unlimited Service Health Software E-LTU	TJ777AAE	Это пакет переноса для пользователей Performance Insight, позволяющий перейти на лицензию HP Service Health Reporter Advanced Core LTU (неограниченное количество узлов).

Получение ключа бессрочной лицензии

Для получения ключа бессрочной лицензии выполните следующие действия.

1. Откройте административную консоль SHR по следующему URL-адресу:

`http://<имя сервера>:21411`

В данном случае `<имя_сервера>` — это полное доменное имя сервера, на котором установлена система SHR.

2. Выберите **Администрирование > Лицензирование**. Откроется страница службы выдачи лицензионных ключей HP.
3. Щелкните ссылку **Generate New licenses (Создать новые лицензии)** в разделе «Welcome (Приветствие)».
4. Выполните вход в службу HP Passport с ID пользователя и паролем. Если учетной записи в этой службе нет, то ее необходимо создать перед продолжением. Откроется страница Order Number (Номер заказа).
5. Введите номер заказа в поле Order number и нажмите кнопку **Next**. Откроется страница выбора продукта.
6. Выберите пункт **PERM** и нажмите кнопку **Next**. Откроется страница License redemption (Погашение лицензии).
7. Выберите вариант Find or create a license owner (Найти или создать владельца лицензии) и введите адрес электронной почты в поле License Owner e-mail address (Адрес электронной почты владельца лицензии).
8. Введите IP-адрес базовой системы SHR и нажмите кнопку **Next**. Откроется страница Create license owner (Создать владельца лицензии).

Примечание. Если SHR настраивается в высокодоступной кластерной среде, вы должны указать логический IP-адрес хоста SHR. Дополнительные сведения о высокодоступной конфигурации см. в документе *HP Service Health Reporter High Availability Guide*.

9. Введите сведения о владельце лицензии:

Поле	Описание
Create license owner (End-User) information (Сведения для создания владельца лицензии (конечного пользователя))	Имя, номер телефона и адрес электронной почты владельца лицензии.
Company e-mail domain (Домен электронной почты компании)	Имя домена для компании владельца лицензии.
Mailing address (Почтовый адрес)	Почтовый адрес владельца лицензии.

Поле	Описание
License owner privacy policy (Optional) (Политика конфиденциальности владельца лицензии, необязательно)	Необязательные параметры для политики конфиденциальности владельца лицензии.

10. Для продолжения нажмите кнопку **Далее**. Откроется страница Transaction summary (Сводка транзакции).
11. Проверьте данные и нажмите кнопку **Next**, чтобы продолжить. Откроется страница License certificate (Сертификат лицензии).
12. Проверьте данные в сертификате лицензии, сохраните лицензию в системе и закройте страницу License certificate (Сертификат лицензии).

Установка ключа бессрочной лицензии

Чтобы установить бессрчную лицензию, выполните следующие действия.

В Windows

1. Выполните вход в систему SHR от имени администратора.
2. Выберите пункт **Пуск > Программы > HP Software > Service Health Reporter > Диспетчер лицензий**. Откроется окно «Получение и установка ключа лицензии».
3. Выберите действие **Установить/восстановить ключ лицензии из файла**. Откроется страница «Установить/восстановить ключ лицензии из файла».
4. Перейдите к расположению, где сохранен сертификат лицензии, нажмите кнопку **Просмотреть содержимое файла**, выберите тип **PERM** и нажмите кнопку **Установить**.

В Linux

1. Выполните вход в систему SHR от имени пользователя root.

Примечание. При использовании клиентского приложения X для удаленного подключения к системе Linux не следует использовать режим BROADCAST, а также необходимо убедиться, что переменная среды DISPLAY в системе Linux настроена корректно.

2. Имя файла лицензии (сохраненного в ["Проверьте данные в сертификате лицензии, сохраните лицензию в системе и закройте страницу License certificate \(Сертификат](#)

лицензии)." **выши**) начинается с символа . (точка). Вы должны переименовать его, удалив точку.

3. Выполните следующую команду:

```
$PMDB_HOME/bin/LicenseManager.sh
```

Откроется окно «Получение и установка ключа лицензии».

4. Выберите действие **Установить/восстановить ключ лицензии из файла**. Откроется страница «Установить/восстановить ключ лицензии из файла».
5. Перейдите к расположению, где сохранен сертификат лицензии, нажмите кнопку **Просмотреть содержимое файла**, выберите тип **PERM** и нажмите кнопку **Установить**.

Повторная активация лицензии SAP BusinessObjects

Лицензия SAP BusinessObjects зависит от действия лицензии SHR. Когда истекает срок действия лицензии SHR, лицензия SAP BusinessObjects автоматически деактивируется, что приводит к отключению всех серверов SAP BusinessObjects. После продления лицензии SHR при обращении к административной консоли SHR автоматически повторно активирует лицензию SAP BusinessObjects. Однако серверы SAP BusinessObjects остаются в отключенном состоянии. Чтобы обеспечить работу SAP BusinessObjects, необходимо вручную включить серверы, выполнив следующие действия.

В Windows

1. Выполните вход в SHR от имени администратора.
2. Выберите **Пуск > Программы > BusinessObjects XI 3.1 > BusinessObjects Enterprise > Central Configuration Manager**. Откроется окно Central Configuration Manager.
3. В столбце Display Name выберите элемент **Server Intelligence Agent (HOML01GEATON)**.
4. На главной панели инструментов щелкните значок Manage Servers. Откроется диалоговое окно Log On.
5. В списке System выберите систему, в которой установлено приложение SAP BusinessObjects.
6. В полях User name и Password введите учетные данные пользователя для сервера SAP BusinessObjects.

По умолчанию используется имя пользователя Administrator, а поле Password остается пустым.
7. Нажмите **Connect**. Откроется окно Manage Servers.
8. Щелкните значок Refresh, чтобы обновить список серверов.

9. Нажмите кнопку **Select All**, чтобы выбрать все указанные серверы, а затем щелкните значок Enable, чтобы перезапустить серверы.
10. Нажмите кнопку **Close**, чтобы закрыть окно.
11. Закройте все открытые окна.
12. Выполните вход в **Central Management Console** по следующему URL-адресу:

`http://<SHR_System_FQDN>:8080/CmcApp`

В данном случае `<SHR_System_FQDN>` — это полное доменное имя системы SHR.

13. Войдите в систему как администратор.

14. Нажмите  **Servers**.

15. Щелкните правой кнопкой мыши отключенный сервер и выберите команду **Enable Server**.

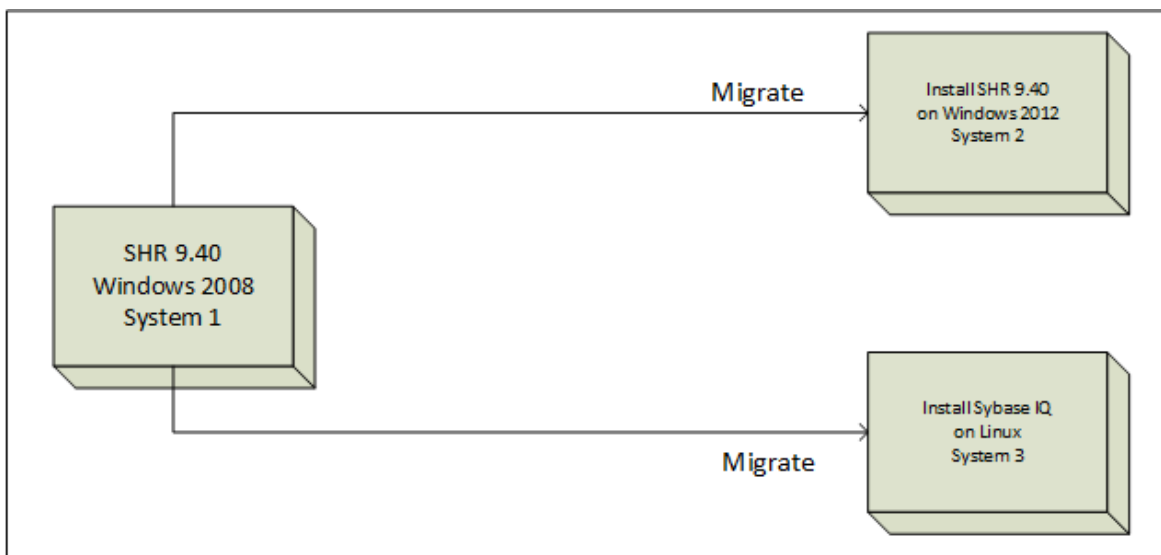
Если серверы SAP BusinessObjects не включаются, перезапустите службу HP_PMDB_Platform_IM.

Часть III: Переход к среде Windows 2012

Вы можете установить SHR 9.40 в Windows 2012. Однако база данных SHR не поддерживается в Windows 2012. Вы можете установить сервер SHR и SAP BusinessObjects в Windows 2012, а базу данных Sybase IQ в системе Linux. В этом разделе представлена процедура переноса установки SHR 9.40 из Windows 2008 в среду Windows 2012 в случае отдельной установки БД Sybase IQ в системе Linux.

Глава 7: Параллельный перенос

Эта процедура позволяет выполнить перенос SHR 9.40 из среды Windows 2008 в среду Windows 2012.



Требования к переносу

Прежде чем начинать перенос SHR, убедитесь, что выполнены следующие задачи.

1. В системе 1 воспользуйтесь установщиком, доступным на носителе SHR, чтобы обновить приложение до последней версии.

Примечание. Создайте резервную копию полной установки SHR на случай потери данных в случае сбоя установки.

Дополнительные сведения см. в разделе [Резервное копирование и восстановление баз данных](#).

2. В системе 2 установите последнюю версию SHR.
3. В системе 3, работающей под управлением ОС Linux, установите ПО Sybase IQ (доступно на носителе SHR 9.40).
4. Выполните все действия пост-установки и настройки в системе 2. Убедитесь, что пароли, указанные при установке, соответствуют старой установке в системе 1.

Пока не настраивайте источник данных и источник топологии.

5. В системе 1 остановите все службы SHR следующим образом:

- a. Выполните вход в систему SHR
- b. Откройте окно "Службы".
- c. Остановите следующие службы:
 - o HP_PMDB_Platform_Administrator
 - o HP_PMDB_Platform_Collection
 - o HP_PMDB_Platform_DB_Logger
 - o HP_PMDB_Platform_Timer
 - o HP_PMDB_Platform_IM
 - o HP_PMDB_Platform_Message_Broker
 - o HP_PMDB_Platform_PostgreSQL
 - o HP_PMDB_Platform_Sybase (*В случае выборочной установки остановите эту службу перед обновлением сервера Sybase IQ*)
 - o Sybase IQ Agent 15.4 Service (*В случае выборочной установки остановите эту службу перед обновлением сервера Sybase IQ*)
 - o Business Objects Webserver Service (*В случае выборочной установки остановите эту службу перед обновлением сервера SAP BusinessObjects*)
6. Откройте диспетчер задач Windows и перейдите на вкладку "Процессы".
 - Если запущены процессы *abcloadNrun*, необходимо дождаться их завершения.
7. Выполните следующую команду, чтобы убедиться, что все необходимые службы и процессы остановлены:

```
%PMDB_HOME%\DR\SHRServiceCheck.bat
```

8. Запустите службы Sybase IQ.
9. Создайте резервную копию полной установки SHR. Список действий см. в разделе [Резервное копирование и восстановление баз данных](#).
10. Убедитесь, что служба PostgreSQL запущена. Выполните следующую команду и создайте резервную копию базы данных управления:

```
Windows: %PMDB_HOME%/../JRE64/bin/java -cp %PMDB_HOME%/lib/utlils.jar  
com.hp.bto.bsmr.common.util.PostgresUpgrade PRE_DB_UPGRADE postgres 21425  
<Backup location> dwabc %PMDB_HOME%
```

11. Восстановите резервную копию Sybase IQ в системе 3 следующим образом:

a. Скопируйте резервную копию Sybase IQ в систему 3

Скопируйте файл %PMDB_HOME%\config\pmdbConfig.cfg из системы 1 в папку %PMDB_HOME%\config в системе 3.

b. Замените имя сервера в %PMDB_HOME%\config\pmdbConfig.cfg на короткое имя удаленной системы IQ

c. Остановите службу Sybase IQ в системе 3.

d. Переместите файлы существующей БД Sybase в другую папку.

e. Запустите службу Sybase IQ в системе 3, выполнив следующую команду.

```
start_iq @/opt/HP/BSM/PMDB/config/pmdbConfig.cfg
```

f. Из системы 2 подключитесь к удаленному серверу Sybase IQ в системе 3 с паролем по умолчанию utility_db и восстановите базу данных следующим образом:

Например:

```
restore DATABASE '<Путь к БД Sybase в системе 3>' from '<Имя файла с абсолютным путем к файлу резервной копии Sybase IQ в системе 3>'/pmdb.db
```

```
RENAME IQ_SYSTEM_MAIN TO '<Путь к файлам базы данных Sybase в системе 3>/SHRDB/pmdb.iq'
```

```
RENAME IQ_SYSTEM_TEMP TO '<Путь к файлам базы данных Sybase в системе 3>/SHRDB/pmdb.iqtmp'
```

```
RENAME IQ_SYSTEM_MSG TO '<Путь к файлам базы данных Sybase в системе 3>/SHRDB/pmdb.iq'
```

```
RENAME pmdb_user_main TO '<Путь к файлам базы данных Sybase в системе 3>/SHRDB/pmdb.iq'
```

12. Восстановите резервную копию сервера SAP BusinessObjects в системе 2. См. раздел [Резервное копирование и восстановление баз данных](#):

Примечание. Используйте имя хоста (короткое имя) системы SHR 1 как имя пользователя репозитория BO.

13. Восстановите резервную копию базы данных управления в системе 2 следующим образом:

- a. Остановите все службы SHR. Дождитесь завершения всех процессов SHR.
- b. Выполните следующую команду, чтобы убедиться, что все необходимые службы и процессы остановлены:

```
%PMDV_HOME%\DR\SHRServiceCheck.bat
```

- c. Запустите службу PostgreSQL.
- d. Запустите команду ниже, чтобы восстановить базу данных управления:
 - o Windows: %PMDV_HOME%\..\JRE64/bin /java -cp %PMDV_HOME%\lib/log4j-1.2.15.jar;%PMDV_HOME%\lib/utis.jar com.hp.bto.bsmr.common.util.PostgresUpgrade POST_DB_UPGRADE postgres 21425 <Путь к резервной копии> dwabc %PMDV_HOME%

14. Восстановите следующие файлы конфигурации:

- collection.properties
- downtime.xml и group.xml, если таковые имеются
- server.xml и web.xml

Примечание. После восстановления измените имени хоста системы 1 в соответствии с именем хоста системы 2 в следующих файлах после и перезапустите службу BO:

```
%PMDV_HOME%/ BOWebServer/webapps/InfoViewApp/WEB-INF/web.xml
```

```
%PMDV_HOME%/ /BOWebServer/webapps/CmcApp/WEB-INF/web.xml
```

- Восстановите хранилище ключей, если таковое имеется

15. Запустите следующую команду с помощью dbisql:

- DELETE FROM IM_PM_OS_INFO_FILLDETAIL WHERE OS_INFO_ID IN (SELECT IM_PM_OS_INFO_ID FROM IM_PM_OS_INFO WHERE upper (HOSTNAME) = UPPER('<короткое имя хоста системы 1>'))
- DELETE FROM IM_PM_OS_INFO WHERE upper (HOSTNAME) = UPPER('<короткое имя хоста системы 1>')
- DELETE FROM IM_PM_APPS_INFO WHERE upper (HOSTNAME) = UPPER('<короткое имя хоста системы 1>')

16. Измените файл config.prp, добавив следующее значение initial history, чтобы закрыть пробелы в данных:

- `dbcollector.initHistory = 48`
- `collector.initHistory = 48`

Выполните следующий запрос с помощью pgAdmin:

```
Truncate dwabc.PA_LAST_POLL;
```

```
Truncate dwabc.DB_LAST_POLL;
```

Если вы выполнили это действие, обязательно верните значение к исходному и перезапустите службу сбора данных, как только нужные данные будут доступны в отчетах.

Выполните следующие действия, чтобы синхронизировать источники данных для сбора:

1. Выполните следующий запрос с помощью pgAdmin:

```
UPDATE dwabc.remote_poller SET datasource_status=0
```

2. Синхронизируйте источники данных для сбора с помощью административной консоли (страница «Администратор > Конфигурация сборщика»)

Примечание. После выполнения переноса следует запустить **Консоль администрирования SHR > Администрирование > Диспетчер развертывания** и обновить пакеты содержимого до самой свежей версии.

Компонент пакета содержимого `SysPerf_SiS_ETL` утсарел. Вместо `SysPerf_SiS_ETL` следует использовать `SysPerf_SiS_DB` или `SysPerf_SiS_API`. Дополнительные сведения см. в *интерактивной справке HP Service Health Reporter для администраторов*.

Если обновление закончится неудачей, восстановите резервную копию предыдущей версии и выберите обновление еще раз.

Конфигурация после переноса

Выполните следующие действия после переноса.

Задача 1. Повторное применение уровней доступа к подключениям среды

В ходе обновления пакетов содержимого SHR происходит повторное создание стандартных подключений среды. В этой связи на каждом уровне подключения необходимо повторное предоставление прав подключениям среды. Указания по настройке уровней доступа пользователей см. в документации по SAP BusinessObjects.

Задача 2. Убедитесь, что SHR работает

Перейдите по следующему адресу и войдите в консоль администрирования с правами администратора.

```
http://<SHR_Server_FQDN>:21411
```

Перейдите по следующему адресу и войдите в консоль InfoView с правами администратора.

```
http://<SHR_Server_FQDN>:8080
```

Если удалось войти под учетной записью администратора, обновление SHR прошло успешно. Если произошла ошибка проверки подлинности, необходимо восстановить резервную копию базы данных, а затем выполнить обновление повторно. Дополнительные сведения см. в разделе [Резервное копирование и восстановление баз данных](#).

Примечание. Повторно создайте службы администратора и сбора данных

Если приложение SHR установлено в домене, заново создайте следующие службы в соответствии с разделом *Настройка служб SHR, когда приложение SHR установлено в домене* документа *Руководство по установке и настройке HP Service Health Reporter*.

- Служба администратора платформы HP PMDB
- Служба сбора данных платформы HP PMDB

Часть IV: Дополнительная настройка

Глава 8: Настройка защищенного подключения для SHR (HTTPS)

В системе SHR используются два консольных интерфейса — административная консоль и консоль SAP BusinessObjects InfoView. Обе консоли можно запустить в защищенной среде с использованием сетевого протокола HTTPS или в незащищенной среде с использованием сетевого протокола HTTP. По умолчанию для обеих консолей используется протокол HTTP. Для запуска административной консоли и консоли SAP BusinessObjects InfoView в защищенной среде необходимо настроить сетевой протокол HTTPS.

Создание файла хранилища ключей

Перед настройкой защищенного подключения необходимо создать файл хранилища ключей, содержащий сертификат сервера SHR и закрытый ключ. Для создания файла хранилища ключей с помощью программы keytool выполните следующую команду:

```
keytool -genkey -keystore keystore.jks -alias mykey
```

Примечание. Файл хранилища ключей также можно создать с помощью других программ.

Файл хранилища ключей защищен паролем. В SHR можно настроить расположение хранилища ключей и пароль с помощью свойств keystorepath и keystorepasswd. В качестве свойства keystorepath в системе Windows должен быть указан путь с использованием символов прямой косой черты. Свойство keystoretype задает тип хранилища ключей; поддерживаются значения JKS и PKCS12. Псевдоним сертификата указывается в хранилище ключей с помощью свойства keyalias, как показано в следующей таблице.

Имя свойства	Пример
Keystorepath	C:/certs/serverkeystore.jks
Keystorepasswd	changeit
Keyalias	shserver
Keystoretype	JKS

Настройка защищенного подключения (HTTPS)

Для административной консоли и консоли InfoView можно настроить защищенное подключение.

Для административной консоли SHR

Для настройки защищенного подключения административной консоли SHR выполните следующие действия.

Задача 1: Остановите службу HP_PMDB_Platform_Administrator

- **Windows**

Чтобы остановить службу HP_PMDB_Platform_Administrator, выполните следующие действия.

- Выберите пункты **Пуск >Выполнить**. Откроется диалоговое окно «Выполнить».
- Введите `services.msc` в поле «Открыть» и нажмите клавишу ВВОД. Откроется окно «Службы».
- В правой части окна щелкните правой кнопкой мыши элемент **HP_PMDB_Platform_Administrator** и выберите команду **Остановить**.

- **Linux**

Выполните команду

```
service HP_PMDB_Platform_Administrator stop
```

Задача 2: Внесите изменения в файл `server.xml`.

Совет. Перед редактированием файла `server.xml` создайте его резервную копию.

- Раскомментируйте тег `SSL Connector` с параметром `port`, имеющим значение 21412.
- Установите следующие значения полей в файле `server.xml`, расположенном в следующем каталоге.

- **Windows**

```
%PMDB_HOME%\adminserver\conf/
```

- **Linux**

```
$PMDB_HOME/adminserver/conf/
```

Поле	Описание
<code>keystorefile</code>	Полный путь к файлу хранилища ключей, в котором вы сохранили загружаемый сертификат сервера.

Поле	Описание
keystorepasswd	Пароль для доступа к сертификату сервера из указанного файла хранилища ключей.
keystoretype	Тип файла хранилища ключей, содержащего сертификат сервера.
keyAlias	Псевдоним сертификата сервера в хранилище ключей.

Задача 3: Внесите изменения в файл config.prp

Совет. Перед редактированием файла config.prp создайте его резервную копию.

Установите следующие значения полей в файле config.prp, расположенном в следующем каталоге.

Windows

%PMDB_HOME%\data

Linux

\$PMDB_HOME/data

Поле	Значение
bo.protocol	https
bo.ssl.enabled.port	8443

Примечание. В поле bo.ssl.enabled.port устанавливается значение номера порта, указанное в атрибуте port тега connector в файле server.xml; значение по умолчанию: 8443.

Задача 4: Запустите службу HP_PMDB_Platform_Administrator

В Windows:

Чтобы остановить службу HP_PMDB_Platform_Administrator, выполните следующие действия.

1. Выберите пункты **Пуск** -> **Выполнить**. Откроется диалоговое окно «Выполнить».
2. Введите services.msc в поле Открыть и нажмите клавишу **ВВОД**. Откроется окно «Службы».
3. В правой части окна щелкните правой кнопкой мыши элемент **HP_PMDB_Platform_Administrator** и выберите команду **Запустить**.

В Linux:

Выполните команду

```
service HP_PMDB_Platform_Administrator start
```

Задача 5: Проверьте конфигурацию.

Для проверки конфигурации выполните вход в административную консоль по следующему URL-адресу:

```
https://<hostname>: 21412
```

где *<hostname>* — имя системы SHR.

Для консоли InfoView SHR

Чтобы настроить подключение HTTPS для консоли InfoView SHR, выполните следующие действия.

Примечание. В случае установки SHR по выбору выполните следующие задачи в системе, в которой установлено ПО SHR BusinessObjects.

Задача 1: Остановите службу SAP BusinessObjects Webserver.**В Windows:**

Остановите службу SAP BusinessObjects WebServer:

1. Выберите пункты **Пуск -> Выполнить**. Откроется диалоговое окно «Выполнить».
2. Введите `services.msc` в поле Открыть и нажмите клавишу **ВВОД**. Откроется окно «Службы».
3. В правой части окна щелкните правой кнопкой мыши элемент **BusinessObject WebServer** и выберите команду **Остановить**.

В Linux:

1. Перейдите в каталог `/opt/HP/BSM/PMDB/BOWebServer/bin`
2. Выполните следующую команду:

```
./shutdown.sh
```

Задача 2: Внесите изменения в файл server.xml.

Совет. Перед редактированием файла `server.xml` создайте его резервную копию.

Откройте файл `server.xml` по следующему пути: `%PMDB_HOME%\BOWebServer\conf` (для Windows) или `$PMDB_HOME/BOWebServer/conf` (для Linux):

Выполните следующие действия.

1. Раскомментируйте тег `SSL Connector` с параметром `port`, имеющим значение 8443.
2. Установите значения полей в файле в соответствии со следующим описанием.

Поле	Описание
<code>keystorefile</code>	Полный путь к файлу хранилища ключей, в котором вы сохранили загружаемый сертификат сервера.
<code>keystorepasswd</code>	Пароль для доступа к сертификату сервера из указанного файла хранилища ключей.
<code>keystoretype</code>	Тип файла хранилища ключей, содержащего сертификат сервера.
<code>keyAlias</code>	Псевдоним сертификата сервера в хранилище ключей.

Задача 3: Запустите SAP BusinessObjects WebServer.

В Windows:

Остановите службу SAP BusinessObjects WebServer:

1. Выберите пункты **Пуск** -> **Выполнить**. Откроется диалоговое окно «Выполнить».
2. Введите `services.msc` в поле Открыть и нажмите клавишу **ВВОД**. Откроется окно «Службы».
3. В правой части окна щелкните правой кнопкой мыши элемент **BusinessObject WebServer** и выберите команду **Остановить**.

В Linux:

1. Перейдите в каталог `/opt/HP/BSM/PMDB/BOWebServer/bin`
2. Выполните следующую команду:

```
./startup.sh
```

Задача 4: Проверьте конфигурацию

Для проверки успешности конфигурации выполните следующие действия.

- Войдите на сайт по адресу `https://<hostname>:8443/InfoViewApp`
где `<hostname>` — имя системы SHR.
- Войдите на сайт по адресу `https://<hostname>:8443/CmcApp`
где `<hostname>` — имя системы SHR.

Глава 9: Сертификат проверки подлинности клиента для SHR

В системе SHR используются два консольных интерфейса — административная консоль и консоль SAP BusinessObjects InfoView. Административная консоль предназначена для администрирования и мониторинга SHR, а консоль SAP BusinessObjects InfoView позволяет просматривать отчеты и панель мониторинга. Обе консоли можно запустить в защищенной среде с использованием сетевого протокола HTTPS или в незащищенной среде с использованием сетевого протокола HTTP. По умолчанию для обеих консолей используется протокол HTTP. Для запуска административной консоли и консоли SAP BusinessObjects InfoView в защищенной среде необходимо настроить подключение HTTPS.

Проверка подлинности и авторизация

В SHR для проверки подлинности и авторизации используется система SAP BusinessObjects. В SAP BusinessObjects управление учетными записями пользователей осуществляется на консоли SAP BusinessObjects Central Management Console. Для доступа к административной консоли SHR требуются права администратора SAP BusinessObjects. По умолчанию в SHR используется механизм проверки подлинности на основе имени пользователя и пароля. Кроме того, SHR можно настроить на использование проверки подлинности на основе сертификатов, выполнив процедуру в "[Задача 4. Настройте проверку подлинности на основе сертификатов.](#)" для административной консоли и "[Настройка SAP BusinessObjects InfoView](#)" для представления SAP BusinessObjects. Пользователь идентифицируется в SHR путем проверки сертификата и авторизуется с помощью системы SAP BusinessObjects.

Предварительные условия проверки подлинности на основе сертификатов

Перед настройкой проверки подлинности на основе сертификатов должны быть выполнены следующие предварительные условия.

Задача 1: Создайте файл хранилища ключей, содержащий сертификат сервера SHR и закрытый ключ.

Файл хранилища ключей защищен паролем. В SHR можно настроить расположение хранилища ключей и пароль с помощью свойств keystorepath и keystorepasswd. Значение Keystorepath должно быть указано в файлах свойств в «[Задаче 4: Настройте проверку подлинности на основе сертификатов](#)» раздела [Настройка административной консоли SHR](#) и «[Задаче 4: Настройте конфигурацию на основе сертификатов](#)» раздела [Настройка SAP BusinessObjects InfoView](#). Свойство keystoretype задает тип хранилища ключей; поддерживаются значения **JKS** и **PKCS12**. Псевдоним сертификата указывается в хранилище ключей с помощью свойства keyalias, как показано в следующей таблице.

Имя свойства	Пример
Keystorepath	Vcerts\serverkeystore.jks (Linux) C:\\certs\\serverkeystore.jks (Windows)
Keystorepasswd	changeit
Keyalias	shserver
Keystoretype	JKS

Задача 2: Создайте файл хранилища ключей, содержащий сертификаты центра сертификации (ЦС).

Необходимо создать файл хранилища ключей, содержащий сертификаты ЦС, доверенные для сервера SHR. Этот файл защищен паролем. В SHR можно настроить хранилище доверенных сертификатов, установив для свойств `truststorepath`, `truststorepasswd` и `truststoretype` значения, указанные в следующей таблице: Значение `truststorepath` должно быть указано в файлах свойств в "Задача 4. Настройте проверку подлинности на основе сертификатов." и "Задача 4. Настройте конфигурацию на основе сертификатов".

Имя свойства	Примеры значений
truststorepath	Vcertrelated\Trustkeystore (Linux) C:\\certrelated\\Trustkeystore (Windows)
truststorepasswd	changeit
truststoretype	JKS

Задача 3: Включите проверку отзыва сертификата, если это требуется.

Установите для свойства `com.sun.net.ssl.checkRevocation` значение `true`, чтобы включить проверку отзыва сертификата. SHR поддерживает два метода проверки отзыва сертификата.

- Список отзыва сертификатов (CRL) — содержит информацию об отозванных сертификатах и загружается из ЦС. SHR извлекает URL-адрес точки распространения CRL из сертификата. Установите для свойства `com.sun.security.enableCRLDP` значение `true`, чтобы включить эту проверку.
- Online Certificate Status Protocol (OCSP) — это протокол для проверки отзыва одного сертификата с использованием веб-службы, называемой ответчиком OCSP. Установите для свойства `ocsp.enable` значение `true`, чтобы включить проверку отзыва с использованием протокола OCSP. SHR извлекает URL-адрес OCSP из сертификата для его проверки. Если требуется настроить локальную службу ответчика OCSP, в SHR ее можно настроить с помощью свойства `ocsp.responderURL`.

Более подробные указания по включению проверки отзыва сертификата с помощью CRL или OCSP в консоли администрирования SHR см. в «задаче 4: Настройте проверку подлинности на основе сертификатов» раздела "Настройка административной консоли SHR "

Более подробные указания по включению проверки отзыва сертификата с помощью CRL или OSCP в SHR BusinessObjects InfoView см. в «задаче 4: Настройте конфигурацию на основе сертификатов» раздела "[Настройка SAP BusinessObjects InfoView](#)".

Задача 4: Определите адрес прокси-сервера, расположенного между сервером SHR и Интернетом (если используется).

Если используется прокси-сервер, его необходимо настроить, чтобы сервер SHR мог загружать списки CRL. Прокси-сервер настраивается следующим образом:

http.proxyHost	Установите имя хоста прокси HTTP
http.proxyPort	Установите номер порта прокси HTTP
https.proxyHost	Установите имя хоста прокси HTTPS
https.proxyPort	Установите номер порта прокси HTTPS

См. в дополнительные сведения в «задаче 4: Настройте проверку подлинности на основе сертификатов» раздела "[Настройка административной консоли SHR](#)".

Задача 5. Определите механизм извлечения имени пользователя.

Механизм извлечения имени пользователя зависит от формата сертификата. Имя пользователя, извлеченное из сертификата, должно совпадать с именем пользователя, настроенным в SAP BusinessObjects. SHR предоставляет два механизма извлечения имени пользователя:

- SubjectDN
- Альтернативное имя субъекта (SAN)

Для настройки механизма извлечения имени пользователя необходимо изменить свойства field, entry, type, pattern и OID в файле **server.xml**.

```
<Realm className="com.hp.bto.bsmr.SHRSecureAuth.auth.SHRRealm" field="SubjectDN"
entry="CN" type="" oid="" pattern="" useSubjectDNOnMatchFail="true"/>
```

- Для извлечения имени пользователя из SubjectDN установите следующие значения свойств.

Имя свойства	Значение
field	SubjectDN
entry	Установите значение CN, чтобы использовать CN в качестве имени пользователя Установите значение OU, чтобы использовать OU в качестве имени пользователя

Свойство entry позволяет указать запись, используемую в качестве имени пользователя в SubjectDN. Кроме того, можно извлекать имя пользователя из SubjectDN с помощью шаблона вместо использования параметра entry. Для настройки шаблона извлечения имени

пользователя из SubjectDN используйте параметр `pattern`. Например, если настроен шаблон `EMAILADDRESS=(.+)@` и в поле `emailaddress` содержится значение `abc@hp.com`, в качестве имени пользователя извлекается строка `abc`.

- Для извлечения имени пользователя из альтернативного имени субъекта (SAN) выполните следующие действия.

Установите для свойства `field` значение `SAN`. Можно настроить часть имени пользователя `SAN rcf822Name` или `otherName` с помощью свойства `Type`. Чтобы настроить часть `rcf822Name`, установите для свойства `Type` значение `rcf822Name`. Чтобы настроить часть `otherName`, установите для свойства `type` значение `otherName` и установите в качестве идентификатора объекта (OID) значение `OID`.

По умолчанию SHR извлекает имя пользователя из `CN`.

Можно настроить SHR таким образом, чтобы пользователи могли входить в систему только с помощью смарт-карты. Для настройки входа с помощью смарт-карты установите для свойства `smartcard.enable` значение `true`.

Расположение файла `server.xml` показано в следующей таблице.

Настройка	Путь
Административная консоль	<code>\$PMDB_HOME/adminserver/conf</code> (для Linux) <code>%PMDB_HOME%\adminserver\conf</code> (для Windows)
SAP Infoview BusinessObjects	<code>\$PMDB_HOME/BOWebServer/conf</code> (для Linux) <code>%PMDB_HOME%\BOWebServer\conf</code> (для Windows)

Задача 6: Импортируйте сертификат и настройте браузер

- Импортируйте сертификат, изданный корневым ЦС для сервера SHR. Его следует импортировать в веб-браузер на вкладке **Доверенные корневые центры сертификации** в Internet Explorer. Дополнительные сведения см. в справке по Internet Explorer.
- Включите в веб-браузере поддержку протокола TLS версии 1.

Примечание. В среде высокой доступности настройте оба сервера.

В SHR можно настроить проверку подлинности на основе сертификатов как для интерфейса административной консоли, так и для интерфейса SAP BusinessObjects InfoViewApp.

Настройка метода извлечения имени пользователя

Извлечение имени пользователя можно настроить в файле `server.xml`, подробные сведения см. в разделе в [«задаче 5: Определите механизм извлечения имени пользователя»](#).

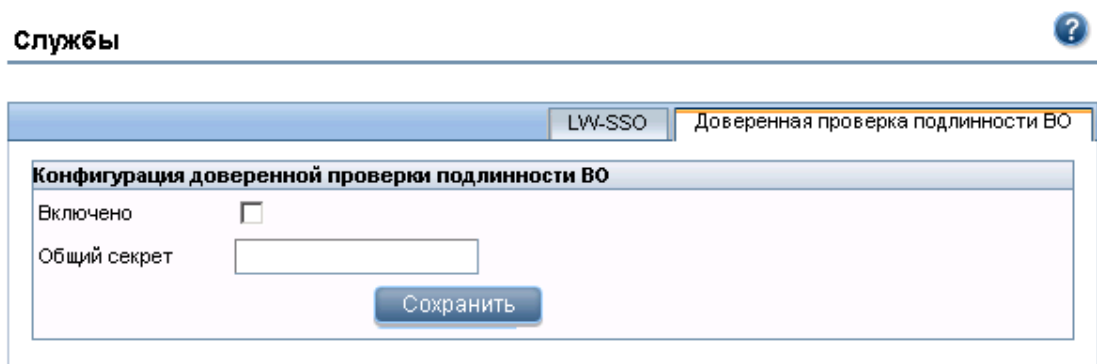
Настройка административной консоли SHR

Прежде чем продолжить, убедитесь, что система SHR была успешно настроена после установки. Чтобы настроить административную консоль SHR для проверки подлинности на основе сертификатов, выполните следующие действия.

Задача 1. Настройте общий секрет

Общий секрет используется для обеспечения доверенной проверки подлинности. Общий секрет можно ввести только в символьном формате.

1. Введите в веб-браузере `http://<HostName>:21411` для входа в административную консоль SHR.
2. В системе SHR выберите **Администрирование > Безопасность > Доверенная проверка подлинности ВО**.



Службы

LW-SSO Доверенная проверка подлинности ВО

Конфигурация доверенной проверки подлинности ВО

Включено

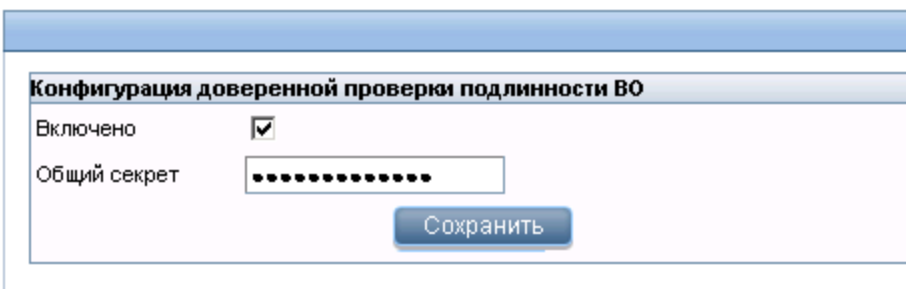
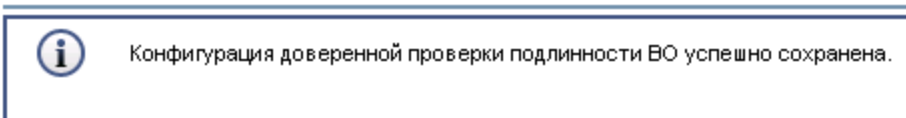
Общий секрет

Сохранить

3. Установите флажок **Включено**.
4. Введите значение в поле **Общий секрет**.
5. Нажмите кнопку **Сохранить**.

После успешной настройки отображается сообщение, показанное далее.

Службы



Задача 2. Остановите службу HP_PMDB_Platform_Administrator

Чтобы остановить службу HP_PMDB_Platform_Administrator, выполните следующие действия:

1. Выберите пункты **Пуск > Выполнить**. Откроется диалоговое окно «Выполнить».
2. Введите `services.msc` в поле Открыть и нажмите клавишу **ВВОД**. Откроется окно «Службы».
3. В правой части окна щелкните правой кнопкой мыши элемент HP_PMDB_Platform_Administrator и выберите команду **Остановить**.

Для Linux

Выполните следующую команду:

```
service HP_PMDB_Platform_Administrator stop
```

Задача 3. Настройте файл config.prp

В файле `config.prp`, который находится в каталоге `%PMDB_HOME%\data` (для Windows) или `$PMDB_HOME/data` (для Linux) введите следующие значения в соответствующие поля.

Поле	Значение
<code>shr.loginMethod</code>	<code>certbased</code>
<code>shr.auth.classes</code>	<code>com.hp.bto.bsmr.security.auth.BOTrustedAuthenticator</code>

Задача 4. Настройте проверку подлинности на основе сертификатов.

Укажите следующие параметры в файле `adminserverclientauth.prp`, который находится в каталоге `$PMDB_HOME/data` (для Linux) или `%PMDB_HOME%\data` (для Windows). В следующих полях укажите значения в соответствии с описанием.

Поле	Описание
truststorepath	Полный путь к файлу хранилища доверенных сертификатов, который используется для проверки сертификатов клиентов.
truststorepasswd	Пароль для доступа к хранилищу доверенных сертификатов.
truststoretype	Тип хранилища ключей, используемого для хранилища доверенных сертификатов.
keystorepath	Полный путь к файлу хранилища ключей, в котором вы сохранили загружаемый сертификат сервера.
keystorepasswd	Пароль для доступа к сертификату сервера из указанного файла хранилища ключей.
keystoretype	Тип файла хранилища ключей, содержащего сертификат сервера.
keyAlias	Псевдоним сертификата сервера в хранилище ключей.
smartcard.enable	Установите значение true, чтобы включить вход с помощью смарт-карты, или значение false, чтобы отключить вход с помощью смарт-карты.
http.proxyHost	Имя хоста прокси HTTP.
http.proxyPort	Номер порта прокси HTTP.
com.sun.net.ssl.checkRevocation	Установите значение true, чтобы включить проверку отзыва, или false, чтобы отключить проверку отзыва.
com.sun.security.enableCRLDP	Установите значение true, чтобы включить проверку отзыва сертификата с помощью CRL, или значение false, если это не требуется.
crlFile	Введите путь к файлу CRL.
ocsp.enable	Установите значение true, чтобы включить проверку отзыва сертификата на основе OCSP, или значение false, если это не требуется.
ocsp.responderURL	Установите URL-адрес ответчика OCSP.

Примечание. Если включена (true) проверка отзыва сертификата на основе CRL, необходимо отключить (false) проверку отзыва сертификата на основе OCSP, и наоборот.

После установки значений свойств выполните следующие действия.

- **Для Linux**

- a. Перейдите в каталог `$PMDB_HOME/bin`.

- b. Выполните команду

```
perl adminserverclientauth.pl -authType clientcert -configFile <config file location>
```

где *<config file location>* представляет собой полный путь к файлу `adminserver.prp`.

например, `$PMDB_HOME/data/adminserverclientauth.prp`

- **Для Windows**

- a. Перейдите в каталог `%PMDB_HOME%\bin`.

- b. Выполните команду

```
perl adminserverclientauth.pl -authType clientcert -configFile <config file location>
```

где *<config file location>* представляет собой полный путь к файлу `adminserver.prp`.

Например, `%PMDB_HOME%\data\adminserverclientauth.prp`

Задача 5: Настройте извлечение имени пользователя.

Система SHR должна извлекать в качестве имени пользователя запись CN из поля SubjectDN. Измените файл `server.xml`, как описано в [задаче 5: Определите механизм извлечения имени пользователя](#).

Задача 6. Запустите службу HP_PMDB_Platform_Administrator

Чтобы запустить службу `HP_PMDB_Platform_Administrator`, выполните следующие действия:

1. Выберите пункты **Пуск > Выполнить**. Откроется диалоговое окно «Выполнить».
2. Введите `services.msc` в поле Открыть и нажмите клавишу **ВВОД**. Откроется окно «Службы».
3. В правой части окна щелкните правой кнопкой мыши элемент `HP_PMDB_Platform_Administrator` и выберите команду **Запустить**.

Для Linux

```
service HP_PMDB_Platform_Administrator start
```

Задача 7: Протестируйте проверку подлинности на основе сертификатов

1. Введите в веб-браузере `http://<HostName>:21411` для входа в административную консоль SHR.
2. Выберите **Войти с цифровым сертификатом**.

Настройка SAP BusinessObjects InfoView

Если вы не настроили общий секрет, сделайте это, выполнив действия, которые приводятся в «задаче 1: Настройте общий секрет» раздела "Настройка административной консоли SHR " на [странице 102](#).

Примечание. При использовании выборочной установки SHR с удаленной системой SAP BusinessObjects скопируйте файл `SHRTrustedPrinciple.conf` из каталога `<Install_Dir>/PMDB/adminServer/conf` в каталог `<Install_Dir>/PMDB/BOWebServer/conf` в системе, в которой установлено ПО SAP BusinessObjects.

Задача 1: Чтобы включить для консоли InfoView и Open Document проверку подлинности на основе сертификатов, выполните следующие действия.

Примечание. В случае установки SHR по выбору выполните следующие задачи в системе, в которой установлено ПО SHR BusinessObjects.

Остановите службу SAP BusinessObjects WebServer.

- **Для Linux**

- a. Перейдите в каталог `/opt/HP/BSM/PMDB/BOWebServer/bin`
- b. Выполните команду

```
./shutdown.sh
```

- **Для Windows**

- a. Выполните вход в систему от имени администратора.
- b. Выберите пункты **Пуск > Выполнить**. Откроется диалоговое окно «Выполнить».
- c. Введите `services.msc` в поле **Открыть** и нажмите клавишу **ВВОД**. Откроется окно «Службы».
- d. Щелкните правой кнопкой мыши **службу Business Objects WebServer** и выберите команду **Остановить**, чтобы ее остановить.

Задача 2. Остановите службу HP_PMDB_Platform_Administrator

Чтобы остановить службу `HP_PMDB_Platform_Administrator`, выполните следующие действия:

1. Выберите пункты **Пуск > Выполнить**. Откроется диалоговое окно «Выполнить».
2. Введите `services.msc` в поле Открыть и нажмите клавишу **ВВОД**. Откроется окно «Службы».
3. В правой части окна щелкните правой кнопкой мыши элемент `HP_PMDB_Platform_Administrator` и выберите команду **Остановить**.

Для Linux

```
service HP_PMDB_Platform_Administrator stop
```

Задача 3: Внесите изменения в файл `config.prp`

В файле `config.prp`, который находится в каталоге `%PMDB_HOME%\data` (для Windows) или `$PMDB_HOME/data` (для Linux) введите следующее значение в соответствующее поле.

Поле	Значение
<code>bo.protocol</code>	<code>https</code>

Задача 4. Настройте конфигурацию на основе сертификатов

Примечание. В случае установки SHR по выбору выполните следующие задачи в системе, в которой установлено ПО SHR BusinessObjects.

Установите значения полей в файле `BOclientauth.prp`, расположенном в каталоге `$PMDB_HOME/data` (для Linux) или `%PMDB_HOME%\data` (для Windows) в соответствии со следующим описанием.

Поле	Описание
<code>truststorepath</code>	Полный путь к файлу <code>truststore</code>
<code>truststorepasswd</code>	Пароль для доступа к хранилищу доверенных сертификатов.
<code>truststoretype</code>	Тип хранилища ключей, используемого для хранилища доверенных сертификатов.
<code>keystorepath</code>	Полный путь к файлу хранилища ключей, в котором вы сохранили загружаемый сертификат сервера.
<code>keystorepasswd</code>	Пароль для доступа к сертификату сервера из указанного файла хранилища ключей.
<code>keystoretype</code>	Тип файла хранилища ключей, содержащего сертификат сервера.
<code>keyAlias</code>	Псевдоним сертификата сервера в хранилище ключей.

Поле	Описание
smartcard.enable	Установите значение true, чтобы включить вход с помощью смарт-карты, или значение false, если это не требуется.
http.proxyHost	Имя хоста прокси HTTP.
http.proxyPort	Номер порта прокси HTTP.
https.proxyHost	Имя хоста прокси HTTPS.
https.proxyPort	Номер порта прокси HTTPS.
com.sun.net.ssl.checkRevocation	Установите значение true, чтобы включить проверку отзыва, или значение false, если это не требуется.
com.sun.security.enable-CRLDP	Установите значение true, чтобы включить проверку отзыва с помощью CRL, или значение false, если это не требуется.
crlFile	Введите путь к файлу CRL.
ocsp.enable	Установите значение true, чтобы включить проверку отзыва на основе OCSP, или значение false, если это не требуется.
ocsp.responderURL	Установите URL-адрес ответчика OCSP.

Примечание. Если включена (true) проверка отзыва сертификата на основе CRL, необходимо отключить (false) проверку отзыва сертификата на основе OCSP, и наоборот.

После установки значений свойств выполните следующие действия.

- **Для Linux**

- a. Перейдите в каталог \$PMDB_HOME/bin.

- b. Выполните команду

```
perl B0clientauth.pl -authType clientcert -configFile <config file location>
```

где <config file location> представляет собой полный путь к файлу B0clientauth.prp.

Например, \$PMDB_HOME/data/B0clientauth.prp.

- **Для Windows**

- a. Перейдите в каталог %PMDB_HOME%\bin.

- b. Выполните команду

```
perl B0clientauth.pl -authType clientcert -configFile <config file location>
```

где *<config file location>* представляет собой полный путь к файлу B0clientauth.prp.
Например, %PMDB_HOME%\data\B0clientauth.prp.

Задача 5. Запустите службу SAP BusinessObjects WebServer.

Примечание. В случае установки SHR по выбору выполните следующие задачи в системе, в которой установлено ПО SHR BusinessObjects.

• Для Linux

- a. Перейдите в каталог /opt/HP/BSM/PMDB/BOWebServer/bin.
- b. Выполните команду ./startup.sh

• Для Windows

- a. Выполните вход в систему от имени администратора.
- b. Выберите пункты **Пуск > Выполнить**.
- c. Введите services.msc в поле Открыть и нажмите клавишу **ВВОД**. Откроется окно «Службы».
- d. Щелкните правой кнопкой мыши **службу SAP BusinessObjects WebServer** и выберите команду **Запустить**, чтобы ее запустить.

Задача 6. Запустите службу HP_PMDB_Platform_Administrator

Чтобы запустить службу HP_PMDB_Platform_Administrator, выполните следующие действия:

1. Выберите пункты **Пуск > Выполнить**. Откроется диалоговое окно «Выполнить».
2. Введите services.msc в поле Открыть и нажмите клавишу **ВВОД**. Откроется окно «Службы».
3. В правой части окна щелкните правой кнопкой мыши элемент HP_PMDB_Platform_Administrator и выберите команду **Запустить**.

Для Linux

```
service HP_PMDB_Platform_Administrator start
```

Задача 7: Протестируйте проверку подлинности на основе сертификатов

1. Введите в веб-браузере http://<HostName>:8080/InfoViewApp для входа в консоль SHR InfoView.
2. Выполните вход в консоль InfoView.

3. Если отображается экран, показанный далее, настройка успешно завершена.



4. Можно выполнить вход в консоль InfoView с помощью цифрового сертификата.

Задача 8: Настройте InfoView для проверки подлинности пользователей посредством LDAP или Active Directory

1. В системе SHR откройте файл `web.xml`, путь: `%PMD_B_HOME%/BOWebServer/webapps/InfoViewApp/WEB-INF/web.xml`.
2. Установите значение `<true>` для параметра `<authentication.visible>`.
3. Сохраните изменения и закройте файл.
4. Перезапустите сервер веб-приложения.

Глава 10: Резервное копирование и восстановление базы данных

SHR позволяет осуществлять резервное копирование и восстановление базы данных для предотвращения потери данных в случае сбоя базы данных. Прежде чем приступить к использованию SHR в производственных условиях, рекомендуется выполнить стандартное резервное копирование базы данных.

Аварийное восстановление SHR включает планирование регулярного резервного копирования баз данных SHR и ключевых файлов конфигурации и лицензий. SHR позволяет осуществлять резервное копирование и восстановление базы данных Sybase IQ и хранилища файлов SAP BusinessObjects для предотвращения потери данных в случае аварии.

SHR предоставляет следующие варианты резервного копирования базы данных:

- **Полное резервное копирование:** полное резервное копирование позволяет создавать полную резервную копию следующих баз данных SHR (включая файлы и журналы транзакций базы данных).
 - Sybase IQ
 - SAP BusinessObjects (SQL Anywhere)
 - Таблицы баз данных управления (PostgreSQL)

Кроме того, вы можете создать полную резервную копию хранилища файлов SAP BusinessObjects.

- **Добавочное резервное копирование:** добавочное резервное копирование позволяет создавать резервную копию журналов транзакций. С его помощью создается резервная копия файлов, которые были изменены или добавлены после последнего полного резервного копирования.

Совет. Полное резервное копирование рекомендуется выполнять раз в неделю, добавочное резервное копирование — раз в день.

Важные примечания.

- Задачи полного и добавочного резервного копирования необходимо планировать для выполнения с регулярной периодичностью.
- В случае сбоя базы данных SHR позволяет восстановить ее, используя резервную копию. Резервная и основная системы должны быть идентичны и иметь одинаковые спецификации оборудования и ОС, версию SHR, пути к файлам, топологии, конфигурации пост-установки и развернутые пакеты содержимого.

- Если вы изменили любые из файлов конфигурации (пример: SAC) для настройки производительности основной конфигурации, внесите соответствующие изменения в резервной конфигурации.

Внимание. SHR требует статического IP-адреса. Вы должны настроить резервную среду SHR (удаленную или локальную) с тем же IP-адресом и именем хоста, что основной сервер SHR для восстановления постоянной лицензии. Дополнительные лицензии не требуются для восстановления SHR.

Создание резервной копии баз данных SHR в Windows

Для базы данных Sybase IQ

При выборочной установке выполните следующие действия на основном сервере SHR, чтобы создать резервную копию базы данных Sybase IQ.

Совет. Для резервного копирования базы данных Sybase IQ при выборочной установке вы должны указать путь к удаленной базе данных Sybase IQ.

Задача 1: Редактирование сценариев резервного копирования

SHR включает два сценария резервного копирования для полного и инкрементного резервного копирования. Перед началом резервного копирования отредактируйте эти сценарии в соответствии со своими требованиями. Сценарии находятся в каталоге %PMDB_HOME%\scripts\Sybase. Файлы сценариев:

- Для полного резервного копирования: %PMDB_HOME%\scripts\Sybase\IQ_backup_full.sql
- Для добавочного резервного копирования: %PMDB_HOME%\scripts\Sybase\IQ_backup_incr_since_full.sql

Для редактирования сценариев выполните следующие действия:

1. Перейдите в папку %PMDB_HOME%\scripts\Sybase.
2. Откройте файл IQ_backup_full.sql с помощью приложения "Блокнот".

В последнем параметре сценария .sql создайте каталог (например, E:\HP-SHR\Backup) для сохранения файлов резервных копий.

Примечание. Не используйте переносы строки (/n, /r) в пути для сохранения файлов

резервных копий. Пример: C:/new, C:/readonly.

```
dsi_pmdb_backup 'FULL',NULL,'READWRITE_FILES_
ONLY',NULL,NULL,NULL,NULL,NULL,'D','location_for_backup'
```

Аналогичным образом для добавочного резервного копирования укажите желаемое расположение файлов, как показано ниже:

```
dsi_pmdb_backup 'INCREMENTAL_SINCE_FULL',NULL,'READWRITE_FILES_
ONLY',NULL,NULL,NULL,NULL,NULL,'D','location_for_backup'
```

Примечание. В случае установки SHR для работы с удаленной базой данных `location_for_backup` обозначает действительный путь на сервере базы данных Sybase IQ.

3. Выполните следующие файлы из каталога `%PMDB_HOME%\DR\`:
 - `Execute_FullBackup_Script.bat` для полного резервного копирования.
 - `Execute_IncrSncFullBackup_Script.bat` для добавочного резервного копирования.

После выполнения сценариев к имени создаваемой резервной копии базы данных добавляется день недели в указанном местоположении.

Сценарии создают следующие файлы журнала:

- Полное резервное копирование - `%PMDB_HOME%\tmp\Execute_IQ_backup_full.out`
- Добавочное резервное копирование - `%PMDB_HOME%\tmp\Execute_backup_incr_since_full.out`

Задача 2: Редактирование сценария копирующей архивации

SHR использует сценарий копирующей архивации, при которой в указанном месте создается резервная копия предыдущего файла полного резервного копирования.

Для редактирования сценария резервного копирования откройте сценарий `%PMDB_HOME%\DR\COPY_Backup.bat`, а затем укажите расположение существующего файла полного резервного копирования и желаемое расположение для сохранения копируемых файлов.

```
COPY "location of existing full backup file" "copy to location"> %PMDB_
HOME%\tmp\COPY_Backup.txt 2>&1 /Y /V
```

Для установки SHR с удаленной базой данных вы должны запустить сценарий в системе, в которой установлена база данных Sybase IQ.

Ниже приведен пример данного сценария:

```
COPY "E:\HP-SHR\Backup\Full*" "E:\HP-SHR\Backup\Old\" > %PMDB_HOME%\tmp\COPY_
Backup.txt 2>&1 /Y /V
```

Задача 3: Планирование резервного копирования

Используйте планировщик задач Windows для планирования и выполнения сценариев резервного копирования. Полное резервное копирование рекомендуется выполнять раз в неделю, добавочное резервное копирование — раз в день.

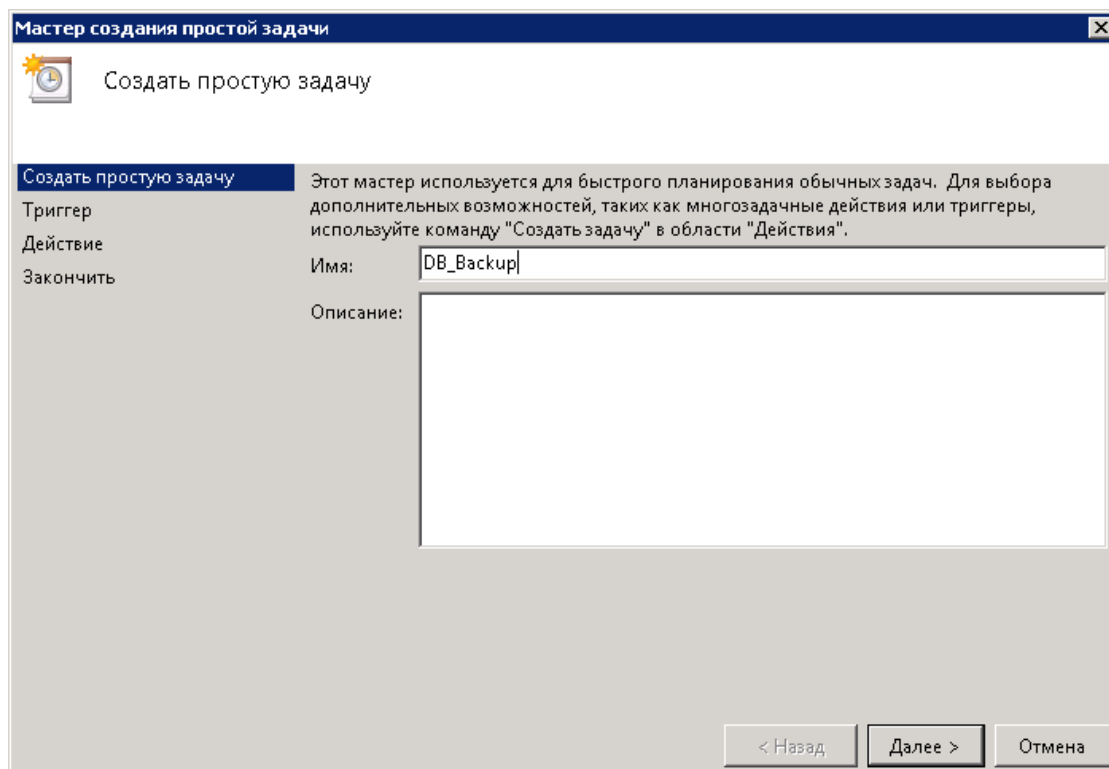
Примечание. Если Sybase IQ установлена в удаленной системе, не планируйте эту задачу в системе SHR. Обязательно запланируйте резервное копирование в системе, в которой установлена база данных Sybase IQ.

Планирование выполнения сценария копирующей архивации

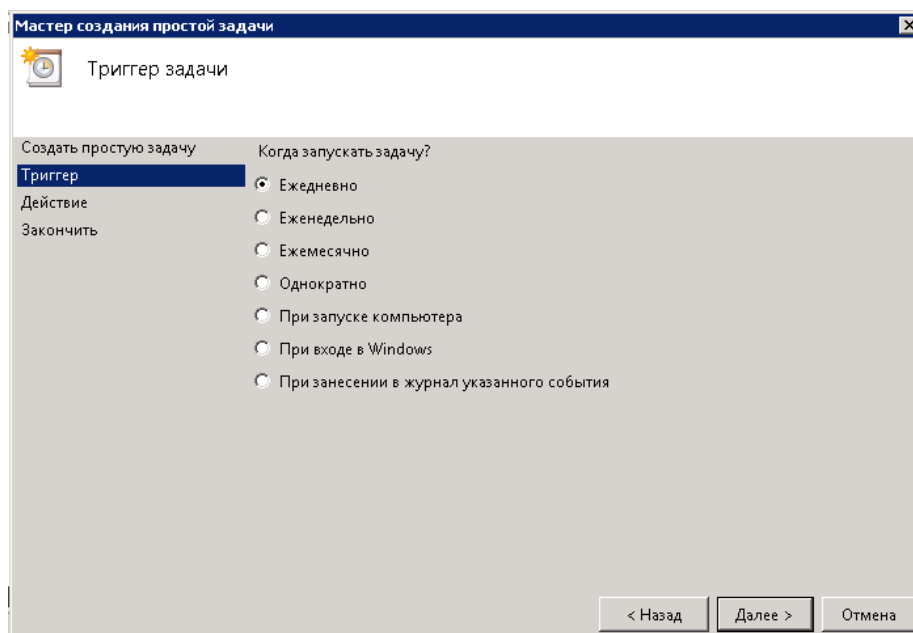
Сценарий копирующей архивации создает копию файлов полного резервного копирования базы данных в указанном месте во избежание перезаписи поверх существующей полной резервной копии. Сценарий копирующей архивации необходимо планировать для запуска каждый раз перед выполнением сценария полного резервного копирования.

В Windows 2008

1. Перейдите к **Пуск > Программы > Администрирование > Планировщик задач**.
Откроется окно планировщика задач.
2. В окне планировщика задач щелкните правой кнопкой пункт **Создать базовую задачу**.
Откроется мастер создания базовой задачи. Введите имя задачи и нажмите кнопку **Далее**.

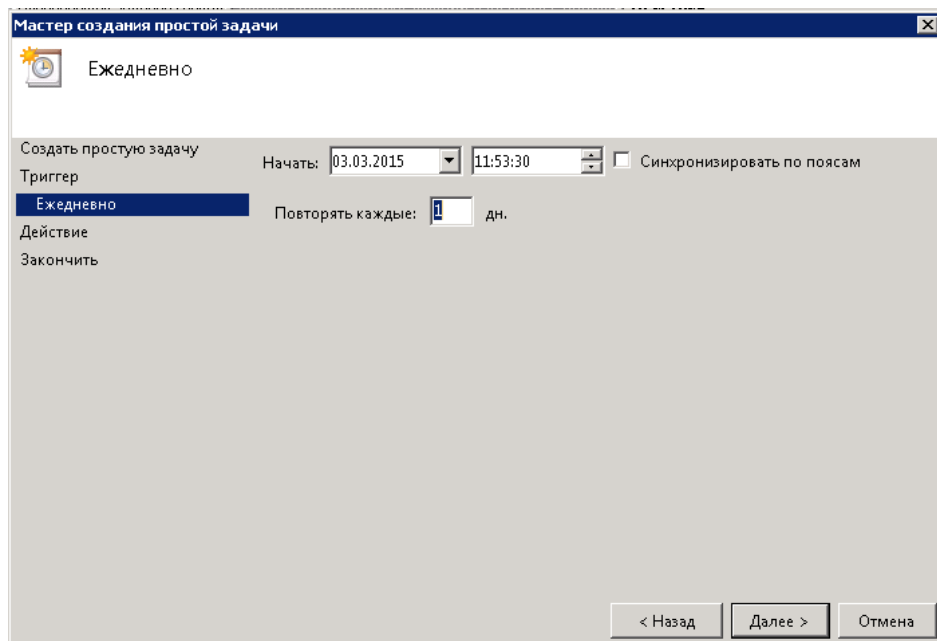


3. Выберите **Ежедневно** и нажмите кнопку **Далее**.

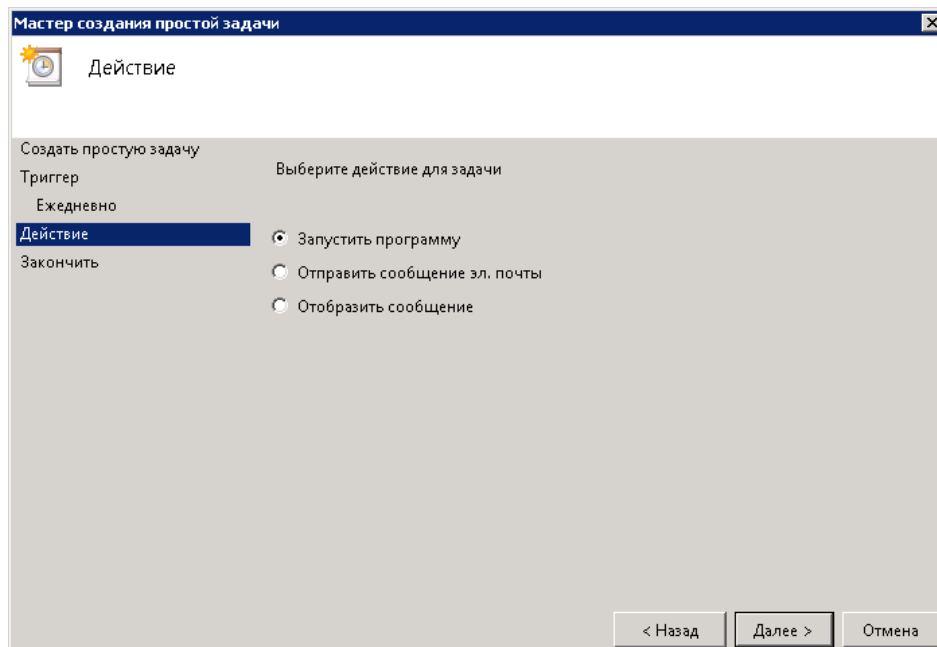


4. Выберите время начала и введите 1 в текстовое поле **Повтор каждые** и нажмите кнопку

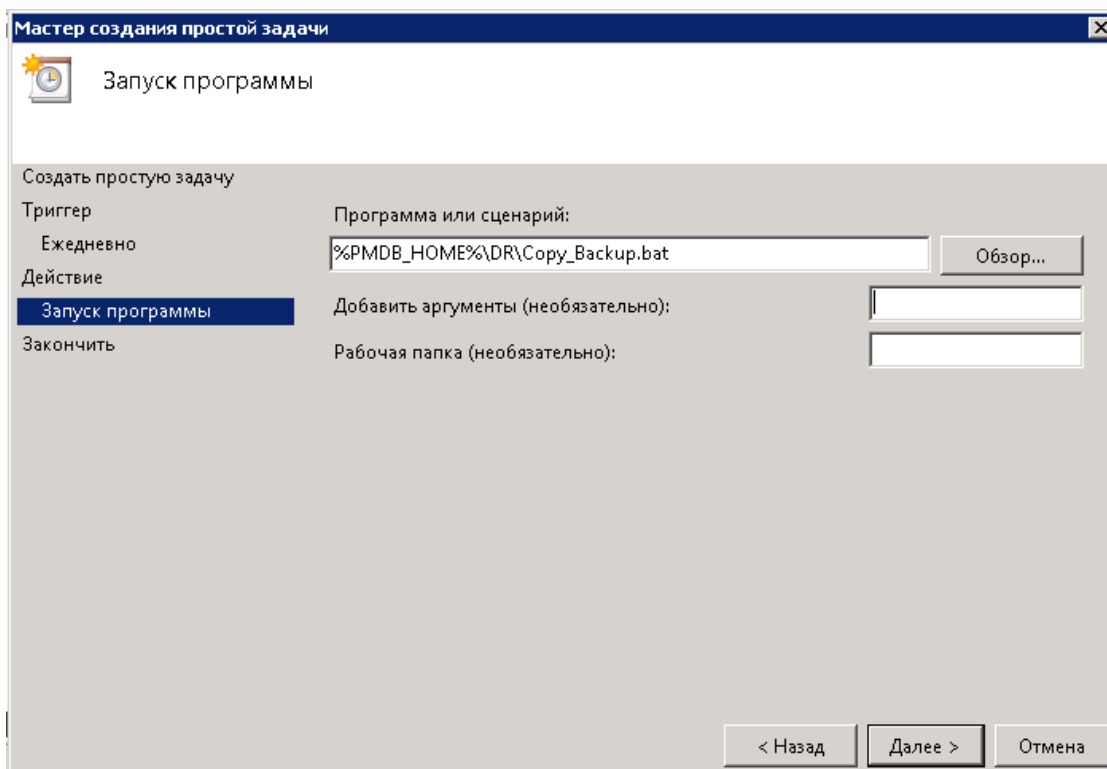
Далее.



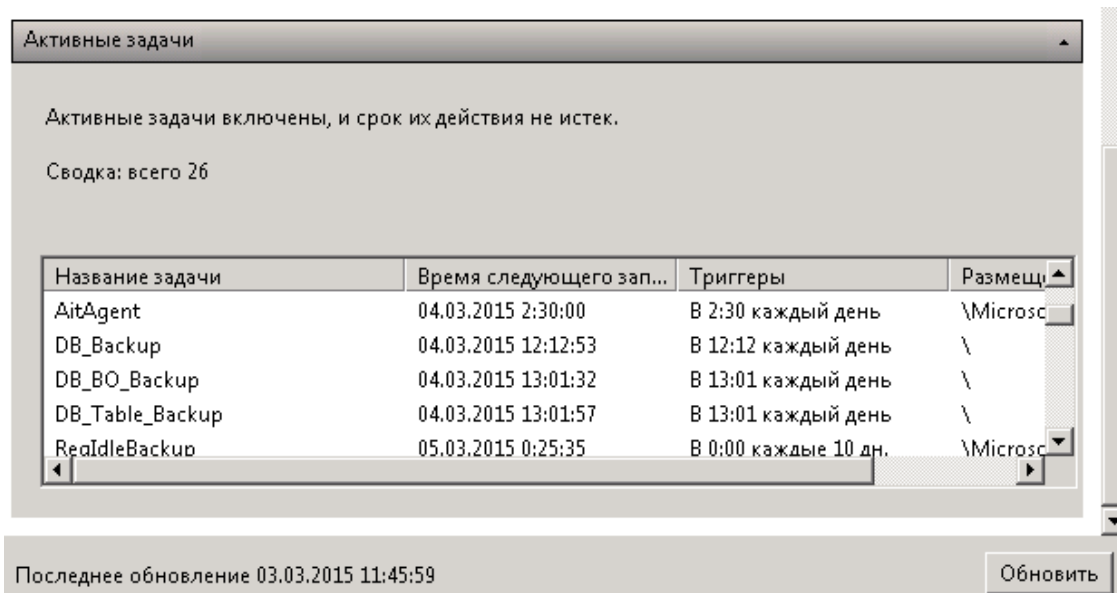
5. Выберите **Запустить программу** и нажмите кнопку **Далее**.



6. Перейдите в каталог %PMDV_HOME%\DR, выберите **Copy_Backup.bat** и нажмите кнопку **Далее**.



7. Нажмите кнопку **Готово**. Вы можете проверить, создана ли задача, в разделе **Активные задачи** окна планировщика задач.

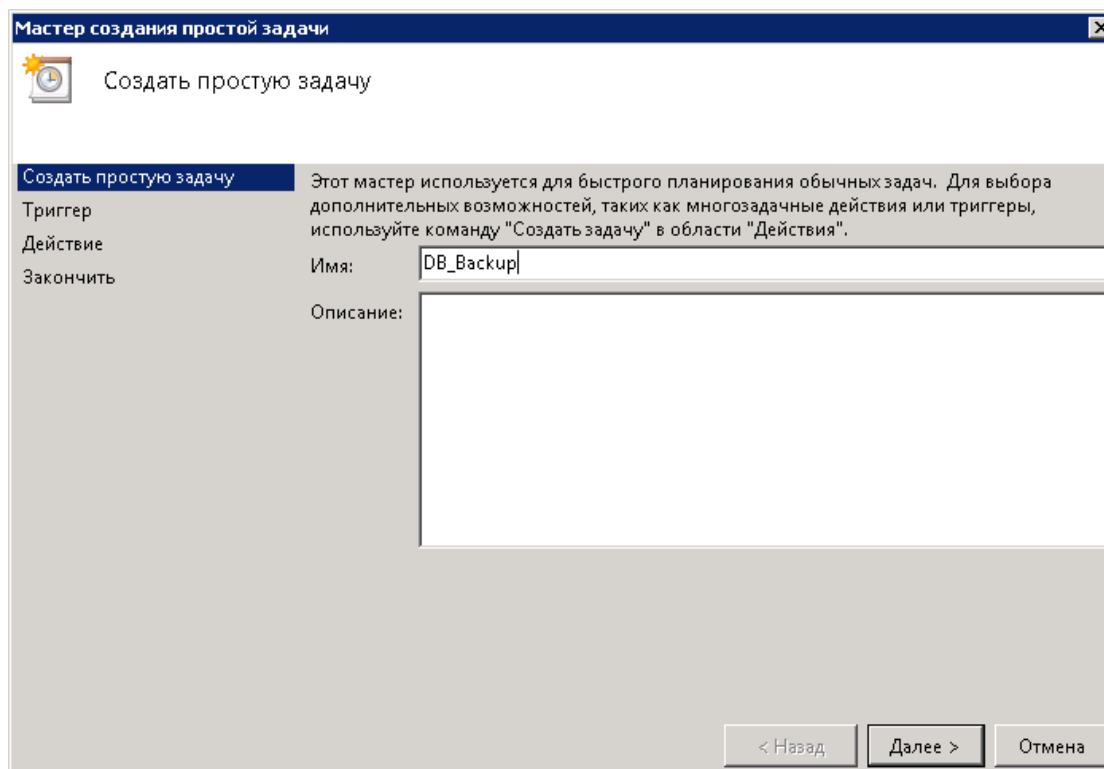


Планирование выполнения сценария полного резервного копирования

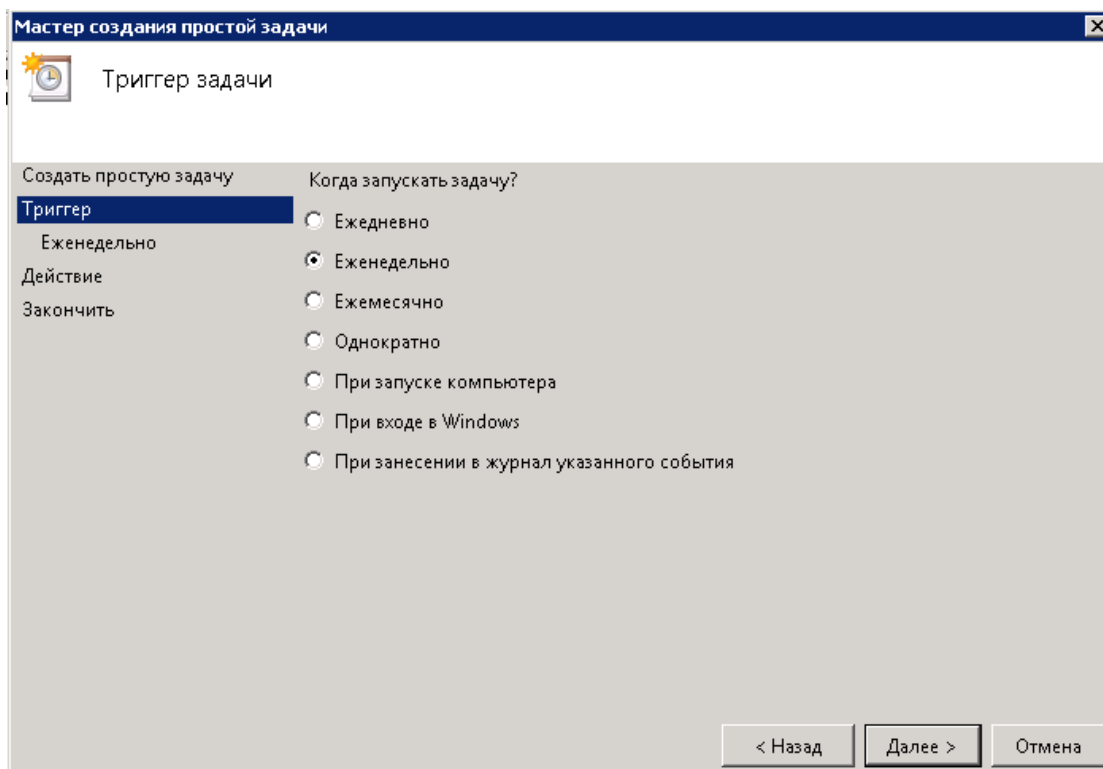
Сценарий полного резервного копирования необходимо планировать для запуска *после* выполнения сценария копирующей архивации.

В Windows 2008

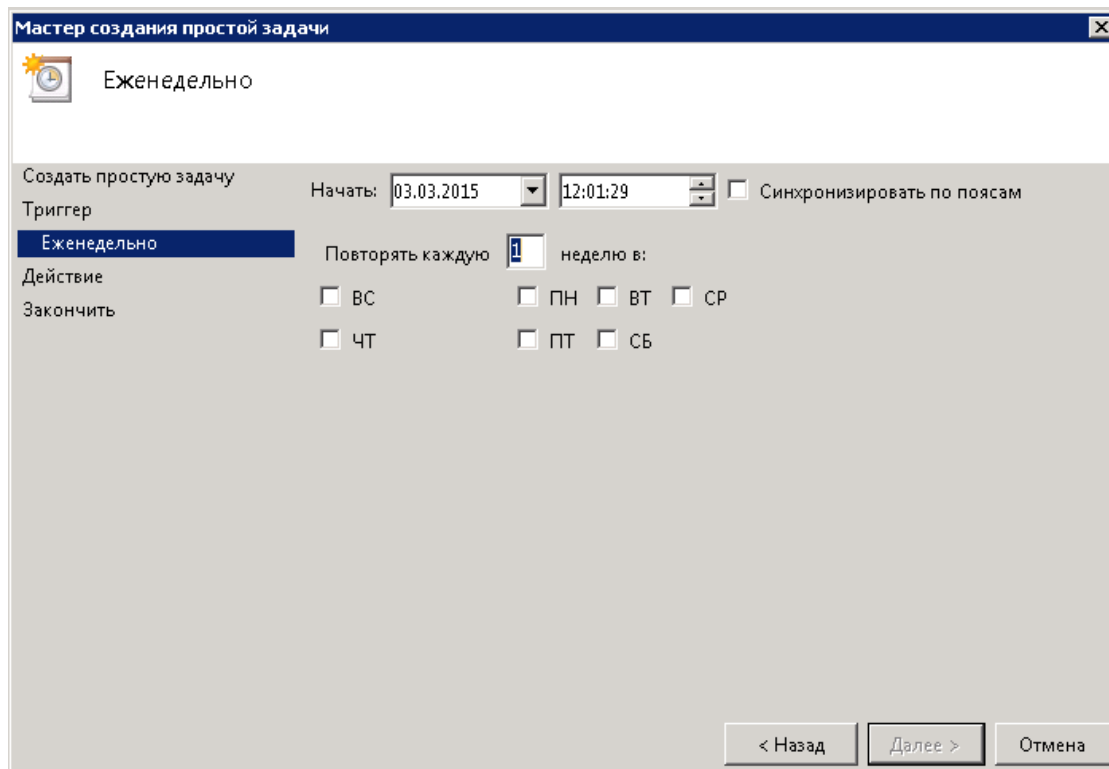
1. Перейдите к **Пуск > Программы > Администрирование > Планировщик задач**.
Откроется окно планировщика задач.
2. В окне планировщика задач щелкните правой кнопкой пункт **Создать базовую задачу**.
Откроется мастер создания базовой задачи. Введите имя задачи и нажмите кнопку **Далее**.



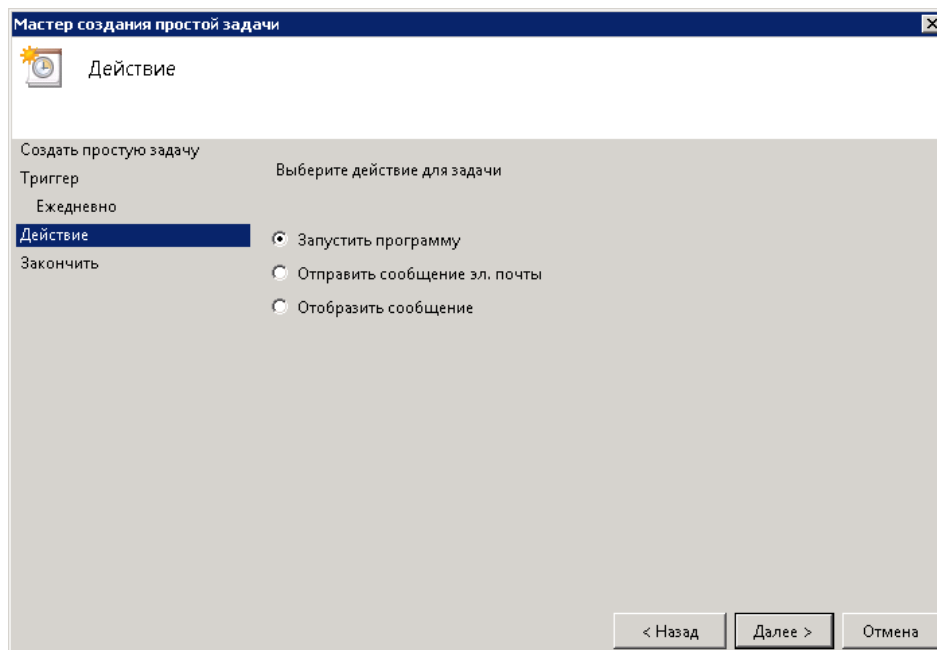
3. Выберите **Еженедельно** и нажмите кнопку **Далее**.



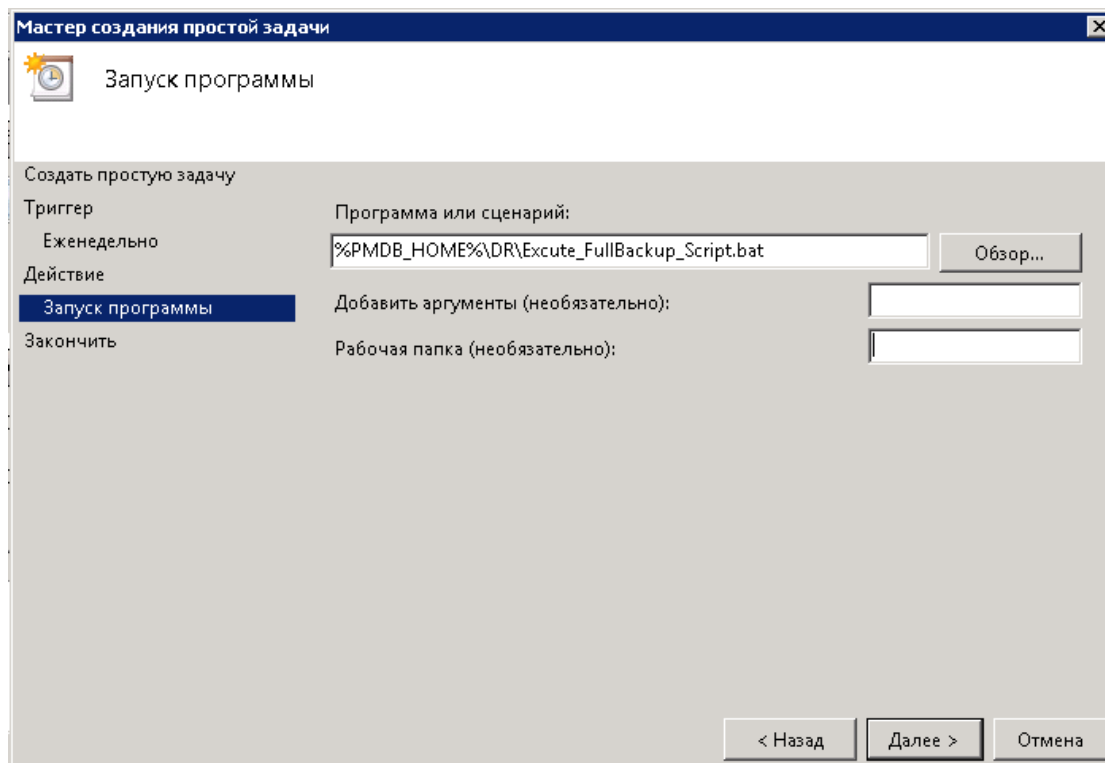
4. Выберите время начала, день недели, введите 1 в текстовое поле **Повтор каждые** и нажмите кнопку **Далее**.



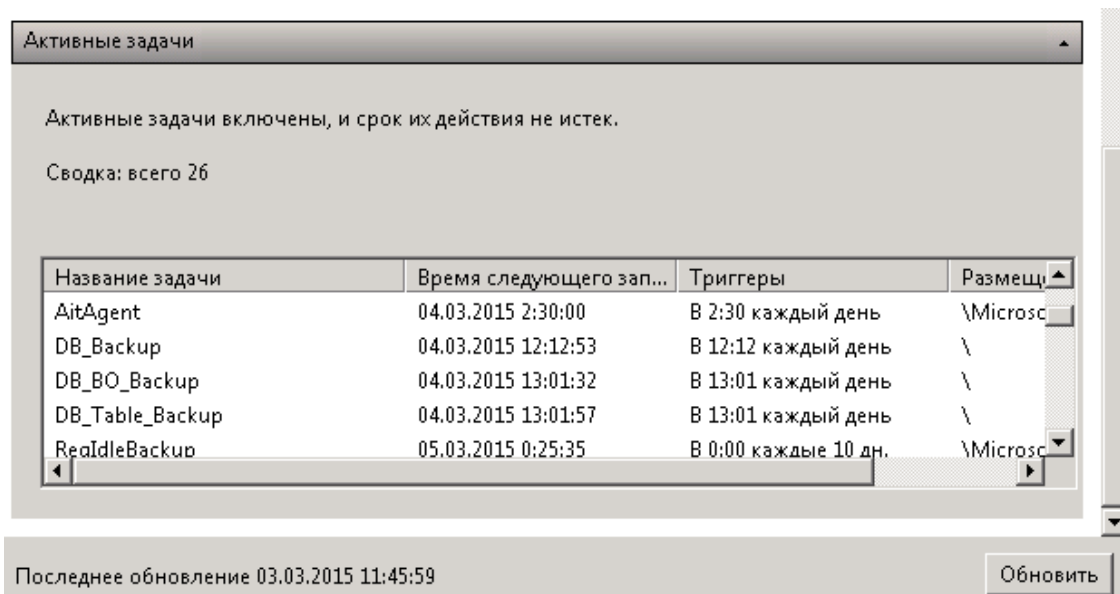
5. Выберите **Запустить программу** и нажмите кнопку **Далее**.



6. Перейдите в каталог %PMDV_HOME%\DR, выберите **Execute_FullBackup_Script.bat** и нажмите кнопку **Далее**.



7. Нажмите кнопку **Готово**. Вы можете проверить, создана ли задача, в разделе **Активные задачи** окна планировщика задач.

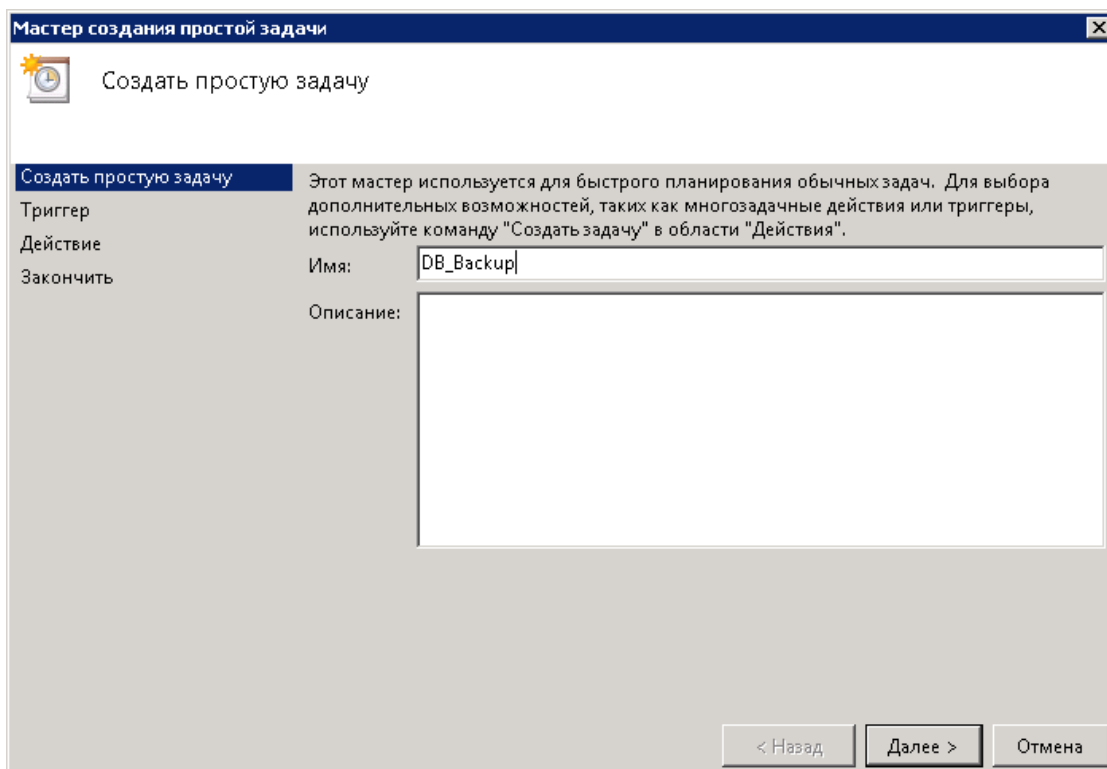


Планирование выполнения сценария добавочного резервного копирования

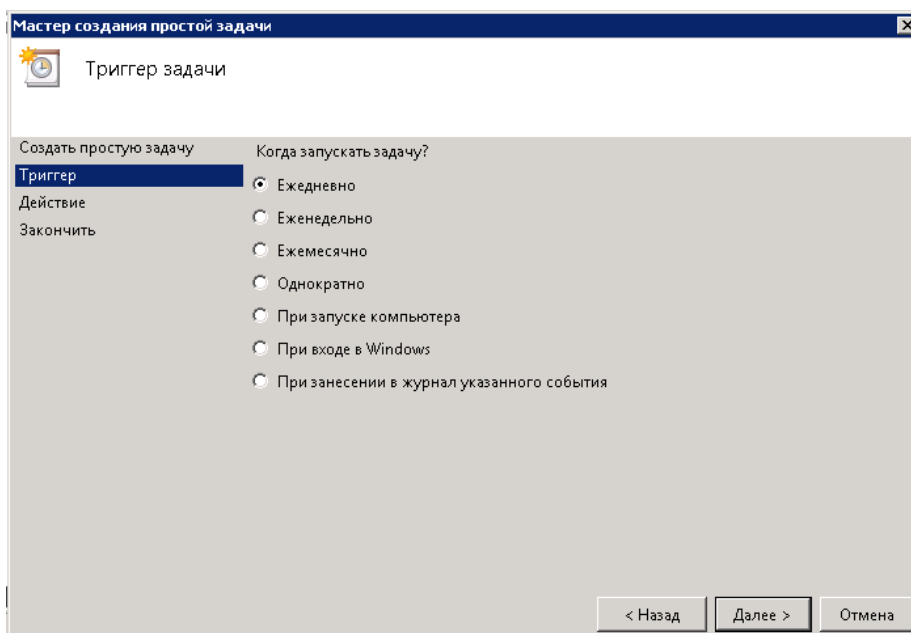
Сценарий добавочного резервного копирования необходимо планировать для выполнения раз в день.

В Windows 2008

1. Перейдите к **Пуск > Программы > Администрирование > Планировщик задач**.
Откроется окно планировщика задач.
2. В окне планировщика задач щелкните правой кнопкой пункт **Создать базовую задачу**.
Откроется мастер создания базовой задачи. Введите имя задачи и нажмите кнопку **Далее**.

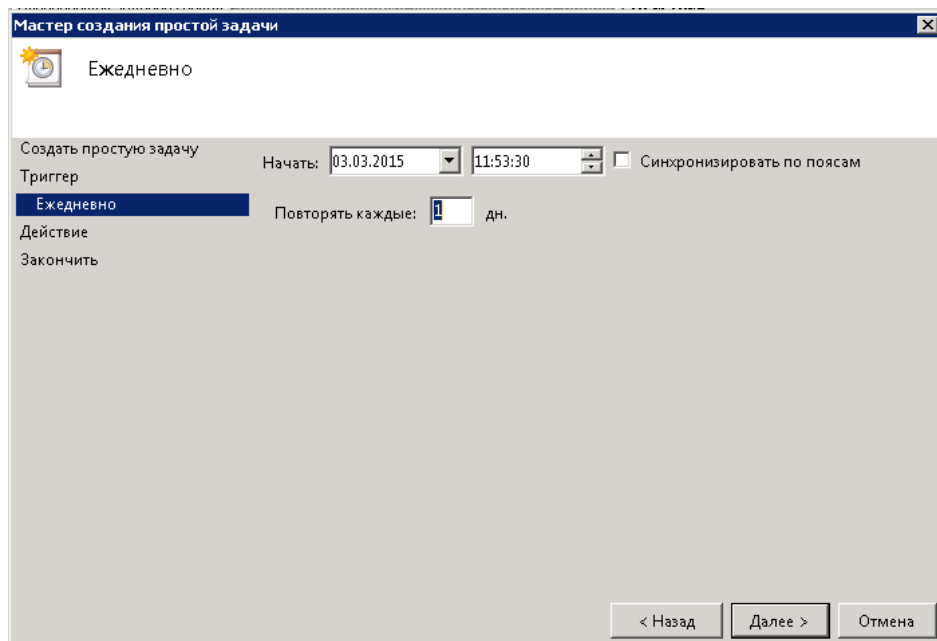


3. Выберите **Ежедневно** и нажмите кнопку **Далее**.

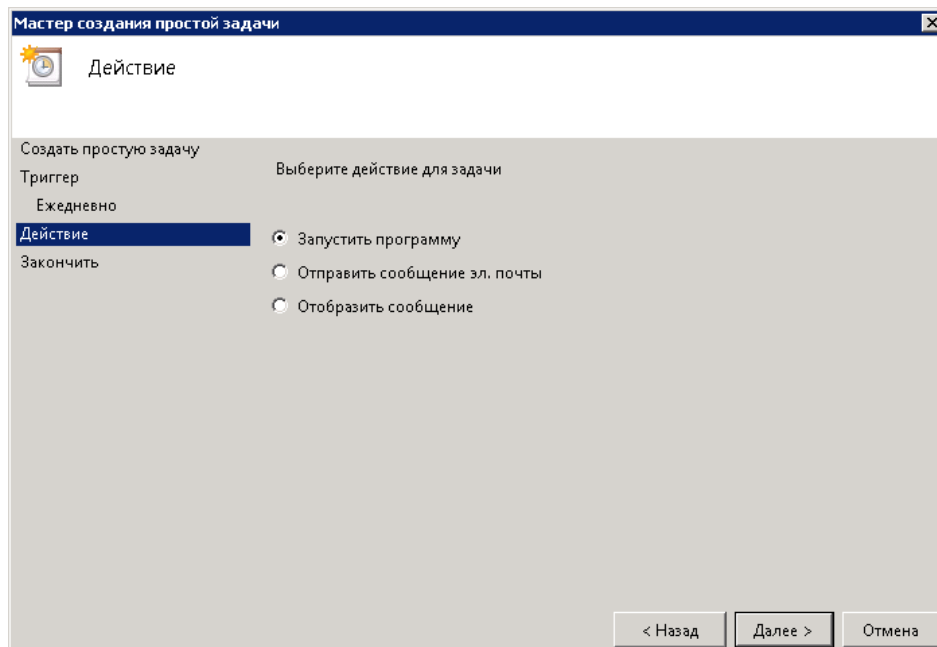


4. Выберите время начала и введите 1 в текстовое поле **Повтор каждые** и нажмите кнопку

Далее.

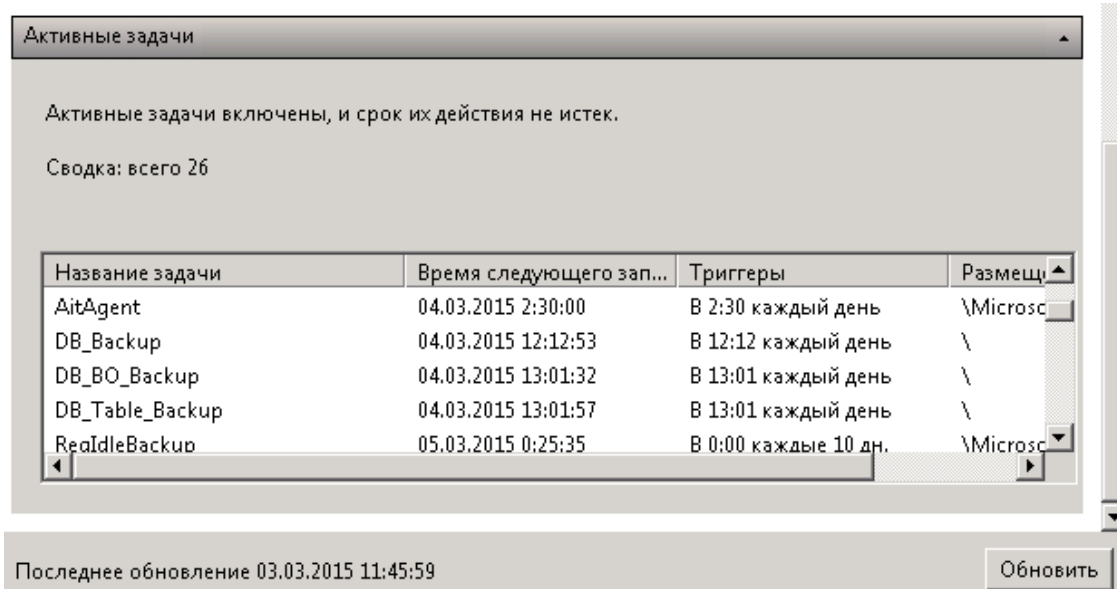


5. Выберите **Запустить программу** и нажмите кнопку **Далее**.



6. Перейдите в каталог %PMDV_HOME%\DR, выберите **Execute_IncSncFullBackup_Script.bat** и нажмите кнопку **Далее**.

7. Нажмите кнопку **Готово**. Вы можете проверить, создана ли задача, в разделе **Активные задачи** окна планировщика задач.



Для базы данных и хранилища файлов SAP BusinessObjects

В сценарии с выборочной установкой войдите в системы, на которых установлено приложение SAP BusinessObjects, и выполните следующие действия для восстановления.

Сценарий %PMDB_HOME%\DR\Execute_BO_FullBackup.bat позволяет создать резервную копию базы данных и хранилища файлов SAP BusinessObjects. Этот сценарий создаст резервные копии файлов лицензий, конфигурации CAC и настраиваемых файлов.

1. Перейдите к папке %PMDB_HOME%\DR.
2. Выполните следующую команду:

```
Execute_BO_FullBackup.bat <backup_path> <SAP_BusinessObjects_InstalledDrive>.
```

<backup_path> — это путь для сохранения файлов и данных резервных копий.

<SAP_BusinessObjects_InstalledDrive> — это диск, на котором установлено ПО SAP BusinessObjects.

Например: %PMDB_HOME%\DR> Execute_BO_FullBackup.bat C:\BO_backup C:\.

Ниже представлены примеры файлов резервных копий базы данных и хранилища файлов BusinessObjects:

SHRDisaster_Backup\Full_SQLAnWr_BackUP.Wed

Добавить в библиотеку ▾ Общий доступ ▾

Имя ^	Дата изменения
BOE120	20.02.2015 11:26
BOE120	20.02.2015 11:26
BOE120_AUDIT	20.02.2015 11:26
BOE120_AUDIT	20.02.2015 11:26
dbbackup_log	20.02.2015 11:26

SHRDisaster_BackupFull_BOFileStore_BackUP.Web\BO\Input

Добавить в библиотеку ▾ Общий доступ ▾ Новая папка





Имя ^	Дата изменения
a_000	02.03.2015 14:14
a_001	02.03.2015 14:14
a_002	02.03.2015 14:14
a_003	02.03.2015 14:14
a_004	02.03.2015 14:14
a_006	02.03.2015 14:14

Ниже представлены примеры файлов резервных копий файлов лицензий, конфигурации CAC и настраиваемых файлов:

Локальный диск (C:) ▾ SHRDisaster_Backup ▾

Библиотеку ▾ Общий доступ ▾ Новая папка

Имя ^	Дата изменения	Тип
Full_BOFileStore_BackUP.Tuesday	03.03.2015 13:33	Папка с файлами
Full_CAC_BackUP.Tuesday	03.03.2015 13:33	Папка с файлами
Full_Configuration_BackUP.Tuesday	03.03.2015 13:33	Папка с файлами
Full_SQLAnWr_BackUP.Tuesday	03.03.2015 13:34	Папка с файлами

Локальный диск (C:) \ SHRDisaster_Backup		
Библиотеку ▾ Общий доступ ▾ Новая папка		
Имя ^	Дата изменения	Тип
 Full_BOFileStore_BackUP.Tuesday	03.03.2015 13:33	Папка с файлами
 Full_CAC_BackUP.Tuesday	03.03.2015 13:33	Папка с файлами
 Full_Configuration_BackUP.Tuesday	03.03.2015 13:33	Папка с файлами
 Full_SQLAnWr_BackUP.Tuesday	03.03.2015 13:34	Папка с файлами

Сценарий создает следующие файлы журнала:

- BO_Backup_log.log - путь <bo_backup_path>\SHRDisaster_Backup\Full_BOFileStore_BackUP.<day of back up taken>

Пример: <bo_backup_path>\SHRDisaster_Backup\Full_BOFileStore_BackUP.Wednesday

- dbbackup_log.log - путь <bo_backup_path>\SHRDisaster_Backup\Full_SQLAnWr_BackUP.<day of back up taken>

Пример: <bo_backup_path>\SHRDisaster_Backup\Full_SQLAnWr_BackUP.Wednesday

- Config_backup_log.log - файлы журналов для файлов лицензий и конфигурации, путь <bo_backup_path>\SHRDisaster_Backup\Full_Configuration_BackUP.<day of back up taken>

Пример: <bo_backup_path>\SHRDisaster_Backup\Full_Configuration_BackUP.Tuesday

- customgroup_backup_log.log - файлы журналов для настраиваемых XML-файлов, путь <bo_backup_path>\SHRDisaster_Backup\Full_Configuration_BackUP.<day of back up taken>

Пример: <bo_backup_path>\SHRDisaster_Backup\Full_Configuration_BackUP.Tuesday

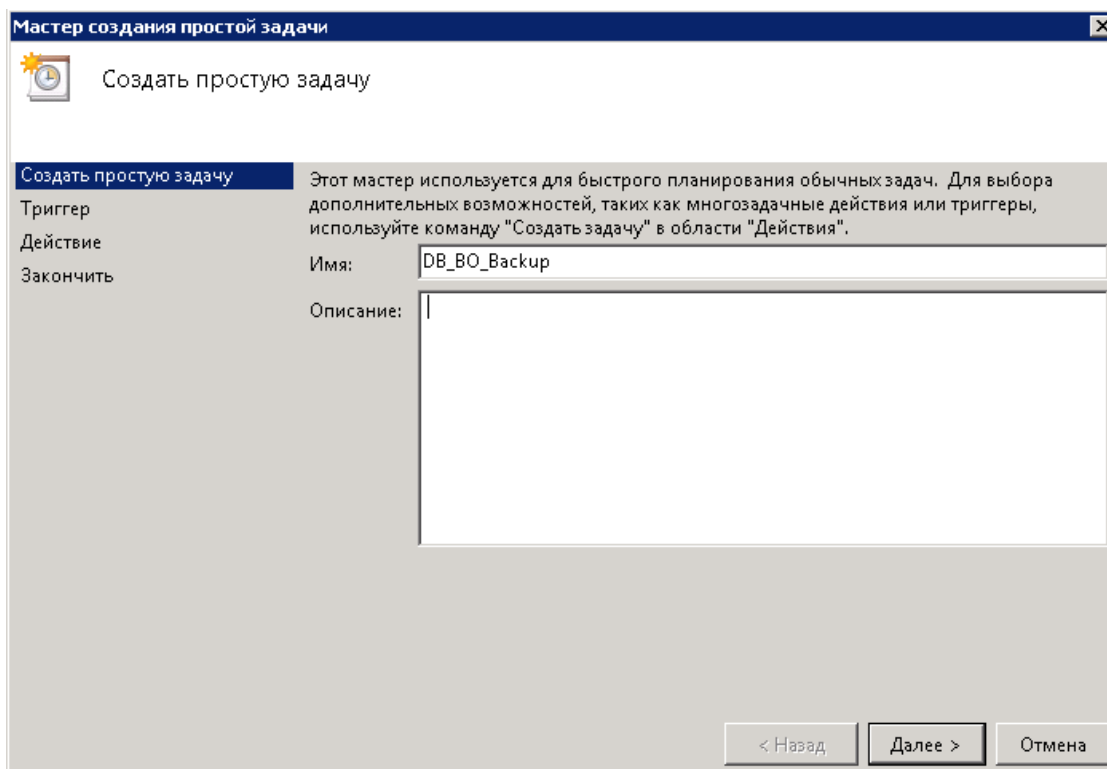
- CAC_backup_log.log - файлы журналов для файлов CAC, путь <bo_backup_path>\SHRDisaster_Backup\Full_CAC_BackUP.<day of back up taken>

Пример: <bo_backup_path>\SHRDisaster_Backup\Full_CAC_BackUP.Tuesday

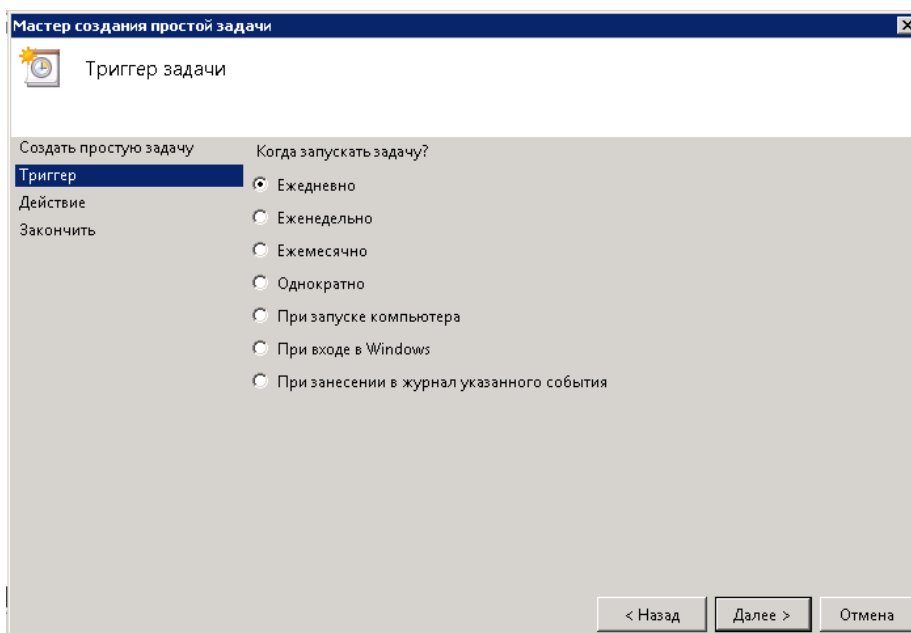
Для планирования резервного копирования выполните следующие действия:

В Windows 2008

1. Перейдите к **Пуск > Программы > Администрирование > Планировщик задач**. Откроется окно планировщика задач.
2. В окне планировщика задач щелкните правой кнопкой пункт **Создать базовую задачу**. Откроется мастер создания базовой задачи. Введите имя задачи и нажмите кнопку **Далее**.

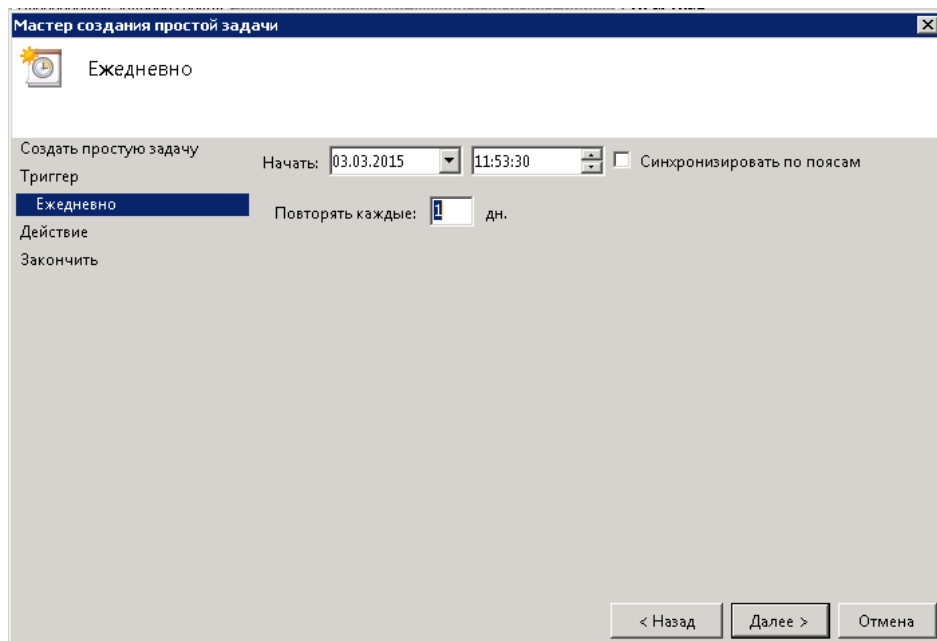


3. Выберите **Ежедневно** и нажмите кнопку **Далее**.

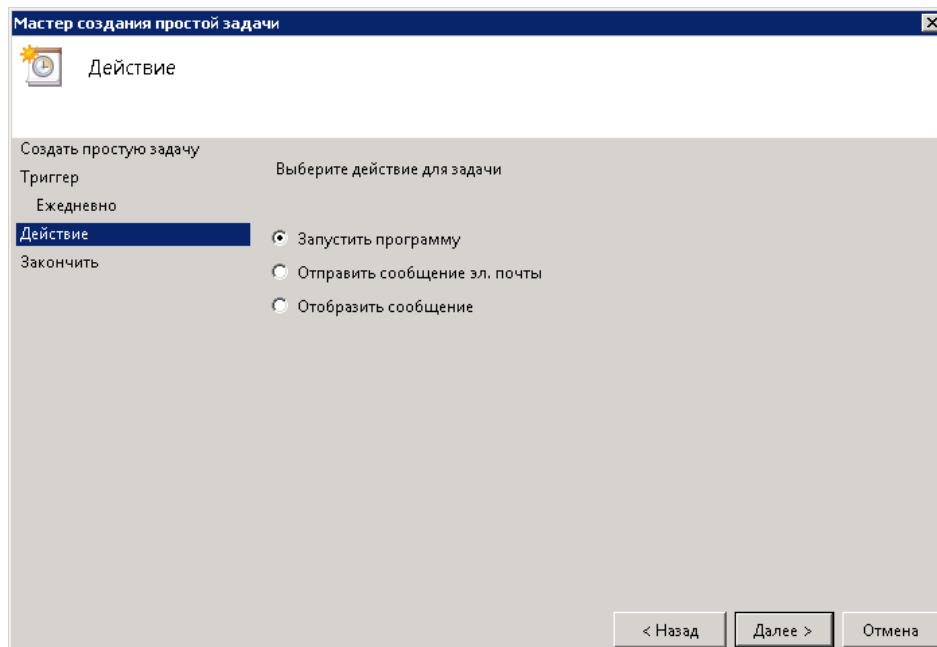


4. Выберите время начала и введите 1 в текстовое поле **Повтор каждые** и нажмите кнопку

Далее.

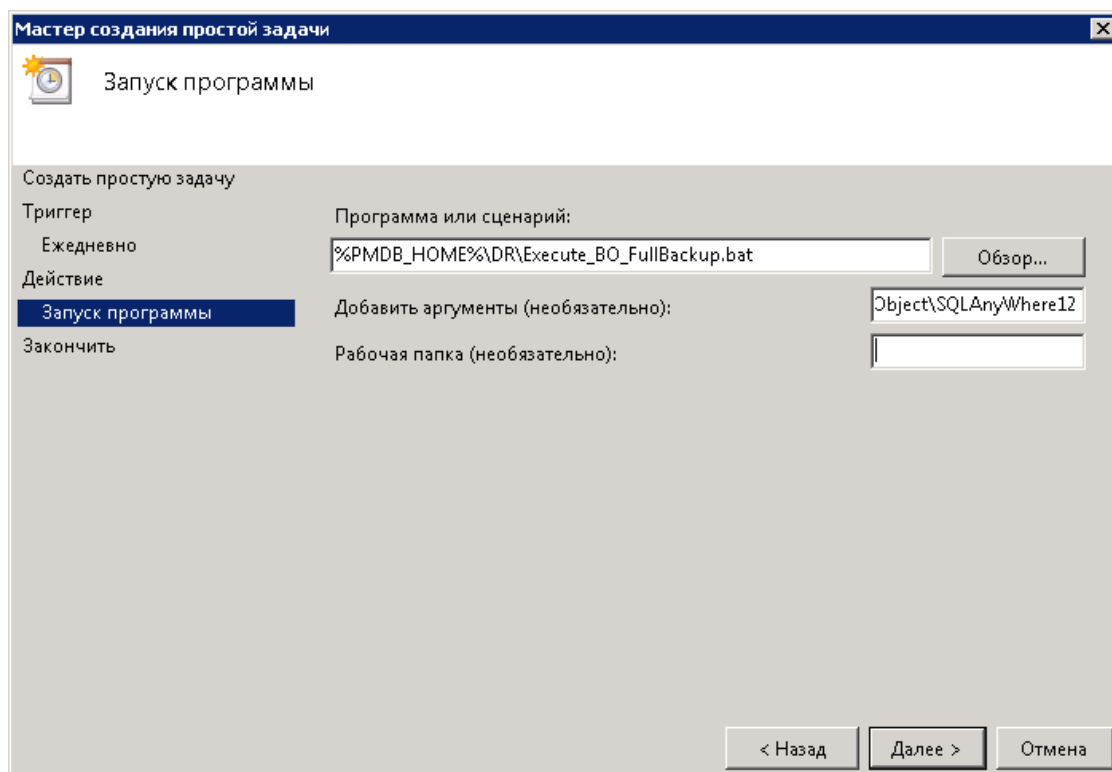


5. Выберите **Запустить программу** и нажмите кнопку **Далее**.



6. Перейдите в каталог %PMDV_HOME%\DR, выберите **Execute_BO_FullBackup.bat** и нажмите

кнопку **Далее**.



7. В поле «Добавить аргументы» введите следующие сведения:

`<backup_path> <SAP_BusinessObjects_InstalledDrive>`

Примечание. Используйте пробел между двумя элементами.

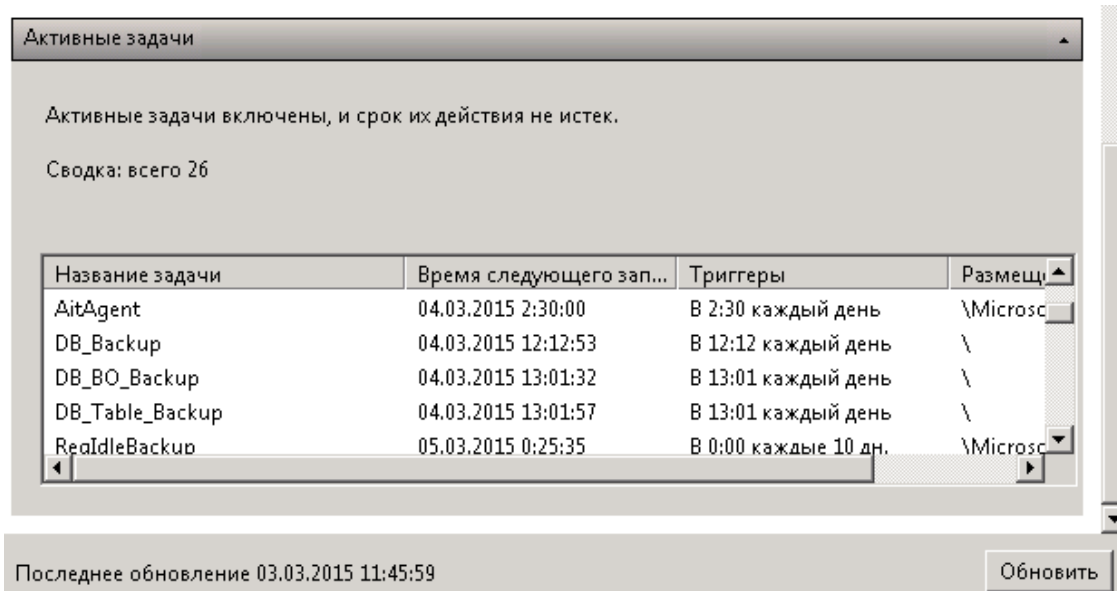
В данном случае:

- `<backup_path>` — это путь для сохранения файлов и данных резервных копий.
- `<SAP_BusinessObjects_InstalledDrive>` — это диск, на котором установлено ПО SAP BusinessObjects. Значение по умолчанию: C:\ drive. Если при установке SHR для SAP BusinessObjects выбран другой диск, укажите его.

Пример: C:\BO_backup C:\

Примечание. Если вы хотите сохранить файлы в настраиваемую папку, ее необходимо создать заранее.

8. Нажмите кнопку **Готово**. Вы можете проверить, создана ли задача, в разделе **Активные задачи** окна планировщика задач.



Для таблицы базы данных управления

При выборочной установке выполните следующие действия на основном сервере SHR, чтобы создать резервную копию базы данных управления.

Задача 1: Редактирование сценариев резервного копирования

SHR содержит сценарии %PMDB_HOME%\scripts\MgmtDB\Postgres\backup_aggregate_control.sql and %PMDB_HOME%\DR\DB_tables_backup.bat для резервного копирования таблицы базы данных управления. Вы должны вручную отредактировать сценарий backup_aggregate_control.sql, чтобы указать расположение резервных копий. Для редактирования сценария выполните следующие действия:

1. Перейдите в папку %PMDB_HOME%\scripts\MgmtDB\Postgres.
2. Откройте файл backup_aggregate_control.sql в текстовом редакторе.
3. Перейдите к следующей строке:

```
\copy dwabc.AGGREGATE_CONTROL TO 'E:\\bo_backup\\backup_AGGREGATE_CONTROL.dat'
```

4. Замените E:\\bo_backup каталогом, в который вы хотите поместить резервные копии.

Совет. При вводе пути к каталогу используйте \\ вместо \.

5. Сохраните файл.
6. Выполните файл DB_tables_backup.bat из каталога %PMDB_HOME%\DR.

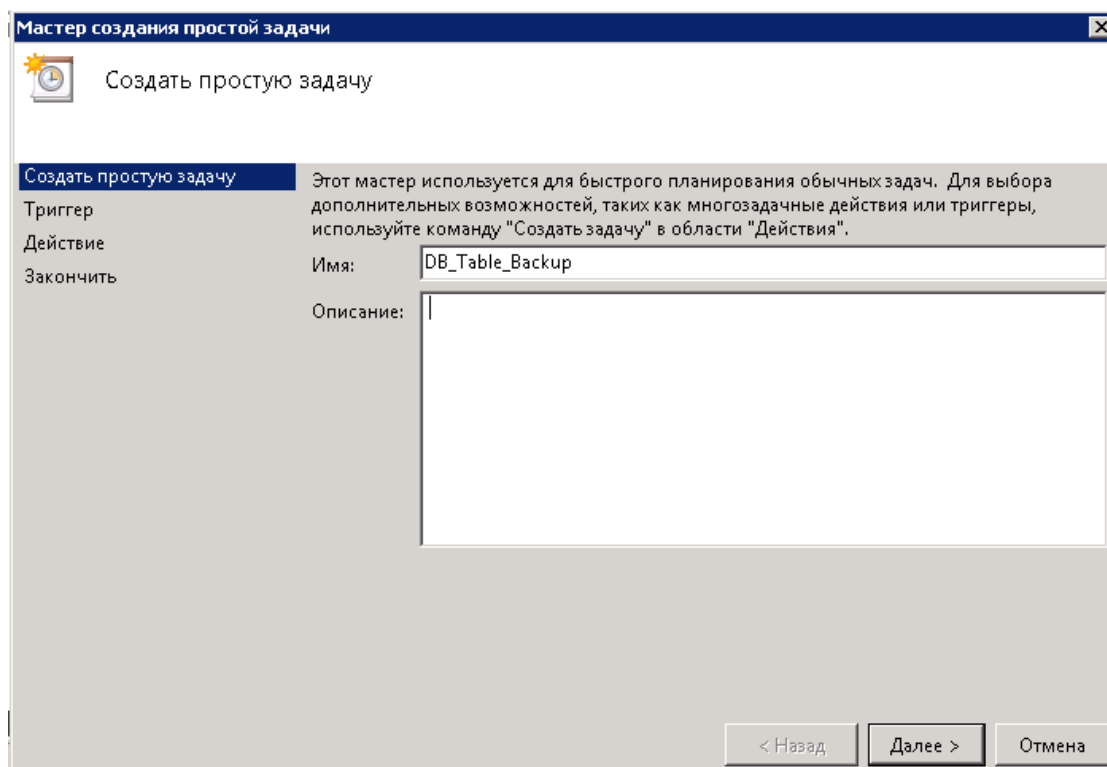
Вы можете проверить резервную копию базы данных в файле backup.AGGREGATE_CONTROL.dat.

Задача 2: Планирование выполнения сценария резервного копирования

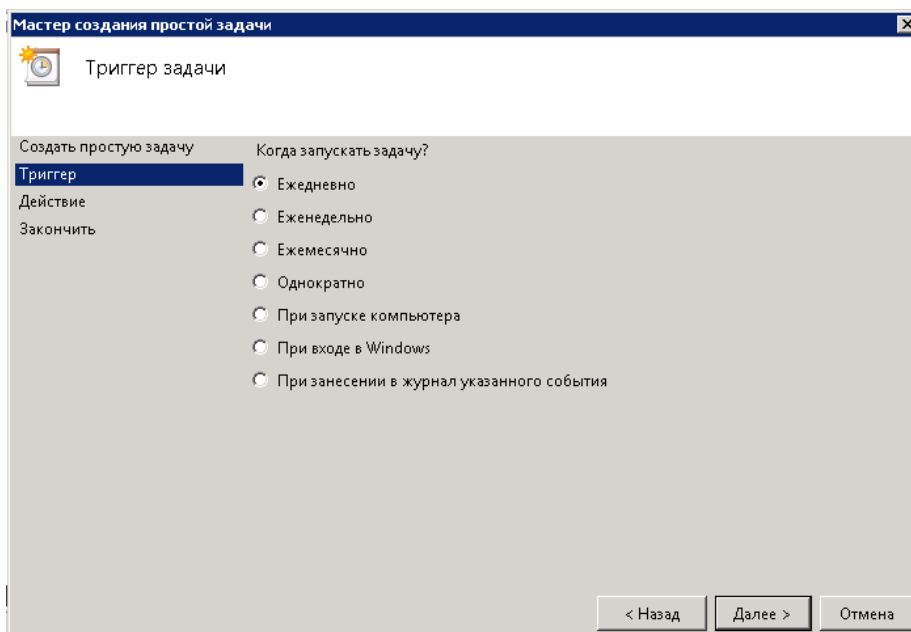
Сценарий резервного копирования необходимо планировать для выполнения раз в день.

В Windows 2008

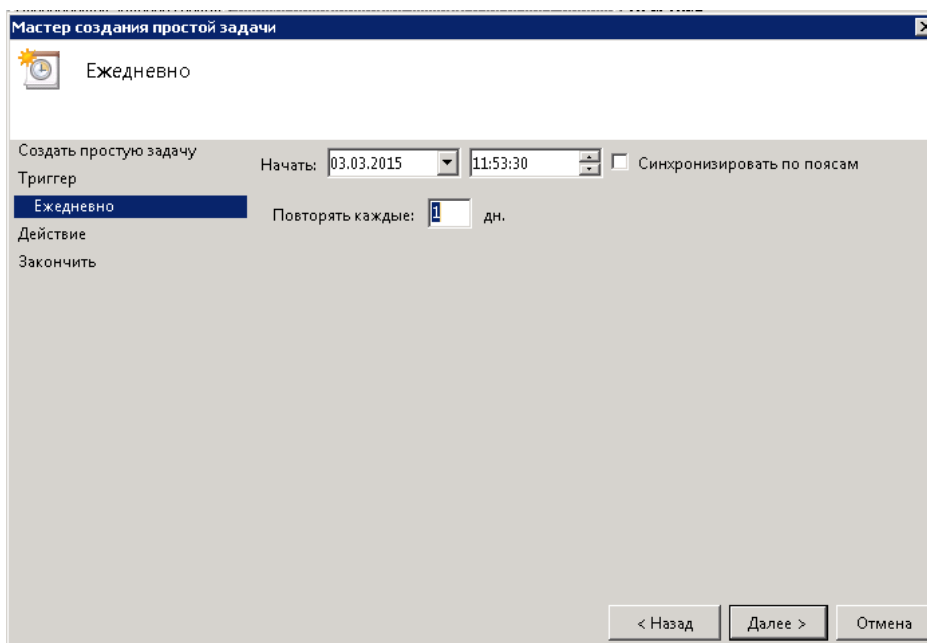
1. Перейдите к **Пуск > Программы > Администрирование > Планировщик задач**. Откроется окно планировщика задач.
2. В окне планировщика задач щелкните правой кнопкой пункт **Создать базовую задачу**. Откроется мастер создания базовой задачи. Введите имя задачи и нажмите кнопку **Далее**.



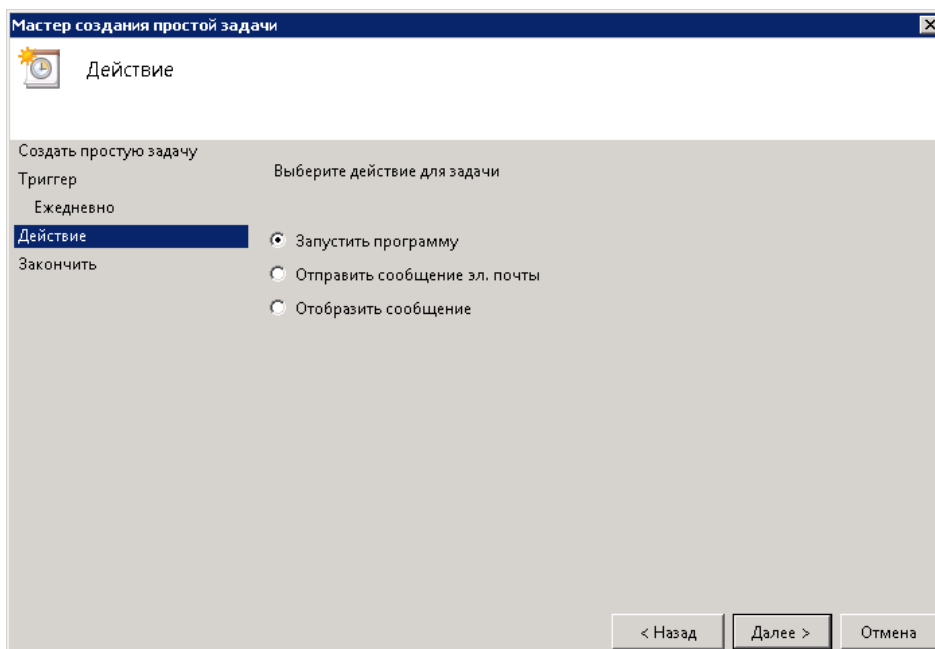
3. Выберите **Ежедневно** и нажмите кнопку **Далее**.



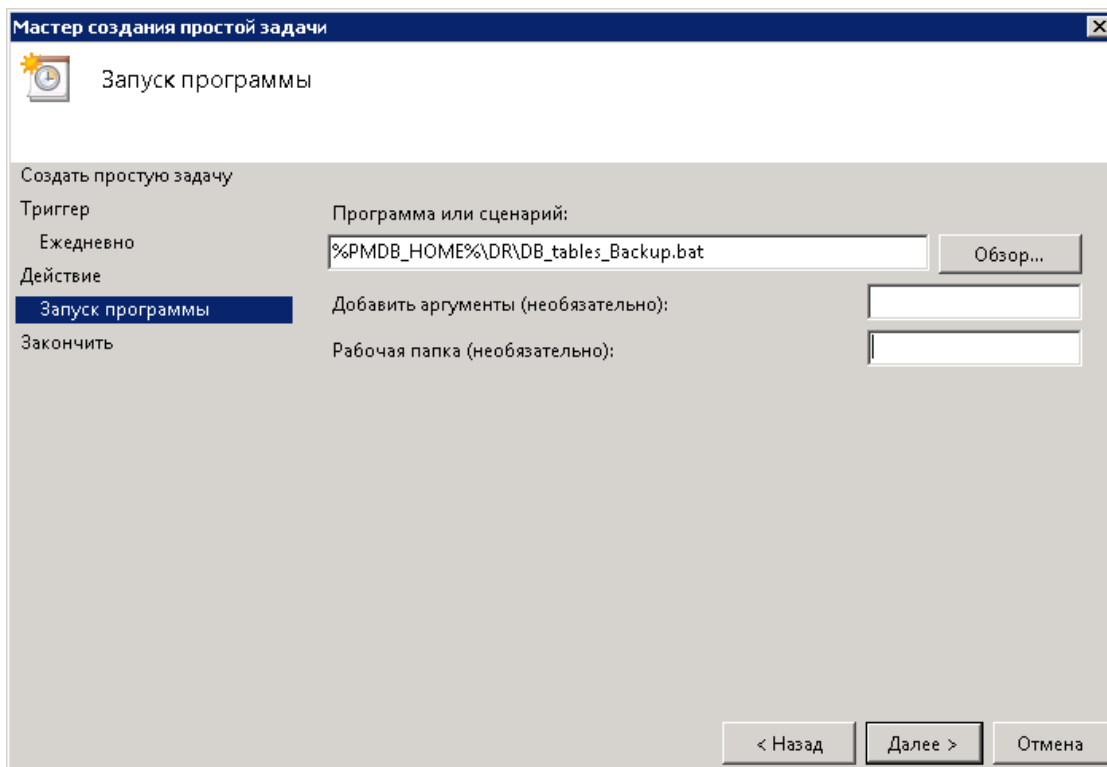
4. Выберите время начала и введите 1 в текстовое поле «Повтор каждые» и нажмите кнопку **Далее**.



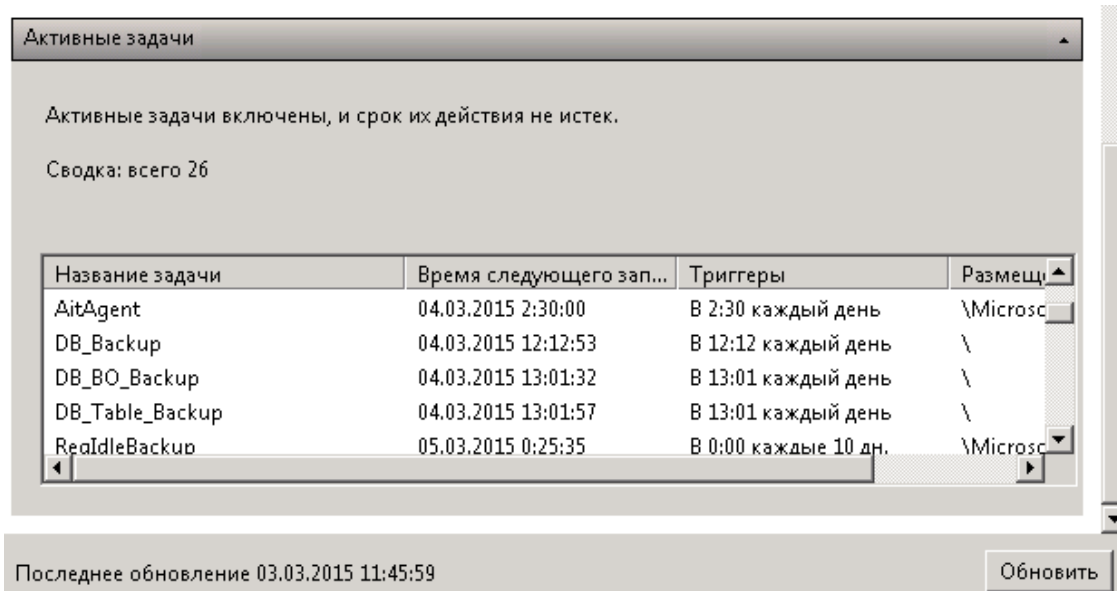
5. Выберите **Запустить программу** и нажмите кнопку **Далее**.



6. Перейдите в каталог %PMDB_HOME%\DR, выберите **DB_tables_Backup.bat** и нажмите кнопку **Далее**.



7. Нажмите кнопку **Готово**. Вы можете проверить, создана ли задача, в разделе **Активные задачи** окна планировщика задач.



Создание резервной копии баз данных SHR в Linux Для базы данных Sybase IQ

При выборочной установке выполните следующие действия на основном сервере SHR, чтобы создать резервную копию базы данных Sybase IQ.

Совет. Вы должны указать путь к удаленной базе данных Sybase IQ.

Задача 1: Редактирование сценариев резервного копирования

SHR включает два сценария резервного копирования для полного и инкрементного резервного копирования. Перед началом резервного копирования отредактируйте эти сценарии в соответствии со своими требованиями.

Сценарии находятся в каталоге `$PMDB_HOME/scripts/Sybase`.

Файлы сценариев:

- Для полного резервного копирования: `IQ_backup_full.sql`.
- Для добавочного резервного копирования: `IQ_backup_incr_since_full.sql`

Для редактирования сценариев выполните следующие действия:

1. Перейдите в папку `$PMDB_HOME/scripts/Sybase`.
2. Откройте файл `IQ_backup_full.sql` в текстовом редакторе.
3. В последнем параметре сценария `.sql` создайте каталог для сохранения файлов резервных копий. То есть замените `расположение_резервной_копии` на желаемое расположение.

Пример:

Строка по умолчанию	После изменения
<code>dsi_pmdb_backup</code>	<code>dsi_pmdb_backup</code>
<code>'FULL',NULL,'READWRITE_FILES_ONLY',NULL,NULL,NULL,NULL,'D','location_for_backup'</code>	<code>'FULL',NULL,'READWRITE_FILES_ONLY',NULL,NULL,NULL,NULL,'D','/backup'</code>

4. Аналогичным образом для сценария добавочного резервного копирования (`IQ_backup_incr_since_full.sql`) замените строку `location_for_backup` фактическим расположением резервной копии.

Пример:

Строка по умолчанию	После изменения
<code>dsi_pmdb_backup</code>	<code>dsi_pmdb_backup</code>
<code>'INCREMENTAL_SINCE_FULL',NULL,'READWRITE_FILES_ONLY',NULL,NULL,NULL,NULL,'D','расположение_резервной_копии'</code>	<code>'INCREMENTAL_SINCE_FULL',NULL,'READWRITE_FILES_ONLY',NULL,NULL,NULL,NULL,'D','/backup'</code>

Совет. Для удаленной установки Sybase IQ значение параметра `location_for_backup` должно быть расположением на удаленном сервере БД.

Выполните сценарии `.sql`, используя следующие сценарии оболочки:

- `Execute_FullBackup_Script.sh` (полное резервное копирование)
- `Execute_IncSncFullBackup_Script.sh` (добавочное резервное копирование)

Эти сценарии оболочки находятся в каталоге `$PMDB_HOME/DR`.

После выполнения этих сценариев к имени создаваемой резервной копии базы данных добавляется день недели в указанном местоположении.

Например:

`Full backup`


```
Full.tuesday.1 Full.tuesday.2
```

```
Incr backup
```

```
Incr_sncfull.tuesday.1
```

Сценарии создают следующие файлы журнала:

- Полное резервное копирование - \$PMDB_HOME/tmp/Execute_IQ_backup_full.out
- Добавочное резервное копирование - \$PMDB_HOME/tmp/Execute_backup_incr_since_full.out

Задача 2: Измените сценарии копирования

SHR включает сценарий для копирования файлов резервной копии в определенный каталог.

Для редактирования сценария копирования, прежде чем приступить к полному резервному копированию, укажите расположение резервной копии базы данных и желаемое расположение для копирования файлов. Вы должны запустить сценарий в системе, в которой установлена база данных Sybase IQ.

```
cp "location of existing full backup file" "copy to location"> $PMDB_HOME/tmp/Copy_Backup.txt 2>&1
```

Замените location of existing full backup и copy to location фактическими расположениями.

Пример сценария:

```
cp "/disk1/HP-SHR/Backup/Full*" "/disk1/HP-SHR/Backup/Old/" > $PMDB_HOME/tmp/Copy_Backup.txt 2>&1
```

Задача 3: Планирование резервного копирования

Для выполнения регулярного резервного копирования базы данных необходимо планировать запуск сценариев резервного копирования, используя планировщик Linux CronJobs. Полное резервное копирование рекомендуется выполнять раз в неделю, добавочное резервное копирование — раз в день.

Сценарий копирующей архивации создает копию файлов полного резервного копирования базы данных в указанном месте во избежание перезаписи поверх существующей резервной копии. Сценарий копирующей архивации необходимо планировать для запуска каждый раз перед выполнением сценария полного резервного копирования.

Для настройки планировщика CronJobs в Linux выполните следующие действия.

1. Для изменения файла crontab введите следующую команду в терминале Linux:

```
crontab -e
```

2. Запланируйте ежедневное выполнение сценария копирующей архивации:

Введите следующую строку в файле crontab.

```
0 15 * * * /opt/HP/BSM/PMDB/DR/Copy_Backup.sh
```

В приведенном выше примере сценарий копирующей архивации выполняется ежедневно в 15:00 часов.

3. Запланируйте еженедельное выполнение сценария полного резервного копирования:

Введите следующую строку в файле `crontab`.

```
0 15 * * 1 /opt/HP/BSM/PMDB/DR/Execute_FullBackup_Script.sh
```

В приведенном выше примере сценарий полного резервного копирования выполняется в первый день недели в 15:00 часов.

4. Запланируйте ежедневное выполнение сценария добавочного резервного копирования:

Введите следующую строку в файле `crontab`.

```
0 15 * * * /opt/HP/BSM/PMDB/DR/Execute_IncSncFullBackup_Script.sh
```

В приведенном выше примере сценарий добавочного резервного копирования выполняется ежедневно в 15:00 часов.

5. После добавления записей сохраните файл `crontab`.

Все файлы журнала для `crontab` находятся в каталоге `/var/mail`.

Для базы данных и хранилища файлов SAP BusinessObjects

В сценарии с выборочной установкой войдите в системы, на которых установлено приложение SAP BusinessObjects, и выполните следующие действия для восстановления.

Сценарий `$PMDB_HOME/DR/Execute_BO_FullBackup.sh` позволяет создать резервную копию базы данных и хранилища файлов SAP BusinessObjects. Этот сценарий создаст резервные копии файлов лицензий, конфигурации CAC и настраиваемых файлов.

1. Перейдите к папке `$PMDB_HOME/DR`.
2. Выполните сценарий `Execute_BO_FullBackup.sh<backup_path>`.

Например: `$PMDB_HOME/DR> Execute_BO_FullBackup.sh/bo_backup`.

Ниже представлены примеры файлов резервных копий базы данных и хранилища файлов BusinessObjects:

```
[root@IWFVM0123480E120 bo_backup]# cd SHRDisaster_Backup/
[root@IWFVM0123480E120 SHRDisaster_Backup]# ls
Full_BOFileStore_BackUP.Wed Full_SQLAnWr_BackUP.Wed
[root@IWFVM0123480E120 SHRDisaster_Backup]# cd Full_BOFileStore_BackUP.Wed/
[root@IWFVM0123480E120 Full_BOFileStore_BackUP.Wed]# ls
BO_Backup_log.log frsinput frsoutput
[root@IWFVM0123480E120 Full_BOFileStore_BackUP.Wed]# cd frsinput/
[root@IWFVM0123480E120 frsinput]# ls
a_000 a_011 a_021 a_030 a_040 a_049 a_057 a_066 a_075 a_086 a_093 a_100 a_107 a_114 a_127 a_136 a_143 a_159 a_230 a_239 a_248
a_002 a_013 a_022 a_032 a_041 a_050 a_058 a_067 a_077 a_087 a_094 a_101 a_108 a_115 a_130 a_137 a_144 a_160 a_231 a_240 a_249
a_003 a_014 a_023 a_033 a_043 a_051 a_059 a_068 a_079 a_088 a_095 a_102 a_109 a_116 a_131 a_138 a_145 a_219 a_232 a_242 a_251
a_004 a_015 a_025 a_034 a_044 a_052 a_061 a_070 a_081 a_089 a_096 a_103 a_110 a_117 a_132 a_139 a_146 a_225 a_233 a_243 a_252
a_006 a_017 a_026 a_036 a_045 a_054 a_062 a_071 a_082 a_090 a_097 a_104 a_111 a_118 a_133 a_140 a_147 a_226 a_234 a_244 a_253
a_007 a_018 a_028 a_038 a_047 a_055 a_063 a_073 a_083 a_091 a_098 a_105 a_112 a_119 a_134 a_141 a_155 a_227 a_236 a_245 a_254
a_009 a_019 a_029 a_039 a_048 a_056 a_064 a_074 a_084 a_092 a_099 a_106 a_113 a_121 a_135 a_142 a_156 a_228 a_237 a_247 temp
```

```
[root@IWFVM0123480E120 SHRDisaster_Backup]# cd Full_SQLAnWr_BackUP.Wed/
[root@IWFVM0123480E120 Full_SQLAnWr_BackUP.Wed]# ls
dbbackup_log.log IWFVM0123480E120_AUDIT.db IWFVM0123480E120_AUDIT.log IWFVM0123480E120.db IWFVM0123480E120.log
```

Ниже представлены примеры файлов резервных копий файлов лицензий, конфигурации CAC и настраиваемых файлов:

```
[root@iwfvm05326 SHRDisaster_Backup]# ls
Full_BOFileStore_BackUP.Tuesday Full_CAC_BackUP.Tuesday Full_Configuration_BackUP.Tuesday Full_SQLAnWr_BackUP.Tuesday
[root@iwfvm05326 SHRDisaster_Backup]#
```

Сценарий создает следующие файлы журнала:

- BO_Backup_log.log - located at <bo_backup_path>/SHRDisaster_Backup/Full_BOFileStore_BackUP.<day of back up taken>

Пример: <bo_backup_path>/SHRDisaster_Backup/Full_BOFileStore_BackUP.Wednesday

- dbbackup_log.log - путь <bo_backup_path>/SHRDisaster_Backup/Full_SQLAnWr_BackUP.<day of back up taken>

Пример: <bo_backup_path>/SHRDisaster_Backup/Full_SQLAnWr_BackUP.Wednesday

- Config_backup_log.log - файлы журналов для файлов лицензий и конфигурации, путь <bo_backup_path>/SHRDisaster_Backup/Full_Configuration_BackUP.<day of back up taken>

Пример: <bo_backup_path>/SHRDisaster_Backup/Full_Configuration_BackUP.Tuesday

- customgroup_backup_log.log - файлы журналов для настраиваемых XML-файлов, путь <bo_backup_path>/SHRDisaster_Backup/Full_Configuration_BackUP.<day of back up taken>

Пример: <bo_backup_path>/SHRDisaster_Backup/Full_Configuration_BackUP.Tuesday

- CAC_Backup_log.log - файлы журналов для файлов CAC, путь <bo_backup_path>/SHRDisaster_Backup/Full_CAC_BackUP.<day of back up taken>

Пример: <bo_backup_path>/SHRDisaster_Backup/Full_CAC_BackUP.Tuesday

Для планирования резервного копирования выполните следующие действия:

1. Выполните вход в систему SHR от имени пользователя root.
2. Для изменения файла crontab введите следующую команду в командной строке:

```
crontab -e
```
3. Добавьте строку в файл crontab для вызова сценария /opt/HP/BSM/PMDB/scripts/DR/DB_tables_backup.sh один раз в неделю.

Пример:

```
0 15 * * 1 /opt/HP/BSM/PMDB/DR/Execute_BO_FullBackup.sh /root/SHR_Backup
```

В примере выше сценарий /opt/HP/BSM/PMDB/DR/Execute_BO_FullBackup.sh выполняется ежедневно в 15:00, и данные сохраняются в папке /root/SHR_Backup.

4. Сохраните файл crontab.

Все файлы журнала для crontab находятся в каталоге /var/mail.

Для таблиц базы данных управления

При выборочной установке выполните следующие действия на основном сервере SHR, чтобы создать резервную копию базы данных управления.

Сценарий DB_Tables_Backup.sh обеспечивает резервное копирование таблиц базы данных управления. Перед планированием выполнения сценария измените сценарий backup_aggregate_control.sql, который используется DB_Tables_Backup.sh.

Задача 1: Измените сценарий backup_aggregate_control.sql

1. Откройте сценарий backup_aggregate_control.sql в каталоге \$PMDB_HOME/scripts/MgmtDB/Postgres в текстовом редакторе.
2. Найдите следующую строку:

```
Copy AGGREGATE_CONTROL TO '<Path of the backupfile>/backup_AGGREGATE_CONTROL.dat'
```

3. Замените <Path of the backupfile> расположением для сохранения резервной копии файл базы данных управления. Не указывайте каталог, который не существует в системе.

Например, для сохранения резервной копии файла базы данных управления в каталоге /tmp/dbtables замените <Path of the backupfile> на /tmp/dbtables.

4. Сохраните файл.
5. Запустите файл DB_tables_backup.sh из каталога \$PMDB_HOME/DR

Вы можете проверить резервную копию базы данных в файле backup.AGGREGATE_CONTROL.dat.

Задача 2: Запланируйте выполнение сценария DB_Tables_Backup.sh

1. Выполните вход в систему SHR от имени пользователя root.
2. Для изменения файла crontab введите следующую команду в командной строке:

```
crontab -e
```
3. Добавьте строку в файл crontab для вызова сценария /opt/HP/BSM/PMDB/scripts/DR/DB_tables_backup.sh один раз в день.

Пример:

```
0 15 * * * /opt/HP/BSM/PMDB/scripts/DR/DB_tables_backup.sh
```

В примере выше сценарий /opt/HP/BSM/PMDB/scripts/DR/DB_tables_backup.sh выполняется ежедневно в 15:00.

4. Сохраните файл crontab.

Все файлы журнала для crontab находятся в каталоге /var/mail.

Восстановление баз данных SHR

Перед восстановлением резервных копий данных, необходимо установить SHR в системе с помощью носителей. По окончании установки вы должны будете отправить все данные резервных копий в локальный каталог системы.

Восстановление SHR в Windows

Для базы данных Sybase IQ

В сценарии с выборочной установкой войдите в системы, на которых установлено приложение Sybase IQ, и выполните следующие действия для восстановления.

1. Остановите службу HP_PMDB_Platform_Sybase, выполнив следующие действия:
 - a. Выберите **Пуск > Выполнить**. Откроется диалоговое окно «Выполнить».
 - b. Введите services.msc в поле **Открыть** и нажмите клавишу **ВВОД**. Откроется окно «Службы».
 - c. В правой части окна щелкните правой кнопкой мыши элемент **HP_PMDB_Platform_Sybase** и выберите команду **Остановить**.
 - d. В диспетчере задач Windows выберите вкладку **Процессы**, найдите процесс iqsrv15.exe, щелкните его правой кнопкой мыши и выберите **Завершить процесс**.

2. Выполните поиск всех файлов с расширениями `.db`, `.log` и `.iq` в каталоге, где расположен файл базы данных, и переместите эти файлы в любой другой каталог в системе. Эти файлы создаются заново в процессе восстановления.
3. Запустите сервер SybaseIQ. Введите в командной строке и выполните следующую команду:

```
start_iq @%PMDV_HOME%\config\pmdvConfig.cfg
```

Введите эту команду одной строкой.

4. Чтобы подключиться к серверу Sybase IQ, выполните следующие действия.
 - a. В системе SHR выберите **Пуск > Выполнить**. Откроется диалоговое окно «Выполнить».
 - b. Введите `dbisql` в поле «Открыть» и нажмите клавишу **ВВОД**. Откроется диалоговое окно **Connect** программы Interactive SQL.
 - c. Введите следующее:
 - В поле User ID введите `dba`
 - В поле Password введите `sql`
 - В поле **Action** выберите **Connect to a running database on this computer** в раскрывающемся списке.
 - В поле Server Name введите имя сервера, на котором установлена база данных SybaseIQ SHR.

Совет. Имя сервера можно найти в файле `pmdvConfig.cfg`. Откройте файл. Имя сервера — это текст после `-n`.

- В поле Database name введите `utility_db`.
- d. Нажмите **Connect**. Откроется окно Interactive SQL.
5. Восстановите полную резервную копию.
 - В окне SQL Statements введите следующую инструкцию `sql`:

```
RESTORE DATABASE <путь к файлам базы данных> FROM <путь к сохраненному файлу резервной копии>.
```


Пример: `RESTORE DATABASE 'E:\SybaseDB\pmdv.db' FROM 'E:\HP-SHR\backup\Full.Sunday'`

- Нажмите F9 или **Execute all SQL Statement(s)**, чтобы выполнить оператор sql.
- Убедитесь, что файлы базы данных восстановлены по предыдущему пути БД.

Например: pmdb_user_main01.iq, pmdb.db, pmdb.iq, pmdb.iqtmp.

Совет. Если вы заметите следующую ошибку при восстановлении базы данных Sybase, пропустите ее и продолжите процесс восстановления.

"Unable to start specified database: Illegal character in database alias."

- Выполните следующие действия, чтобы остановить сервер SybaseIQ:
 - В разделе уведомлений на панели задач найдите значок Sybase IQ .
 - Щелкните значок правой кнопкой мыши и выберите **Shut down <имя сервера>**.
 - Нажмите **Yes**.
 - В окне служб выберите службу **HP_PMDB_Platform_Sybase** и нажмите **Пуск**.
6. После восстановления полной резервной копии восстановите добавочную резервную копию (если имеется).

При наличии нескольких файлов добавочной резервной копии выберите и восстановите самую последнюю добавочную резервную копию. Например, если сбой базы данных произошел в четверг, а полная резервная копия была создана в предыдущее воскресенье, необходимо восстановить файлы полной резервной копии, затем добавочную резервную копию, созданную в предыдущую среду.


- Для восстановления добавочной резервной копии в окне SQL Statements введите следующую инструкцию sql:

RESTORE DATABASE < путь к файлам базы данных> FROM <путь к сохраненному файлу резервной копии>.

Пример: RESTORE DATABASE 'E:\SybaseDB\pmdb.db' FROM 'E:\HP-SHR\backup\Incr_sncfull.Wednesday'

- Нажмите F9 или **Execute all SQL Statement(s)**, чтобы выполнить оператор sql.
- Убедитесь, что файлы базы данных восстановлены по предыдущему пути БД.

Например: pmdb_user_main01.iq, pmdb.db, pmdb.iq, pmdb.iqtmp.

- Выполните следующие действия, чтобы остановить сервер SybaseIQ:
 - В разделе уведомлений на панели задач найдите значок Sybase IQ .
 - Щелкните значок правой кнопкой мыши и выберите **Shut down <имя сервера>**.
 - Нажмите **Yes**.
- В окне служб выберите службу **HP_PMDB_Platform_Sybase** и нажмите **Пуск**.

Для базы данных и хранилища файлов SAP BusinessObjects

В сценарии с выборочной установкой войдите в системы, в которых установлено приложение SAP BusinessObjects, и выполните следующие действия для восстановления.

Чтобы восстановить базу данных и хранилище файлов SAP BusinessObjects, выполните следующие действия.

1. Войдите в систему SHR и откройте SAP BusinessObjects Central Configuration Manager.
2. Остановите агент Server Intelligence Agent и веб-сервер BusinessObjects.
3. В окне **Службы** выберите службу **BOE120SQLAW** и нажмите **Остановить**.
4. Переименуйте существующую папку хранилища файлов. Расположение хранилища файлов по умолчанию: C:\Program Files (x86)\BusinessObjects\BusinessObjects Enterprise 12.0\FileStore.

Вы можете переименовать его в FileStore_old.

5. Запустите сценарий восстановления:

```
Execute_BO_FullRestore.bat <BO Full Backup FileStore Path><BO Full Backup SQL AnWr Backup file path><BO Drive>
```

В данном случае:

- *FullRestore.bat* находится в каталоге %pmdb_home%\DR.
- <BO Full Backup SQL AnWr Backup file path> — это каталог базы данных SAP BusinessObjects (по умолчанию: E:\Program Files (x86)\Business Objects\SQLAnywhere12\bin)
- <BO Full Backup FileStore Path> — это каталог хранилища файлов SAP BusinessObjects (по умолчанию: E:\Program Files (x86)\Business Objects\BusinessObjects Enterprise 12.0\FileStore\BO)

Например: E:\HP-SHR\PMDB\DR>Execute_BO_FullRestore.bat "E:\BO_backup\SHRDisaster_Backup\Full_BOFileStore_BackUP.Friday" "E:\BO_backup\SHRDisaster_Backup\Full_SQLAnWr_BackUP.Friday" E:

Этот сценарий восстановит резервные копии файлов лицензий, конфигурации CAC и настраиваемых файлов.

Ниже представлены файлы журналов, которые находятся в каталоге %pmdb_home%\log:

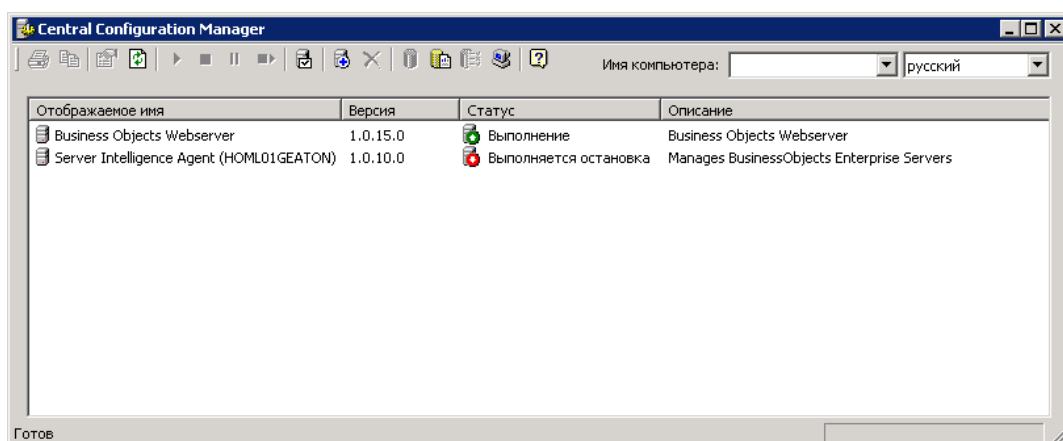
- SQLAnWr_Restore.log
- BO_Restore.log
- Config_Restore.log — файлы журналов для файлов лицензий, конфигурации CAC и настраиваемых файлов.
- CAC_Restore.log — журнал для файлов CAC.

6. Удалите исходный сервер SAP BusinessObjects:

- a. Перейдите в главный каталог SQL Anywhere. Путь по умолчанию: <SAP_BusinessObjects_Install_Drive>\Program Files (x86)\BusinessObjects\SQLAnywhere12\bin.
- b. Дважды щелкните файл dbisqlc. Откроется окно Connect to SQL Anywhere.
- c. В окне Connect to SQL Anywhere введите следующие сведения:
 - User ID: Введите имя хоста системы SHR (не полное доменное имя)
 - Пароль: Введите pmdb_admin.
 - Выберите **Start and connect to the running database** в раскрывающемся списке.
 - Выберите путь к **файлу базы данных**, нажав кнопку **Browse**. Путь к базе данных по умолчанию: C:\Program Files (x86)\Business Objects\SQLAnywhere12\bin\BOE120.db.
 - Оставьте поле Database Name пустым.
 - Имя сервера. BOE120SQLAW_<SHR_hostname>
 - Выберите **Stop database after last disconnect**, не изменяйте другие параметры.
 - Нажмите кнопку **OK**. Откроется консоль SQL Anywhere.
- d. В командной строке введите следующий запрос:

```
delete from cms_infoobjects6 where parentid=16 or parentid=59;
```

- e. Нажмите **Execute**. Появится сообщение с числом удаленных записей.
 - f. Закройте окно Connect to SQL Anywhere.
7. Создайте новый агент Server Intelligence Agent:
- a. В меню **Пуск** выберите **Программы > BusinessObjects XI 3.1 > BusinessObjects Enterprise > Central Configuration Manager**. Откроется окно Central Configuration Manager.
 - b. В окне **Central Configuration Manager** запишите имя агента Server Intelligence Agent (отображается в скобках).



- c. Перейдите в каталог `<SAP_BusinessObjects_Install_Directory>\BusinessObjects Enterprise 12.0\win32_x86`.

Каталог установки SAP BusinessObjects по умолчанию: `C:\Program Files (x86)\BusinessObjects\BusinessObjects Enterprise 12.0`.

- d. Удалите все файлы, которые начинаются с **_boe**.
- e. Удалите агент Server Intelligence Agent, выполнив следующую команду:


```
sc delete BOE120SIA<name>
```

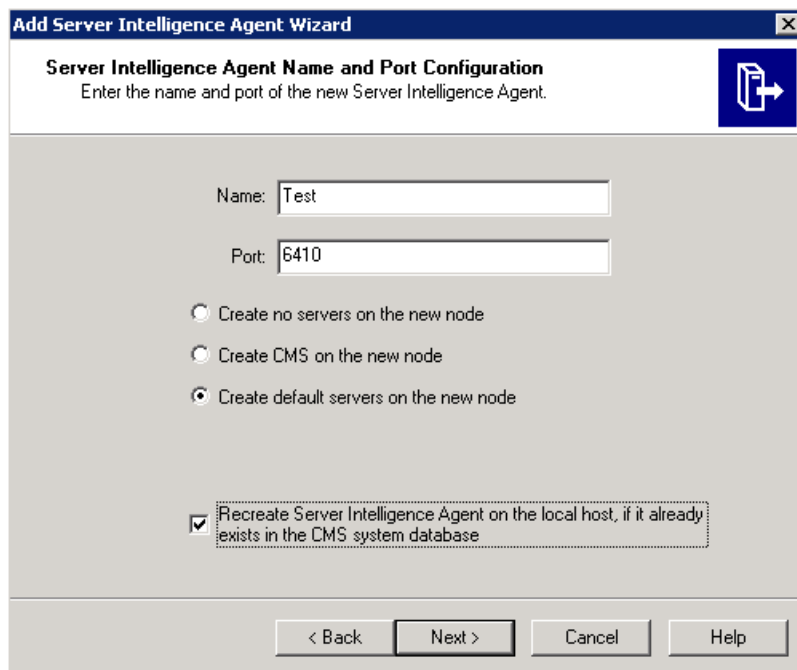
В данном случае `<name>` — это имя агента Sever Intelligence Agent, записанное во время ["Для базы данных и хранилища файлов SAP BusinessObjects" на странице 144](#).

В консоли командной строки появится следующее сообщение:

```
[SC] DeleteService SUCCESS
```

- f. Нажмите кнопку **Refresh** в окне **Central Configuration Manager** и убедитесь, что ПО Server Intelligence Agent удалено.

- g. В окне **Службы** выберите службу **BOE120SQLAW** и нажмите **Запустить**.
- h. В окне Central Configuration Manager щелкните правой кнопкой и остановите BusinessObjects Webserver, а затем нажмите **Add Server Intelligent Agent** (). Откроется мастер добавления агента Server Intelligence Agent.
- i. В мастере добавления агента Server Intelligence Agent введите имя агента Server Intelligence Agent, укажите порт 6410, установите флажки **Create Default Servers** и **Recreate Server Intelligence Agent on** и нажмите кнопку **Next**. Откроется окно New CMS Configuration.



Add Server Intelligence Agent Wizard

Server Intelligence Agent Name and Port Configuration
Enter the name and port of the new Server Intelligence Agent.

Name:

Port:

Create no servers on the new node

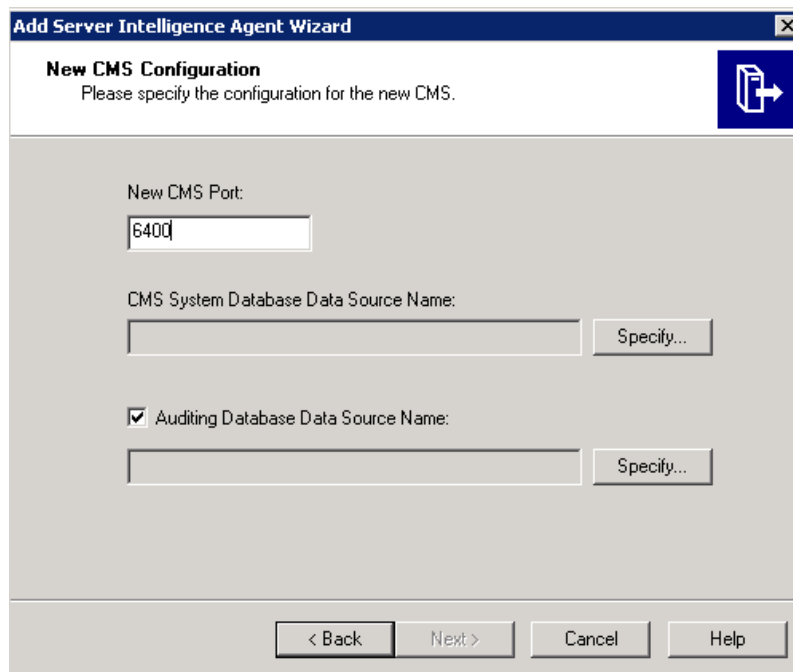
Create CMS on the new node

Create default servers on the new node

Recreate Server Intelligence Agent on the local host, if it already exists in the CMS system database

< Back Next > Cancel Help

- j. На странице New CMS Configuration введите **6400** в поле **New CMS Port**.



- k. В CMS System Database... нажмите **Specify**. Откроется диалоговое окно Create Database Driver.
- l. В диалоговом окне Create Database Driver выберите **SQL Anywhere (ODBC)** и нажмите кнопку **OK**. Откроется окно Select Data Source.
- m. В окне Select Data Source перейдите в раздел Machine Data Source, выберите **BOE120** и нажмите **OK**.
- n. В окне Connect to SQL Anywhere введите имя хоста системы SHR в качестве идентификатора пользователя, введите пароль для базы данных SQL Anywhere (пароль по умолчанию: pmdb_admin) и нажмите **OK**. Не изменяйте другие параметры. Не выбирайте **Encrypt Password**.
- o. *Необязательно*. Включите аудит.
 - Рядом с флажком Auditing Database Data Source... выберите **Specify**. Откроется диалоговое окно Create Database Driver.
 - В диалоговом окне Create Database Driver выберите **SQL Anywhere (ODBC)** и нажмите кнопку **OK**. Откроется окно Select Data Source.
 - В окне Select Data Source перейдите в раздел Machine Data Source, выберите **BOE120_Audit** и нажмите **OK**.
 - В окне Connect to SQL Anywhere введите имя хоста системы SHR в качестве идентификатора пользователя, введите пароль для базы данных SQL Anywhere

(пароль по умолчанию: `pmdb_admin`) и нажмите **ОК**. Не изменяйте другие параметры. Не выбирайте **Encrypt Password**.

Примечание. Убедитесь, что пароль администратора (пользователя по умолчанию) соответствует основной конфигурации.

- p. Нажмите кнопку **Далее**.
 - q. Нажмите кнопку **Далее**.
 - r. Нажмите кнопку **Готово**. Новый агент Server Intelligence Agent создан.

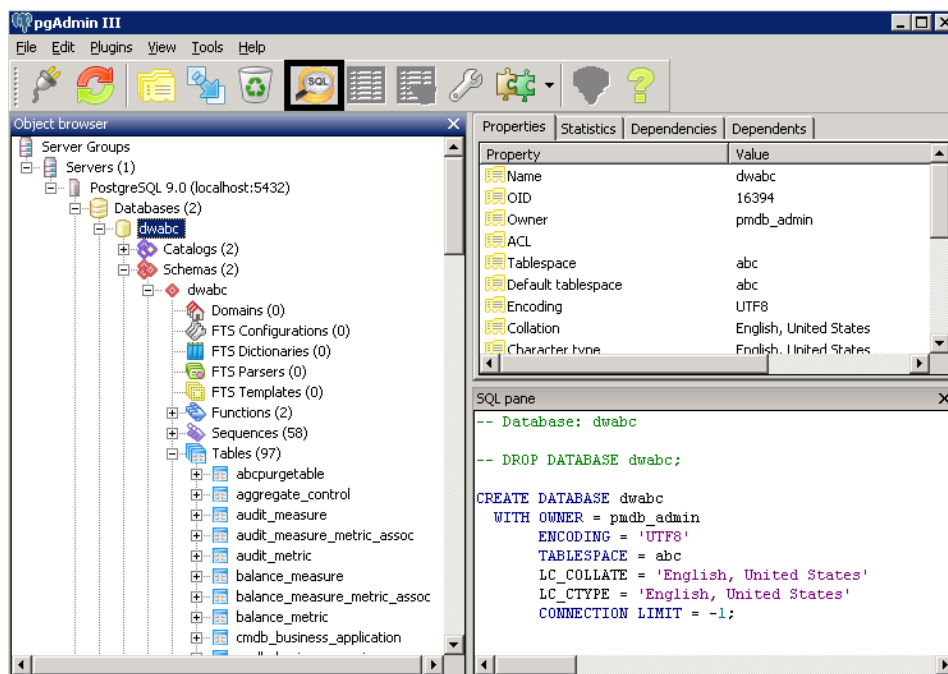
Пример: Если агент Server Intelligence Agent создан с именем *test*, отображаемое имя будет *Server Intelligence Agent (test)*.
 - s. Дважды щелкните Server Intelligence Agent и в окне **Server Intelligence Agent (test) Properties** выберите **Dependency**.
 - t. Откроется окно **Add Dependency**, выберите **BOE120SQLAW** в списке и нажмите **Add**, а затем **ОК**.
 - u. Запустите агент Server Intelligence Agent и веб-сервер BusinessObjects.
8. После запуска служб выполните следующие действия:
- a. Запустите Central Management Console (CMC).
 - b. Войдите в CMC с учетной записью администратора.
 - c. Нажмите Servers.
 - d. Дважды щелкните сервер **InputFileRepository**.
 - e. В контекстном меню щелкните **Properties**.
 - f. Введите путь в поле **Temporary Directory**. (Например: <installation directory of BOE>:\Program Files\Business Objects\BusinessObjects Enterprise12.0\FileStore\Input\Temp)
 - g. Введите путь в поле **File Store Directory**. (Например: <installation directory of BOE>:\Program Files\Business Objects\BusinessObjects Enterprise12.0\FileStore\Input).
 - h. Нажмите **Save & Close**.
 - i. Перезапустите сервер **InputFileRepository**.
 - j. Выполните шаги от d до i для сервера **OutputFileRepository**.

Для таблицы базы данных управления

В сценарии с выборочной установкой войдите в системы, на которых установлена база данных управления, и выполните следующие действия для восстановления.

Чтобы восстановить таблицу базы данных управления, выполните следующие действия.

1. Выполните вход в систему SHR.
2. В меню «Пуск» выберите **Программы > PostgreSQL 9.0 > pgAdmin III**.
3. Подключитесь к базе данных с паролем PMDB92_admin@hp. Запустите анализатор sql-запросов, щелкнув значок sql.



4. Запустите следующий запрос для восстановления таблиц базы данных:

```
Delete From dwabc.aggregate_control
```

```
Copy AGGREGATE_CONTROL TO '<Path of the backupfile>/backup_AGGREGATE_
CONTROL.dat'
```

В данном случае *<backup_path>* — это каталог, в который вы поместили резервную копию таблицы базы данных управления.

Например: COPY dwabc.aggregate_control from 'E://bo_backup//backup_AGGREGATE_
CONTROL.dat'

Восстановление SHR в Linux

Для базы данных Sybase IQ

В сценарии с выборочной установкой войдите в системы, на которых установлено приложение Sybase IQ, и выполните следующие действия для восстановления.

Примечание. Проверьте наличие достаточного свободного места, прежде чем выполнять восстановление.

Чтобы восстановить базу данных Sybase, выполните следующие действия.

1. Остановите службу HP_PMDB_Platform_Sybase:

- `cd /etc/init.d`
- `service HP_PMDB_Platform_Sybase stop`

2. Выполните команду: `ps -ef|grep iqsrv15`

Запишите ИД процесса, отображенный в результате выполнения команды.

3. Выполните команду ниже, указав идентификатор процесса вместо `<pid>`: `kill -9 <pid>`

4. Выполните поиск всех файлов с расширениями `.db`, `.log` и `.iq` в каталоге, где расположен файл базы данных, и переместите эти файлы в любой другой каталог в системе. Эти файлы создаются заново в процессе восстановления.

5. Запустите сервер SybaseIQ. Введите в командной строке и выполните следующую команду:

```
start_iq @/opt/HP/BSM/PMDB/config/pmdbConfig.cfg
```

Введите эту команду одной строкой.

6. Подключитесь к серверу SybaseIQ:

```
dbisql -nogui -c "uid=dba;pwd=sql;dbn=utility_db;eng=<server_name>;commlinks=tcPIP(host=<host_name>;port=21424)"
```

Пример:

```
dbisql -nogui -c "uid=dba;pwd=sql;dbn=utility_db;eng=abc;commlinks=tcPIP(host=abc.com;port=21424).
```

7. Восстановите полную резервную копию в исходном каталоге на исходном диске:

В окне SQL Statements введите следующую инструкцию sql:

```
RESTORE DATABASE <путь к файлам базы данных> FROM <путь к сохраненному файлу резервной копии.>
```

Пример:

```
RESTORE DATABASE '/root/SHR_Sybase/pmdb.db' FROM  
'/root/HPSHR/backup/Full.Sunday'
```

Совет. Если вы заметите следующую ошибку при восстановлении базы данных Sybase, пропустите ее и продолжите процесс восстановления.

"Unable to start specified database: Illegal character in database alias."

8. Выполните следующую команду для восстановления базы данных в другом каталоге или на другом диске:

```
RESTORE DATABASE <путь к файлам базы данных> from <путь к сохраненному файлу резервной копии.>
```

```
RENAME IQ_SYSTEM_MAIN TO <путь к pmdb.iq>
```

```
RENAME IQ_SYSTEM_TEMP TO <путь к pmdb.iqtmp>
```

```
RENAME pmdb_user_main TO <путь к pmdb_user_main01.iq>
```

Убедитесь, что путь к файлу pmdb.db существует.

Выполните все приведенные выше команды вместе.

9. После восстановления полной резервной копии восстановите добавочную резервную копию (если имеется).

При наличии нескольких файлов добавочной резервной копии выберите и восстановите самую последнюю добавочную резервную копию.

Для восстановления добавочной резервной копии в исходном каталоге на исходном диске в окне SQL Statements введите следующую инструкцию sql:

```
RESTORE DATABASE <путь к файлам базы данных> FROM <путь к сохраненному файлу инкрементной резервной копии>
```

```
RENAME IQ_SYSTEM_MAIN TO <путь к pmdb.iq>
```

```
RENAME IQ_SYSTEM_TEMP TO <путь к pmdb.iqtmp>
```

```
RENAME pmdb_user_main TO <путь к pmdb_user_main01.iq>
```

10. Остановите и запустите службы Sybase:

- `service HP_PMDB_Platform_Sybase stop`
- `service HP_PMDB_Platform_Sybase start`

Для базы данных и хранилища файлов SAP BusinessObjects

В сценарии с выборочной установкой войдите в системы, в которых установлено приложение SAP BusinessObjects, и выполните следующие действия для восстановления.

Чтобы восстановить базу данных и хранилище файлов SAP BusinessObjects, выполните следующие действия.

1. Скопируйте резервную копию базы данных и хранилища файлов SAP BusinessObjects в систему, в которой установлено ПО SAP BusinessObjects. Резервная копия также включает резервные копии файлов лицензий, конфигурации CAC и настраиваемых файлов.
2. Выполните вход в систему от имени пользователя root.
3. Выполните следующую команду, чтобы остановить веб-сервер.

```
sh /opt/HP/BSM/BO/bobje/tomcatshutdown.sh
```

4. Переключитесь на администратора SAP BusinessObjects, выполнив следующую команду:

```
su - SHRBOADMIN
```

5. Выполните следующую команду, чтобы остановить все серверы Server Intelligence Agent.

```
sh /opt/HP/BSM/BO/bobje/stopservers
```

6. Остановите службу SQL Anywhere:

```
sh /opt/HP/BSM/BO/bobje/sawstop.sh
```

При появлении запроса на ввод пароля укажите пароль к базе данных SQL Anywhere.

7. Создайте резервную копию всех файлов базы данных SQL Anywhere, выполнив следующую команду:

```
cp /opt/HP/BSM/BO/bobje/SQLAW/Bin/*BOE120*<backup_path>
```

В данном случае *<backup_path>* — это каталог, в который следует скопировать файлы существующей базы данных SQL Anywhere.

8. Переключитесь на пользователя root, выполнив следующую команду:

```
su root
```

9. Скопируйте резервную копию файла базы данных SAP BusinessObjects (созданную в ["Для](#)

базы данных и хранилища файлов SAP BusinessObjects" на странице 138), выполнив следующую команду:

```
cd /opt/HP/BSM/BO/bobje/SQLAW/Bin
```

```
cp <bo_backup_path>/SHRDisaster_Backup/Full_SQLAnWr_BackUP.Wednesday/*BOE120*
```

Введите у для перезаписи существующих файлов.

10. Запустите следующие права, чтобы предоставить необходимые права пользователю SAP BusinessObjects:

```
chown SHRBOADMIN:root *BOE120*
```

```
chmod 755 *BOE120*
```

11. Войдите в систему как пользователь SHRBOADMIN, а не как root.

```
su - SHRBOADMIN
```

12. Запустите службу SQL Anywhere. Выполните следующую команду для запуска SQL Anywhere.

```
sh $PMDB_HOME/../../BO/bobje/sawstartup.sh
```

Появится следующее сообщение:

```
STARTING SQL AnyWhere12 SERVER
```

```
SQL Anywhere Start Server In Background Utility Version 12.0.1.3457
```

13. Создайте новый экземпляр Server Intelligence Agent, выполнив следующую команду:

```
sh /opt/HP/BSM/BO/bobje/serverconfig.sh
```

Мастер SAP BusinessObjects откроется в окне командной строки.

```
-----  
SAP BusinessObjects  
  
What would you like to do?  
  
1 - Add a Server Intelligence Agent  
2 - Delete a Server Intelligence Agent  
3 - Modify a Server Intelligence Agent  
4 - List all Server Intelligence Agents in the config file  
  
[quit(0)]  
-----  
[4]1
```

14. Введите 1 и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
If it already exists in the CMS system database, do you want to recreate the  
Server Intelligence Agent on the local host?  
  
Use this option only if this Server Intelligence Agent does not exist on any hosts in the deployment.  
  
[yes(3)/no(2)/back(1)/quit(0)]  
-----  
[no]3
```

15. Введите 3 и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
Please enter the name of the new Server Intelligence Agent.  
  
[back(1)/quit(0)]  
-----  
[SHRLR02]SHRM2
```

16. Укажите имя агента (рекомендуется указывать имя хоста системы в качестве имени агента)

и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
Please enter the port of the new Server Intelligence Agent.  
  
[back(1)/quit(0)]  
-----  
[ ] 6410 █
```

17. Введите 6400 в качестве номера порта и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
noservers (Create no servers on the new node)  
cms (Create CMS on the new node)  
defaultservers (Create default servers on the new node)  
  
[noservers(4)/cms(3)/defaultservers(2)/back(1)/quit(0)]  
-----  
[noservers] 2 █
```

18. Введите 2 (сервер по умолчанию) и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
Enter the port of the new CMS.  
  
[back(1)/quit(0)]  
-----  
[default (6400)] █
```

19. Введите 6400 в качестве номера порта и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
Specify Destination CMS database connection information.  
  
Select the type of database connection from the following:  
[Oracle (6) /DB2 (5) /Sybase (4) /MySQL (3) /SQL Anywhere (2) /back(1) /quit (0) ]  
-----  
[Oracle]2 █
```

20. Введите 2 ((SQL Anywhere) и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
Specify Destination CMS database connection information.  
  
Enter the ODBC data source name (DSN) for connecting to your SQL Anywhere database.  
  
[back(1)/quit(0)]  
-----  
[SHRLR02BOE120] █
```

21. Нажмите клавишу **ВВОД** (правильный сервер будет выбран по умолчанию).

```
-----  
SAP BusinessObjects  
  
Specify Destination CMS database connection information.  
  
Enter the user name for connecting to your SQL Anywhere database.  
  
[back(1)/quit(0)]  
-----  
[SHR] █
```

- 22. Нажмите клавишу **ВВОД** (правильное имя пользователя будет выбрано по умолчанию).

```
-----  
SAP BusinessObjects  
  
Specify Destination CMS database connection information.  
  
Enter the password for connecting to your SQL Anywhere database.  
  
[back(1)/quit(0)]  
-----  
[] █
```

- 23. Введите пароль (запишите его для справки) и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
Would you like to enable auditing?  
  
[yes(3)/no(2)/back(1)/quit(0)]  
-----  
[yes] █
```

- 24. Выберите **Yes** и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
Specify auditing database connection information.  
  
Select the type of database connection from the following:  
[Oracle (6) / DB2 (5) / Sybase (4) / MySQL (3) / SQL Anywhere (2) / back (1) / quit (0) ]  
-----  
[SQL Anywhere]2█
```

- 25. Введите 2 ((SQL Anywhere) и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
Specify auditing database connection information.  
  
Enter the ODBC data source name (DSN) for connecting to your SQL Anywhere database.  
  
[back(1) / quit (0) ]  
-----  
[SHRLR02BOE120]SHRLR02BOE120_AUDIT█
```

- 26. Укажите имя источника данных ODBC и нажмите клавишу **ВВОД**.

Имя источника данных должно иметь следующий формат:

<agent_name>**BOE120_Audit**

<agent_name> — это имя, выбранное во время шага 14.

```
-----  
SAP BusinessObjects  
  
Specify auditing database connection information.  
  
Enter the user name for connecting to your SQL Anywhere database.  
  
[back(1)/quit(0)]  
-----  
[SHR] █
```

27. Нажмите клавишу **ВВОД** (правильное имя пользователя будет выбрано по умолчанию).

```
-----  
SAP BusinessObjects  
  
Specify auditing database connection information.  
  
Enter the password for connecting to your SQL Anywhere database.  
  
[back(1)/quit(0)]  
-----  
[ ] █
```

28. Введите пароль (запишите его для справки) и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
Enter the user name to connect to this CMS.  
  
[back(1)/quit(0)]  
-----  
[Administrator] █
```


29. Нажмите клавишу **ВВОД**. Правильный пользователь (Administrator) будет выбран по умолчанию.
30. Нажмите клавишу **ВВОД** при запросе пароля.

```
-----  
SAP BusinessObjects  
  
Choose the number of the type of authentication to  
use when contacting the CMS  
  
1 - secEnterprise  
2 - secLDAP  
  
[back/quit(0)]  
-----  
[1]
```

31. Введите 1 (secEnterprise) и нажмите клавишу **ВВОД**.
32. Введите Yes и нажмите клавишу **ВВОД**.

```
-----  
SAP BusinessObjects  
  
The following information will be used to create the new  
Server Intelligence Agent.  
  
CMS Name: SHRLR02  
Server Intelligence Agent Name: PRD_SHR  
Server Intelligence Agent Port: 6410  
Create Default Servers: yes  
CMS Port: 6400  
CMS Database: SHRLR02BOE120  
Audit Database: SHRLR02BOE120_AUDIT  
  
Do you want to create the Server Intelligence Agent?  
  
[yes(3)/no(2)/back(1)/quit(0)]  
-----  
[yes]  
Adding Server Intelligence Agent...  
.....  
Please press Enter to continue...  
█
```

33. Нажмите клавишу **ВВОД**.

```
-----
                SAP BusinessObjects
What would you like to do?

1 - Add a Server Intelligence Agent
2 - Delete a Server Intelligence Agent
3 - Modify a Server Intelligence Agent
4 - List all Server Intelligence Agents in the config file

[quit(0)]
-----

[4]4
```

34. Введите 4 и нажмите клавишу **ВВОД**. Откроется список агентов Server Intelligence Agent.
35. Введите 0 для выхода и нажмите клавишу **ВВОД**. Появится сообщение "*Thank you for choosing SAP BusinessObjcets...*"
36. Выполните следующую команду, чтобы запустить добавленный агент:

```
sh /opt/HP/BSM/BO/bobje/startservers
```

37. Выполните следующую команду:

- a. `cd /opt/HP/BSM/BO/bobje`
- b. `./ccm.sh -updateobjects -cms <SHR_hostname>:6400.`

Если у вас есть пароль для ССМ, выполните следующую команду:

```
./ccm.sh -updateobjects -cms SHR_hostname>:6400 -username Administrator -  
password <administratorpassword>
```

```
Creating session manager...  
Logging onto CMS...  
Creating infostore...  
Objects requiring update: 0  
Adding objects...  
CMS Data Source setup finished.
```

Для таблицы базы данных управления

В сценарии с выборочной установкой войдите в системы, на которых установлена база данных управления, и выполните следующие действия для восстановления.

1. Выполните следующие команды для запуска PgAdminIII:

- a. `cd $PMDB_HOME/./Postgres/bin`

- b. `./psql -U pmdb_admin -d dwabc -p 21425`

2. Подключитесь к базе данных с паролем, который был задан после установки.
3. Запустите анализатор sql-запросов
4. Запустите следующий запрос для восстановления таблиц базы данных:

```
Delete From aggregate_control
```

```
COPY aggregate_control from '<backup_path>/backup_AGGREGATE_CONTROL.dat';
```

В данном случае *<backup_path>* — это каталог, в который вы поместили файл базы данных управления.

Часть V: Справочник

Приложение А: Мониторы SiteScore для SHR

В следующей таблице перечислены мониторы, используемые для сбора метрик виртуализации.

Имя монитора	Счетчик	Имя показателя
Производительность VMware	Базовая система\Состояние	hardware.memorySize
Производительность VMware	Базовая система\Состояние	summary.hardware.numCpuCores
Производительность VMware	Базовая система\Состояние	summary.hardware.cpuMhz
Производительность VMware	Базовая система\Состояние	summary.hardware.numNics
Производительность VMware	Базовая система\Режим реального времени\Система	uptime.latest[]
Производительность VMware	Базовая система\Режим реального времени\Память	usage.average[]
Производительность VMware	Базовая система\Режим реального времени\Память	consumed.average[]
Производительность VMware	Базовая система\Режим реального времени\ЦП	usage.average[]
Производительность VMware	Базовая система\Режим реального времени\ЦП	ready.summation[]
Производительность VMware	Базовая система\Режим реального времени\Диск	usage.average[]

Имя монитора	Счетчик	Имя показателя
Производительность VMware	Базовая система\Режим реального времени\Диск	read.average[]
Производительность VMware	Базовая система\Режим реального времени\Диск	write.average[]
Производительность VMware	Базовая система\Режим реального времени\Сеть	received.average[]
Производительность VMware	Базовая система\Режим реального времени\Сеть	transmitted.average[]
Производительность VMware	Базовая система\Режим реального времени\Сеть	packetsRx.summation[]
Производительность VMware	Базовая система\Режим реального времени\Сеть	packetsTx.summation[]
Производительность VMware	Базовая система\Режим реального времени\Сеть	usage.average[]
Производительность VMware	Виртуальная машина\Состояние	config.hardware.memoryMB
Производительность VMware	Виртуальная машина\Состояние	config.cpuAllocation.shares.shares
Производительность VMware	Виртуальная машина\Состояние	config.hardware.numcpu
Производительность VMware	Виртуальная машина\Состояние	config.memoryAllocation.reservation
Производительность VMware	Виртуальная машина\Состояние	config.memoryAllocation.limit

Имя монитора	Счетчик	Имя показателя
Производительность VMware	Виртуальная машина\Состояние	config.cpuAllocation.reservation
Производительность VMware	Виртуальная машина\Состояние	config.cpuAllocation.limit
Производительность VMware	Виртуальная машина\Режим реального времени\Система	uptime.latest[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	usage.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	consumed.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	active.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	overhead.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	swpin.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	swapout.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	vmmemctltarget.average[]

Имя монитора	Счетчик	Имя показателя
Производительность VMware	Виртуальная машина\Режим реального времени\Память	usage.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	ready.summation[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	usagemhz.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	wait.summation[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	ready.summation[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	usage.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	read.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	write.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	received.average[]

Имя монитора	Счетчик	Имя показателя
Производительность VMware	Виртуальная машина\Режим реального времени\Память	transmitted.average[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	packetsRx.summation[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	packetsTx.summation[]
Производительность VMware	Виртуальная машина\Режим реального времени\Память	usage.average[]

В следующей таблице перечислены мониторы, используемые для сбора метрик управления системой.

Имя монитора	Счетчик	Имя показателя
<i>Windows</i>		
Ресурсы Windows	Память	Память\ (вывод страниц в секунду)
Ресурсы Windows	Память	Память\ (процент используемых зафиксированных байтов)
Ресурсы Windows	Сетевой интерфейс	Получено пакетов в секунду
Ресурсы Windows	Сетевой интерфейс	Отправлено пакетов в секунду
Ресурсы Windows	Сетевой интерфейс	Получено байтов в секунду
Ресурсы Windows	Сетевой интерфейс	Отправлено байтов в секунду
Ресурсы Windows	Сетевой интерфейс	Пакеты в секунду

Имя монитора	Счетчик	Имя показателя
Ресурсы Windows	Сетевой интерфейс	Сетевой интерфейс\ (процент байтов всего в секунду)
Ресурсы Windows	Физический диск	Физический диск_Общие\ (байтов диска в секунду)
Ресурсы Windows	Физический диск	(байтов диска в секунду)
Ресурсы Windows	Физический диск	(скорость чтения с диска, байт/с)
Ресурсы Windows	Физический диск	(записано байтов диска в секунду)
Ресурсы Windows	Системный	Система\Размер очереди процессора
Ресурсы Windows	Системный	Время работоспособности системы
Память	нет данных	(свободных Мбайт)
Память	нет данных	(процент загрузки)
ЦП	нет данных	(загрузка)
ЦП	нет данных	(загрузка ЦП#)
<i>Unix</i>		
Ресурсы Unix	Файловые системы	Емкость
Ресурсы Unix	Файловые системы	Кбайт
Ресурсы Unix	Файловые системы	Процент использования
Ресурсы Unix	Файловые системы	Используется
Ресурсы Unix	Файловые системы	Емкость
Ресурсы Unix	Файловые системы	Используется
Ресурсы Unix	Файловые системы	Процент использования
Ресурсы Unix	Файловые системы	(1024 блока)-(свободно)
Ресурсы Unix	Сетевой интерфейс	Пакеты
Ресурсы Unix	Статистика сети	Статистика сети\ Входящие пакеты

Имя монитора	Счетчик	Имя показателя
Ресурсы Unix	Статистика сети	Статистика сети\Исходящие пакеты
Ресурсы Unix	Сетевой интерфейс	Полученные байты
Ресурсы Unix	Сетевой интерфейс	Переданные байты
Ресурсы Unix	Сетевой интерфейс	ipackets
Ресурсы Unix	Сетевой интерфейс	opackets
Ресурсы Unix	Сетевой интерфейс	Полученные байты
Ресурсы Unix	Сетевой интерфейс	Исходящие байты
Ресурсы Unix	Длина очереди	Длина очереди\Очередь выполнения — размер
Ресурсы Unix	Статистика очередей\Компьютер\Состояние	Статистика очередей\Очередь выполнения — размер
Ресурсы Unix	Время работоспособности	Время работоспособности\Время работоспособности

Приложение В: Установка Xcelsius

Отчет Xcelsius — это интерактивный документ на основе Flash, который составляется программой SAP BusinessObjects Xcelsius Enterprise. Для создания Flash-отчетов Xcelsius в SHR необходимо установить приложение Xcelsius, доступное на установочном носителе SHR. Приложение Xcelsius не обязательно для просмотра отчетов SHR, поэтому его установка является факультативной.

Примечание. Для работы Xcelsius необходимо приложение Microsoft Excel.

Требования к оборудованию и программному обеспечению

Список требований к оборудованию и ПО для Xcelsius 2008 Service Pack 5, см. в документации [SAP](#).

Установка Xcelsius (необязательно)

Файл `setup` для установки Xcelsius 2008 Service Pack 5 находится на установочном носителе SHR.

Выполните следующие действия для получения исполняемого файла `setup`:

1. На установочном носителе SHR перейдите в папку `\packages`.
2. Выберите файл `Xcelsius.zip`, скопируйте его в нужное расположение и распакуйте.
3. В извлеченной папке перейдите в папку `\Xcelsius_2008_SP5` и выполните устанавливаемый файл установки.

См. дополнительные сведения об установке в документе *SAP BusinessObjects Xcelsius 2008 Installation Guide* на сайте [SAP](#).

Отправить отзыв о документации

Если вы хотите прокомментировать этот документ, [отправьте электронное письмо](#) в группу разработки документации. Если в этой системе сконфигурирован почтовый клиент, щелкните ссылку вверху, и окно электронной почты откроется со следующей информацией в строке темы.

Отзыв о документе Руководство по настройке (Service Health Reporter 9.40)

Просто впишите свой отзыв и нажмите кнопку "Отправить".

Если почтовый клиент отсутствует, скопируйте приведенный ниже текст в новое сообщение в почтовом веб-клиенте и отправьте его по адресу docfeedback@hp.com.

Нам важно ваше мнение!