HP Universal CMDB

Для операционных систем Windows и Red Hat Enterprise Linux

Версия программного обеспечения: 10.00

Повышение безопасности HP Universal CMDB и Configuration Manager

Дата выпуска документа: Июнь 2012 г.

Дата выпуска программного обеспечения: Июнь 2012 г.

Правовые уведомления

Гарантия

Гарантии на продукты и услуги HP формулируются только в заявлениях о прямой гарантии, сопровождающих эти продукты и услуги. Никакая часть настоящего документа не может быть истолкована как дополнительная гарантия. Компания HP не несет ответственности за содержащиеся здесь технические или редакционные ошибки.

Приводимые в настоящем документе сведения могут быть изменены без предварительного уведомления.

Пояснение об ограниченных правах

Конфиденциальное компьютерное программное обеспечение. Для обладания, использования или копирования необходима действующая лицензия от компании HP. В соответствии с нормами FAR 12.211 и 12.212, коммерческое компьютерное программное обеспечение, документация на компьютерное программное обеспечение и технические данные для коммерческих позиций лицензируются государственным организациям США на условиях стандартной коммерческой лицензии поставщика.

Заявление об авторских правах

Заявления о товарных знаках

Adobe™ является товарным знаком компании Adobe Systems Incorporated.

Microsoft® и Windows® являются зарегистрированными в США товарными знаками корпорации Microsoft Corporation.

UNIX® является зарегистрированным товарным знаком группы The Open Group.

Обновления документации

На титульном листе настоящего документа приведены следующие идентификационные данные.

- Номер версии программного обеспечения для указания версии ПО.
- Дата выпуска документа, которая меняется при каждом обновлении документа.
- Дата выпуска ПО, которая указывает дату выпуска текущей версии программного обеспечения.

Чтобы проверить наличие обновлений или убедиться в том, что используется последняя редакция документа, откройте веб-сайт

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

Чтобы воспользоваться этим сайтом, необходимо зарегистрировать идентификатор HP Passport и войти в систему. Регистрация HP Passport ID производится на сайте

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

или по ссылке **New users - please register** на странице входа в HP Passport.

Оформление подписки в службе поддержки соответствующего продукта также позволит получать обновленные и новые редакции. Обратитесь в торговое представительство компании HP для получения подробной информации.

Поддержка

Используйте веб-сайт технической поддержки программного обеспечения компании HP по адресу

http://www.hp.com/go/hpsoftwaresupport

Этот веб-сайт содержит контактную информацию и дополнительные сведения о продуктах, услугах и поддержке, которые предоставляет HP Software.

Веб-сайт технической поддержки программного обеспечения компании HP предоставляет возможности самостоятельного решения проблем. Это позволяет быстро и эффективно получить доступ к интерактивным средствам технической поддержки, необходимым для управления компанией. Каждый клиент службы поддержки может пользоваться следующими функциями веб-сайта технической поддержки:

- поиск документов базы знаний;
- отправка и отслеживание обращений и запросов на расширение возможностей;
- загрузка исправлений ПО;
- управление договорами на техническую поддержку;
- поиск контактов технической поддержки HP;
- проверка сведений о доступных услугах;
- участие в обсуждениях различных вопросов с другими заказчиками ПО;
- исследование определенных проблем и регистрация для обучения работе с программным обеспечением.

В большинстве случаев для получения поддержки требуется регистрация HP Passport, а также договор на услуги технической поддержки. Чтобы зарегистрироваться для получения идентификатора HP Passport ID, перейдите на веб-сайт

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

Дополнительные сведения об уровнях доступа представлены на сайте

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

Содержание

Глава 1

Введение в повышение безопасности

Данная глава включает:

Обзор повышения безопасности

В данном разделе описывается понятие защищенного приложения HP Universal CMDB, а также методы планирования и архитектура, необходимые для реализации защиты. Настоятельно рекомендуется ознакомиться с данным разделом перед изучением вопросов повышения безопасности в других главах.

HP Universal CMDB может быть частью защищенной архитектуры и противостоять возможным угрозам для безопасности.

Указания по повышению безопасности описывают настройки, необходимые для повышения уровня защиты HP Universal CMDB.

Предоставленная информация о повышении безопасности предназначена в первую очередь для администраторов HP Universal CMDB, которым следует ознакомиться с настройками и рекомендациями до начала работ по повышению безопасности.

Для создания безопасной архитектуры настоятельно рекомендуется использовать с HP Universal CMDB обратный прокси-сервер. Подробнее о настройке обратного прокси-сервера для HP Universal CMDB см. в разделе "Использование обратного прокси-сервера" на странице 34.

Если с HP Universal CMDB необходимо использовать иной тип безопасной архитектуры, чем описан в этом документе, обратитесь в службу поддержки HP Software, чтобы определить оптимальный тип архитектуры.

Дополнительные сведения по повышению безопасности зонда потока данных см. в разделе "Повышение безопасности зонда потока данных" на странице 64.

Примечание.

- Описанные процедуры повышения безопасности основаны на допущении, что выполняются только шаги, перечисленные в соответствующих главах, и никакие другие действия.
- Описанные шаги по повышению безопасности конкретной распределенной архитектуры не подразумевают, что данная архитектура является оптимальной для организации пользователя.
- Предполагается, что описанные в следующих главах процедуры выполняются на компьютерах, выделенных для HP Universal CMDB. Использование компьютеров для других целей помимо HP Universal CMDB может вызвать проблемы в работе.
- Информация о повышении безопасности, приведенная в данном разделе, не является руководством по анализу уровня риска компьютерной системы.

Подготовка к повышению безопасности

- Оцените состояние и угрозы для безопасности сети в целом, что поможет принять решение о способе интеграции HP Universal CMDB в сеть.
- Хорошо изучите техническую платформу HP Universal CMDB и функции безопасности HP Universal CMDB.
- Изучите рекомендации по повышению безопасности.
- Убедитесь в полной работоспособности HP Universal CMDB перед началом работы по повышению безопасности.
- Выполняйте процедуры повышения безопасности по порядку в каждой главе. Например, если решено настроить сервер HP Universal CMDB на поддержку SSL, прочтите "Включение поддержки Secure Sockets Layer (SSL)" на странице 18 и выполните инструкции по порядку.
- HP Universal CMDB не поддерживает обычную проверку подлинности с пустыми паролями. Не используйте пустых паролей при установке параметров обычной проверки подлинности.

Совет. Распечатайте процедуры повышения безопасности и сверяйтесь с получившимися документами по мере их реализации.

Развертывание UCMDB в безопасной архитектуре

Для обеспечения безопасности развернутых серверов HP Universal CMDB, рекомендуется применить несколько мер:

- **Архитектура демилитаризованной зоны (DMZ) с брандмауэром**

  Безопасная архитектура, о которой говорится в данном документе, это архитектура DMZ, использующая устройство как брандмауэр. Основная идея такой архитектуры состоит в полном отделении клиентов HP Universal CMDB от сервера HP Universal CMDB и предотвращении прямого доступа между ними.

- **Безопасный браузер**

  Internet Explorer и FireFox в среде Windows должны быть настроены на безопасную обработку сценариев, апплетов и файлов "cookie" Java.

- **Протокол связи SSL**

  Протокол Secure Sockets Layer (SSL) обеспечивает безопасность связи между клиентом и сервером. URL-адреса, требующие подключения SSL, используют безопасную версию (HTTPS) протокола передачи гипертекста. Дополнительные сведения см. в разделе "Включение поддержки Secure Sockets Layer (SSL)" на странице 18.

- **Архитектура обратного прокси-сервера**

  Одно из более безопасных и рекомендуемых решений состоит в развертывании HP Universal CMDB с использованием обратного прокси-сервера. HP Universal CMDB полностью поддерживает безопасную архитектуру на основе обратного прокси-сервера. Дополнительные сведения см. в разделе "Использование обратного прокси-сервера" на странице 34.

Доступ к системе

Повышение безопасности доступа к Java JMX

Примечание. Описанная здесь процедура может также использоваться для консоли JMX зонда потока данных.

Чтобы сделать порт JMX RMI только при указании учетных данных пользователя, выполните следующие действия:

1. В файле **wrapper.conf**, расположенном на сервере в директории **C:\hp\UCMDB\UCMDBServer\bin**, задайте следующие настройки:

   wrapper.java.additional.16=-Dcom.sun.management.jmxremote.authenticate=true

   Эта настройка требует, чтобы консоль JMX запрашивала проверку подлинности.

   - **В консоли JMX зонда потока данных** выполните следующие действия:

     Задайте в файлах **WrapperGateway.conf** и **WrapperManager.conf** в директории **C:\hp\UCMDB\DataFlowProbe\bin** следующие настройки:

     wrapper.java.additional.17=-Dcom.sun.management.jmxremote.authenticate=true

2. Переименуйте файл **jmxremote.password.template** (в директории

C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management) в **jmxremote.password**.

> **Примечание.** В консоли JMX зонда потока данных этот файл находится в следующей директории: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

3. В файле **jmxremote.password** задайте пароли для ролей **monitorRole** и **controlRole**.

   Пример:

   monitorRole QED

   controlRole R&D

   назначит пароль **QED** для **monitorRole** и **R&D** для **controlRole**.

   > **Примечание.** Проверьте, чтобы доступ на чтение и запись к файлу **jmxremote.password** были только у владельца, т.к. в нем хранятся незашифрованные пароли. Владельцем файла должен быть пользователь, от имени которого запущен сервер UCMDB.

4. В файле **jmxremote.access** (в директории **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) предоставьте доступ для **monitorRole** и **controlRole**.

   Пример:

   monitorRole readonly

   controlRole readwrite

   это откроет доступ для чтения роли **monitorRole**, а также для чтения и записи роли **controlRole**.

   > **Примечание.** В консоли JMX зонда потока данных этот файл находится в следующей директории: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

5. Защитите файлы следующим образом:

   - **Только для Windows:** Выполните следующую команду в командной строке:

     cacls jmxremote.password /P <username>:F

     cacls jmxremote.access /P <username>:R

     где **<username>** – владелец файлов, указанный в их свойствах. Откройте свойства файлов и убедитесь, что они заданы правильно и имеют только одного владельца.

   - **Для ОС Solaris и Linux:** Задайте права доступа к файлу с паролями при помощи следующей команды:

     chmod 600 jmxremote.password

6. **Для обновления с помощью пакетов обслуживания, переноса сервера и восстановления после аварий:** Измените владельца **jmxremote.access** (в директории **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) на пользователя операционной системы, от имени которого выполняется обновление или перенос.

Примечание. В консоли JMX зонда потока данных этот файл находится в следующей директории: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

Изменение имени пользователя или пароля для консоли JMX

Консоль JMX использует системных пользователей, т.е. пользователей, охватывающих нескольких клиентов, в среде с несколькими клиентами. В консоль JMX можно войти, используя имя любого системного пользователя. Имя пользователя и пароль по умолчанию — **sysadmin/sysadmin**.

Пароль можно изменить либо через консоль JMX, либо через средство управления сервером.

Чтобы изменить имя или пароль по умолчанию системного пользователя через консоль JMX:

1. Запустите веб-браузер и введите следующий адрес: **http://localhost.<domain_ name>:8080/jmx-console**.
2. Введите реквизиты проверки подлинности консоли JMX, которые по умолчанию имеют следующие значения:
   - Имя для входа = **sysadmin**
   - Пароль = **sysadmin**
3. Найдите строку **UCMDB:service=Authorization Services** и щелкните ссылку, чтобы открыть страницу "Operations".
4. Найдите операцию **resetPassword**.
   - В поле **userName** введите **sysadmin**.
   - В поле **password** введите новый пароль.
5. Щелкните **Invoke** для сохранения изменений.

Чтобы изменить имя или пароль по умолчанию системного пользователя через средство управления сервером:

1. **Для Windows:** запустите следующий файл: **C:\hp\UCMDB\UCMDBServer\tools\server_management.bat.**

   Если используется Linux: Запустите **server_management.sh**, расположенный в следующей папке: **/opt/hp/UCMDB/UCMDBServer/tools/**.
2. Войдите в средство при помощи учетных данных проверки подлинности: **sysadmin/sysadmin**.
3. Щелкните ссылку Пользователи.
4. Выберите системного пользователя и щелкните **Изменить пароль для вошедшего пользователя**.
5. Введите старый и новый пароль, а затем нажмите **OK**.

Изменение пользователя службы HP Universal CMDB Server

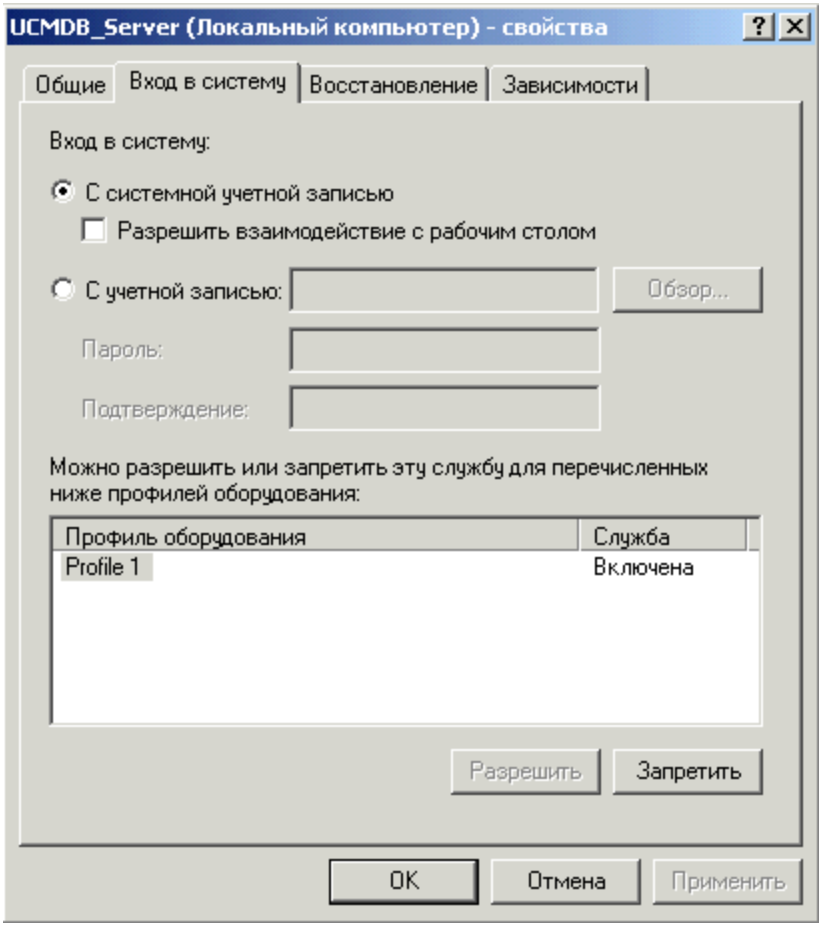
На платформе Windows служба HP Universal CMDB, выполняющая все службы и процессы HP Universal CMDB, устанавливается при запуске служебной программы настройки сервера и базы данных. По умолчанию данная служба запускается пользователем локальной системы. Однако иногда необходимо запускать службу от имени другого пользователя (например, при использовании проверки подлинности NTLM).

Пользователь, от имени которого запускается служба, должен иметь следующие права доступа:

- достаточные права доступа к базе данных (определяется администратором базы данных)
- достаточные права доступа к сети
- Права доступа администратора на локальном сервере

Чтобы сменить пользователя-владельца службы:

1. Отключите HP Universal CMDB через меню "Пуск" (**Пуск > Все программы> HP UCMDB > Остановить HP Universal CMDB Server**), либо остановив службу HP Universal CMDB Server. Дополнительные сведения см. в разделе "Запуск и остановка службы HP Universal CMDB Server" на странице 1.
2. В окне **Службы** в Windows дважды щелкните на **UCMDB_Server**. Откроется диалоговое окно **Свойства UCMDB_Server (локальный компьютер).**
3. Щелкните вкладку Вход в систему.



4. Выберите **С учетной записью** и перейдите по списку допустимых пользователей на компьютере, чтобы выбрать нужного пользователя.
5. Выберите и подтвердите пароль данного пользователя для входа в Windows.
6. Щелкните **Применить** для сохранения настроек, а затем **OK**, чтобы закрыть диалоговое окно.
7. Включите HP Universal CMDB через меню "Пуск" (**Пуск > Все программы> HP UCMDB > Запустить HP Universal CMDB Server**), либо запустив службу HP Universal CMDB Server. Дополнительные сведения см. в разделе "Запуск и остановка службы HP Universal CMDB Server" на странице 1.

Шифрование пароля базы данных для Configuration Manager

Пароль базы данных CM хранится в файле **<директория установки Configuration Manager>\conf\database.properties**. Механизм шифрования пароля, используемый по умолчанию, соответствует стандартам FIPS 140-2.

Шифрование осуществляется при помощи ключа. Затем сам ключ шифруется при помощи другого, т.н. главного ключа. При шифровании обоих ключей используется один и тот же

алгоритм. Подробнее о параметрах шифрования см. в разделе "Параметры шифрования пароля базы данных для Configuration Manager" ниже

Внимание! В случае изменения алгоритма шифрования все ранее зашифрованные пароли становятся недоступными.

Изменение шифрования пароля базы данных:

1. Откройте файл **<директория установки Configuration Manager>\conf \encryption.properties** и измените значения следующих полей:
   - **engineName.** Введите название алгоритма шифрования.
   - **keySize.** Введите размер главного ключа для выбранного алгоритма шифрования.
2. Запустите сценарий **generate-keys.bat**, который создаст следующий файл: **<директория установки Configuration Manager>\security\encrypt_repository** и ключ шифрования.
3. Запустите программу **bin\encrypt-password.bat** и зашифруйте пароль. Флаг **-h** позволяет просмотреть доступные параметры.
4. Скопируйте зашифрованный пароль в файл **conf\database.properties**.

Параметры шифрования пароля базы данных для Configuration Manager

В следующей таблице перечислены параметры, указанные в файле **encryption.properties**, который используется для шифрования пароля базы данных CM. Дополнительные сведения о шифровании пароля базы данных см. в разделе "Шифрование пароля базы данных для Configuration Manager" на предыдущей странице

параметр	Описание
cryptoSource	Указывает на инфраструктуру реализации алгоритма шифрования. Возможные варианты: • **lw.** Используется облегченная реализация Bouncy Castle (по умолчанию) • **jce.** Java Cryptography Enhancement (стандартная инфраструктура шифрования Java)
storageType	Указывает тип хранилища ключей. В настоящее время поддерживается только **binary file** (двоичный файл).
binaryFileStorageName	Указывает на место в файле, где хранится главный ключ.
cipherType	Тип шифра. В настоящее время поддерживается только **symmetricBlockCipher**.
engineName	Название алгоритма шифрования.

параметр	Описание
	Доступны следующие параметры: • **AES.** Алгоритм American Encryption Standard. Шифрование соответствует стандартам FIPS 140-2. (Значение по умолчанию) • **Blowfish** • **DES** • **3DES.** (Соответствует стандартам FIPS 140-2) • **Null**. Без шифрования
keySize	Размер главного ключа. Размер определяется алгоритмом: • **AES.** 128, 192 или 256 (значение по умолчанию – 256) • **Blowfish.** 0-400 • **DES.** 56 • **3DES.** 156
encodingMode	Кодировка ASCII двоичных результатов шифрования. Доступны следующие параметры: • **Base64** (по умолчанию) • **Base64Url** • **Hex**
algorithmModeName	Режим алгоритма. В настоящее время поддерживается только **CBC**.
algorithmPaddingName	Используемый алгоритм холостого заполнения. Доступны следующие параметры: • **PKCS7Padding** (по умолчанию) • **PKCS5Padding**
jceProviderName	Название алгоритма шифрования JCE. **Примечание:** Имеет значение, только если crytpSource равно jce. Для lw используется engineName.

Глава 2

Включение поддержки Secure Sockets Layer (SSL)

Данная глава включает:

Включение SSL на сервере с самоподписанным сертификатом - UCMDB

В следующих разделах описана настройка HP Universal CMDB для поддержки обмена информацией с использованием SSL.

HP Universal CMDB использует Jetty 6.1 как веб-сервер по умолчанию.

1. **Необходимые условия**

   a. Перед выполнением следующих шагов удалите старый файл **server.keystore** (папка установки **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**).

b. Разместите хранилище ключей HP Universal CMDB (тип JKS) в папке **C:\hp\UCMDB\UCMDBServer\conf\security**.

2. **Создание хранилища ключей на сервере**

a. Создание ключа (типа JKS) с самоподписанным сертификатом и соответствующим частным ключом:

- Выполните следующую команду из **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**:

```
keytool -genkey -alias hpcert -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
```

Отобразится диалоговое окно консоли.

- Введите пароль хранилища ключей. Если пароль изменился, выполните операцию JMX **changeKeystorePassword** в **UCMDB:service=Security Services**. Если пароль не изменился, используйте пароль по умолчанию **hppass**.
- Ответьте на вопрос **Ваши имя и фамилия?** Введите имя веб-сервера HP Universal CMDB. Введите другие параметры для организации.
- Введите пароль ключа. Пароль ключа ДОЛЖЕН совпадать с паролем хранилища ключей.

  Будет создано хранилище ключей JKS с именем **tomcat.keystore** и сертификатом сервера **hpcert**.

b. Экспортируйте самоподписанный сертификат в файл:

Выполните следующую команду из **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**:

```
keytool -export -alias hpcert -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass
<your password> -file hpcert
```

3. **Поместите сертификат в хранилище надежных сертификатов клиента.**

Создав **server.keystore** и экспортировав сертификат сервера, поместите сертификат в хранилище надежных сертификатов каждого клиента, которому необходимо связываться с HP UCMDB по SSL при помощи данного самоподписанного сертификата.

> **Примечание.** В **server.keystore** может храниться только один сертификат сервера.

4. **Отключите порт HTTP 8080**

Дополнительные сведения см. в разделе "Включение или отключение портов HTTP/HTTPS" на странице 29.

> **Примечание.** Перед закрытием порта HTTP убедитесь, что соединение HTTPS работает.

5. **Перезапуск сервера**

6. **Откройте HP Universal CMDB**

Для проверки безопасности сервера UCMDB введите в веб-браузере следующий URL-адрес: **https://<UCMDB Server name or IP address>:8443/ucmdb-ui**.

Включение SSL на сервере с самоподписанным сертификатом - Configuration Manager

В следующих разделах описана настройка в Configuration Manager поддержки проверки подлинности и шифрования с использованием протокола Secure Sockets Layer (SSL).

Configuration Manager использует в качестве сервера приложений Tomcat 7.0.19.

Примечание. Местоположение всех директорий и файлов зависит от настроек платформы, ОС и установки.

1. ## Необходимые условия

   Перед выполнением следующих шагов удалите старый файл **tomcat.keystore** из папки **<Configuration Manager installation directory>\java\windows\x86_64\lib\security** или **<Configuration Manager installation directory>\java\linux\x86_64\lib\security** (если он существует).

2. ## Создание хранилища ключей на сервере

   Создание ключа (типа JKS) с самоподписанным сертификатом и соответствующим частным ключом:

   - В директории bin установки Java в директории установки Configuration Manager выполните следующую команду:

     ```
     keytool -genkey -alias tomcat -keyalg RSA -keystore ..\lib\
     security\tomcat.keystore
     ```

     Отобразится диалоговое окно консоли.

   - Введите пароль хранилища ключей. Если пароль изменился, измените его вручную в файле.
   - Ответьте на вопрос **Ваши имя и фамилия?** Введите имя веб-сервера Configuration Manager. Введите другие параметры для организации.
   - Введите пароль ключа. Пароль ключа ДОЛЖЕН совпадать с паролем хранилища ключей.

     Будет создано хранилище ключей JKS с именем **tomcat.keystore** и сертификатом сервера **hpcert**.

3. ## Помещение сертификата в хранилище надежных сертификатов клиента

   Поместите сертификат в хранилище надежных сертификатов клиента в Internet Explorer на локальной машине (**Сервис > Свойства обозревателя > Содержимое > Сертификаты**). В противном случае при первой попытке использования Configuration Manager система сама предложит сделать это.

Ограничение: В **tomcat.keystore** может храниться только один сертификат сервера.

4. **Изменение файла server.xml**

   Откройте файл **server.xml** в папке **<директория установки Configuration Manager>\servers\server-0\conf**. Найдите раздел, начинающийся с

   ```
   Connector port="8143"
   ```

   в комментариях. Активируйте сценарий, удалив символ комментария, и добавьте следующие атрибуты в коннектор HTTPS:

   ```
   keystoreFile="<tomcat.keystore file location>" (см. шаг 2)
   keystorePass="<password>"
   ```

   Закомментируйте следующую строку:

   ```
   <Listener className="org.apache.catalina.core.AprLifecycleListener"
   SSLEngine="on" />
   ```

   Примечание. Не следует блокировать порт соединения HTTP. Для этих целей лучше использовать брандмауэр.

5. **Перезапуск сервера**

   Перезапустите сервер Configuration Manager.

6. **Проверка безопасности сервера**

   Для проверки безопасности сервера Configuration Manager введите в веб-браузере следующий URL-адрес: **https://<Configuration Manager Server name or IP address>:8143/cnc**.

   Совет. Если не удается установить соединение, используйте другой браузер или более новую версию.

Включение SSL на сервере с сертификатом, подписанным центром сертификации - UCMDB

Для использования сертификата, выданного центром сертификации, хранилище ключей должно быть в формате Java. В следующем примере описано, как отформатировать хранилище ключей на машине с Windows.

1. **Необходимые условия**

   Перед выполнением следующих шагов удалите старый файл **server.keystore** (папка установки **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**).

2. **Создание хранилища ключей на сервере**

   a. Создайте сертификат, подписанный центром сертификации, и установите его в Windows.

   b. Экспортируйте сертификат в файл ***.pfx** (включая закрытые ключи) при помощи Microsoft Management Console (**mmc.exe**).

      Задайте пароль для файла **pfx**. (Данный пароль потребуется при преобразовании хранилища ключей в формат Java.) Файл **.pfx** теперь содержит открытый сертификат и закрытый ключ. Файл защищен паролем.

   c. Скопируйте файл **.pfx** в следующую папку: **C:\hp\UCMDB\UCMDBServer\conf\security**.

   d. Откройте командную строку и смените папку установки на **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**.

      Измените тип хранилища ключей с **PKCS12** на **JAVA** при помощи следующей команды:

      ```
      keytool -importkeystore -srckeystore
      c:\hp\UCMDB\UCMDBServer\conf\security\<имя файла pfx> -
      srcstoretype PKCS12 -destkeystore server.keystore
      ```

      Будет запрошен пароль к исходному файлу (**.pfx**). Это пароль, указанный при создании файла **pfx** в шаге b.)

   e. Введите пароль целевого хранилища ключей. Пароль должен совпадать с паролем, определенным ранее в методе JMX **changeKeystorePassword** служб безопасности. Если пароль не изменился, используйте пароль по умолчанию **hppass**.

   f. После создания сертификата отключите порт HTTP 8080. Подробнее см. в разделе "Включение или отключение портов HTTP/HTTPS" на странице 29.

   g. В случае использования иного пароля, чем **hppass**, либо пароля, использованного для файл **.pfx**, выполните метод JMX **changeKeystorePassword** и убедитесь, что ключ использует тот же пароль.

      Примечание. Перед закрытием порта HTTP убедитесь, что соединение HTTPS работает.

3. **Перезапуск сервера**

4. **Проверка безопасности сервера**

   Для проверки безопасности сервера UCMDB введите в веб-браузере следующий URL-адрес: **https://<UCMDB Server name or IP address>:8443/ucmdb-ui**.

   Внимание! В **server.keystore** может храниться только один сертификат сервера.

Включение SSL на сервере с сертификатом, подписанным центром сертификации - Configuration Manager

Чтобы Configuration Manager использовал сертификат, выданный центром сертификации, хранилище ключей должно быть в формате Java. В следующем примере описано, как отформатировать хранилище ключей на машине с Windows.

1. ### Необходимые условия

   Перед выполнением следующих шагов удалите старый файл **tomcat.keystore** из папки **<Configuration Manager installation directory>\java\windows\x86_64\lib\security** или **<Configuration Manager installation directory>\java\linux\x86_64\lib\security** (если он существует).

2. ### Создание хранилища ключей на сервере

   a. Создайте сертификат, подписанный центром сертификации, и установите его в Windows.

   b. Экспортируйте сертификат в файл ***.pfx** (включая закрытые ключи) при помощи Microsoft Management Console (**mmc.exe**).

   Задайте пароль для файла **pfx**. (Данный пароль потребуется при преобразовании хранилища ключей в формат Java.)
   Файл **.pfx** теперь содержит открытый сертификат и закрытый ключ. Файл защищен паролем.

   Скопируйте файл **.pfx** в следующую папку: **<Configuration Manager installation directory>\java\lib\security**.

   c. Откройте командную строку и смените папку на **<Configuration Manager installation directory>\java\bin**.

   Измените тип хранилища ключей с **PKCS12** на **JAVA** при помощи следующей команды:

   ```
   keytool -importkeystore -srckeystore <Configuration Manager
   installation directory>\conf\security\<pfx file name> -
   srcstoretype PKCS12 -destkeystore tomcat.keystore
   ```

   Будет запрошен пароль к исходному файлу (**.pfx**). Это пароль, указанный при создании файла pfx в шаге b.

3. ### Изменение файла server.xml

   Откройте файл **server.xml** в папке **<директория установки Configuration Manager>\servers\server-0\conf**. Найдите раздел, начинающийся с

   ```
   Connector port="8143"
   ```

   в комментариях. Активируйте сценарий, удалив символ комментария, и добавьте следующие две строки:

```
keystoreFile="../../java/lib/security/tomcat.keystore"
keystorePass="password" />
```

Закомментируйте следующую строку:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />
```

Примечание. Не следует блокировать порт соединения HTTP. Для этих целей лучше использовать брандмауэр.

4. **Перезапуск сервера**

   Перезапустите сервер Configuration Manager.

5. **Проверка безопасности сервера**

   Для проверки безопасности сервера Configuration Manager введите в веб-браузере следующий URL-адрес: **https://<Configuration Manager Server name or IP address>:8143/cnc**.

Ограничение: В **tomcat.keystore** может храниться только один сертификат сервера.

Примечание. Местоположение директорий и файлов зависит от настроек платформы, операционной системы, а также особенностей установки.

Пример: `java/{os name}/lib`.

Включение SSL на клиентских машинах - UCMDB

Если сертификат, используемым веб-сервером HP UCMDB, выдан известным центром сертификации, веб-браузер, скорее всего, сможет проверить сертификат самостоятельно.

Если веб-браузер не считает центр сертификации надежным, следует либо импортировать путь доверия сертификата целиком, либо импортировать сертификат, используемый HP Universal CMDB, напрямую в доверительное хранилище веб-браузера.

Ниже показан пример импортирования самоподписанного сертификата **hpcert** в доверительное хранилище Windows, которое будет использоваться Internet Explorer.

Чтобы импортировать сертификат в доверительное хранилище Windows:

1. Найдите сертификат **hpcert** и переименуйте его в **hpcert.cer**.

   В Проводнике отобразится пиктограмма, указывающая, что файл является сертификатом безопасности.

2. Дважды щелкните на **hpcert.cer**, чтобы открыть диалоговое окно сертификатов в Internet Explorer.

3. Следуйте инструкциям по включению доверия, установив сертификат с помощью Мастера импорта сертификатов.

Примечание. Другой метод импорта сертификата, выданного сервером UCMDB веб-браузеру, заключается во входе в UCMDB и установке сертификата, при появлении предупреждения о ненадежном сертификате.

Включение SSL с сертификатом клиента - Configuration Manager

Если сертификат, используемый веб-сервером Configuration Manager, выдан известным центром сертификации, веб-браузер, скорее всего, сможет проверить сертификат самостоятельно.

Если сервер не считает центр сертификации надежным, импортируйте этот сертификат в хранилище надежных сертификатов сервера.

Ниже показан пример импортирования самоподписанного сертификата **hpcert** в хранилище надежных сертификатов сервера (cacerts).

Импортирование сертификата в хранилище надежных сертификатов сервера:

1. Найдите на машине клиента сертификат **hpcert** и переименуйте его в **hpcert.cer**.
2. Скопируйте **hpcert.cer** в папку **<директория установки Configuration Manager>\java\bin** на сервере.
3. На сервере импортируйте сертификат центра сертификации в хранилище надежных сертификатов (cacerts) при помощи утилиты keytool, введя следующую команду:

```
<директория установки Configuration Manager>\java\bin\keytool.exe -
import
-alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
```

4. Измените файл **server.xml** (в папке **<директория установки Configuration Manager>\servers\server-0\conf**) следующим образом:
   a. Внесите изменения, описанные в шаге "Изменение файла server.xml" на странице 23.
   b. Сразу после этих изменений добавьте следующие атрибуты в коннектор HTTPS:

```
truststoreFile="../../java/lib/security/cacerts"
truststorePass="changeit" />
```

   c. Задайте параметр `clientAuth="true"`.
5. Проверьте безопасность сервера, как описано в разделе "Проверка безопасности сервера" на предыдущей странице.

Включение SSL на клиентских SDK

Передачу HTTPS можно использовать между SDK клиента и SDK сервера:

1. На клиентском компьютере, в продукте, в который внедрен SDK клиента, найдите параметры передачи и убедитесь, что они настроены на использование HTTPS, а не HTTP.
2. Загрузите сертификат ЦС/самоподписанный открытый сертификат на компьютер клиента и импортируйте его в доверительное хранилище **cacerts** на JRE, который будет подключаться к серверу.

   Используйте следующую команду:

   ```
   Keytool -import -alias <имя ЦС> -trustcacerts -file <путь открытого сертификата сервера> -keystore <путь к доверенному хранилищу cacerts jre клиента (т.е. x:\program files\java\jre\lib\security\cacerts)>
   ```

Включение взаимной проверки подлинности сертификатов для SDK

Этот режим использует SSL и включает как проверку подлинности сервера UCMDB, так и проверку подлинности клиента клиентом UCMDB-API. И сервер, и клиент UCMDB-API отправляют свои сертификаты соответствующей сущности для проверки их подлинности.

Примечание. Приведенный ниже метод включения SSL на SDK с взаимной проверкой подлинности является наиболее безопасным из методов и, в силу этого, рекомендуемым режимом связи.

1. Повысьте безопасность соединителя клиента UCMDB-API в UCMDB:
   a. Откройте консоль JMX UCMDB: Запустите веб-браузер и введите следующий адрес: **http://<имя или IP-адрес компьютера UCMDB>:8080/jmx-console**. Возможно, потребуется ввести имя пользователя и пароль для входа в систему (по умолчанию — sysadmin/sysadmin).
   b. Найдите **UCMDB:service=Ports Management Services** и щелкните ссылку, чтобы открыть страницу "Operations".
   c. Найдите операцию **PortsDetails** и щелкните **Invoke**. Обратите внимание на номер порта HTTPS с проверкой подлинности клиента. Порт по умолчанию — 8444, и он должен быть включен.
   d. Вернитесь на страницу "Operations".
   e. Чтобы сопоставить соединитель ucmdb-api с режимом взаимной проверки подлинности, вызовите метод **mapComponentToConnectors** со следующими параметрами:
      - **componentName**: ucmdb-api
      - **isHTTPSWithClientAuth**: true
      - Все остальные флаги: false

      Выводится следующее сообщение:

```
Operation succeeded. Component ucmdb-api is now mapped to:
HTTPS_CLIENT_AUTH ports.
```

f. Вернитесь на страницу "Operations".

2. Убедитесь, что у JRE, на котором работает UCMDB-API, имеется хранилище ключей, содержащее сертификат клиента.
3. Экспортируйте сертификат клиента UCMDB-API из хранилища ключей.
4. Импортируйте экспортированный сертификат клиента UCMDB-api в доверительное хранилище UCMDB Server.
   a. На компьютере UCMDB скопируйте созданный файл сертификата клиента UCMDB-API в следующий каталог UCMDB:

      C:\HP\UCMDB\UCMDBServer\conf\security

   b. Выполните следующую команду:

      C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file <exported UCMDB-api client certificate> - alias ucmdb-api

   c. Введите пароль доверительного хранилища UCMDB Server (по умолчанию — **hppass**).

   d. При появлении вопроса **Доверять этому сертификату?** нажмите **y**, а затем **Ввод**.

   e. Убедитесь, что отобразился результат **Сертификат добавлен в хранилище ключей**.
5. Экспортируйте сертификат сервера UCMDB из хранилища ключей сервера.
   a. Выполните следующую команду на компьютере UCMDB:

      C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore C:\HP\UCMDB\UCMDBServer\conf\security\server.keystore -file C:\HP\UCMDB\conf\security\server.cert

   b. Введите пароль доверительного хранилища UCMDB Server (по умолчанию — **hppass**).

   c. Убедитесь, что в следующем каталоге создан сертификат:

      C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
6. Импортируйте экспортированный сертификат клиента UCMDB в клиентское доверительное хранилище UCMDB-API.
7. Перезапустите сервер UCMDB и клиент UCMDB-API.
8. Для подключения клиента UCMDB-API к серверу UCMDB-API, используйте следующий код:

```
UcmdbServiceProvider provider =
UcmdbServiceFactory.getServiceProvider("https", <SOME_HOST_NAME>,
<HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER (default:8444)>));
UcmdbService ucmdbService = provider.connect
(provider.createCertificateCredentials(<TheClientKeystore. e.g:
```

```
"c:\\client.keystore">, <KeystorePassword>),
provider.createClientContext(<ClientIdentification>));
```

Изменение паролей хранилища ключей сервера

После установки сервера, открывается порт HTTPS и хранилище защищается ненадежным паролем (пароль по умолчанию **hppass**). Если предполагается работа только с SSL, необходимо изменить пароль.

В нижеследующей процедуре показывается, как изменить только пароль **server.keystore**. Эта же процедура используется и для изменения пароля **server.truststore**.

Примечание. Следует выполнять все шаги данной процедуры.

1. Запустите сервер UCMDB.
2. Выполните изменение пароля в консоли JMX.
   a. Запустите веб-браузер и введите адрес сервера: **http://<Имя или IP-адрес UCMDB Server>:8080/jmx-console**.

      Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

   b. В разделе UCMDB нажмите **UCMDB:service=Security Services**, чтобы открыть страницу "Operations".

   c. Найдите и исполните операцию **changeKeystorePassword**.

      Поле не должно быть пустым, и его длина должна составлять не менее шести символов. Пароль меняется только в базе данных.
3. Остановите сервер UCMDB.
4. Выполните команды.

   В **C:\hp\UCMDB\UCMBServer\bin\jre\bin** выполните следующие команды:

   a. Изменение пароля хранилища:

      keytool -storepasswd -new <new_keystore_pass> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <current_ keystore_pass>

   b. Следующая команда отображает внутренний ключ хранилища ключей. Первый параметр — это псевдоним. Сохраните этот параметр для следующей команды:

      keytool -list -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

   c. Измените пароль ключа (если хранилище не пустует):

      keytool -keypasswd -alias <alias> -keypass <currentPass> -new <newPass> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

   d. Введите новый пароль.

5. Запустите сервер UCMDB.
6. Повторите процедуру для доверительного хранилища сервера.

Включение или отключение портов HTTP/HTTPS

Порты HTTP и HTTPS можно включать и отключать из интерфейса пользователя или из консоли JMX.

Для включения или отключения портов HTTP/HTTPS из интерфейса пользователя:

1. Войдите в систему HP Universal CMDB.
2. Выберите **Администрирование > Настройки инфраструктуры**.
3. Введите **http** или **https** в окно **Фильтр по именам** для отображения настроек HTTP.
   - **Включить HTTP(S)-соединения**. **True**: порт включен. **False**: порт отключен.
4. Перезапустите сервер, чтобы применить изменение.

> **Внимание!** Порт HTTPS открыт по умолчанию, закрытие этого порта не дает работать **Server_Management.bat**.

Для включения или отключения портов HTTP/HTTPS из консоли JMX:

1. Запустите веб-браузер и введите следующий адрес: http://localhost.<domain_name>:8080/jmx-console.
2. Введите реквизиты проверки подлинности консоли JMX, которые по умолчанию имеют следующие значения:
   - Имя для входа = **sysadmin**
   - Пароль = **sysadmin**
3. Найдите **UCMDB:service=Ports Management Services** и щелкните ссылку, чтобы открыть страницу "Operations".
4. Для включения или отключения порта HTTP, найдите операцию **HTTPSetEnable** и установите значение.
   - **True:** порт включен.
   - **False:** порт отключен.
5. Для включения или отключения порта HTTPS, найдите операцию **HTTPSSetEnable** и установите значение.
   - **True:** порт включен.
   - **False:** порт отключен.
6. Для включения или отключения порта HTTPS с проверкой подлинности клиента, найдите операцию **HTTPSClientAuthSetEnable** и установите значение.

- **True:** порт включен.
- **False:** порт отключен.

Сопоставление веб-компонентов UCMDB с портами

Каждый из компонентов UCMDB можно сопоставить с доступными портами из консоли JMX.

Для просмотра текущих конфигураций компонентов:

1. Запустите веб-браузер и введите следующий адрес: **http://localhost.<domain_name>:8080/jmx-console**.
2. Введите реквизиты проверки подлинности консоли JMX, которые по умолчанию имеют следующие значения:

   Имя для входа = **sysadmin**

   Пароль = **sysadmin**
3. Найдите **UCMDB:service=Ports Management Services** и щелкните ссылку, чтобы открыть страницу "Operations".
4. Найдите метод **ComponentsConfigurations** и щелкните **Invoke**.
5. Отобразятся допустимые порты и сопоставленные в настоящий момент порты для каждого из компонентов.

Для сопоставления компонентов:

1. Найдите **UCMDB:service=Ports Management Services** и щелкните ссылку, чтобы открыть страницу "Operations".
2. Найдите метод **mapComponentToConnectors**.
3. Введите имя компонента в окно "Значение". Выберите **True** или **False** для каждого из портов, соответствующих выбранному компоненту. Нажмите кнопку **Invoke**. Выбранный компонент будет сопоставлен с выбранными портами. Имена компонентов можно находить, вызывая метод **serverComponentsNames**.
4. Повторяйте процесс для каждого из соответствующих компонентов.

Примечание.

- Каждый компонент должен быть сопоставлен с минимум одним портом. Если не сопоставить компонент хотя бы с одним портом, он сопоставляется по умолчанию с портом HTTP.
- Если сопоставить компонент как с портом HTTPS, так и с портом HTTPS с проверкой подлинности клиента, сопоставляется только второй вариант (первый, в данном случае, является дублирующим).

Также можно изменить значения, назначенные каждому из портов.

Чтобы установить значения для портов:

1. Найдите **UCMDB:service=Ports Management Services** и щелкните ссылку, чтобы открыть страницу "Operations".
2. Чтобы установить значение для порта HTTP, найдите метод **HTTPSetPort** и введите значение в окно **Значение**. Нажмите кнопку **Invoke**.
3. Чтобы установить значение для порта HTTPS, найдите метод **HTTPSSetPort** и введите значение в окно **Значение**. Нажмите кнопку **Invoke**.
4. Чтобы установить значение для порта HTTPS с проверкой подлинности клиента, найдите метод **HTTPSClientAuthSetPort** и введите значение в окно **Значение**. Нажмите кнопку **Invoke**.

Настройка Configuration Manager для работы с UCMDB через SSL

Можно настроить Configuration Manager для работы с UCMDB через Secure Sockets Layer (SSL). По умолчанию в UCMDB включен SSL-коннектор (порт 8443).

1. Перейдите в папку **<директория установки UCMDB>\bin\jre\bin** и выполните команду:

   ```
   keytool -export -alias hpcert -keystore <UCMDB server dir>
   \conf\security\server.keystore -storepass hppass -file
   <certificatefile>
   ```

2. Скопируйте файл сертификата во временную папку на локальной машине Configuration Manager.
3. Заново установите или перенастройте уже установленный Configuration Manager. Подробнее см. в соответствующем разделе интерактивного документа *Руководство по развертыванию HP Universal CMDB*.

   На странице настройки UCMDB выберите протокол HTTPS и сертификат, скопированный в шаге 2.

Чтобы настроить Configuration Manager для работы с другими продуктами (например, балансировщиками нагрузки) через SSL, импортируйте сертификат безопасности продукта в хранилище truststore Configuration Manager (хранилище jre по умолчанию) при помощи следующей команды:

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias <alias>
-keystore <CM_JAVA_HOME>\lib\security\cacerts -storepass changeit
-file <certificatefile>
```

Работа UCMDB KPI Adapter через SSL

Можно настроить отправку данных адаптера KPI UCMDB через Secure Sockets Layer (SSL).

1. Экспортируйте сертификат Configuration Manager:

   ```
   <CM_JAVA_HOME>\bin\keytool -export -alias tomcat -keystore
   <CM_JAVA_HOME>\lib\security\tomcat.keystore -storepass
   <keystore pass> -file <certificate file name>
   ```

2. Импортируйте сертификат из Configuration Manager в доверительное хранилище UCMDB:

   ```
   <UCMDB server dir>\bin\jre\bin keytool -import -trustcacerts
   -alias tomcat -keystore <UCMDB server dir>\bin\jre\lib
   \security\cacerts -storepass changeit -file <certificatefile>
   ```

3. Импортируйте сертификат из Configuration Manager в доверительное хранилище зонда:

   a. Откройте командную строку и выполните команду:

   ```
   <DataFlowProbe dir>\bin\jre\bin\keytool.exe -import -v -keystore
   <DataFlowProbe dir>\conf\security\MAMTrustStoreExp.jks -file
   <certificatefile> -alias tomcat
   ```

   b. Введите пароль хранилища ключей: logomania

   c. При появлении вопроса **Доверять этому сертификату?** нажмите **y**, а затем **Enter**.

   Выводится следующее сообщение:

   Сертификат добавлен в хранилище ключей.

   Дополнительные сведения по повышению безопасности зонда потока данных см. в разделе "Повышение безопасности зонда потока данных" на странице 64.

4. Перезапустите UCMDB, зонд потока данных и Configuration Manager.

Настройка поддержки SSL в браузере UCMDB

Примечание. Приведенные здесь инструкции относятся к браузеру UCMDB версии 1.7. При использовании более новой версии браузера UCMDB, которая была обновлена отдельно от остального набора продуктов UCMDB, см. раздел о настройке поддержки SSL в *Руководстве по установке и настройке браузера UCMDB* для соответствующей версии.

Для установки и настройки поддержки SSL на Tomcat:

1. Создайте файл хранения закрытого ключа сервера и самозаверяющего сертификата при помощи следующей команды:

   - Для Windows: **%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA**
   - Для UNIX: **$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA**

   В обоих случаях используйте пароль **changeit** (во всех других полях диалогового окна консоли можно использовать любое значение).

2. Снимите символ комментария в строке **SSL HTTP/1.1 Connector** файла **$CATALINA_BASE/conf/server.xml**, где **$CATALINA_BASE** – директория установки Tomcat.

> **Примечание.** Полное описание настройки использования SSL в файле **server.xml** см. на официальном сайте Apache Tomcat. http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html

3. Перезапустите сервер Tomcat.

Для использования при подключении к серверу UCMDB HTTPS-протокола:

1. В **ucmdb_browser_config.xml** укажите значение **https** для тега **<protocol>** и назначьте для тега **<port> значение порта HTTPS сервера UCMDB (8443 по умолчанию).**
2. Загрузите открытый сертификат сервера UCMDB на компьютер с браузером UCMDB (если на сервере UCMDB используется SSL, сертификат может предоставить администратор UCMDB) и импортируйте его в доверительное хранилище **cacerts** на JRE, который будет подключаться к серверу, при помощи следующей команды:

   "%JAVA_HOME%\bin\keytool" -import -alias ucmdb -trustcacerts -file <UCMDB-Server-certificate-file> -keystore "%JAVA_HOME%\jre\lib\security\cacerts"

   где **<UCMDB-Server-certificate-file>** – это полный путь к файлу открытого сертификата сервера UCMDB.
3. Перезапустите сервер Tomcat.

Глава 3

Использование обратного прокси-сервера

В данном разделе описываются последствия использования обратных прокси-серверов с точки зрения безопасности, а также содержатся инструкции по использованию обратного прокси-сервера с HP Universal CMDB и Configuration Manager. Излагаются только аспекты использования обратного прокси-сервера, связанные с безопасностью, без прочих аспектов, таких как кэширование и балансировка нагрузки.

Данная глава включает:

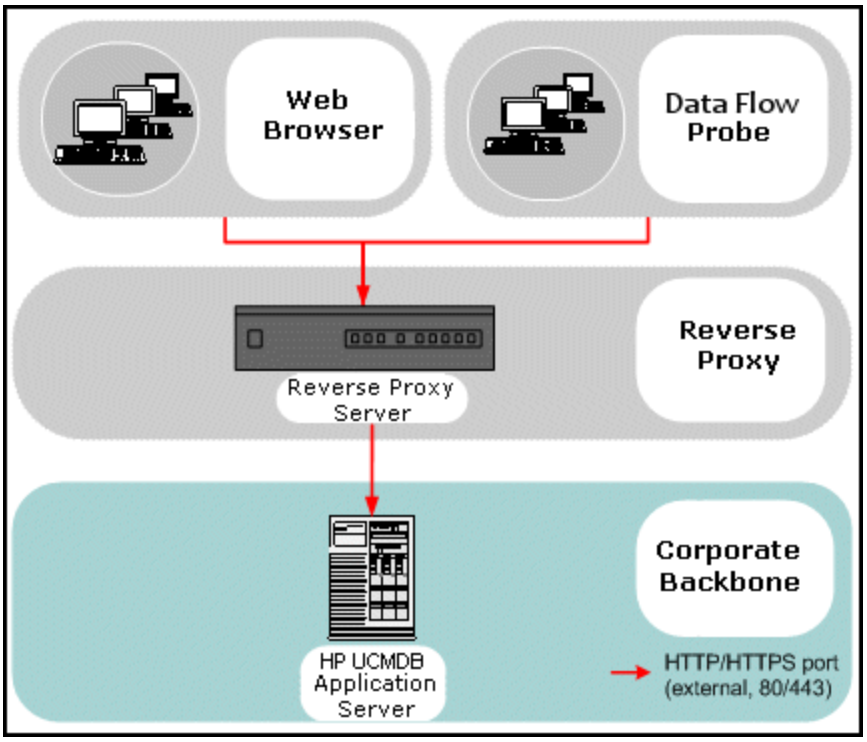
Обзор обратного прокси-сервера

Обратный прокси-сервер — это промежуточный сервер, расположенный между компьютером клиента и веб-серверами. Для компьютера клиента обратный прокси-сервер представляется стандартным веб-сервером, обслуживающим запросы протокола HTTP этого компьютера.

Компьютер клиента отправляет обычные запросы веб-содержимого, используя имя обратного прокси-сервера вместо имени веб-сервера. Обратный прокси-сервер пересылает запрос одному из веб-серверов. Хотя ответ приходит на компьютер клиента от обратного прокси-сервера, этому компьютеру он кажется пришедшим от веб-сервера.

Можно создать несколько обратных прокси-серверов с разными URL-адресами, которые будут представлять один и тот же экземпляр UCMDB/CM. И наоборот, задав разные корневые контексты для нескольких серверов UCMDB/CM, можно использовать один обратный прокси-сервер для доступа к нескольким серверам UCMDB/CM.

HP Universal CMDB и Configuration Manager поддерживают обратные прокси-серверы в архитектуре DMZ. Обратный прокси-сервер является HTTP-посредником между зондом потока данных, веб-клиентом и сервером HP Universal CMDB/CM.



Примечание.

- Различные типы обратных прокси-серверов требуют различных синтаксисов конфигурации. Пример конфигурации обратного прокси-сервера Apache 2.0.x см. в разделе " Пример: Настройка Apache 2.0.x " на странице 37.
- При создании прямой ссылки на отчет с помощью Планировщика достаточно настроить только интерфейсный URL-адрес.

Аспекты использования обратного прокси-сервера, связанные с безопасностью

Обратный прокси-сервер служит компьютером-бастионом. Прокси-сервер настраивается так, чтобы быть единственным компьютером, к которому обращаются внешние клиенты, и тем самым он закрывает остальную внутреннюю сеть. Благодаря обратному прокси-серверу сервер приложений можно разместить на отдельном компьютере во внутренней сети.

В данном разделе рассказывается об использовании демилитаризованной зоны (DMZ) и обратного прокси-сервера в среде с топологией, включающей два межсетевых экрана (back-to-back).

Основные преимущества использования обратного прокси-сервера в подобной среде таковы:

- Преобразования протоколов в DMZ не происходит. Входящий и исходящий протоколы идентичны (изменяется только заголовок).

- Доступ к обратному прокси-серверу возможен только посредством HTTP, что помогает межсетевым экранам с контролем состояния соединений обеспечивать безопасность связи.
- На обратном прокси-сервере может быть определен статический, ограниченный набор перенаправляемых запросов.
- Большинство функций безопасности веб-сервера доступны на обратном прокси-сервере (методы проверки подлинности, шифрование и т.д.).
- Обратный прокси-сервер маскирует IP-адреса настоящих серверов, равно как и архитектуру внутренней сети.
- Единственным доступным клиентом на веб-сервере остается обратный прокси-сервер.
- Такая конфигурация (в отличии от других решений) поддерживает межсетевые экраны с NAT.
- Обратный прокси-сервер требует минимального количества открытых портов в межсетевом экране.
- Обратный прокси-сервер обеспечивает хорошую, по сравнению с другими решениями бастиона, производительность.

Настройка обратного прокси-сервера

В данном разделе описывается настройка обратного прокси-сервера.

Настройка обратного прокси-сервера с помощью настроек инфраструктуры

Следующая процедура показывает, как использовать настройки инфраструктуры для конфигурирования обратного прокси-сервера. Эти настройки используются только при создании прямой ссылки на отчет с помощью Планировщика.

Настройка обратного прокси-сервера:

1. Выберите **Администрирование > Настройки инфраструктуры > Общие параметры**.
2. Измените параметр Интерфейсный URL-адрес. Введите адрес, например, **https://my_proxy_server:443/**.

Примечание. После внесения этого изменения доступ к серверу HP Universal CMDB напрямую через клиент становится невозможен. Конфигурацию обратного прокси-сервера можно изменить через консоль JMX на компьютере сервера. Подробнее см. в разделе Настройка обратного прокси-сервера с помощью консоли JMX ниже.

Настройка обратного прокси-сервера с помощью консоли JMX

Для изменения конфигурации обратного прокси-сервера можно использовать консоль JMX на компьютере сервера HP Universal CMDB. Эти настройки используются только при создании прямой ссылки на отчет с помощью Планировщика.

Для изменения конфигурации обратного прокси-сервера:

1. На компьютере, где установлен сервер HP Universal CMDB, запустите веб-браузер и введите следующий адрес:

   http://<имя или IP-адрес компьютера>.<domain_name>:8080/jmx-console

   где **<имя или IP-адрес компьютера>** относятся к компьютеру, на котором установлена HP Universal CMDB. Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

2. Щелкните ссылку **UCMDB-UI > UCMDB-UI:name=UI Server frontend settings**.

   Введите URL-адрес прокси-сервера в поле **setUseFrontendURLBySettings**, например `https://my_proxy_server:443/`.

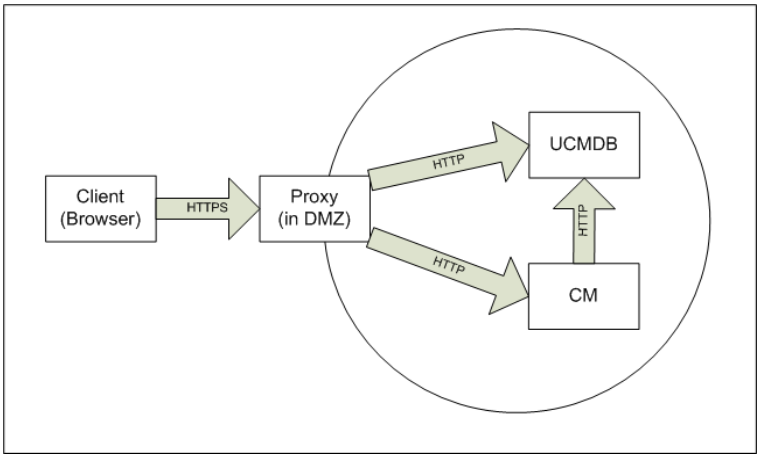
3. Нажмите кнопку **Invoke**.

4. Для просмотра значения этого параметра используйте метод **showFrontendURLInSettings**.

Пример: Настройка Apache 2.0.x

В данном разделе приводится пример файла конфигурации, поддерживающего использование обратного прокси-сервера Apache 2.0.x в случае, когда и зонды потока данных, и пользователи приложений подключаются к HP Universal CMDB.

На иллюстрации ниже представлен процесс настройки обратного прокси-сервера для Configuration Manager и UCMDB.



Примечание.

- В этом примере в качестве имени DNS и порта компьютера HP Universal CMDB используется UCMDB_server.
- В этом примере в качестве имени DNS и порта компьютера HP Configuration Manager используется UCMDB_CM.
- Эти изменения следует вносить только пользователям, знакомым с администрированием Apache.

1. Откройте файл **<корневой каталог компьютера с Apache>\Webserver\conf\httpd.conf**.

2. Включите следующие модули:
   - **LoadModule proxy_module modules/mod_proxy.so**
   - **LoadModule proxy_http_module modules/mod_proxy_http.so**
   - **LoadModule headers_module modules/mod_headers.so**
3. Добавьте следующие строки в файл httpd.conf:

```
ProxyRequests off

<Proxy *>

Order deny,allow

Deny from all

Allow from all

</Proxy>

ProxyPass /mam http://UCMDB_server/mam

ProxyPassReverse /mam http://UCMDB_server/mam

ProxyPass /mam_images http://UCMDB_server/mam_images

ProxyPassReverse /mam_images http://UCMDB_server/mam_images

ProxyPass /mam-collectors http://UCMDB_server/mam-collectors

ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors

ProxyPass /ucmdb http://UCMDB_server/ucmdb

ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb

ProxyPass /site http://UCMDB_server/site

ProxyPassReverse /site http://UCMDB_server/site

ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui

ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui

ProxyPass /status http://UCMDB_server/status

ProxyPassReverse /status http://UCMDB_server/status

ProxyPass /jmx-console http://UCMDB_server/jmx-console

ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console

ProxyPass /axis2 http://UCMDB_server/axis2

ProxyPassReverse /axis2 http://UCMDB_server/axis2

ProxyPass /icons http://UCMDB_server/icons

ProxyPassReverse /icons http://UCMDB_server/icons

ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api

ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
```

```
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs

ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs

ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0

ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0

ProxyPass /cm http://UCMDB_Server/cm

ProxyPassReverse /cm http://UCMDB_Server /cm

ProxyPass /cnc http://UCMDB_CM_server/cnc

ProxyPassReverse /cnc http://UCMDB_CM_server/cnc

ProxyPass /docs http://UCMDB_CM_server/docs

ProxyPassReverse /docs http://UCMDB_CM_server/docs

ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser

ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-
browser

ProxyPreserveHost On

RequestHeader set X-Reverse-Proxy "https://<SRP host>:<SRP port>"
```

Примечание. Строка `ProxyPreserveHost On` необходима только при наличии виртуального хоста.

Внимание! Важно добавить строку `RequestHeader set X-Reverse-Proxy "https://<SRP host>:<SRP port>"`. Без нее конфигурация не будет работоспособной.

4. Сохраните изменения.

Подключение зонда потока данных посредством обратного прокси-сервера или балансировщика нагрузки при помощи взаимной проверки подлинности

Для подключения зонда потока данных посредством обратного прокси-сервера или балансировщика нагрузки со взаимной проверкой подлинности выполните следующие действия. Данная процедура применяется для следующей конфигурации:

- Взаимная проверка подлинности через SSL между зондом и обратным прокси-сервером или балансировщиком нагрузки на основании сертификата клиента, предоставленного зондом и необходимого обратному прокси-серверу или балансировщику нагрузки.
- Обычное соединение, защищенное SSL, между обратным прокси-сервером или балансировщиком нагрузки и сервером UCMDB.

Примечание. Нижеследующие инструкции используют хранилище ключей **cKeyStoreFile** в качестве хранилища ключей зонда. Это предопределенное хранилище ключей, являющееся частью установки зонда потока данных и содержащее самоподписанные сертификаты. Дополнительные сведения см. в разделе "Хранилище ключей и доверительное хранилище по умолчанию для сервера и зонда потока данных" на странице 79.

Рекомендуется создать новое, уникальное хранилище ключей, в котором будет находиться свежесозданный ключ. Дополнительные сведения см. в разделе "Создание хранилища ключей для зонда потока данных" на странице 78.

Получение сертификата от центра сертификации

Получите корневой сертификат центра сертификации и импортируйте его в следующие местоположения:

- доверительное хранилище зонда потока данных
- JVM cacerts зонда потока данных
- доверительное хранилище сервера UCMDB
- доверительное хранилище обратного прокси-сервера

1. Импортируйте корневой сертификат центра сертификации в доверительное хранилище зонда потока данных.

   a. Поместите корневой сертификат центра сертификации в следующую директорию: <директория установки зонда потока данных>\conf\security\<имя файла сертификата>.

   b. Импортируйте корневой сертификат центра сертификации в доверительное хранилище зонда потока данных, запустив следующий сценарий:

   ```
   <директория установки зонда потока
   данных>\bin\jre\bin\keytool.exe -import -trustcacerts -alias
   <YourAlias> -file C:\hp\UCMDB\DataFlowProbe\conf\security\<имя
   файла сертификата> -keystore <директория установки зонда потока
   данных>\conf\security\MAMTrustStoreExp.jks
   ```

   Пароль по умолчанию: **logomania**.

2. Импортируйте корневой сертификат центра сертификации в JVM cacerts зонда потока данных, запустив следующий сценарий:

   ```
   <директория установки зонда потока данных>\bin\jre\bin\keytool.exe
   -import -trustcacerts -alias <YourAlias> -file <директория
   установки зонда потока данных>\conf\security\<имя файла
   сертификата> -keystore <директория установки зонда потока
   данных>\bin\jre\lib\security\cacerts
   ```

   Пароль по умолчанию: **changeit**.

3. Импортируйте корневой сертификат центра сертификации в доверительное хранилище UCMDB.

a. Поместите корневой сертификат центра сертификации в следующую директорию: <директория установки UCMDB>\conf\security\<имя файла сертификата>.

b. Импортируйте корневой сертификат центра сертификации в доверительное хранилище UCMDB, запустив следующий сценарий:

```
<директория установки UCMDB>\bin\jre\bin\keytool.exe -import -
trustcacerts -alias <YourAlias> -file <директория установки
UCMDB>\conf\security\<имя файла сертификата> -keystore
<директория установки UCMDB>\conf\security\sever.truststore
```

Пароль по умолчанию: **hppass**.

4. Импортируйте корневой сертификат центра сертификации в доверительное хранилище обратного прокси-сервера. Данная процедура зависит от используемого обратного прокси-сервера.

Преобразование сертификата в хранилище ключей Java

Получите сертификат клиента (и закрытый ключ) для зонда потока данных от центра сертификации в формате PFX/PKCS12 и преобразуйте его в хранилище ключей Java с помощью следующего сценария:

```
<директория установки зонда потока данных>\bin\jre\bin\keytool.exe -
importkeystore -srckeystore <полный путь к хранилищу ключей PFX> -
destkeystore <полный путь к новому хранилищу ключей> -srcstoretype
PKCS12
```

При этом будут запрошены пароли к исходному и целевому хранилищам ключей.

Для исходного хранилища ключей введите тот же пароль, который использовался при экспорте хранилища ключей PFX.

Пароль по умолчанию к целевому хранилищу ключей зонда потока данных: **logomania**.

Примечание. Если введенный пароль к целевому хранилищу ключей отличается от заданного по умолчанию (logomania), необходимо поместить новый пароль в зашифрованном виде в файл **<директория установки зонда потока данных>\conf\ssl.properties** (javax.net.ssl.keyStorePassword). Дополнительные сведения см. в разделе "Шифрование паролей хранилища ключей и доверительного хранилища" на странице 78.

Поместите новое хранилище ключей в следующую директорию: **<директория установки зонда потока данных>\conf\security**.

Внимание! Не перезаписывайте файл **MAMKeyStoreExp.jks**.

Настройка использования нового хранилища ключей в файле свойств SSL

Укажите в качестве хранилища ключей, содержащего сертификат клиента, в файле **<директория установки зонда потока данных>\conf\ssl.properties** значение **javax.net.ssl.keyStore**.

Если пароль к хранилищу ключей отличается от заданного для хранилища ключей зонда потока данных по умолчанию (logomania), зашифруйте пароль и обновите **javax.net.ssl.keyStorePassword**. Подробнее о шифровании паролей см. в разделе "Шифрование паролей хранилища ключей и доверительного хранилища" на странице 78.

Проверка конфигурации зонда потока данных

Измените файл **<директория установки зонда потока данных>\conf\DataFlowProbe.properties** следующим образом:

```
appilog.agent.probe.protocol = HTTPS

serverName = <адрес обратного прокси-сервера>

serverPortHttps = <порт HTTPS, который слушает обратный прокси-сервер
для перенаправления запросов в UCMDB>
```

Включение в UCMDB работу через SSL

Дополнительные сведения см. в разделе "Включение поддержки Secure Sockets Layer (SSL) " на странице 18.

Если сертификат сервера UCMDB выдан тем же центром сертификации, что и остальные сертификаты в данной процедуре, обратный прокси-сервер или балансировщик нагрузки будет доверять сертификату UCMDB.

Глава 4

Управление учетными данными потока данных

Данная глава включает:

Управление учетными данными потока данных: обзор

Для выполнения обнаружения или интеграции необходимо установить учетные данные для доступа к удаленной системе. Учетные данные настраиваются в окне "Настройка зонда для потока данных" и сохраняются на сервере UCMDB. Подробнее см. в разделе, посвященном установке зонда потока данных, в документе *Руководство по управлению потоками данных в HP Universal CMDB*.

Хранилище учетных данных управляется компонентом Confidential Manager. Дополнительные сведения см. в разделе "Confidential Manager" на странице 93.

Зонд потока может получать доступ к учетным данным, используя клиент Confidential Manager. Клиент Confidential Manager находится в зонде потока данных и обменивается данными с сервером Confidential Manager, находящимся на сервере UCMDB. Обмен информацией между клиентом Confidential Manager и сервером Confidential Manager шифруется. Клиент Confidential Manager запрашивает проверку подлинности при подключении к серверу Confidential Manager.

Для проверки подлинности клиента Confidential Manager на сервере Confidential Manager используется компонент LW-SSO. Перед подключением к серверу Confidential Manager клиент Confidential Manager в первую очередь отправляет LW-SSO файл "cookie". Сервер Confidential Manager проверяет файл "cookie". После успешной проверки начинается обмен информацией с клиентом Confidential Manager. Подробнее об LW-SSO см. в разделе "Настройка параметров LW-SSO" на странице 48.

Обмен информацией между клиентом Confidential Manager и сервером Confidential Manager шифруется. Подробнее об обновлении конфигурации шифрования см. в разделе "Установка настроек шифрования при передаче данных Confidential Manager " на странице 48.

Внимание! При проверке подлинности средствами Confidential Manager используется универсальное время, заданное на компьютере (UTC). Для успешной проверки подлинности время на сервере UCMDB и зонде потока данных должно совпадать. Сервер и зонд могут находиться в разных часовых поясах, поскольку время UTC не зависит от часового пояса или настроек летнего времени.

Клиент Confidential Manager сохраняет локальный кэш учетных данных. Клиент Confidential Manager настроен на загрузку всех учетных данных с сервера Confidential Manager и сохранение их в кэше. Изменения учетных данных автоматически и постоянно синхронизируются с сервера Confidential Manager. Кэш может сохраняться в файловой системе или в памяти, в зависимости от предварительных настроек. Кроме того, кэш шифруется и недоступен для внешнего доступа. Подробнее об обновлении настроек кэша см. в разделе "Настройка режима кэша клиента Confidential Manager на зонде" на странице 53. Подробнее об обновлении шифрования кэша см. в разделе "Установка настроек шифрования кэша клиента Confidential Manager на зонде" на странице 53.

Подробнее об устранении неполадок см. в разделе "Изменение уровня сообщений в файле журнала клиента Confidential Manager" на странице 56.

Информацию об учетных данных можно копировать с одного сервера UCMDB на другой. Дополнительные сведения см. в разделе "Экспорт и импорт учетных данных и сведений о диапазонах в зашифрованном формате" на странице 54.

Примечание. DomainScopeDocument (DSD), использовавшийся для хранения учетных данных в зонде (в версии UCMDB 9.01 и более ранних), более не содержит информации, входящей в учетные данные. Теперь в этом файле содержатся список зондов и сведения о сетевом диапазоне. В нем также содержится список записей учетных данных для каждого домена. Каждая запись включает идентификатор учетных данных и сетевой диапазон (определенный для этой конкретной записи учетных данных).

Этот раздел охватывает следующие темы:

Исходные предположения безопасности

Обратите внимание на следующее исходное предположение:

Настройки безопасности сервера UCMDB и консоли JMX предоставляют доступ к системе UCMDB только администраторам, предпочтительно только доступ localhost.

Работа зонда потока данных в режиме отдельного выполнения

Когда шлюз зонда и Диспетчер работают как отдельные процессы, клиентский компонент Confidential Manager становится частью процесса CM. Учетные данные кэшируются и используется только Диспетчером зондов. Для доступа к серверу Confidential Manager в системе UCMDB запрос клиента Confidential Manager обрабатывается процессом шлюза и перенаправляется системе UCMDB.

Эта конфигурация создается автоматически, когда зонд настраивается в режиме отдельного выполнения.

Регулярное обновление кэша учетных данных

При первом успешном подключении к серверу Confidential Manager клиент Confidential Manager загружает все соответствующие учетные данные (все учетные данные, настроенные в домене зонда). После первого успешного обмена информацией клиент Confidential Manager сохраняет постоянную синхронизацию с сервером Confidential Manager. Дифференциальная синхронизация выполняется с интервалами в одну минуту, в течение которых синхронизируются только различия между сервером Confidential Manager и клиентом Confidential Manager. Если учетные данные изменены на стороне сервера UCMDB (например, добавлены новые учетные данные, либо обновлены или удалены существующие), клиент Confidential Manager немедленно получает информацию от сервера UCMDB и выполняет дополнительную синхронизацию.

Синхронизация всех зондов с изменениями конфигурации

Для успешного обмена информацией конфигурация проверки подлинности сервера Confidential Manager (строка инициализации LW-SSO) и его конфигурация шифрования (шифрование связи Confidential Manager) должны переноситься на клиент Confidential Manager. Например, когда строка инициализации меняется на сервере, зонду должна быть известна новая строка инициализации, для успешного выполнения проверки подлинности.

Сервер UCMDB постоянно отслеживает изменения в конфигурациях шифрования связи и проверки подлинности Confidential Manager. Они проверяются каждые 15 секунд; в случае обнаружения изменений, обновленная конфигурация отсылается зондам. Конфигурация передается зондам в зашифрованной форме и сохраняется в безопасных хранилищах на стороне зондов. Шифрование отправляемой конфигурации выполняется с помощью ключа симметричного шифрования. По умолчанию, сервер UCMDB и зонд потока данных устанавливаются с одним и тем же ключом симметричного шифрования по умолчанию. Для достижения оптимального уровня безопасности настоятельно рекомендуется изменить ключ, перед добавлением к системе учетных данных. Дополнительные сведения см. в разделе "Создание или обновление ключа шифрования" на странице 57.

Примечание. Из-за того, что интервал мониторинга составляет 15 секунд, конфигурация клиента Confidential Manager на стороне зонда может быть обновлена с задержкой до 15 секунд.

В случае отключения автоматической синхронизации конфигурации связи и проверки подлинности Confidential Manager на сервере UCMDB и зонде потока данных, при каждом обновлении конфигурации связи и проверки подлинности Confidential Manager на стороне сервера UCMDB следует обновить и все зонды соответствующим образом. Дополнительные сведения см. в разделе "Отключение автоматической синхронизации настроек проверки подлинности и шифрования клиента Confidential Manager между сервером и зондами" на странице 50.

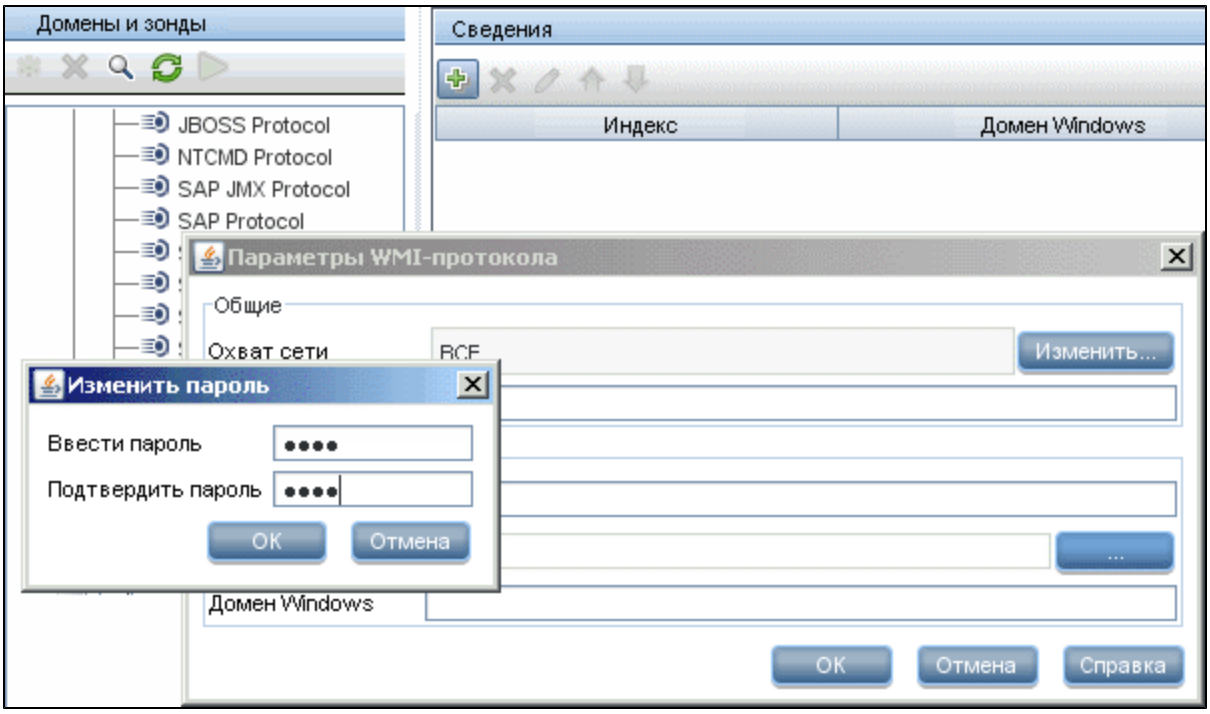
Безопасное хранение в зонде

Вся конфиденциальная информация (такая как конфигурация связи и проверки подлинности Confidential Manager, а также ключ шифрования) хранится в безопасном хранилище зонда, которым является файл **secured_storage.bin**, расположенный в каталоге **C:\hp\UCMDB\DataFlowProbe\conf\security**. Безопасное хранилище шифруется с использованием DPAPI и применением пароля пользователя Windows в процессе шифрования. DPAPI — стандартный метод защиты конфиденциальных данных, таких как сертификаты и закрытые ключи, на системах Windows. Зонд всегда должен запускаться одним и тем же пользователем Windows, чтобы даже при изменении пароля зонд мог бы прочесть его из безопасного хранилища.

Просмотр учетных данных

Примечание. В данном разделе описывается процедура просмотра учетных данных, когда данные передаются от CMDB в HP Universal CMDB

Пароли не отправляются от CMDB в приложение. То есть, HP Universal CMDB отображает звездочки (*) в поле пароля, вне зависимости от содержимого:



Обновление учетных данных

Примечание. В данном разделе описывается процедура обновления учетных данных, когда данные передаются от HP Universal CMDB в CMDB.

- Связь в этом направлении не шифруется, поэтому следует подключиться к серверу UCMDB, используя https\SSL, либо обеспечить подключение через доверенную сеть.

  Хотя связь не шифруется, пароли не отсылаются по сети открытым текстом. Они шифруются с помощью ключа по умолчанию, так что для обеспечения конфиденциальности при передаче настоятельно рекомендуется использовать SSL.

- В паролях можно использовать специальные символы и буквы иных алфавитов, кроме английского.

Установка настроек проверки подлинности и шифрования клиента Confidential Manager

В данной задаче описывается настройка проверки подлинности и шифрования клиента Confidential Manager на сервере UCMDB. Задача включает следующие шаги:

- "Настройка параметров LW-SSO" ниже
- "Установка настроек шифрования при передаче данных Confidential Manager " ниже

Настройка параметров LW-SSO

Данная процедура описывает изменение строки инициализации LW-SSO на сервере UCMDB. Данное изменение автоматически отправляется зондам (в форме зашифрованной строки), если такая отправка не отключена в настройках сервера UCMDB. Дополнительные сведения см. в разделе "Отключение автоматической синхронизации настроек проверки подлинности и шифрования клиента Confidential Manager между сервером и зондами" на странице 50.

1. Запустите веб-браузер на компьютере сервера UCMDB и введите следующий адрес: **http://localhost:8080/jmx-console**.
2. Щелкните **UCMDB-UI:name=LW-SSO Configuration**, чтобы открыть страницу просмотра JMX MBEAN.
3. Найдите метод **setInitString**.
4. Введите новую строку инициализации LW-SSO.
5. Нажмите кнопку Invoke.

Установка настроек шифрования при передаче данных Confidential Manager

Данная процедура описывает изменение настроек шифрования связи на сервере UCMDB. Эти настройки указывают, как шифруется обмен информацией между клиентом Confidential Manager и сервером Confidential Manager. Данное изменение автоматически отправляется зондам (в форме зашифрованной строки), если такая отправка не отключена в настройках сервера UCMDB. Дополнительные сведения см. в разделе "Отключение автоматической синхронизации настроек проверки подлинности и шифрования клиента Confidential Manager между сервером и зондами" на странице 50.

1. Запустите веб-браузер на компьютере сервера UCMDB и введите следующий адрес: **http://localhost:8080/jmx-console.**
2. Щелкните **UCMDB:service=Security Services**, чтобы открыть страницу просмотра JMX MBEAN.
3. Щелкните метод **CMGetConfiguration**.
4. Нажмите кнопку **Invoke**.

   Отобразится XML текущей конфигурации Confidential Manager.
5. Скопируйте содержимое отображенного XML.
6. Вернитесь на страницу просмотра JMX MBean **Службы безопасности**.
7. Щелкните метод **CMSetConfiguration**.
8. Вставьте скопированный XML в поле **Значение**.
9. Обновите настройки, относящиеся к транспорту.

   Подробнее о значениях, которые могут быть обновлены, см. в "Настройки шифрования Confidential Manager" на странице 61.

   Пример:

```
<transport>
        <encryptTransportMode>true</encryptTransportMode>
        <CMEncryptionDecryption>
                <encryptDecryptInitString>radiohead</encryptDecryptInitString>
                <cryptoSource>lw</cryptoSource>
                <lwJCEPBECompatibilityMode>true</lwJCEPBECompatibilityMode>
                <cipherType>symmetricBlockCipher</cipherType>
                <engineName>AES</engineName>
                <algorithmModeName>CBC</algorithmModeName>
                <algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
                <keySize>256</keySize>
                <pbeCount>20</pbeCount>
                <pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
                <encodingMode>Base64Url</encodingMode>
                <useMacWithCrypto>false</useMacWithCrypto>
                <macType>hmac</macType>
                <macKeySize>256</macKeySize>
                <macHashName>SHA256</macHashName>
        </CMEncryptionDecryption>
```

```
</transport>
```

10. Нажмите кнопку **Invoke**.

Установка настроек проверки подлинности и шифрования клиента Confidential Manager вручную на зонде

Эта задача включает следующие шаги:

- "Отключение автоматической синхронизации настроек проверки подлинности и шифрования клиента Confidential Manager между сервером и зондами" ниже
- "Установка настроек проверки подлинности и шифрования клиента Confidential Manager на зонде" на следующей странице
- "Установка настроек шифрования при передаче данных Confidential Manager на зонде" на следующей странице

Отключение автоматической синхронизации настроек проверки подлинности и шифрования клиента Confidential Manager между сервером и зондами

По умолчанию сервер UCMDB настроен на автоматическую отправку настроек Confidential Manager/LW-SSO всем зондам. Эта информация отправляется как зашифрованная строка всем зондам, а зонды ее дешифруют. Автоматическую отправку файлов конфигурации Confidential Manager/LW-SSO всем зондам можно отключить в настройках сервера UCMDB. В таком случае, перенос обновленных настроек Confidential Manager/LW-SSO на зонды необходимо выполнять вручную.

Чтобы отключить автоматическую синхронизацию настроек Confidential Manager/LWSSO:

1. В UCMDB щелкните **Администрирование > Диспетчер настроек инфраструктуры > Общие параметры**.
2. Выберите В**ключить автоматическую синхронизацию конфигурации CM/LW-SSO и строки инициализации с зондом**.
3. Щелкните поле **Значение** и измените **True** на **False**.
4. Нажмите кнопку **Save**.
5. Перезапустите CMDB.

Установка настроек проверки подлинности и шифрования клиента Confidential Manager на зонде

Эта процедура актуальна, если в настройках сервера UCMDB указано не отправлять зондам конфигурацию и настройки LW-SSO/Confidential Manager автоматически. Дополнительные сведения см. в разделе "Отключение автоматической синхронизации настроек проверки подлинности и шифрования клиента Confidential Manager между сервером и зондами" на предыдущей странице.

1. Запустите веб-браузер на компьютере зонда и введите следующий адрес: **http://localhost:1977**.

   Примечание. Если Диспетчер зондов и шлюз зонда работают как отдельные процессы, адрес следует вводить на компьютере, где работает Диспетчер зондов, как показано ниже: **http://localhost:1978**.

2. Щелкните **type=CMClient**, чтобы открыть страницу просмотра JMX MBEAN.
3. Найдите метод **setLWSSOInitString** и введите ту же строку инициализации, которая была введена для конфигурации LW-SSO в UCMDB.
4. Нажмите кнопку **setLWSSOInitString**.

Установка настроек шифрования при передаче данных Confidential Manager на зонде

Эта процедура актуальна, если в настройках сервера UCMDB указано не отправлять зондам конфигурацию и настройки LW-SSO/Confidential Manager автоматически. Дополнительные сведения см. в разделе "Отключение автоматической синхронизации настроек проверки подлинности и шифрования клиента Confidential Manager между сервером и зондами" на предыдущей странице.

1. Запустите веб-браузер на компьютере зонда и введите следующий адрес: **http://localhost:1977**.

   Примечание. Если Диспетчер зондов и шлюз зонда работают как отдельные процессы, адрес следует вводить на компьютере, где работает Диспетчер зондов, как показано ниже: **http://localhost:1978**.

2. Щелкните **type=CMClient**, чтобы открыть страницу просмотра JMX MBEAN.
3. Обновите следующие настройки, относящиеся к транспорту:

   Примечание. Необходимо обновить те же настройки, которые были обновлены на сервере UCMDB. Для выполнения этого, некоторые из методов, обновляемые на

зонде, могут потребовать более одного параметра. Чтобы увидеть текущую конфигурацию зонда, щелкните **displayTransportConfiguration** на странице просмотра JMX MBEAN. Дополнительные сведения см. в разделе "Установка настроек шифрования при передаче данных Confidential Manager " на странице 48. Подробнее о значениях, которые могут быть обновлены, см. в "Настройки шифрования Confidential Manager" на странице 61.

a. **setTransportInitString** изменяет настройку **encryptDecryptInitString**.

b. **setTransportEncryptionAlgorithm** изменяет настройки Confidential Manager на зонде в соответствии со следующими сопоставлениями:

   - **Имя механизма** относится к записи <engineName>
   - **Размер ключа** относится к записи <keySize>
   - **Имя холостого заполнения алгоритма** относится к записи <algorithmPaddingName>
   - **Счетчик PBE** относится к записи <pbeCount>
   - **Алгоритм представления PBE в краткой форме** относится к записи <pbeDigestAlgorithm>

c. **setTransportEncryptionLibrary** изменяет настройки Confidential Manager на зонде в соответствии со следующими сопоставлениями:

   - **Имя библиотеки шифрования** относится к записи <cryptoSource>
   - **Поддерживать предыдущие версии упрощенной криптографии** относится к записи <lwJCEPBECompatibilityMode>

d. **setTransportMacDetails** изменяет настройки Confidential Manager на зонде в соответствии со следующими сопоставлениями:

   - **Использовать MAC с криптографией** относится к записи <useMacWithCrypto>
   - **Размер ключа MAC** относится к записи <mackeySize>

4. Нажмите кнопку **reloadTransportConfiguration**, чтобы ввести в силу сделанные на зонде изменения.

Подробнее о различных настройках и их возможных значениях см. в разделе "Настройки шифрования Confidential Manager" на странице 61.

Настройка кэша клиента Confidential Manager

Эта задача включает следующие шаги:

- "Настройка режима кэша клиента Confidential Manager на зонде" на следующей странице
- "Установка настроек шифрования кэша клиента Confidential Manager на зонде" на следующей странице

Настройка режима кэша клиента Confidential Manager на зонде

Клиент Confidential Manager сохраняет учетные данные в кэше и обновляет их при изменении информации на сервере. Кэш может храниться в файловой системе или в памяти:

- **При сохранении в файловой системе** учетные данные будут доступны даже в случае перезапуска зонда и невозможности подключиться к серверу.
- **При сохранении в памяти** в случае перезапуска зонда и сопутствующей очистки кэша все данные необходимо снова получить от сервера. Если сервер недоступен, зонд останется без учетных данных, делая невозможным выполнение обнаружения или интеграции.

Чтобы изменить эту настройку:

1. Откройте в текстовом редакторе файл **DataFlowProbe.properties**. Этот файл расположен в папке **c:\hp\UCMDB\DataFlowProbe\conf**
2. Найдите следующий атрибут:
   com.hp.ucmdb.discovery.common.security.storeCMData=true
   - Для сохранения информации в файловой системе оставьте значение по умолчанию (**true**).
   - Для сохранения информации в памяти введите **false**.
3. Сохраните файл **DataFlowProbe.properties**.
4. Перезапустите зонд.

Установка настроек шифрования кэша клиента Confidential Manager на зонде

Данная процедура описывает изменение настроек шифрования в файле кэша файловой системы клиента Confidential Manager. Обратите внимание, что изменение настроек шифрования для кэша файловой системы клиента Confidential Manager вызывает создание файла кэша файловой системы заново. Процесс этого создания заново требует перезапуска зонда и полной синхронизации с сервером UCMDB.

1. Запустите веб-браузер на компьютере зонда и введите следующий адрес:
   http://localhost:1977.

   Примечание. Если Диспетчер зондов и шлюз зонда работают как отдельные процессы, адрес следует вводить на компьютере, где работает Диспетчер зондов, как показано ниже: **http://localhost:1978**.
2. Щелкните **type=CMClient**, чтобы открыть страницу просмотра JMX MBEAN.
3. Обновите следующие настройки, относящиеся к кэшу:

Примечание. Некоторые из методов, обновляемые на зонде, могут потребовать более одного параметра. Чтобы увидеть текущую конфигурацию зонда, щелкните **displayCacheConfiguration** на странице просмотра JMX MBEAN.

a. **setCacheInitString** изменяет настройку кэша файловой системы <encryptDecryptInitString>.

b. **setCacheEncryptionAlgorithm** изменяет настройки кэша файловой системы в соответствии со следующими сопоставлениями:

- **Имя механизма** относится к записи <engineName>
- **Размер ключа** относится к записи <keySize>
- **Имя холостого заполнения алгоритма** относится к записи <algorithmPaddingName>
- **Счетчик PBE** относится к записи <pbeCount>
- **Алгоритм представления PBE в краткой форме** относится к записи <pbeDigestAlgorithm>

c. **setCacheEncryptionLibrary** изменяет настройки кэша файловой системы в соответствии со следующими сопоставлениями:

- **Имя библиотеки шифрования** относится к записи <cryptoSource>
- **Поддерживать предыдущие версии упрощенной криптографии** относится к записи <lwJCEPBECompatibilityMode>

d. **setCacheEncryptionDetails** изменяет настройки кэша файловой системы в соответствии со следующими сопоставлениями:

- **Использовать MAC с криптографией** относится к записи <useMacWithCrypto>
- **Размер ключа MAC** относится к записи <mackeySize>

4. Нажмите кнопку **reloadCacheConfiguration**, чтобы ввести в силу сделанные на зонде изменения. Это вызовет перезапуск зонда.

Примечание. Убедитесь, что на зонде не выполняется никаких заданий во время этого действия.

Подробнее о различных настройках и их возможных значениях см. в разделе "Настройки шифрования Confidential Manager" на странице 61.

Экспорт и импорт учетных данных и сведений о диапазонах в зашифрованном формате

Учетные данные и информацию о сетевых диапазонах можно импортировать и экспортировать в зашифрованном формате для копирования учетных данных с одного

сервера UCMDB на другой. Например, эту операцию может понадобиться выполнить при восстановлении системы после сбоя или при обновлении.

- **При экспорте учетных данных** необходимо ввести пароль (по своему выбору). Информация шифруется с помощью этого пароля.
- **При импорте учетных данных** необходимо использовать тот же пароль, который был определен при экспорте файла DSD.

Примечание. Экспортированный документ учетных данных также содержит сведения о диапазонах, определенных в системе, из которой экспортирован документ. При экспорте документа учетных данных экспортируются и сведения о диапазонах.

Внимание! Для импорта учетных данных из domainScopeDocument UCMDB версии 8.02 необходимо использовать файл key.bin, расположенный на системе версии 8.02.

Для экспорта учетных данных с сервера UCMDB:

1. Запустите веб-браузер на компьютере сервера UCMDB и введите следующий адрес: **http://localhost:8080/jmx-console**. Возможно, потребуется ввести имя пользователя и пароль для входа в систему.
2. Нажмите **UCMDB:service=DiscoveryManager**, чтобы открыть страницу JMX MBEAN View.
3. Найдите операцию **exportCredentialsAndRangesInformation**. Выполните следующие действия:
   - Введите свой идентификатор клиента (по умолчанию — 1).
   - Введите имя экспортированного файла.
   - Введите свой пароль.
   - Установить **isEncrypted=True**, если необходимо, чтобы экспортированный файл был зашифрован с помощью предоставленного пароля, либо **isEncrypted=False**, если экспортированный файл не следуют шифровать (в этом случае пароли и иная конфиденциальная информация не экспортируются).
4. Нажмите **Invoke**, чтобы выполнить экспорт.

   После успешного выполнения процесса экспорта файл будет сохранен по следующему пути: **C:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**.

Для импорта учетных данных с сервера UCMDB:

1. Запустите веб-браузер на компьютере сервера UCMDB и введите следующий адрес: **http://localhost:8080/jmx-console**.

   Возможно, потребуется ввести имя пользователя и пароль для входа в систему.
2. Нажмите **UCMDB:service=DiscoveryManager**, чтобы открыть страницу JMX MBEAN View.
3. Выберите одну из следующих операций:

- Найдите операцию **importCredentialsAndRangesInformation**, если импортируемый файл был экспортирован с сервера UCMDB более поздней версии, чем 8.02.
- Найдите операцию **importCredentialsAndRangesWithKey**, если импортируемый файл был экспортирован с сервера UCMDB версии 8.02.

4. Введите свой идентификатор клиента (по умолчанию — 1).
5. Введите имя файла, который следует импортировать. Этот файл должен быть расположен в директории **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**.
6. Введите пароль. Это должен быть тот же пароль, который был использован при экспорте файла.
7. Если файл был экспортирован из системы UCMDB версии 8.02, введите имя файла **key.bin**. Этот файл должен быть расположен в каталоге **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**, вместе с файлом, который предстоит импортировать.
8. Нажмите **Invoke**, чтобы импортировать учетные данные.

Изменение уровня сообщений в файле журнала клиента Confidential Manager

Зонд предоставляет два файла журнала, содержащих сведения об обмене информацией Confidential Manager между клиентом Confidential Manager и сервером Confidential Manager. Это следующий файлы:

- "Файл журнала клиента Confidential Manager" ниже
- "Файл журнала LW-SSO" на следующей странице

Файл журнала клиента Confidential Manager

Файл **security.cm.log** расположен в папке **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

Данный журнал содержит информационные сообщения, которыми обмениваются клиент Confidential Manager и сервер Confidential Manager. По умолчанию, уровень журнала этих сообщений установлен на "Сведения".

Чтобы сменить уровень журнала на "Отладка":

1. На сервере Диспетчера зондов потоков данных перейдите к **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Откройте в текстовом редакторе файл **security.properties**.
3. Измените строку:

   ```
   loglevel.cm=INFO
   ```

   на:

   ```
   loglevel.cm=DEBUG
   ```

4. Сохраните файл.

Файл журнала LW-SSO

Файл **security.lwsso.log** расположен в каталоге **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

Данный журнал содержит информационные сообщения, относящиеся к LW-SSO. По умолчанию, уровень журнала этих сообщений установлен на "Сведения".

Чтобы сменить уровень журнала на "Отладка":

1. На сервере Диспетчера зондов потоков данных перейдите к **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Откройте в текстовом редакторе файл security.properties.
3. Измените строку:

   ```
   loglevel.lwsso=INFO
   ```

   на:

   ```
   loglevel.lwsso=DEBUG
   ```

4. Сохраните файл.

Создание или обновление ключа шифрования

Пользователь может создать или обновить ключ шифрования, используемый для шифрования или дешифрования конфигураций связи и проверки подлинности Confidential Manager, которыми обмениваются сервер UCMDB и зонд потока данных. В обоих случаях (создания или обновления), сервер UCMDB создает новый ключ шифрования, основанный на предоставленных параметрах (длина ключа, дополнительные циклы PBE, поставщик JCE) и распределяет его между зондами.

Результатом выполнения метода **generateEncryptionKey** является создание нового ключа шифрования. Этот ключ хранится только в защищенном хранилище. Его название и сведения о нем остаются неизвестны. Если переустановить существующий зонд потока данных, либо подключить новый зонд к серверу UCMDB, этот новый ключ не распознается новым зондом. В таких случаях предпочтительно использовать метод **changeEncryptionKey** для изменения ключей шифрования. Это позволяет, в случае переустановки зонда или установки нового, импортировать существующий ключ (имя и местоположение которого известны), запустив метод **importEncryptionKey** на консоли Probe JMX.

Примечание.

- Различие между методами, используемыми для создания ключа (**generateEncryptionKey**) и обновления ключа (**changeEncryptionKey**), состоит в том, что **generateEncryptionKey** создает новый, случайный ключ шифрования, тогда как **changeEncryptionKey** импортирует ключ шифрования, имя которого предоставлено пользователем.

- В системе может существовать только один ключ шифрования, вне зависимости от числа установленных зондов.

Эта задача включает следующие шаги:

- "Создание нового ключа шифрования" ниже
- "Обновление ключа шифрования на сервере UCMDB" на следующей странице
- "Обновление ключа шифрования на зонде" на странице 60
- "Изменение ключа шифрования вручную, когда Диспетчер зондов и шлюз зонда установлены на отдельных компьютерах" на странице 61
- "Определение нескольких поставщиков JCE" на странице 61

Создание нового ключа шифрования

Пользователь может создать новый ключ для использования сервером UCMDB и зондом потока данных в целях шифрования или дешифрования. Сервер UCMDB замещает старый ключ свежесозданным ключом и распределяет этот ключ среди зондов.

Чтобы создать новый ключ шифрования через консоль JMX:

1. Запустите веб-браузер на компьютере сервера UCMDB и введите следующий адрес: **http://localhost:8080/jmx-console**.

   Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

2. Нажмите **UCMDB:service=DiscoveryManager**, чтобы открыть страницу JMX MBEAN View.

3. Найдите операцию generateEncryptionKey.

   a. В окне параметров **customerId** введите 1 (значение по умолчанию).

   b. В **keySize** укажите длину ключа шифрования. Допустимые значения – 128, 192 или 256.

   c. Для **usePBE**, укажите **True** или **False**:

      - **True:** использовать дополнительные циклы хеша PBE.
      - **False:** не использовать дополнительные циклы хеша PBE.

   d. Для **jceVendor** можно использовать иного поставщика JCE, чем поставщик по умолчанию. Если окно пусто, будет использован поставщик по умолчанию

   e. Для **autoUpdateProbe**, укажите **True** или **False**:

      - **True:** сервер автоматически рассылает новый ключ зондам.
      - **False:** новый ключ следует разослать зондам вручную.

   f. Для **exportEncryptionKey**, укажите **True** или **False**:

      - **True:** Помимо создания нового пароля и размещения его в безопасном хранилище, сервер экспортирует новый пароль в файловую систему

(**c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**). Этот вариант позволяет вручную перевести зонды на новый пароль.

- **False:** Новый пароль не экспортируется в файловую систему. Чтобы обновить зонды вручную, установите **autoUpdateProbe** на False и **exportEncryptionKey** на True.

> **Примечание.** Убедитесь, что зонд работает и подключен к серверу. В случае отключения зонда, ключ не достигнет его. Если изменить ключ перед отключением зонда, то при последующем включении зонда ключ будет отправлен ему снова. Однако если ключ был изменен более чем один раз перед отключением зонда, то его необходимо будет изменить вручную через консоль JMX. (Выберите **False** для **exportEncryptionKey**).

4. Щелкните **Invoke**, чтобы создать ключ шифрования.

Обновление ключа шифрования на сервере UCMDB

Метод **changeEncryptionKey** можно использовать для импорта собственного ключа шифрования на сервер UCMDB и распространения его среди зондов.

Чтобы обновить ключ шифрования через консоль JMX:

1. Запустите веб-браузер на компьютере сервера UCMDB и введите следующий адрес: **http://localhost:8080/jmx-console.**

   Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

2. Нажмите **UCMDB:service=DiscoveryManager**, чтобы открыть страницу JMX MBEAN View.

3. Найдите операцию **changeEncryptionKey**.

   a. В окне параметров **customerId** введите **1** (значение по умолчанию).

   b. Введите имя нового ключа в **newKeyFileName**.

   c. В **keySizeInBits** укажите длину ключа шифрования. Допустимые значения – 128, 192 или 256.

   d. Для **usePBE**, укажите **True** или **False**:

      - **True:** использовать дополнительные циклы хеша PBE.
      - **False:** не использовать дополнительные циклы хеша PBE.

   e. Для **jceVendor** можно использовать иного поставщика JCE, чем поставщик по умолчанию. Если окно пусто, будет использован поставщик по умолчанию

   f. Для **autoUpdateProbe**, укажите **True** или **False**:

- **True:** сервер автоматически рассылает новый ключ зондам.
- **False:** новый ключ следует разослать зондам вручную, с помощью консоли JMX зонда.

> **Примечание.** Убедитесь, что зонд работает и подключен к серверу. В случае отключения зонда, ключ не достигнет его. Если изменить ключ перед отключением зонда, то при последующем включении зонда ключ будет отправлен ему снова. Однако если ключ был изменен более чем один раз перед отключением зонда, то его необходимо будет изменить вручную через консоль JMX. (Выберите **False** для **autoUpdateProbe**).

4. Щелкните **Invoke**, чтобы создать и обновить ключ шифрования.

Обновление ключа шифрования на зонде

Если решено не рассылать ключ шифрования с сервера UCMDB всем зондам автоматически (по соображениям безопасности), следует загрузить новый ключ шифрования на все зонды и использовать метод **importEncryptionKey** на зонде:

1. Поместите файл ключа шифрования в директорию **C:\hp\UCMDB\DataFlowProbe\conf\security**.
2. Запустите веб-браузер на компьютере зонда и введите следующий адрес: **http://localhost:1977**.

   Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

   > **Примечание.** Если Диспетчер зондов и шлюз зонда работают как отдельные процессы, адрес следует вводить на компьютере, где работает Диспетчер зондов, как показано ниже: **http://localhost:1978**.

3. на машине зонда нажмите **type=SecurityManagerService**.
4. Найдите метод **importEncryptionKey**.
5. Введите название файла ключа шифрования, находящегося в директории **C:\hp\UCMDB\DataFlowProbe\conf\security** Этот файл содержит ключ, который следует импортировать.
6. Нажмите кнопку **importEncryptionKey**.
7. Перезапустите зонд.

Изменение ключа шифрования вручную, когда Диспетчер зондов и шлюз зонда установлены на отдельных компьютерах

1. Запустите службу шлюза зонда на компьютере Диспетчера зондов (**Пуск > Программы > HP UCMDB > Шлюз зонда**).
2. Импортируйте ключ с сервера, используя JMX Диспетчера зонда. Дополнительные сведения см. в разделе "Создание нового ключа шифрования" на странице 58.
3. После успешного импорта ключа шифрования перезапустите службы Диспетчера зондов и шлюза зонда.

Определение нескольких поставщиков JCE

После создания ключа шифрования с помощью консоли JMX можно определить нескольких поставщиков JCE, используя методы **changeEncryptionKey** и **generateEncryptionKey**.

Чтобы сменить поставщика JCE по умолчанию:

1. Зарегистрируйте файлы jar поставщика JCE в директории **$JRE_HOME/lib/ext**.
2. Скопируйте файлы jar в папку $JRE_HOME:
   - Для сервера CMDB: $JRE_HOME находится в папке: **c:\hp\UCMDB\UCMDBServer\bin\jre**
   - Для зонда потока данных: $JRE_HOME находится в папке: **c:\hp\UCMDB\DataFlowProbe\bin\jre**
3. Добавьте класс поставщика в конец списка поставщиков, находящегося в файле **$JRE_HOME\lib\security\java.security**.
4. Обновите файлы **local_policy.jar** и **US_export_policy.jar**, чтобы они включали неограниченное количество политик JCE. Эти файлы jar можно загрузить с вебсайта Sun.
5. Перезапустите сервер UCMDB и зонд потока данных.
6. Найдите поле поставщика JCE для метода **changeEncryptionKey** или **generateEncryptionKey** и добавьте имя поставщика JCE.

Настройки шифрования Confidential Manager

В данной таблице перечислены настройки шифрования, которые можно изменить с помощью различных методов JMX. Эти настройки относятся к шифрованию обмена информацией между клиентом Confidential Manager и сервером Confidential Manager, а также кэша клиента Confidential Manager.

Имя настройки Confidential Manager	Имя настройки Confidential Manager на зонде	Описание настройки	Возможные значения	Значение по умолчанию
cryptoSource	Имя библиотеки шифрования	Эта настройка определяет, какую библиотеку шифрования следует использовать.	lw, jce, windowsDPAPI, lwJCECompatibl-e	lw
lwJCEPBE Compatibility Mode	Поддерживать предыдущие версии упрощенной криптографии	Эта настройка определяет, следует ли поддерживать предыдущие версии упрощенной криптографии.	true, false	true
engineName	Имя механизма	Имя механизма шифрования	AES, DES, 3DES, Blowfish	AES
keySize	Размер ключа	длина ключа шифрования в битах	Для AES – 128, 192 или 256; Для DES - 64; Для 3DES - 192; для Blowfish — любое число между 32 и 448	256
algorithm Padding Name	Имя холостого заполнения алгоритма	Стандарты холостого заполнения	PKCS7Padding, PKCS5Padding	PKCS7Paddin-g
pbeCount	Счетчик PBE	Число циклов хеширования для создания ключа из пароля (строки инициализации)	Любое положительное число	20
pbeDigest Algorithm	Алгоритм представления PBE в краткой форме	Тип хеширования	SHA1, SHA256, MD5	SHA1
useMacWith Crypto	Использовать MAC с криптографией	Указание использовать MAC с криптографией	true, false	false
macKeySize	Размер ключа MAC	Зависит от алгоритма MAC	256	256

Устранение неполадок и ограничения

При смене имени домена по умолчанию на сервере UCMDB необходимо сначала отключить зонды потока данных. После применения нового имени домена по умолчанию необходимо запустить сценарий **DataFlowProbe\tools\clearProbeData.bat** на зонде потока данных.

Примечание. Выполнение сценария clearProbeData.bat запустит цикл обнаружения на зонде потока данных после запуска зонда.

Глава 5

Повышение безопасности зонда потока данных

Данная глава включает:

Изменение зашифрованного пароля базы данных MySQL

В данном разделе объясняется, как изменить зашифрованный пароль для пользователя базы данных MySQL.

1. Создание зашифрованной формы пароля (AES, 192-битный ключ)

   a. Войдите в консоль JMX зонда потока данных. Запустите веб-браузер и введите следующий адрес: **http://<имя или IP-адрес компьютера зонда потока**

данных>:1977. В случае, если зонд потока данных работает локально, введите **http://localhost:1977**.

Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

Примечание. Если пользователь не создан, используйте для входа в систему имя пользователя по умолчанию sysadmin и пароль sysadmin.

b. Найдите службу **Type=MainProbe** и щелкните ссылку, чтобы открыть страницу "Operations".

c. Найдите операцию **getEncryptedDBPassword**.

d. В поле **DB Password** введите пароль для шифрования.

e. Вызовите операцию, нажав кнопку **getEncryptedDBPassword**.

Результатом вызова станет зашифрованная строка пароля, например:

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,
112,65,61,61
```

2. Остановка зонда потока данных

Пуск > Все программы > HP UCMDB > Остановить зонд потока данных

3. Выполните сценарий set_dbuser_password.cmd

Этот сценарий расположен в следующей папке:
C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\set_dbuser_password.cmd

Запустите сценарий **set_dbuser_password.cmd** с новым паролем в качестве первого аргумента и паролем к корневой учетной записи MySQL в качестве второго аргумента (или оставьте второй аргумент пустым, если корневая учетная запись MySQL не защищена паролем).

Пример:

set_dbuser_password <my_password><root_password>.

Пароль должен быть введен в незашифрованной форме (открытым текстом).

4. Обновите пароль в файлах конфигурации зонда потока данных

a. Пароль должен находиться в файлах конфигурации зашифрованным. Для извлечения зашифрованной формы пароля, используйте метод JMX **getEncryptedDBPassword**, как описано в шаге 1.

b. Добавьте зашифрованный пароль в следующие свойства в файле **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

- **appilog.agent.probe.jdbc.pwd**

  Пример:

```
appilog.agent.probe.jdbc.user = mamprobe
appilog.agent.probe.jdbc.pwd =
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,
114,112,65,61,61
```

- **appilog.agent.local.jdbc.pwd**
- **appilog.agent.normalization.jdbc.pwd**

5. Запустите зонд потока данных

   Пуск > Все программы > HP UCMDB > Запустить зонд потока данных

Сценарий clearProbeData.bat: Использование

Сценарий **clearProbeData.bat** воссоздает пользователя базы данных, не изменяя его текущий пароль.

Сценарий ожидает пароль корневой учетной записи MySQL в качестве первого аргумента. Если параметр не передан, сценарий считает, что пароль корневой учетной записи MySQL не задан.

После выполнения сценария:

- Проверьте на наличие ошибок следующий файл: **C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log**
- Удалите следующий файл, поскольку он содержит пароль базы данных: **C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log**

Указание зашифрованного пароля консоли JMX

В данном разделе объясняется, как зашифровать пароль для пользователя консоли JMX. Зашифрованный пароль хранится в файле DataFlowProbe.properties. Для доступа к консоли JMX пользователь должен войти в систему.

1. **Создание зашифрованной формы пароля (AES, 192-битный ключ)**

   a. Войдите в консоль JMX зонда потока данных. Запустите веб-браузер и введите следующий адрес: **http://<имя или IP-адрес компьютера зонда потока данных>:1977**. В случае, если зонд потока данных работает локально, введите **http://localhost:1977**.

   Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

   > **Примечание.** Если пользователь не создан, используйте для входа в систему имя пользователя по умолчанию sysadmin и пароль sysadmin.

   b. Найдите службу **Type=MainProbe** и щелкните ссылку, чтобы открыть страницу "Operations".

   c. Найдите операцию **getEncryptedKeyPassword**.

   d. Введите пароль для шифрования в поле **Key Password**.

   e. Вызовите операцию, нажав кнопку **getEncryptedKeyPassword**.

Результатом вызова станет зашифрованная строка пароля, например:

```
85,-9,-61,11,105,-93,-81,118
```

2. **Остановка зонда потока данных**

   Пуск > Все программы > HP UCMDB > Остановить зонд потока данных

3. **Добавление зашифрованного пароля**

   Добавьте зашифрованный пароль в следующее свойство в файле **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

   appilog.agent.Probe.JMX.BasicAuth.Pwd

   Пример:

```
appilog.agent.Probe.JMX.BasicAuth.User=sysadmin
appilog.agent.Probe.JMX.BasicAuth.Pwd=12,-35,-37,82,-2,20,57,-40,
38,80,-111,-99,-64,-5,35,-122
```

   Примечание. Для отключения проверки подлинности, оставьте эти поля пустыми. В этом случае пользователи смогут открывать главную страницу консоли JMX зонда, не удостоверяя свою подлинность.

4. **Запустите зонд потока данных**

   Пуск > Все программы > HP UCMDB > Запустить зонд потока данных

   Протестируйте результаты в веб-браузере.

Установка пароля UpLoadScanFile

В данном разделе объясняется, как задать пароль **UpLoadScanFile**, который используется для внешнего сохранения результатов сканирования. Зашифрованный пароль хранится в файле **DataFlowProbe.properties**. Для доступа к консоли JMX пользователь должен войти в систему.

1. **Создание зашифрованной формы пароля (AES, 192-битный ключ)**

   a. Войдите в консоль JMX зонда потока данных. Запустите веб-браузер и введите следующий адрес: **http://<имя или IP-адрес компьютера зонда потока данных>:1977**. В случае, если зонд потока данных работает локально, введите **http://localhost:1977**.

   Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

   Примечание. Если пользователь не создан, используйте для входа в систему имя пользователя по умолчанию sysadmin и пароль sysadmin.

   b. Найдите службу **Type=MainProbe** и щелкните ссылку, чтобы открыть страницу "Operations".

   c. Найдите операцию **getEncryptedKeyPassword**.

d. Введите пароль для шифрования в поле **Key Password**.

e. Вызовите операцию, нажав кнопку **getEncryptedKeyPassword**.

Результатом вызова станет зашифрованная строка пароля, например:

```
85,-9,-61,11,105,-93,-81,118
```

2. **Остановка зонда потока данных**

Пуск > Все программы > HP UCMDB > Остановить зонд потока данных

3. **Добавление зашифрованного пароля**

Добавьте зашифрованный пароль в следующее свойство в файле **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

appilog.agent.Probe.JMX.BasicAuth.Pwd

Пример:

```
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User=UploadScanFile
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd=116,116,21,34,-59,
77,-108,14,127,4,-89,101,-33,-31,116,53
```

4. **Запустите зонд потока данных**

Пуск > Все программы > HP UCMDB > Запустить зонд потока данных

Протестируйте результаты в веб-браузере.

Удаленный доступ к серверу MySQL

В данном разделе описывается, как разрешить/ограничить доступ к учетной записи MySQL зонда потока данных с удаленных машин.

Примечание.

- По умолчанию доступ запрещен.
- Доступ к учетной записи MySQL зонда потока данных с удаленных машин закрыт.

Чтобы разрешить доступ к MySQL:

1. Запустите в командной строке следующий сценарий:

C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\enable_remote_user_access.cmd

2. По запросу введите пароль корневой учетной записи MySQL в качестве первого аргумента (этот пароль совпадает с указанным при установке зонда).

Чтобы ограничить доступ к MySQL:

1. Запустите в командной строке следующий сценарий:

C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\remove_remote_user_access.cmd

2. По запросу введите пароль корневой учетной записи MySQL в качестве первого аргумента (этот пароль совпадает с указанным при установке зонда).

Включение использования SSL с взаимной проверкой подлинности между сервером UCMDB и зондом потока данных

Для сервера UCMDB и зонда потока данных можно установить проверку подлинности с помощью сертификатов. Сертификат для каждого компонента отправляется и проверяется перед установкой подключения.

Примечание. Нижеприведенный метод включения SSL на зонде потока данных с взаимной проверкой подлинности является наиболее безопасным из методов и в силу этого рекомендуемым режимом связи. Данный метод заменяет процедуру обычной проверки подлинности.

Этот раздел охватывает следующие темы:

Обзор

UCMDB поддерживает следующие режимы связи между сервером UCMDB и зондом потока данных:

- **Проверка подлинности сервера.** Этот режим использует SSL. Зонд проверяет подлинность сертификата сервера UCMDB. Дополнительные сведения см. в разделе "Включение SSL с проверкой подлинности сервера (односторонней)" на следующей странице.
- **Взаимная проверка подлинности.** Этот режим использует SSL и включает как проверку подлинности сервера зондом, так и проверку подлинности клиента сервером. Дополнительные сведения см. в разделе "Включение взаимной проверки подлинности (двусторонней)" на странице 73.
- **Стандартный режим HTTP.** Без использования SSL. Это режим по умолчанию, в котором компонент зонда потока данных в UCMDB не требует никаких сертификатов. Зонд потока данных обменивается информацией с сервером через простой протокол HTTP.

Примечание. Использование цепочек сертификатов в процессе обнаружения при использовании SSL не поддерживается. Поэтому при использовании цепочек сертификатов необходимо создать самоподписанный сертификат, который позволит зонду потока данных подключиться к серверу UCMDB.

Хранилища ключей и доверительные хранилища

Серверы UCMDB и зонды потока данных работают с хранилищами ключей и доверительными хранилищами:

- **Хранилище ключей.** Файл, содержащий записи ключа (сертификат и соответствующий ему закрытый ключ).
- **Доверительное хранилище.** Файл, содержащий сертификаты, используемые для проверки удаленного хоста (например, при использовании проверки подлинности сервера, хранилище доверия зонда потока данных должно включать сертификат сервера UCMDB).

Ограничение взаимной проверки подлинности

Хранилище ключей зонда потока данных (определенное в **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**) должно содержать 1 (одну) запись ключа.

Включение SSL с проверкой подлинности сервера (односторонней)

Этот режим использует SSL. Зонд проверяет подлинность сертификата сервера.

Эта задача охватывает следующие темы:

- "Необходимые условия" ниже
- "Конфигурация сервера UCMDB" ниже
- "Конфигурация зонда потока данных" на странице 72
- "Перезапуск компьютеров" на странице 72

Необходимые условия

1. Убедитесь, что работает и UCMDB, и зонд потока данных.

   Примечание. Если зонд установлен в режиме отдельного выполнения, эти инструкции относятся к шлюзу зонда.

2. Если UCMDB или зонд потока данных установлены в нестандартных директориях, измените команды соответствующим образом.

Конфигурация сервера UCMDB

1. **Экспортируйте сертификат UCMDB**

   a. Откройте командную строку и выполните команду:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias
   <keystore alias> -keystore <Keystore file path> -file
   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

где:

- **keystore alias** – это имя, присвоенное хранилищу ключей.
- **Keystore file path** – полный путь к файлу хранилища ключей.

К примеру, для стандартного хранилища ключей сервера используется следующая команда:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -
alias hpcert -keystore
C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
```

b. Введите пароль хранилища ключей. Например, пароль к стандартному хранилищу ключей – **hppass**

c. Убедитесь, что в следующем каталоге создан сертификат: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Защитите соединитель зонда потока данных в UCMDB**

a. Откройте консоль JMX UCMDB: В веб-браузере введите следующий URL-адрес: **http://<имя или IP-адрес компьютера UCMDB>:8080/jmx-console**. Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

b. Выберите службу: **Ports Management Services**.

c. Вызовите метод **PortsDetails** и обратите внимание, какой порт используется для HTTPS. (По умолчанию: 8443) Убедитесь, что в столбце **Is Enabled** указано значение **True**.

d. Вернитесь в **Ports Management Services**.

e. Чтобы сопоставить соединитель зонда потока данных с режимом проверки подлинности сервера, вызовите метод **mapComponentToConnectors** со следующими параметрами:

- **componentName**: mam-collectors
- **isHTTPS**: true
- **Все остальные флаги**: false

Выводится следующее сообщение:

Operation succeeded. Component mam-collectors is now mapped to: порты HTTPS.

f. Вернитесь в **Ports Management Services**.

g. Чтобы сопоставить соединитель Confidential Manager с режимом взаимной проверки подлинности, вызовите метод **mapComponentToConnectors** со следующими параметрами:

- **componentName**: cm
- **isHTTPS**: true
- **Все остальные флаги**: false

Выводится следующее сообщение:

Operation succeeded. Component cm is now mapped to: порты HTTPS.

3. **Скопируйте сертификат UCMDB на каждую машину зонда**

   Скопируйте файл сертификата, **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**, с машины сервера UCMDB на каждую машину зонда потока данных **C:\HP\UCMDB\DataFlowProbe\conf\security**

Конфигурация зонда потока данных

Примечание. Необходимо настроить каждую машину зонда потока данных.

1. **Импортируйте файл server.cert, созданный в** "Экспортируйте сертификат UCMDB" на странице 70**, в доверительное хранилище на зонде.**

   a. Откройте командную строку и выполните команду:

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore C:\HP\UCMDB\DataFlowProbe\conf\security\MAMTrustStoreExp.jks -file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -alias ucmdbcert
   ```

   b. Введите пароль хранилища ключей: logomania

   c. При появлении вопроса **Доверять этому сертификату?** нажмите **y**, а затем **Enter**.

   Выводится следующее сообщение:

   Сертификат добавлен в хранилище ключей.

2. **Откройте файл DiscoveryProbe.properties, расположенный в папке: C:\HP\UCMDB\DataFlowProbe\conf**

   a. Смените свойство **appilog.agent.probe.protocol** на **HTTPS**.

   b. Укажите в свойстве **serverPortHttps** соответствующий номер порта. (Используйте номер порта из шага 2c в задаче "Конфигурация сервера UCMDB" на странице 70.)

Перезапуск компьютеров

Перезапустите сервер UCMDB и машины с зондами.

Включение взаимной проверки подлинности (двусторонней)

Этот режим использует SSL и включает как проверку подлинности сервера зондом, так и проверку подлинности клиента сервером. И сервер, и зонд отправляют свои сертификаты соответствующей сущности для проверки их подлинности.

Эта задача охватывает следующие темы:

Необходимые условия

1. Убедитесь, что работает и UCMDB, и зонд потока данных.

   Примечание. Если зонд установлен в режиме отдельного выполнения, эти инструкции относятся к шлюзу зонда.

2. Если UCMDB или зонд потока данных установлены в нестандартных директориях, измените команды соответствующим образом.

Начальная конфигурация сервера UCMDB

1. **Экспортируйте сертификат UCMDB**

   a. Откройте командную строку и выполните команду:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias
   <keystore alias> -keystore <Keystore file path> -file
   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   где:

   - **keystore alias** – это имя, присвоенное хранилищу ключей.
   - **Keystore file path** – полный путь к файлу хранилища ключей.

   К примеру, для стандартного хранилища ключей сервера используется следующая команда:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -
   alias hpcert -keystore
   C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file
   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   b. Введите пароль хранилища ключей. Например, пароль к стандартному хранилищу ключей – **hppass**

c. Убедитесь, что в следующем каталоге создан сертификат: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Защитите соединитель зонда потока данных в UCMDB**

a. Откройте консоль JMX UCMDB: В веб-браузере введите следующий URL-адрес: **http://<имя или IP-адрес компьютера UCMDB>:8080/jmx-console**. Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

b. Выберите службу: **Ports Management Services**.

c. Вызовите метод **PortsDetails** и обратите внимание, какой порт используется для HTTPS с проверкой подлинности клиента. (По умолчанию: 8444) Убедитесь, что в столбце **Is Enabled** указано значение **True**.

d. Вернитесь в **Ports Management Services**.

e. Чтобы сопоставить соединитель зонда потока данных с режимом взаимной проверки подлинности, вызовите метод **mapComponentToConnectors** со следующими параметрами:

- **componentName**: mam-collectors
- **isHTTPSWithClientAuth**: true
- **Все остальные флаги**: false

Выводится следующее сообщение:

Operation succeeded. Component mam-collectors is now mapped to: HTTPS_CLIENT_AUTH ports.

f. Вернитесь в **Ports Management Services**.

g. Чтобы сопоставить соединитель Confidential Manager с режимом взаимной проверки подлинности, вызовите метод **mapComponentToConnectors** со следующими параметрами:

- **componentName**: cm
- **isHTTPSWithClientAuth**: true
- **Все остальные флаги**: false

Выводится следующее сообщение:

Operation succeeded. Component cm is now mapped to: HTTPS_CLIENT_AUTH ports.

3. **Скопируйте сертификат UCMDB на каждую машину зонда**

Скопируйте файл сертификата, **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**, с машины сервера UCMDB на каждую машину зонда потока данных **C:\HP\UCMDB\DataFlowProbe\conf\security**

Конфигурация зонда потока данных

Примечание. Необходимо настроить каждую машину зонда потока данных.

1. **Импортируйте файл server.cert, созданный в задаче** "Экспортируйте сертификат UCMDB" на странице 73**, в доверительное хранилище на зонде.**

   a. Откройте командную строку и выполните команду:

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -
   keystore
   C:\HP\UCMDB\DataFlowProbe\conf\security\MAMTrustStoreExp.jks -
   file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -alias
   ucmdbcert
   ```

   b. Введите пароль хранилища ключей: logomania

   c. При появлении вопроса **Доверять этому сертификату?** нажмите **y**, а затем **Enter**.

   Выводится следующее сообщение:

   Сертификат добавлен в хранилище ключей.

2. **Создайте новый файл client.keystore**

   a. Откройте командную строку и выполните команду:

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool -genkey -alias
   <ProbeName> -keyalg RSA -keystore
   C:\HP\UCMDB\DataFlowProbe\conf\security\client.keystore
   ```

   где **ProbeName** – уникальный псевдоним зонда потока данных.

   Примечание. Чтобы обеспечить уникальность этого псевдонима, используйте идентификатор имени зонда, присвоенный зонду при его создании.

   b. Введите пароль для хранилища ключей (не менее 6 символов) и запишите его.

   c. Введите пароль повторно для подтверждения.

   d. Нажмите **Enter**, чтобы ответить на следующие вопросы:

   Ваши имя и фамилия? [Unknown]:

   Как называется ваше подразделение?[Unknown]:

   Как называется ваша организация?[Unknown]:

   Как называется ваш населенный пункт?[Unknown]:

   Как называется ваш штат или область?[Unknown]:

   Какой двухсимвольный код страны используется для данного подразделения?[Unknown]:

   e. Введите **yes**, чтобы ответить на вопрос **Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?**

f. Нажмите **Enter**, чтобы ответить на следующий вопрос:

Введите пароль для <probekey> (нажмите Enter, если он совпадает с паролем к хранилищу ключей):

g. Убедитесь, что в следующей папке создан файл, размер которого не равен 0: **C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore**

3. **Экспортируйте новый сертификат клиента**

a. Откройте командную строку и выполните команду:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias
<ProbeName> -keystore
C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore -file
C:\hp\UCMDB\DataFlowProbe\conf\security\<ProbeName>.cert
```

b. По запросу введите пароль хранилища ключей. (Это пароль, указанный в шаге 2b выше.)

Выводится следующее сообщение:

Сертификат, хранящийся в файле <C:\hp\UCMDB\DataFlowProbe\conf\security\<ProbeName>.cert>

4. **Откройте файл DiscoveryProbe.properties, расположенный в папке: C:\HP\UCMDB\DataFlowProbe\conf**

a. Смените свойство **appilog.agent.probe.protocol** на **HTTPS**.

b. Укажите в свойстве **serverPortHttps** соответствующий номер порта. (Используйте номер порта из шага 2c в задаче "Начальная конфигурация сервера UCMDB" на странице 73.)

5. **Откройте файл ssl.properties, расположенный в папке: C:\HP\UCMDB\DataFlowProbe\conf\security**

a. Укажите в свойстве **javax.net.ssl.keyStore** значение, равное значению **client.keystore**.

b. Зашифруйте пароль, указанный в шаге 2b выше:

i. Запустите зонд потока данных (или убедитесь, что он уже работает).

ii. Откройте консоль JMX зонда. Перейдите по адресу: **http://<probe_ hostname>:1977**

Например, если зонд запущен на локальной машине, перейдите по адресу: **http://localhost:1977**.

iii. Нажмите на ссылку **type=MainProbe**.

iv. Найдите операцию **getEncryptedKeyPassword**.

v. Введите пароль в поле **Key Password**.

vi. Нажмите кнопку **getEncryptedKeyPassword**.

c. Скопируйте и вставьте зашифрованный пароль, чтобы обновить свойство

javax.net.ssl.keyStorePassword.

Примечание. Числа разделяются запятыми. Пример: -20,50,34,-40,-50.)

6. **Скопируйте сертификат зонда на машину UCMDB**

   Скопируйте файл **C:\HP\UCMDB\DataFlowProbe\conf\security\client.cert** с машины зонда потока данных на машину UCMDB в папку **C:\HP\UCMDB\UCMDBServer\conf\security\<ProbeName>.cert**.

Дальнейшая конфигурация сервера UCMDB

1. **Добавьте сертификат каждого зонда в доверительное хранилище UCMDB**

   Примечание. Для каждого сертификата зонда необходимо выполнить следующие действия.

   a. Откройте командную строку и выполните команду:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -
   keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.truststore
   -file C:\hp\UCMDB\UCMDBServer\conf\security\<ProbeName>.cert -
   alias <ProbeName>
   ```

   b. Введите пароль хранилища ключей. Например, пароль к стандартному хранилищу ключей – **hppass**

   c. При появлении вопроса **Доверять этому сертификату?** нажмите **y**, а затем **Enter**.

   Выводится следующее сообщение:

   Сертификат добавлен в хранилище ключей

Перезапуск компьютеров

Перезапустите сервер UCMDB и машины с зондами.

Управление местоположением файла domainScopeDocument File

Файловая система зонда содержит (по умолчанию), как ключ шифрования, так и файл **domainScopeDocument**. При каждом запуске зонда зонд извлекает файл **domainScopeDocument** с сервера и сохраняет его в файловой системе. Чтобы предотвратить несанкционированное получение пользователями этих учетных данных, зонд можно настроить таким образом, что файл **domainScopeDocument** будет оставаться в памяти зонда, а не сохраняться в его файловой системе.

Для управления местоположением файла domainScopeDocument File:

1. Откройте **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** и измените:

   ```
   appilog.collectors.storeDomainScopeDocument=true
   ```

на:

```
appilog.collectors.storeDomainScopeDocument=false
```

Папки serverData Диспетчера зондов и шлюза зонда теперь не содержат файла **domainScopeDocument**.

Подробнее использовании файла **domainScopeDocument** в целях повышения безопасности DFM см. в разделе "Управление учетными данными потока данных" на странице 43.

2. Перезапустите зонд.

Создание хранилища ключей для зонда потока данных

1. Выполните следующую команду на компьютере зонда:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool -genkey -alias
probekey -keyalg RSA -keystore
C:\HP\UCMDB\DataFlowProbe\conf\security\client.keystore
```

2. Введите пароль для нового хранилища ключей.
3. Введите свою информацию при появлении вопроса.
4. При появлении вопроса **Is CN=… C=… Correct?**, введите **yes** и нажмите **Ввод**.
5. Нажмите **Ввод** снова, чтобы принять пароль хранилища ключей как пароль ключа.
6. Убедитесь, что **client.keystore** создан в следующем каталоге: **C:\HP\UCMDB\DataFlowProbe\conf\security**.

Шифрование паролей хранилища ключей и доверительного хранилища

Пароли хранилища ключей и доверительного хранилища зонда хранятся в зашифрованном виде в **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**. Данная процедура показывает, как зашифровать пароль.

1. Запустите зонд потока данных (или убедитесь, что он уже работает).
2. Войдите в консоль JMX зонда потока данных: Запустите веб-браузер и введите следующий адрес: http://<имя или IP-адрес машины зонда потока данных>:1977. Если зонд потока данных запущен на локальной машине, введите http://localhost:1977.

> **Примечание.** Возможно, потребуется ввести имя пользователя и пароль для входа в систему. Если пользователь не создан, используйте для входа в систему имя пользователя по умолчанию sysadmin и пароль sysadmin.

3. Найдите службу **Type=MainProbe** и щелкните ссылку, чтобы открыть страницу "Operations".

4. Найдите операцию **getEncryptedKeyPassword**.
5. Введите пароль хранилища ключей или доверительного хранилища в поле **Пароль ключа** и запустите операцию, щелкнув **getEncryptedKeyPassword**.
6. Результатом вызова станет зашифрованная строка пароля, например:

   ```
   66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,
   112,65,61,61
   ```

7. Скопируйте зашифрованный пароль в строку следующего файла, относящуюся либо к хранилищу ключей, либо к доверительному хранилищу: **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties.**

Хранилище ключей и доверительное хранилище по умолчанию для сервера и зонда потока данных

Этот раздел охватывает следующие темы:

- "UCMDB Server" ниже
- "Зонд потока данных" ниже

UCMDB Server

Файлы находятся в следующем каталоге: **C:\HP\UCMDB\UCMDBServer\conf\security.**

Сущность	Имя файла/термин	Пароль/термин	Псевдоним
Хранилище ключей сервера	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
Доверительное хранилище сервера	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	clientcert (доверенная запись по умолчанию)
Хранилище ключей клиента	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

Зонд потока данных

Файлы находятся в следующем каталоге: **C:\HP\UCMDB\DataFlowProbe\conf\security.**

Сущность	Имя файла/термин	Пароль/термин	Псевдоним
Хранилище ключей зонда	MAMKeyStoreExp.jks (pKeyStoreFile)	logomania (pKeyStorePass)	mam
Зонд потока данных использует хранилище ключей **cKeyStoreFile** как хранилище ключей по умолчанию, во время процедуры взаимной проверки подлинности. Это			

Сущность	Имя файла/термин	Пароль/термин	Псевдоним
хранилище ключей, являющееся частью установки UCMDB.			
Доверительное хранилище зонда	MAMTrustStoreExp.jks (pTrustStoreFile)	logomania (pTrustStorePass)	mam (доверенная запись по умолчанию)
Пароль **cKeyStorePass** является паролем по умолчанию для **cKeyStoreFile**.			

Глава 6

Система проверки подлинности Lightweight Single Sign-On (LW-SSO) – Общие сведения

Данная глава включает:

Проверка подлинности LW-SSO: обзор

LW-SSO — это метод контроля доступа, который позволяет пользователю один раз выполнить вход и получить доступ к нескольким системам ПО без необходимости повторного ввода учетных данных. Приложения внутри настроенной группы программных систем доверяют данной аутентификации, поэтому при переходе от одного приложения к другому не требуется дальнейшей проверки подлинности.

Информация в данном разделе относится к LW-SSO версий 2.2 и 2.3.

- **Срок действия маркеров LW-SSO**

  Срок действия маркеров LW-SSO определяет срок действия сессий приложения. Следовательно, срок действия маркеров должен быть не меньше срока действия сессий приложения.

- **Рекомендуемые настройки срока действия маркеров LW-SSO**

  Для каждого приложения, использующего LW-SSO, необходимо настроить срок действия маркеров. Рекомендуемое значение – 60 минут. Для приложений, не требующих высокого уровня безопасности, допустимо значение в 300 минут.

- **Время GMT**

  Все приложения, задействованные в интеграции LW-SSO, должны использовать одно время GMT с разбежкой не более 15 минут.

- **Поддержка нескольких доменов**

  Для функции поддержки нескольких доменов требуется, чтобы во всех приложениях, задействованных в интеграции LW-SSO, были настроены параметры trustedHosts (или **protectedDomains**), если необходимо, чтобы они интегрировались с приложениями в

других доменах DNS. Кроме того, необходимо добавить правильный домен в элемент конфигурации **lwsso**.

- **Функция получения маркера безопасности для URL-адреса**

  Для получения информации, отправленной как **SecurityToken for URL** из других приложений, приложение хоста должно настроить правильный домен в элементе конфигурации **lwsso**.

Системные требования

Приложение	Версия	Комментарии
Java	1.5 и выше	
API-интерфейс сервлетов HTTP	2.1 и выше	
Internet Explorer	6.0 и выше	В браузере необходимо включить поддержки сессионных файлов cookie для HTTP и функцию перенаправления HTTP 302.
FireFox	2.0 и выше	В браузере необходимо включить поддержки сессионных файлов cookie для HTTP и функцию перенаправления HTTP 302.
Проверка подлинности в JBoss	JBoss 4.0.3 JBoss 4.3.0	
Проверка подлинности в Tomcat	Standalone Tomcat 5.0.28 Standalone Tomcat 5.5.20	
Проверка подлинности в Acegi	Acegi 0.9.0 Acegi 1.0.4	
Механизмы веб-служб	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

Предупреждения о безопасности LW-SSO

В этом разделе описываются предупреждения безопасности, относящиеся к конфигурации LW-SSO:

- **Конфиденциальный параметр InitString в LW-SSO.**LW-SSO использует симметричное шифрование для проверки и создания маркера LW-SSO. Параметр **initString** в конфигурации используется для инициализации секретного ключа. Приложение создает маркер, который проверяется каждым приложением, использующим тот же параметр initString.

  Внимание!

  - LW-SSO невозможно использовать без установки параметра **initString**.
  - Параметр **initString** является конфиденциальной информацией, что необходимо учитывать при публикации, транспортировке и хранении.
  - Параметр **initString** должен совместно использоваться только приложениями, которые интегрируются с помощью LW-SSO.
  - Минимальная длина параметра **initString** составляет 12 символов.

- **LW-SSO следует включать только при необходимости.**Если необходимости в LW-SSO нет, его следует отключить.

- **Уровень безопасности при проверке подлинности**. Приложение, использующее самую слабую платформу проверки подлинности и выдающее маркер LW-SSO, который другие интегрированные приложения считают надежным, определяет уровень безопасности при проверке подлинности для всех приложений.

  Рекомендуется, чтобы маркеры LW-SSO могли создавать только приложения со стойкими и надежными платформами проверки подлинности.

- **Особенности симметричного шифрования.**LW-SSO использует симметричное шифрование для проверки и создания маркеров LW-SSO. Поэтому любое приложение, использующее LW-SSO, может создать маркер, которому будут доверять все приложения с тем же параметром initString. Это может представлять угрозу, если одно из приложений с данным параметром initString находится в ненадежном местоположении или доступно из него.

- **Сопоставление (синхронизация) пользователей.**Платформа LW-SSO не обеспечивает сопоставление пользователей интегрированных приложений. Поэтому интегрированное приложение должно самостоятельно отслеживать отображение пользователей. Рекомендуется, чтобы все интегрированные приложения использовали один реестр пользователей (напр., LDAP/AD).

  Неверное отображение пользователей может нанести ущерб безопасности и вызвать проблемы в работе приложений. К примеру, в разных приложениях разным фактическим пользователям может быть присвоено одно и то же имя пользователя.

  Кроме того, в случае, если пользователь входит в приложение (AppA), а затем использует второе приложение (AppB) с проверкой подлинности на уровне контейнера или

приложения, из-за неверного отображения пользователю придется снова входить во второе приложение, вводя имя пользователя. Если же пользователь введет не то имя пользователя, которое использовалось для входа в AppA, возможна следующая ситуация: Если после этого пользователь войдет в третье приложение (AppC) из AppA или AppB, при этом будут использованы имена пользователей соответственно из AppA и AppB.

- **Диспетчер удостоверений**. При использовании в целях проверки пользователей все незащищенные ресурсы в Диспетчере удостоверений должны иметь настройку **nonsecureURLs** в файле конфигурации LW-SSO.
- **Режим демонстрации LW-SSO.**
  - Демонстрационный режим должен использоваться только в целях демонстрации.
  - Работа в режиме демонстрации допускается только в незащищенных сетях.
  - Не допускается использование демонстрационного режима в рабочей среде. Не допускается использование режима демонстрации одновременно с рабочим режимом.

Устранение неполадок и ограничения

В этом разделе описываются известные проблемы и ограничения при проверке подлинности средствами LW-SSO.

Известные проблемы

В этом разделе описываются известные проблемы проверки подлинности LW-SSO.

- **Контекст безопасности.** Контекст безопасности LW-SSO поддерживает только одно значение каждого атрибута.

  Поэтому, если маркер SAML2 отправляет более одного значения для одного атрибута, платформа LW-SSO принимает только одно значение.

  Аналогичным образом, если маркер IdM отправляет более одного значения для одного атрибута, платформа LW-SSO принимает только одно значение.

- **Функциональность выхода из нескольких доменов при использовании браузера Internet Explorer 7.** Функция выхода из нескольких доменов может работать с проблемами при следующих условиях:
  - Используется браузер Internet Explorer 7, и приложение вызывает три последовательных команды перенаправления HTTP 302 в процедуре выхода.

  В этом случае браузер Internet Explorer 7 может неправильно обрабатывать ответ перенаправления HTTP 302 и отображать ошибку **Internet Explorer не может отобразить эту веб-страницу**.

  В качестве обходного пути, если возможно, рекомендуется уменьшить количество команд перенаправления приложения в последовательности выхода.

Ограничения

При работе с проверкой подлинности LW-SSO действуют следующие ограничения:

- **Доступ клиентов к приложению.**

  Если в конфигурации LW-SSO определен домен:

- Клиент должен получать доступ к приложению с использованием полного доменного имени в URL-адресе для входа, например, http://myserver.**companydomain**.com/WebApp.
- LW-SSO не поддерживает URL-адреса с IP-адресами, например, http://192.168.12.13/WebApp.
- LW-SSO не поддерживает URL-адреса без домена, например, http://myserver/WebApp.

Если в конфигурации LW-SSO не определен домен: Клиент может войти в приложение без полного доменного имени в URL-адресе входа. В этом случае создается сессионный файл cookie LW-SSO для конкретной машины без доменной информации. Поэтому файл cookie не передается в другой браузер или другим компьютерам в том же домене DNS. Таким образом, LW-SSO не работает в том же домене.

- **Интеграция с платформой LW-SSO.** Использование приложениями функций LW-SSO возможно только при предварительной их интеграции с платформой LW-SSO.
- **Поддержка нескольких доменов.**
  - Функциональность поддержки нескольких доменов основывается на источнике ссылок HTTP. Таким образом, LW-SSO поддерживает ссылки из одного приложения на другое приложение, но не поддерживает ввод URL-адреса в окне браузера за исключением случаев, когда оба приложения находятся в одном домене.
  - Первая ссылка между доменами с использованием **HTTP POST** не поддерживается.

    Функция поддержки нескольких доменов не поддерживает первый запрос **HTTP POST** к второму приложению (поддерживается только запрос **HTTP GET**). К примеру, если в приложении есть ссылка HTTP на второе приложение, поддерживается только запрос **HTTP GET**, но не **HTTP FORM**. Все последующие запросы могут иметь вид **HTTP POST** или **HTTP GET**.
  - Размер маркеров LW-SSO:

    Объем информации, передаваемой средствами LW-SSO между приложениями в различных доменах, ограничен 15 группами/ролями/атрибутами (каждый элемент в среднем имеет длину 15 символов).
  - Ссылки с защищенной страницы (HTTPS) на незащищенную страницу (HTTP) в сценарии с несколькими доменами:

    Функциональность поддержки нескольких доменов не работает в случае ссылок с защищенной (HTTPS) на незащищенную (HTTP) страницу. Это ограничение браузера, т.к. в ссылке с защищенных ресурсов на незащищенные не передается заголовок ссылающейся страницы. Пример:
    `http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP`
  - Поведение сторонних файлов "cookie" в браузере Internet Explorer.

    Обозреватель Microsoft Internet Explorer 6 содержит модуль, поддерживающий "Спецификацию P3P", т.е. файлы "cookie" со сторонних доменов по умолчанию блокируются в зоне безопасности Интернета. Сеансовые "cookie" также считаются браузером Internet Explorer сторонними файлами "cookie", а поэтому блокируются, что приводит к остановке работы LW-SSO. См. дополнительные сведения в разделах: `http://support.microsoft.com/kb/323752/en-us`.

Чтобы решить эту проблему, добавьте запущенное приложение (или подмножество DNS-домена в виде *.mydomain.com) в зону "Интрасеть/Надежные узлы" на компьютере (в браузере Microsoft Internet Explorer выберите **Меню > Сервис > Свойства обозревателя > Безопасность > Местная интрасеть > Узлы > Дополнительно**), что позволит принимать файлы "cookie".

Внимание! Сеансовый файл "cookie" LW-SSO — это единственный файл "cookie", используемый сторонним приложением, который блокируется.

- **Маркер SAML2**
  - При использовании маркера SAML2 не поддерживается выход из системы.

    Поэтому при использовании маркера SAML2 для доступа к второму приложению выход пользователя из первого приложения не влечет за собой его выход из второго приложения.
  - **Истечение срока действия маркера SAML2 не отражается в системе управления сессиями приложения.**

    Поэтому при использовании маркеров SAML2 для доступа к второму приложению управления сессиями в двух приложениях осуществляется независимо.
- **Область JAAS.** Область JAAS в Tomcat не поддерживается.
- **Использование пробелов в директориях Tomcat.** Использование пробелов в директориях Tomcat не поддерживается.

  Использование LW-SSO невозможно, если путь установки Tomcat (названия директорий) содержит пробелы (напр., Program Files), а файл конфигурации LW-SSO находится в папке Tomcat **common\classes**.
- **Настройка балансировки нагрузки.** В системе балансировки нагрузки, развернутой с LW-SSO, должно быть настроено использование закрепленных (sticky) сессий.
- **Режим демонстрации.** В режиме демонстрации LW-SSO поддерживает ссылки из одного приложения на другое приложение, но не поддерживает ввод URL-адреса в окне браузера, поскольку в этом случае отсутствует заголовок HTTP referer.

Глава 7

Проверка подлинности при входе в систему HP Universal CMDB

Данная глава включает:

Настройка метода метода проверки подлинности

Проверка подлинности может выполняться:

- **Средствами внутренней службы HP Universal CMDB.**
- **Через Lightweight Directory Access Protocol (LDAP) .** Вместо внутренней службы HP Universal CMDB данные, необходимые для проверки подлинности, могут храниться на внешнем выделенном сервере LDAP. Сервер LDAP должен находиться в той же подсети, что и все серверы HP Universal CMDB.

  Подробнее о LDAP см. в разделе о сопоставлении LDAP (*Руководство по администрированию HP Universal CMDB*).

  По умолчанию проверка подлинности осуществляется внутренней службой HP Universal CMDB. Данный метод не требует какого-либо изменения настроек системы.

  Эти параметры применяются при входе как через веб-службы, так и через интерфейс пользователя.

- **Через LW-SSO.** В HP Universal CMDB настроено использование LW-SSO. LW-SSO позволяет входить в HP Universal CMDB и автоматически получать доступ к другим настроенным приложениям в том же домене без необходимости входа в эти приложения.

  При включении поддержки LW-SSO (по умолчанию она отключена) необходимо проверить, чтобы в других приложениях в той же среде также была включена поддержка LW-SSO и задано то же значение параметра initString.

Включение проверки подлинности при входе в систему в HP Universal CMDB при помощи LW-SSO

Чтобы включить поддержку LW-SSO в HP Universal CMDB, выполните следующие действия:

1. Для доступа к консоли JMX введите в браузер следующий адрес: **http://<server_name>:8080/jmx-console**, где **<server_name>** – это имя машины, на которой установлена HP Universal CMDB.
2. В разделе **UCMDB-UI**, нажмите **name=LW-SSO configuration**, чтобы открыть страницу "Операции".
3. Задайте параметр initString при помощи метода **setInitString**.
4. Задайте доменное имя машины, на которой установлена UCMDB, при помощи метода **setDomain**.
5. Вызовите метод **setEnabledForUI**, установив для его параметра значение **True**.
6. **Необязательно**. Чтобы использовать поддержку нескольких доменов, выберите метод **addTrustedDomains**, введите значения доменов и нажмите **Invoke**.
7. **Необязательно.** Чтобы включить поддержку обратного прокси-сервера, выберите метод **updateReverseProxy**, укажите для параметра **Is reverse proxy enabled** значение **True**, введите URL-адрес в качестве значения параметра **Reverse proxy full server URL** и нажмите Invoke. Если с UCMDB необходимо работать как напрямую, так и через обратный прокси-сервер, задайте дополнительные параметры конфигурации: выберите метод **setReverseProxyIPs**, введите IP-адрес в значение параметра Reverse proxy ip/s и нажмите **Invoke.**
8. **Необязательно**. Чтобы разрешить доступ к UCMDB через внешнюю точку проверки подлинности, выберите метод **setValidationPointHandlerEnable**, задайте для параметра **Is validation point handler enabled** значение **True**, введите URL-адрес точки проверки подлинности в параметре **Authentication point server** и нажмите **Invoke.**
9. Для просмотра сохраненной в настройках конфигурации LW-SSO вызовите метод **retrieveConfigurationFromSettings**.
10. Для просмотра фактической загруженной конфигурации LW-SSO вызовите метод **retrieveConfiguration**.

Примечание. LW-SSO нельзя включить через интерфейс пользователя.

Установка защищенного соединения при помощи протокола SSL

Поскольку процедура входа в систему подразумевает передачу конфиденциальных сведений между HP Universal CMDB и сервером LDAP, имеет смысл защитить

передаваемые данные. Для этого соединение между сервером LDAP и HP Universal CMDB защищается при помощи SSL.

HP Universal CMDB поддерживает сертификаты SSL, выданные надежным центром сертификации.

Большинство серверов LDAP, включая Active Directory, имеют защищенный порт для подключений по протоколу SSL. Для использования Active Directory с частным ЦС необходимо внести данный ЦС в список надежных центров сертификации в JRE.

Подробнее о настройке поддержки SSL в HP Universal CMDB см. в разделе "Включение поддержки Secure Sockets Layer (SSL)" на странице 18.

Добавление ЦС в список надежных центров сертификации и открытие защищенного порта для соединений:

1. Экспортируйте сертификат из ЦС и импортируйте его в JVM, которую использует HP Universal CMDB, следующим образом:
   a. Откройте на UCMDB Server директорию **UCMDBServer\bin\JRE\bin** .
   b. Выполните следующую команду:

   ```
   Keytool -import -file <файл сертификата> -keystore
   C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
   ```

   Пример:

   ```
   Keytool -import -file c:\ca2ss_ie.cer -keystore
   C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
   ```

2. Выберите **Администрирование > Настройки инфраструктуры > Общие настройки LDAP**.

   Примечание. Эти настройки также можно изменить через консоль JMX. Дополнительные сведения см. в разделе "Настройка параметров LDAP с помощью консоли JMX" на следующей странице.

3. Найдите параметр **URL-адрес сервера LDAP** и введите значение в следующем формате:

   ```
   ldaps://<ldapHost>[:<port>]/[<baseDN>][??scope]
   ```

   Пример:

   ```
   ldaps://my.ldap.server:389/ou=People,o=myOrg.com??sub
   ```

   Обратите внимание на **s** в **ldaps**.

4. Нажмите **Сохранить** для сохранения значения или **Восстановить значение по умолчанию**, чтобы вернуть стандартное значение (пусто).

Использование консоли JMX для проверки соединений LDAP

В данном разделе описывается метод проверки конфигурации проверки подлинности через LDAP при помощи консоли JMX.

1. Запустите веб-браузер и введите следующий адрес: **http://<server_name>:8080/jmx-console**, где **<server_name>** – это имя машины, на которой установлена HP Universal CMDB.

   Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

2. В разделе **UCMDB** нажмите **UCMDB-UI:name=LDAP Settings**, чтобы открыть страницу "Операции".

3. Найдите строку **testLDAPConnection**.

4. В поле **Значение** для параметра **customer id** введите идентификатор клиента.

5. Нажмите кнопку **Invoke**.

   На странице "Результат операции JMX MBEAN" отображается результат подключения к LDAP. Если подключение выполнено успешно, на странице отображаются корневые группы LDAP.

Настройка параметров LDAP с помощью консоли JMX

В данном разделе описывается настройка параметров проверки подлинности в LDAP при помощи консоли JMX.

Настройка параметров проверки подлинности в LDAP:

1. Запустите веб-браузер и введите следующий адрес: **http://<server_name>:8080/jmx-console**, где **<server_name>** – это имя машины, на которой установлена HP Universal CMDB.

   Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

2. В разделе **UCMDB** нажмите **UCMDB-UI:name=LDAP Settings**, чтобы открыть страницу "Операции".

3. Для просмотра текущих параметров проверки подлинности в LDAP найдите метод **getLDAPSettings**. Нажмите кнопку **Invoke**. Откроется таблица со всеми настройками LDAP и их значениями.

4. Чтобы изменить параметры проверки подлинности в LDAP, найдите метод **configureLDAP**. Введите значения необходимых параметров и нажмите **Invoke**. На странице "Результат операции JMX MBEAN" отображается результат изменения настроек.

Примечание. Параметры, для которых не введены новые значения, сохраняют предыдущие значения.

5. Завершив настройку параметров LDAP, можно проверить учетные данные пользователя LDAP. Найдите метод **verifyLDAPCredentials**. Введите идентификатор клиента, имя пользователя и пароль, а затем нажмите Invoke. На странице "Результат операции JMX MBEAN" отображается результат проверки подлинности пользователя в LDAP.

Включение и определение метода проверки подлинности LDAP

Можно включить и настроить метод проверки подлинности LDAP для системы HP Universal CMDB.

Включение и настройка проверки подлинности через LDAP:

1. Выберите **Администрирование > Настройки инфраструктуры > Общие настройки LDAP**.
2. Выберите **URL-адрес сервера LDAP** и введите адрес в следующем формате:

   ldap://<ldapHost>[:<port>]/[<baseDN>][??scope]

   Пример:

   ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub

3. Выберите категорию **Определение групп LDAP** и в поле **Базовое различаемое имя групп** введите различительное имя общей группы.
4. Затем в поле **Базовое различаемое имя корневой группы** введите различительное имя корневой группы.
5. Выберите категорию **Общие настройки LDAP** и убедитесь, что в настройке **Включить синхронизацию пользователей** установлено значение **True** (истина).
6. Выберите категорию **Общая проверка подлинности LDAP** и в поле **Пароль пользователя с правами поиска** введите пароль.
7. Выберите категорию **Параметры LDAP для классов и атрибутов**, найдите пункт **Класс объекта группы** и укажите имя класса объектов (**group** для Microsoft Active Directory или **groupOfUniqueNames** для Oracle Directory Server).
8. Найдите пункт **Атрибут члена группы** и укажите имя атрибута (**member** для Microsoft Active Directory или **uniqueMember** для Oracle Directory Server).
9. Найдите пункт **Класс объектов пользователей** и укажите имя класса объектов (**user** для Microsoft Active Directory или **inetOrgPerson** для Oracle Directory Server).
10. Найдите пункт **Атрибут UUID** и укажите идентифицирующий атрибут для пользователя на сервере директорий. Необходимо выбрать атрибут, уникальный для сервера

директорий. Например, на сервере SunOne/Oracle Directory Server атрибут UID не является уникальным. В этом случае следует использовать адрес эл. почты или различительное имя. Использование неуникальных атрибутов для идентификации пользователей в UCMDB может вызвать ошибки при входе в систему.

11. Сохраните новые значения. Чтобы вернуть исходные значения полей, нажмите **Восстановить значение по умолчанию**.
12. Если параметр **Is case-sensitivity enforced when authenticating with LDAP** в разделе **Общие настройки LDAP** имеет значение **True**, при проверке подлинности учитывается регистр.

    Внимание! При изменении значения этой настройки инфраструктуры администратор UCMDB должен вручную удалить всех внешних пользователей.

13. Сопоставление групп пользователей LDAP с группами пользователей UCMDB. Дополнительные сведения см. в разделе "Проверка подлинности при входе в систему HP Universal CMDB" на странице 87.
14. Чтобы дать пользователям в группе LDAP, не имеющей сопоставления, стандартный набор прав доступа, выберите категорию **Общие настройки LDAP**, найдите параметр **Automatically Assigned User Group** и введите имя группы.

По умолчанию для обмена данными с сервером LDAP используется протокол TCP, однако вместо него можно использовать SSL. Дополнительные сведения см. в разделе "Установка защищенного соединения при помощи протокола SSL" на странице 88.

Примечание. Для каждого пользователя LDAP в локальном репозитории хранятся имя, фамилия и адрес электронной почты. Если значение любого из этих параметров, сохраненное на сервер LDAP, отличается от значения в локальном репозитории, при каждом входе в систему значения с сервера LDAP записываются поверх сохраненных локально значений.

Извлечение текущей конфигурации LW-SSO в распределенной среде

При использовании UCMDB в составе распределенной среды (например, в рамках системы BSM) данные о текущей конфигурации LW-SSO на обрабатывающей машине можно получить следующим способом:

Извлечение данных о текущей конфигурации LW-SSO:

1. Запустите веб-браузер и введите следующий адрес: `http://localhost.<domain_name>:8080/jmx-console`.

   Возможно, потребуется ввести имя пользователя и пароль для входа в систему.
2. Найдите **UCMDB:service=Security Services** и щелкните ссылку, чтобы открыть страницу "Operations".
3. Найдите операцию **retrieveLWSSOConfiguration**.
4. Чтобы извлечь данные о текущей конфигурации, нажмите **Invoke**.

Глава 8

Confidential Manager

Данная глава включает:

Confidential Manager: обзор

Платформа Confidential Manager решает проблему администрирования и распространения конфиденциальных данных для HP Universal CMDB и других продуктов HP Software.

Confidential Manager состоит из двух основных компонентов: клиента и сервера. Эти компоненты отвечают за передачу данных в защищенном виде.

- Клиент Confidential Manager – это библиотека, с помощью которой приложения получают доступ к конфиденциальным данным.
- Сервер Confidential Manager получает запросы от клиентов Confidential Manager или сторонних клиентов и выполняет необходимые задачи. Сервер Confidential Manager отвечает за сохранение данных в защищенном виде.

Confidential Manager шифрует учетные данные при передаче, в кэш-буфере клиента, при сохранении состояния и в памяти. Для передачи учетных данных между клиентом и сервером Confidential Manager используется симметричное шифрование с общим секретом. Для шифрования кэш-буфера, данных сохранения состояния и данных при передаче в Confidential Manager используются разные секретные ключи (зависит от конфигурации).

Подробные сведения об управлении шифрованием учетных данных в зонде потока данных см. в разделе "Управление учетными данными потока данных" на странице 43.

Указания по обеспечению безопасности

- В алгоритме безопасности можно использовать ключи следующих размеров: 128, 192 и 256 бит. Чем меньше длина ключа, тем быстрее работает алгоритм, но и тем менее надежным является шифрование. В большинстве случаев длина 128 бит является достаточной.
- Для повышение надежности установите значение MAC: установите для **useMacWithCrypto** значение **true.** Дополнительные сведения см. в разделе "Свойства

шифрования" на странице 95.

- В целях еще большей защиты клиентов можно использовать режим JCE.

Настройка HP Universal CMDB Server

При работе с HP Universal CMDB необходимо настроить секретный ключ и свойства шифрования при помощи следующих методов JMX:

1. На машине, где установлен HP Universal CMDB Server, запустите веб-браузер и введите адрес сервера: **http://<Имя или IP-адрес UCMDB Server>:8080/jmx-console**.

   Возможно, потребуется ввести имя пользователя и пароль для входа в систему.

2. В разделе UCMDB нажмите **UCMDB:service=Security Services**, чтобы открыть страницу "Operations".

3. Чтобы извлечь данные о текущей конфигурации, найдите операцию **CMGetConfiguration**.

   Нажмите **Invoke** для отображения XML-файла конфигурации сервера Confidential Manager.

4. Чтобы изменить конфигурацию, скопируйте извлеченный XML-файл в текстовый редактор. Внесите изменения согласно указаниям, приведенным в таблице в разделе "Свойства шифрования" на следующей странице.

   Найдите операцию **CMSetConfiguration**. Скопируйте измененную конфигурацию в поле **Значение** и нажмите **Invoke**. Новая конфигурация записывается в UCMDB Server.

5. Чтобы добавить в Confidential Manager пользователей для их дальнейшей авторизации и репликации, найдите операцию **CMAddUser**. Данный процесс также удобен для репликации. В процессе репликации подчиненный сервер общается с главным сервером через учетную запись привилегированного пользователя.

   - **username**. Имя пользователя.
   - **заказчик.** Значение по умолчанию – ALL_CUSTOMERS.
   - **ресурс.** Имя ресурса. Значение по умолчанию – ROOT_FOLDER.
   - **право доступа.** Выберите один из вариантов: ALL_PERMISSIONS, CREATE, READ, UPDATE или DELETE. Значение по умолчанию – ALL_PERMISSIONS.

   Нажмите кнопку **Invoke**.

6. При необходимости перезапустите HP Universal CMDB.

   Примечание. В большинстве случаев сервер можно не перезапускать. Перезагрузка сервера может потребоваться при изменении какого-либо из следующих ресурсов:

   - Тип системы хранения данных
   - Имя таблицы или столбцов в базе данных
   - Создатель подключения к базе данных

- Свойства подключения к базе данных (URL-адрес, имя пользователя, пароль, имя класса драйвера)
- Тип базы данных

Примечание.

- При этом важно, чтобы у UCMDB Server и его клиентов совпадали свойства шифрования при передаче данных. В случае изменения этих свойств на сервере UCMDB необходимо обновить их на всех клиентах. (Это не относится к зонду потоков данных, поскольку он работает в том же процессе, что и UCMDB Server, вследствие чего не требуется шифрования данных при передаче).
- Репликация в Confidential Manager по умолчанию отключена. При необходимости ее можно настроить.
- Если репликация в Confidential Manager включена, при изменении свойства Transportation **initString** или других свойств шифрования на главном сервере необходимо внести такие же изменения на всех подчиненных серверах.

Определения

Свойства шифрования при хранении данных. Конфигурация, определяющая хранение и шифрование данных на сервере (в базе данных или файле, какие свойства используются для шифрования и расшифровки данных и т.д.), хранение учетных данных в защищенном виде, обработку шифрования и т.д.

Свойства шифрования при передаче данных. Конфигурация, определяющая шифрование данных при их передаче между клиентами и сервером, передачу учетных данных в защищенном виде, обработку шифрования и т.д. На сервере и клиенте должны быть установлены одинаковые свойства шифрования и расшифровки данных при передаче.

Репликация и ее свойства шифрования. Confidential Manager обеспечивает защищенную репликацию данных между несколькими серверами. Эти свойства определяют передачу данных между главным и подчиненными серверами.

Примечание.

- В базе данных конфигурация сервера Confidential Manager хранится в следующей таблице: **CM_CONFIGURATION.**
- Файл конфигурации Confidential Manager по умолчанию расположен в app-infra.jar под именем **defaultCMServerConfig.xml.**

Свойства шифрования

В следующей таблице описаны свойства шифрования. Подробнее об использовании параметров см. в разделе "Настройка HP Universal CMDB Server" на предыдущей странице.

параметр	Описание	Рекомендуемое значение
encryptTransportMode	Шифрование данных при передаче: true false	true
encryptDecrypt initString	Пароль для шифрования	Длиннее 8 символов
cryptoSource	Используемая библиотека шифрования: • lw • jce • windowsDPAPI • lwJCECompatible	lw
lwJCEPBE CompatibilityMode	Поддержка предыдущих версий облегченного шифрования: • true • false	true
cipherType	Тип шифра, используемый Confidential Manager. Confidential Manager поддерживает только одно значение: **symmetricBlockCipher**	symmetric BlockCipher
engineName	• AES • Blowfish • DES • 3DES • Ничего (без шифрования)	AES
algorithmModeName	Режим алгоритма блочного шифрования: • CBC	CBC
algorithmPaddingName	Стандарты заполнения: • PKCS7Padding • PKCS5Padding	PKCS7Padding
keySize	Зависит от алгоритма (что поддерживает **engineName**)	256
pbeCount	Число циклов хеширования для создания ключа из **encryptDecryptInitString**. Любое положительное число.	1000

параметр	Описание	Рекомендуемое значение
pbeDigestAlgorithm	Тип хеширования: • SHA1 • SHA256 • MD5	SHA256
encodingMode	Представление зашифрованного объекта в ASCII: • Base64 • Base64Url	Base64Url
useMacWithCrypto	Определяет использование MAC при шифровании: • true • false	false
macType	Тип кода проверки подлинности сообщения (MAC): • hmac	hmac
macKeySize SHA256	Зависит от алгоритма MAC	256
macHashName	Алгоритм хеширования MAC: • SHA256	SHA256


Java™
COMPATIBLE