HP Universal CMDB 9.10 Configuration Manager

для операционной системы Windows

Руководство по развертыванию

Дата выпуска документа: ноябрь 2010 г.
Дата выпуска программы: ноябрь 2010 г.

Правовые уведомления

Гарантия

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

Приводимые в них сведения могут быть изменены без какого-либо уведомления.

Расшифровка ограничения прав

Конфиденциальное компьютерное ПО. Для обладания, использования или копирования необходима действующая лицензия от компании HP. Согласно FAR 12.211 и 12.212, выдача лицензий на коммерческое компьютерное ПО, документацию на компьютерное ПО и технические данные для коммерческих элементов правительству США производится на условиях стандартной коммерческой лицензии поставщика.

Уведомления об авторских правах

Обновления документации

Титульная страница этого документа содержит следующие идентификационные данные:

- дата выхода документа, которая изменяется при каждом обновлении документа;
- дата выпуска программы, которая указывает дату выпуска данной версии ПО.

Чтобы проверить наличие последних обновлений или убедиться в том, что используется последняя редакция документа, перейдите на вебсайт:

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

Данный сайт требует регистрации и входа в HP Passport. Чтобы зарегистрировать учетную запись HP Passport, перейдите на вебсайт:

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

или щелкните ссылку **New users - please register** на странице входа в HP Passport.

Обновленные или новые редакции можно получать, подписавшись на соответствующую службу поддержки продукта. Для получения дополнительных сведений обратитесь к торговому представителю HP.

Поддержка

Посетите вебсайт HP Software Support:

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

На этом сайте можно найти контактную информацию и сведения о продуктах, услугах и технической поддержке, предлагаемых HP Software.

Интерактивная техническая поддержка HP Software предоставляет заказчику возможности самостоятельного поиска решений. Она обеспечивает быстрый и эффективный доступ к интерактивным средствам технической поддержки, которые необходимы для управления бизнесом. Клиенты службы поддержки могут воспользоваться следующими преимуществами сайта:

- поиск интересующих документов базы знаний;
- отправка и контроль описаний конкретных случаев и расширенных запросов для получения технической поддержки;
- загрузка исправлений ПО;
- управление договорами на техническую поддержку;
- поиск контактов в HP для технической поддержки;
- проверка сведений о доступных услугах;
- участие в обсуждении 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 зарегистрировать учетную запись HP Passport, перейдите по адресу:

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

Для получения дополнительных сведений об уровнях доступа см.:

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

Оглавление

1

Установка и настройка

Данная глава содержит следующую информацию:

Обзор Configuration Manager

HP Universal CMDB Configuration Manager (Configuration Manager) позволяет анализировать и контролировать данные в системе управления конфигурациями (CMS), а также создает среду управления инфраструктурой CMS, включающую различные источники данных, и позволяет обслуживать различные продукты и приложения.

Развертывание Configuration Manager в корпоративной сети – процесс, требующий планирования ресурсов и проектирования архитектуры системы. Перед началом установки Configuration Manager ознакомьтесь с информацией в данном разделе, включая сведения о системных требованиях.

Системные требования Configuration Manager

Системные требования к серверу

В следующей таблице описаны системные требования для сервера Configuration Manager.

ЦП	Intel Pentium 4, мин. 4 ядра
Память (ОЗУ)	Минимум 4 ГБ
Платформа	x64
Операционная система	Поддерживаются следующие 64-разрядные операционные системы Windows: ➤ Windows 2003 Enterprise SP2 и R2 SP2 ➤ Windows 2008 Enterprise SP2 и R2

База данных	➤ Microsoft SQL Server 2005 SP2; 2005 режим совместимости 80; (выпуски Enterprise Edition для всех) ➤ Oracle 11.1.x
HP Universal CMDB	➤ HP Universal CMDB версии 9.03 (обычная установка CMDB) Полный список системных требований для данной версии см. в документации по HP Universal CMDB.

Требования к клиенту

В следующей таблице описаны требования к клиенту для просмотра Configuration Manager.

Веб-обозреватель	➤ Microsoft Internet Explorer 7.0, 8.0. ➤ Mozilla Firefox 3.x
Flash Player - подключаемый модуль обозревателя	Flash Player версии 9 или выше
Разрешение экрана	➤ Минимальное: 1024x768 ➤ Рекомендуемое: 1280x1024
Качество цветопередачи	Минимум 16 бит

Рекомендации по установке

В следующей таблице приведены рекомендации по установке Configuration Manager.

LDAP	Поддерживаются следующие среды LDAP: ➤ Active Directory ➤ SunONE 6.x
Минимальный рекомендуемый размер схемы базы данных	2 ГБ

Ограничения емкости Configuration Manager

В следующей таблице приведены ограничения емкости Configuration Manager.

Рекомендованное максимальное число представлений	100
Рекомендованное максимальное число политик	300
Рекомендованное максимальное число составных ЭК в представлении	5000
Рекомендованное максимальное число одновременно работающих пользователей	50

Настройка базы данных или пользовательской схемы

Для работы с Configuration Manager необходимо создать схему базы данных. Configuration Manager поддерживает Microsoft SQL Server и Oracle Database Server. В данной задаче объясняется, как настроить свойства подключения для базы данных или пользовательской схемы Configuration Manager с помощью мастера установки.

Примечание. Подробнее о системных требованиях Microsoft SQL Server и Oracle Server см. в разделе "Системные требования к серверу" на стр. 8.

Настройка базы данных

1 Выделите базу данных Microsoft SQL Server или пользовательскую схему Oracle Server.

- Для **Microsoft SQL Server 2005**: активируйте функцию изоляции моментального снимка.

  После создания базы данных один раз выполните следующую команду:

  ```
  alter database <ccm_database_name> set read_committed_snapshot on
  ```

  Для получения дополнительных сведений о функции изоляции моментального снимка в SQL Server см. http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx.

- Для **Oracle**: предоставьте пользователю Oracle только роли **Connect** и **Resource**.
  (Предоставление привилегии **Выбор любой таблицы** вызывает сбой процедуры заполнения схемы.)

2 Убедитесь в наличии следующих сведений, которые необходимы в процессе настройки.

✔	**Необходимые сведения**
	Имя хоста и порт БД
	Имя пользователя и пароль БД
	Для MS SQL: имя базы данных
	Для Oracle: системный идентификатор (SID)

3 Запустите Мастер установки Configuration Manager. Дополнительные сведения см. в разделе "Установка Configuration Manager" на стр. 12.

Установка Configuration Manager

В данной задаче описывается процедура установки Configuration Manager на сервере, настройки соединения с базой данных и интеграции с UCMDB. Для получения справки по установке нажмите **Help** на любой странице мастера. Подробное описание страниц мастера см. в разделе "Configuration Manager Мастер послеустановочной настройки" на стр. 23.

Порядок установки Configuration Manager

1 В корневом каталоге DVD-диска Configuration Manager найдите файл: **install.bat**.

2 Двойным щелчком на файле запустите Мастер установки Configuration Manager.

3 Нажмите **Next**, чтобы открыть страницу Лицензионного соглашения с конечным пользователем.

4 Примите условия лицензии и нажмите **Next**, чтобы открыть страницу установки продукта.

5. Выберите продукты, которые необходимо установить (UCMDB и Configuration Manager) и укажите место установки. Если используется нестандартная лицензия на UCMDB, установите соответствующий флажок. Нажмите **Next** для запуска установки UCMDB. Подробнее об установке UCMDB см. в документе *Руководство по развертыванию HP Universal CMDB (PDF)*.
6. По окончании установки UCMDB и послеустановочных процедур автоматически запускается Мастер послеустановочной настройки Configuration Manager.
7. Нажмите **Next** на странице приветствия, чтобы открыть страницу настройки соединения с базой данных.
8. Выберите тип базы данных (Oracle или Microsoft SQL Server), введите имя пользователя и пароль. Рекомендуется проверить соединения при помощи кнопки **Test**. Если проверка пройдена успешно, нажмите **Next**, чтобы открыть страницу настройки сервера приложений.

Примечание. По окончании работы мастера можно настроить расширенные параметры соединения с базой данных. Дополнительные сведения см. в разделе "Настройка расширенных параметров соединения с базой данных" на стр. 15.

---

9. Введите имя хоста и нажмите **Next**, чтобы открыть страницу настройки службы Windows.
10. Если необходимо установить Configuration Manager как службу Windows, установите соответствующий флажок. Нажмите **Next**, чтобы открыть страницу ввода реквизитов пользователя.
11. Введите имя пользователя и пароль для пользователя-администратора и пользователя интеграции. Нажмите **Next**, чтобы открыть страницу настройки соединения с HP UCMDB.
12. Если на данной или другой машине уже установлено UCMDB, перед продолжением убедитесь, что сервер UCMDB запущен.

Если UCMDB устанавливается на другую машину, убедитесь, что установлен соответствующий флажок, и введите необходимые параметры. Рекомендуется проверить соединения при помощи кнопки **Тест**. Если проверка пройдена успешно, нажмите **Next**, чтобы открыть страницу обзора действий после установки.

13 Ознакомьтесь с информацией на странице обзора действий после установки. Если указанные сведения верны, нажмите **Next** для перехода к послеустановочным действиям.

14 Нажмите **Finish** на последней странице для завершения послеустановочных процедур.

15 Если это не первый запуск UCMDB, необходимо изменить размер столбцов в UCMDB следующим образом:

a Откройте **Администрирование > Менеджер настроек инфраструктуры**. Найдите настройку **Корневой элемент объектов** и измените ее на **data**. Для вступления изменения в силу выйдите из UCMDB и войдите снова.

b Откройте **Моделирование > Менеджер типов ЭК**. Выберите тип ЭК **data** в дереве, а затем выберите закладку "Атрибуты". Измените атрибут **Метка пользователя**, изменив **Размер значения** на 900.

c Вернитесь в **Менеджер настроек инфраструктуры** и верните изначальное значение настройки **Корневой элемент объектов**. Для вступления изменения в силу выйдите из UCMDB и войдите снова.

16 Если в UCMDB уже запускалось управление потоком данных, данные истории могут быть повреждены. Для решения данной проблемы выполните следующие действия:

a Запустите веб-обозреватель и введите следующий адрес: http://<адрес сервера UCMDB>.<domain_name>:8080/jmx-console.

Введите реквизиты проверки подлинности консоли JMX, которые по умолчанию имеют следующие значения:

- Имя входа = **sysadmin**
- Пароль = **sysadmin**

b В разделе **UCMDB** выберите **History DB Services**.

c Выберите метод **Fix902EndTimeRecords**.

d Для клиента фактического состояния введите **1** в поле ID заказчика и нажмите **Вызвать**.

e Если операция выполнена успешно, появится сообщение "БД истории успешно обновлена".

f Для клиента авторизованного состояния введите **100001** в поле ID заказчика и нажмите **Вызвать**.

g Если операция выполнена успешно, появится сообщение "БД истории успешно обновлена".

Настройка расширенных параметров соединения с базой данных

Если для подключения к базе данных необходимо настроить расширенные параметры соединения, это можно сделать по окончании работы послеустановочного Мастера. Configuration Manager поддерживает все параметры соединения с базой данных, которые поддерживаются драйвером JDBC поставщика и могут быть настроены с URL-адресом подключения к базе данных. Для настройки расширенных параметров необходимо отредактировать свойство **jdbc.url** в файле **<директория установки Configuration Manager>\conf\database.properties**.

Ниже приведены примеры расширенных параметров Microsoft SQL Server:

- **Аутентификация Windows (NTLM).** Чтобы использовать аутентификацию Windows, добавьте свойство домена в URL-адрес подключения JTDS в файле database.properties. Укажите домен Windows для проверки подлинности.

  Пример:

  ```
  jdbc:jtds:sqlserver://myServer:1433/myDatabase;sendStringParametersAsUnicode=false;domain=myDomain
  ```

- **SSL.** Подробнее о защите соединения с MS SQL при помощи SSL см. по адресу http://jtds.sourceforge.net/faq.html.

Ниже приведены примеры расширенных параметров Oracle Database Server:

- **URL-адрес Oracle.** Укажите URL-адрес подключения для встроенного драйвера Oracle. При этом необходимо указать имя существующего сервера Oracle и системный идентификатор (SID). Если же используется **Oracle RAC**, необходимо указать параметры конфигурации Oracle RAC.

  Примечание. Подробнее о настройке формата URL-адреса для подключения драйвера Oracle JDBC см. http://www.orafaq.com/wiki/JDBC#Thin_driver. Подробнее о настройке URL-адреса для Oracle RAC см. http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm.

- **SSL.** Подробнее о защите соединения с Oracle при помощи SSL см. в следующих объяснениях:
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6

Настройка базы данных - поддержка MLU (многоязычных элементов)

В данном разделе описываются настройки базы данных для поддержки локализации.

Настройки Oracle Server

В следующей таблице приведены необходимые настройки для Oracle Server:

Параметр	Поддерживается	Рекомендуется	Примечания
Набор символов	WE8ISO8859P1; UTF8,AL32UTF8	AL32UTF8	

Настройки Microsoft SQL Server

В следующей таблице приведены необходимые настройки для Microsoft SQL Server:

Параметр	Поддерживается	Рекомендуется	Примечания
Сортировка	Без учета регистра. Не поддерживается двоичный порядок сортировки и учет регистра. Поддерживается только сортировка без учета регистра с сочетанием настроек акцентов, кана и ширины.	Сортировка настраивается при помощи диалогового окна "Параметры сортировки". Не устанавливайте флажок "двоичная". Настройки учета акцентов, кана и ширины задаются с учетом требований языка данных. Выбранный язык должен совпадать с заданным в региональных настройках ОС Windows.	Ограничено региональными настройками сортировки и стандартными англоязычными определениями.
Свойство базы данных: сортировка	По умолчанию на сервере		

Примечание.

Для всех языков: **<язык>_CI_AS** – минимально необходимый параметр. К примеру, если для японского языка необходимо задать учет кана и ширины, рекомендуются следующие параметры: **Japanese_CI_AS_KS_WS** или **Japanese_90_CI_AS_KS_WS**. Данные параметры определяют, что для японских символов включен учет акцентов, кана и ширины.

- **Учет акцентов (_AS).** Различение акцентированных и неакцентированных символов. Например, **a** и á. Если данный параметр не выбран, Microsoft SQL Server при сортировке не делает различий между акцентированными и неакцентированными символами.
- **Учет кана (_KS).** Различение двух видов японской слоговой азбуки кана: хирагана и катакана. Если данный параметр не выбран, Microsoft SQL Server при сортировке не делает различий между символами хираганы и катаканы.
- **Учет ширины (_KS).** Различение однобайтных символов и этих же символов в двухбайтном виде. Если данный параметр не выбран, Microsoft SQL Server при сортировке не делает различий между однобайтным и двухбайтным вариантами одного символа.

Включение Lightweight Single Sign-On

У некоторых пользователей Configuration Manager также есть право входа в UCMDB. Для удобства в Configuration Manager есть прямая ссылка на интерфейс пользователя UCMDB (выберите **Администрирование > Открыть UCMDB**). Чтобы использовать единый вход в систему (т.е. не входить в UCMDB после входа в Configuration Manager), необходимо включить LW-SSO для Configuration Manager и UCMDB и убедиться, что обе системы работают с одним и тем же параметром initString. В данной задаче описывается процедура включения LW-SSO в Configuration Manager и UCMDB.

Включение LW-SSO:

1 Откройте следующий файл в директории установки Configuration Manager: **\servers\server-0\webapps\cnc\WEB-INF\classes\cnclwssofmconf.xml**.

Примечание. Данный файл появляется только после запуска Configuration Manager.

---

2 Найдите следующий раздел:

enableLWSSO enableLWSSOFramework="true"

и убедитесь, что установлено значение **true**.

3 Найдите следующий раздел:

lwssoValidation id="ID000001">
<domain> </domain>

и введите домен сервера Configuration Manager после **<domain>**.

4. Найдите следующий раздел:

   <initString="This string should be replaced"></crypto>

   и замените "This string should be replaced" на общую строку, используемую всеми надежными приложениями, работающими с LW-SSO.

5. Найдите следующий раздел:

   <!--multiDomain>
   <trustedHosts>
   <DNSDomain>This value should be replaced by your application domain</DNSDomain>
   <DNSDomain>This value should be replaced by domain of other application</DNSDomain>
   </trustedHosts>
   </multiDomain-->

   Удалите символ комментария в начале и введите домены сервера Configuration Manager в элементы DNSDomain (вместо This value should be replaced by your application domain). Список должен включать домен сервера, введенный в шаге 3 на стр. 20.

6. Сохраните измененный файл и перезапустите сервер.

7. Запустите веб-обозреватель и введите следующий адрес: http://<адрес сервера UCMDB>.<domain_name>:8080/jmx-console.

   Введите реквизиты проверки подлинности консоли JMX, которые по умолчанию имеют следующие значения:

   - Имя входа = **sysadmin**
   - Пароль = **sysadmin**

8. В разделе **UCMDB-UI** выберите **Настройка LW-SSO**, чтобы открыть страницу просмотра JMX MBEAN.

9. Выберите метод **setEnabledForUI**, задайте значение **true** и нажмите **Вызвать**.

10. Выберите метод **setDomain**. Введите имя домена сервера UCMDB и нажмите **Вызвать**.

11. Выберите метод **setInitString**. Введите значение initString, которое было введено для Configuration Manager в шаге 4 на стр. 21 и нажмите **Вызвать**.
12. Если Configuration Manager и UCMDB находятся в разных доменах, выберите метод **addTrustedDomains** и введите имена доменов серверов UCMDB и Configuration Manager. Нажмите **Вызвать**.
13. Для просмотра сохраненной в настройках конфигурации LW-SSO выберите метод **retrieveConfigurationFromSettings** и нажмите **Вызвать**.
14. Для просмотра фактической загруженной конфигурации LW-SSO выберите метод **retrieveConfiguration** и нажмите **Вызвать**.

Поддержка IPv6

Configuration Manager поддерживает адреса IPv6 только в части, обращенной к пользователю.

Работа с Configuration Manager через адрес IPv6:

1. Убедитесь, что операционная система поддерживает IPv6. Подробнее см. в документации по операционной системе.
2. Откройте файл **client-config.properties**, расположенный в директории **conf** внутри **<директории установки Configuration Manager>**. Измените значение параметра **bsf.server.url** на адрес IPv6, заключенный в квадратные скобки. Пример:

   bsf.server.url=http://[2620:0:a17:e008:d840:5b0f:2040:519c]:8080/bsf

2

Configuration Manager Мастер послеустановочной настройки

Данная глава содержит следующую информацию:

Мастер послеустановочной настройки Configuration Manager: обзор

В данной главе приводится подробное описание страниц Мастера послеустановочной настройки Configuration Manager, а также соответствующих процедур настройки. Данные материалы открываются при нажатии **Справка** на любой странице мастера.

Страница подключения к базе данных

Этот раздел включает следующие темы:

Общие

Необходимо настроить подключение к базе данных со стандартным URL-адресом. Чтобы настроить расширенные параметры, например, Oracle Real Application Cluster, настройте стандартное подключение, а затем вручную внесите необходимые изменения в файл **database.properties**.

Configuration Manager использует встроенные драйверы для Oracle и Microsoft SQLServer. Таким образом, как правило, поддерживаются все функции встроенных драйверов, которые можно настроить в URL-адресе базы данных. URL-адрес находится в файле **database.properties**.

Примечание. Настройка расширенных параметров должна проводиться после завершения процесса послеустановочной настройки и создания рабочей конфигурации.

Параметры

Для создания подключения к базе данных введите следующие параметры:

Параметр	Рекомендуемое значение	Описание
Поставщик	<определяется пользователем>	Поставщик базы данных Возможные значения: **Oracle** или **Microsoft** HP Universal CMDB можно установить при помощи того же мастера установки, что и Configuration Manager, либо отдельно. Если Configuration Manager и UCMDB устанавливаются на одной машине при помощи одного и того же мастера установки, значением по умолчанию для данного параметра является поставщик базы данных, уже выбранный в мастере послеустановочной настройки UCMDB. Значения по умолчанию устанавливаются только в случае установки обоих приложений при помощи одного и того же мастера установки. При использовании отдельных пакетов установки, даже если UCMDB устанавливается на ту же машину, что и Configuration Manager, значения по умолчанию НЕ устанавливаются в мастере послеустановочной настройки.
Имя хоста	<определяется пользователем>	Имя хоста сервера базы данных Если Configuration Manager и UCMDB устанавливаются на одной машине, значением по умолчанию для данного параметра является сервер базы данных, уже выбранный в мастере послеустановочной настройки UCMDB. **Данное значение является обязательным.**

Параметр	Рекомендуемое значение	Описание
Порт	<определяется пользователем>	Порт прослушивания базы данных Если Configuration Manager и UCMDB устанавливаются на одной машине, значением по умолчанию для данного параметра является порт базы данных, уже выбранный в мастере послеустановочной настройки UCMDB. Для Oracle значение по умолчанию – **1521**. Для Microsoft SQL Server значение по умолчанию – **1433**. **Данное значение является обязательным.**
SID/DB	<определяется пользователем>	Имя Oracle SID или базы данных Microsoft SQL Server Если Configuration Manager и UCMDB устанавливаются на одной машине, значением по умолчанию для данного параметра является sid/db базы данных, уже выбранный в мастере послеустановочной настройки UCMDB. **Данное значение является обязательным.**
Имя пользователя	<определяется пользователем>	Имя пользователя для входа в базу данных. **Данное значение является обязательным.**
Пароль	<определяется пользователем>	Пароль для входа в базу данных.

Настройки

Также доступны следующие настройки:

Параметр	Рекомендуемое значение	Описание
Шифровать пароль	<определяется пользователем>	Если включено, пароль в файле **database.properties** шифруется. В целях безопасности рекомендуется шифровать пароли, хранящиеся в текстовых файлах.
Создать объекты схемы	<определяется пользователем>	Если включено, создаются объекты схемы, необходимые для запуска Configuration Manager. Снимите данный флажок, если при установке используется существующая схема, заполненная объектами Configuration Manager.

Тест

Примечание. Перед продолжением настоятельно рекомендуется проверить свойства подключения.

Для проверки подключения нажмите **Тест**. Мастер попытается подключиться к базе данных для проверки соединения. Результаты проверки отображаются справа от кнопки **Тест**.

База данных создает различные сообщения об ошибках. Их значение ясно из текста – как правило, они вызваны неверным вводом имени пользователя или пароля. Перед продолжением настройки необходимо исправить ошибку и добиться успешной проверки подключения.

Страница сервера приложений

Этот раздел включает следующие темы:

Общие

Настройте сервер приложений Configuration Manager, указав номера портов по умолчанию, перечисленные ниже.

Параметры

Для настройки сервера приложений Configuration Manager введите следующие параметры:

Параметр	Рекомендуемое значение	Описание
Имя хоста	<определяется пользователем>	Внешнее имя сервера приложений По умолчанию в качестве этого значения используется полное доменное имя машины, на которой запущен мастер (и Configuration Manager). В некоторых системах данное имя должно отличаться – напр., при развертывании веб-сервера перед сервером приложения Configuration Manager.
Настройка портов	<определяется пользователем>	По умолчанию данный параметр отключен. Если его включить, появится возможность изменения стандартных портов сервера приложений.

Параметр	Рекомендуемое значение	Описание
порт HTTP	<определяется пользователем>	Порт HTTP сервера приложения Configuration Manager Значение по умолчанию: **8080** Значение по умолчанию при установке на одной машине с HP Universal CMDB: **8180**
порт HTTPS	<определяется пользователем>	Порт HTTPS сервера приложения Configuration Manager Значение по умолчанию: **8443** Значение по умолчанию при установке на одной машине с UCMDB: **8143**
Порт Tomcat	<определяется пользователем>	Порт управления сервером приложения Configuration Manager Значение по умолчанию: **8005**
Порт AJP	<определяется пользователем>	Порт протокола AJP (Apache Java Protocol) сервера приложения Configuration Manager Значение по умолчанию: **8009**
Порт JMX HTTP	<определяется пользователем>	Порт JMX HTTP сервера приложения Configuration Manager Значение по умолчанию: **39900**
Удаленный порт JMX	<определяется пользователем>	Удаленный порт JMX сервера приложения Configuration Manager Значение по умолчанию: **39600**

Страница конфигурации службы Windows

Укажите, следует ли устанавливать Configuration Manager как службу Windows. Данный параметр доступен только при установке на машину с Windows.

Настроить службу Windows можно вручную при помощи утилиты **create-windows-service.bat**, расположенной в директории **cnc-home/bin**.

Страница реквизитов пользователей

Этот раздел включает следующие темы:

➤ "Общие" на стр. 30

Общие

Настройте следующих начальных пользователей Configuration Manager:

Параметр	Рекомендуемое значение	Описание
Пользователь Admin	<определяется пользователем>	Администратор Configuration Manager – "суперпользователь"
Пользователь интеграции	<определяется пользователем>	Пользователь, создаваемый средствами Configuration Manager в HP Universal CMDB для целей интеграции

Примечание. Необходимо указать имена пользователей и пароли для пользователя-администратора и пользователя интеграции.

Страница подключения к HP Universal CMDB

Этот раздел включает следующие темы:

Общие

Настраивать подключение к HP Universal CMDB не обязательно.

При совместной установке Configuration Manager и UCMDB на одну машину данная страница не требует ввода параметров.

Если же UCMDB устанавливается отдельно или на другую машину (даже если при подключении к UCMDB используется localhost), либо если UCMDB устанавливается до установки Configuration Manager, необходимо запустить UCMDB и ввести данные параметры подключения.

Примечание. При установке с использованием удаленного экземпляра UCMDB необходимо убедиться, что экземпляр запущен. При установке Configuration Manager и UCMDB на одну машину необходимо отключить UCMDB на время работы данного мастера.

Параметры

Для настройки подключения к UCMDB введите следующие параметры:

Параметр	Рекомендуемое значение	Описание
Использовать HP UCMDB на другом хосте	<определяется пользователем>	При установке Configuration Manager и UCMDB на разных машинах включите данный параметр, чтобы активировать все остальные свойства.
Имя хоста	<определяется пользователем>	Имя хоста, на котором установлено UCMDB
Порт	<определяется пользователем>	Порт прослушивания UCMDB
Протокол	<определяется пользователем>	HTTP или HTTPS
Клиент	<определяется пользователем>	Клиент UCMDB
Имя пользователя-администратора	<определяется пользователем>	Имя пользователя системного администратора UCMDB
Пароль пользователя-администратора	<определяется пользователем>	Пароль системного администратора UCMDB

Тест

Примечание. Перед продолжением настоятельно рекомендуется проверить свойства подключения.

Для проверки подключения нажмите **Тест**. Мастер попытается подключиться к UCMDB для проверки соединения. Результаты проверки отображаются справа от кнопки **Тест**.

UCMDB создает различные сообщения об ошибках. Их значение ясно из текста – как правило, они вызваны неверным вводом имени пользователя или пароля. Перед продолжением настройки необходимо исправить ошибку и добиться успешной проверки подключения.

Страница сводки

На данной странице отображаются все параметры, настроенные на других страницах мастера. Проверьте правильность всех настроек и при необходимости внесите изменения. Затем нажмите **Далее**, и мастер выполнит необходимую настройку.

Страница завершения

Это последняя страница **Мастера послеустановочной настройки** Configuration Manager. Послеустановочная настройка завершена. Нажмите **Завершить**, чтобы закрыть мастер.

Примечание. Даже при успешном выполнении всех задач рекомендуется проверить журнал в файле **cnc-home/tmp/chp/app.log**.

3

Настройка LDAP

В HP UCMDB Configuration Manager управление пользователями, ролями и правами доступа осуществляется при помощи LDAP. В данной главе описываются процедуры настройки и диагностики неисправностей LDAP.

Данная глава содержит следующую информацию:

Обзор LDAP

Configuration Manager поставляется со встроенным сервером LDAP (отмеченным в интерфейсе пользователя как **Общий**), но может также подключаться к серверу LDAP организации. В Configuration Manager эти серверы используются для поиска пользователей, групп и ролей, хранения данных персонализации, а также для проверки подлинности пользователей. Для каждой из перечисленных выше функций может использоваться либо внутренний сервер, либо сервер организации.

В типичном варианте установки внутренний (общий) сервер LDAP используется для хранения ролей, а внешний (сервер организации) – для всех остальных данных.

Выбор поставщиков

1. Войдите в **Configuration Manager** с правами администратора.
2. Откройте меню **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями** и выберите ОБЩИЙ (SHARED) или ВНЕШНИЙ (EXTERNAL) для каждого из следующих атрибутов (по умолчанию везде выбрано ОБЩИЙ):
   - ➤ Поставщик проверки подлинности
   - ➤ Поставщик групп
   - ➤ Поставщик персонализации
   - ➤ Поставщик ролей
   - ➤ Поставщик связей ролей
3. Сохраните набор конфигурации.

Подключение к серверу LDAP организации

В HP UCMDB Configuration Manager изначально настроено использование внутреннего (общего) сервера LDAP. В данной главе описывается процедура подключения к серверу LDAP организации.

Этот раздел включает следующие темы:

Настройка подключения к LDAP

В данном разделе описывается процедура подключения Configuration Manager к внешнему серверу LDAP. В качестве внешнего сервера LDAP выступает сервер LDAP организации, где хранятся все пользователи организации.

1 Войдите в **Configuration Manager** с правами администратора.

2 Откройте меню **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями> Внешнее хранилище пользователей** и настройте значения следующих атрибутов согласно свойствам сервера LDAP организации:

Общее подключение к LDAP

ldapHost: <Имя хоста LDAP>

ldapPort: <Номер порта LDAP>

enableSSL: <True/false— использование SSL при подключении к LDAP>

useAdministrator: <True/false— использование пользователя при подключении к LDAP>

ldapAdministrator: <имя пользователя LDAP (необходимо, если **useAdministrator=true)**>

ldapAdministratorPassword: <пароль пользователя LDAP (необходим, если **useAdministrator=true)**>

3 Сохраните набор конфигурации.

Настройка поставщиков групп и пользователей

Данная процедура позволяет настроить сервер LDAP организации (внешнее хранилище) как поставщика групп и пользователей. При этом для проверки подлинности по-прежнему используется внутренний сервер LDAP (общее хранилище), однако данные о пользователях и группах берутся с внешнего сервера LDAP. Этот режим используется для тестирования конфигурации с внешним сервером LDAP, а также для предоставления прав доступа пользователям в организации.

Настройка поставщиков групп и пользователей:

1 Откройте страницу **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями > Внешнее хранилище пользователей**. Убедитесь, что используется черновик набора конфигурации, сохраненный в разделе "Настройка подключения к LDAP" на стр. 37.

2 Измените значения следующих атрибутов согласно свойствам сервера LDAP организации:

   a **Поиск пользователей**

      usersBase: <Базовое различительное имя для поиска пользователей>

      usersScope: <Сфера поиска пользователей>

      usersFilter: <Фильтр для поиска пользователей>

   b **Класс объектов пользователей** (зависит от поставщика LDAP)

      usersObjectClass: <Класс объектов пользователей LDAP>

      usersUniqueIDAttribute: <Атрибут LDAP уникального кода пользователя>

      Следующие атрибуты являются необязательными:

         usersDisplayNameAttribute: <Отображаемое имя пользователя - атрибут LDAP>

         usersLoginNameAttribute: <Имя для входа пользователя - атрибут LDAP>

         usersFirstNameAttribute: <Имя пользователя - атрибут LDAP>

         usersLastNameAttribute: <Фамилия пользователя - атрибут LDAP>

         usersEmailAttribute: <Адрес эл. почты пользователя - атрибут LDAP>

         usersPreferredLanguageAttribute: <Язык пользователя - атрибут LDAP>

         usersPreferredLocationAttribute: <Местоположение пользователя - атрибут LDAP>

usersTimeZoneAttribute: <Часовой пояс пользователя - атрибут LDAP>

usersDateFormatAttribute: <Формат даты пользователя - атрибут LDAP>

usersNumberFormatAttribute: <Формат чисел пользователя - атрибут LDAP>

usersWorkWeekAttribute: <Рабочая неделя пользователя - атрибут LDAP>

usersTenantIDAttribute: <Код клиента пользователя – атрибут LDAP>

usersPasswordAttribute: <Пароль пользователя - атрибут LDAP>

c **Поиск групп**

groupsBase: <Базовое различительное имя для поиска групп>

groupsScope: <Сфера LDAP для поиска групп>

groupsFilter: <Фильтр для поиска групп>

rootGroupsBase: <Базовое различительное имя для поиска корневых групп>

rootGroupsScope: <Сфера LDAP для поиска корневых групп>

rootGroupsFilter: <Фильтр для поиска групп>

d **Класс объектов групп** (зависит от поставщика LDAP)

groupsObjectClass: <Класс объектов групп LDAP>

groupsMembersAttribute: <Члены групп - атрибут LDAP>

Следующие атрибуты являются необязательными:

groupsNameAttribute: <Уникальное имя групп – атрибут LDAP>

groupsDisplayNameAttribute: <Отображаемое имя групп – атрибут LDAP>

groupsDescriptionAttribute: <Описание групп - атрибут LDAP>

enableDynamicGroups: <Включить динамические группы>

dynamicGroupsClass: <Динамические группы – класс объектов LDAP>

dynamicGroupsMemberAttribute: <Члены динамических групп - атрибут LDAP>

dynamicGroupsNameAttribute: <Уникальное имя динамических групп – атрибут LDAP>

dynamicGroupsDisplayNameAttribute: <Отображаемое имя динамических групп – атрибут LDAP>

dynamicGroupsDescriptionAttribute: <Описание динамических групп - атрибут LDAP>

e **Иерархия групп** (если на сервере LDAP организации используется иерархия групп)

enableNestedGroups: <Включить поддержку вложенных групп>

maximalAllowedGroupsHierarchyDepth: <Максимальная глубина иерархии групп>

f **Расширенная настройка**

ldapVersion: <Версия LDAP>

baseDistinguishNameDelimiter: <Разделитель базового различительного имени>

scopeDelimiter: <Разделитель сферы>

attributeValuesDelimiter: <Разделитель значений атрибутов LDAP>

3 Сохраните черновик набора конфигурации.

Активация набора конфигурации

1 Откройте меню **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями** и установите следующие параметры.

Внешний источник UUM: True

Поставщик групп: ВНЕШНИЙ

Поставщик пользователей: ВНЕШНИЙ

2 Сохраните и активируйте настройки.

3 Выйдите из системы и перезапустите сервер **Configuration Manager**.

Предоставление пользователям прав доступа

С помощью данной процедуры пользователю в организации присваивается роль **Системный администратор**. Пользователь с ролью **Системный администратор** имеет право назначать соответствующие роли другим пользователям в организации.

1. Войдите в **Configuration Manager** с правами администратора.
2. Откройте модуль **Управление пользователями** (**Администрирование > Управление пользователями**).
3. Убедитесь, что отображаются группы и пользователи с сервера LDAP организации.
4. Откройте **Управление пользователями > панель Поиск пользователей** и найдите пользователей, которых необходимо сделать администраторами. Например: Имя = и*, Фамилия = Иванов.
5. Присвойте пользователями роль **Системный администратор**.

Настройка внешнего сервера LDAP как поставщика проверки подлинности

Данная процедура позволяет настроить сервер LDAP организации как поставщика проверки подлинности.

1. Откройте меню **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями** и установите следующие параметры.

   Поставщик проверки подлинности: ВНЕШНИЙ
2. Сохраните и активируйте настройки.
3. Выйдите из системы и перезапустите сервер **Configuration Manager**.
4. Войдите в систему с данными пользователя организации, которому назначена роль **Системный администратор**.

Импортирование сертификата LDAP

Если для подключения к серверу LDAP организации необходим сертификат, выполните следующие действия:

1 Экспортируйте сертификат в файл.

2 Остановите службу Configuration Manager в Windows.

3 Выполните следующую команду:

<директория установки Configuration Manager>\java\windows\x86_64\bin\keytool.exe -import -trustcacerts -alias <псевдоним сертификата> -keystore <директория установки Configuration Manager>\java\windows\x86_64\lib\security\cacerts -storepass changeit -file <путь к файлу сертификата>

4 Запустите службу Configuration Manager в Windows.

Настройка внутреннего (общего) LDAP

Изменение пароля внутреннего (общего) сервера LDAP (необязательно)

Для повышения безопасности можно изменить пароль внутреннего (общего) сервера LDAP.

1 Войдите в **HP Universal CMDB Configuration Manager**.

2 Откройте командную строку и перейдите в папку **<директория установки Configuration Manager>\ldap\serverRoot\bat**.

3 Выполните команду **ldappasswordmodify -h localhost -p <порт ldap> -D "cn=Directory Manager" -w <пароль администратора ldap> -c <пароль администратора ldap> -n <новый пароль администратора ldap>**.

   a По умолчанию используется пароль администратора ldap **ldapadmin**.

   b Номер порта по умолчанию – **2389**.

   c Убедитесь, что команда выполнена успешно, и только затем переходите к следующему шагу.

4 В **UCMDB Configuration Manager** выберите **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями > Общее хранилище пользователей**.

5 Измените пароль в атрибуте **ldapAdministratorPassword**.

6 Сохраните и активируйте настройки.

7 Выйдите из **UCMDB Configuration Manager**.

8 Перезапустите сервер **UCMDB Configuration Manager**.

Настройка порта внутреннего (общего) LDAP

Возможно, порт по умолчанию, 2389, уже используется другим приложением. Чтобы изменить номер порта, выполните следующие действия:

Настройка порта внутреннего LDAP:

1 Откройте командную строку и перейдите в папку **<директория установки Configuration Manager>\ldap\serverRoot\bat**.

2 Выполните следующую команду:
dsconfig -h localhost -p 2444 -D "cn=directory manager" -w <ldap admin password> --trustAll -X -n set-connection-handler-prop --handler-name "LDAP Connection Handler" --set listen-port:<новый порт>

По умолчанию используется <пароль администратора ldap> **ldapadmin**.

3 Убедитесь в отсутствии сообщений об ошибках и только затем переходите к следующему шагу.

4 Войдите в HP Universal CMDB Configuration Manager

5 В UCMDB Configuration Manager выберите **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями > Общее хранилище пользователей** и измените номер порта в атрибуте **ldapPort**.

6 Сохраните и активируйте настройки.

7 Выйдите из UCMDB Configuration Manager.

8 Перезапустите сервер UCMDB Configuration Manager.

Устранение неисправностей в LDAP

Проблема: Не удается установить связь с сервером LDAP. В журнале появляется сообщение об ошибке подключения.

Решение: Проверьте настройки имени хоста и номера порта LDAP, а также SSL:

a Убедитесь в правильности настройки имени хоста и номера порта LDAP:
Выберите **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями > Внешнее хранилище пользователей** и проверьте настройки **ldapHost, ldapPort**.

b Проверьте, правильно ли настроен режим SSL. Узнайте у администратора сервера LDAP организации, необходим ли для подключения к LDAP пользователь с правами администратора. Выберите **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями > Внешнее хранилище пользователей** и проверьте настройку **enableSSL**.

c Проверьте, установлен ли необходимый сертификат сервера. Выполните следующую команду:

<директория установки Configuration Manager>\java\windows\x86_64\bin\keytool.exe -list -trustcacerts [-alias <certificate alias>] -keystore <директория установки Configuration Manager>\java\windows\x86_64\lib\security\cacerts -storepass changeit

d Узнайте у администратора сервера LDAP организации, необходим ли для подключения к LDAP пользователь с правами администратора. Выберите **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями > Внешнее хранилище пользователей** и проверьте следующие настройки. **useAdministrator, ldapAdministrator, ldapAdministratorPassword**

Проблема: На странице управления пользователями и группами не отображаются группы. В журнале нет сообщений об ошибках.

Решение: Проверьте следующие параметры:

a Убедитесь в правильности настройки фильтров пользователей и групп: Выберите **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями > Внешнее хранилище пользователей** и измените следующие свойства. **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**

b Откройте браузер клиента LDAP и найдите пользователей под базовым DN.

Проблема: Медленно работает интерфейс пользователя.

Решение: Как правило, замедление работы вызвано слишком большим числом настроенных в LDAP пользователей или групп. Настройте базовое DN и фильтры для уменьшения числа групп в соответствующем подмножестве следующим образом:

a Выберите **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями > Внешнее хранилище пользователей**.

b Измените следующие настройки: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**

Проблема: На странице управления пользователями и группами не отображаются некоторые известные пользователи.

Решение: На странице управления пользователями и группами отображаются только пользователи, принадлежащие к какой-либо группе. Поместите пользователей в соответствующую группу в LDAP, после чего они отобразятся на главной странице.

Проблема: Вход в систему занимает слишком много времени.

Решение: Возможно, пользователь принадлежит к очень большому числу групп. Для оптимизации времени входа можно изменить настройки фильтра поиска групп так, чтобы он возвращал меньшее число групп. Для этого:

a Выберите **Администрирование > Администрирование сервера > Управление пользователями > Настройка управления пользователями > Внешнее хранилище пользователей**.

b Измените настройку **groupsFilter** .

4

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

Данная глава включает:

Обзор проверки подлинности LW-SSO

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.

Данный раздел включает следующие темы:

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, задействованные 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**.

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.

- **Отображение (синхронизация) пользователей.** Платформа LW-SSO не обеспечивает отображение пользователей между интегрированными приложениями. 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 для целей проверки пользователей все незащищенные ресурсы в Диспетчере удостоверений должны иметь настройку **nonsecureURLs** в файле конфигурации LW-SSO.

Устранение неполадок и ограничения

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 обозревателя Internet Explorer 7**. Функция выхода из нескольких доменов может работать с проблемами при следующих условиях:

  - Используется обозреватель Internet Explorer 7, и приложение вызывает три последовательных команды перенаправления HTTP 302 в процедуре выхода.

  В этом случае обозреватель 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 обозревателя 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

- **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.

5

Проверка подлинности через Диспетчер удостоверений

Данная глава включает:

Включение проверки подлинности через Диспетчер удостоверений

Если используется Диспетчер удостоверений, и необходимо добавить HP Universal CMDB Configuration Manager, выполните следующие действия.

В данной задаче описывается настройка в HP Universal CMDB Configuration Manager поддержки проверки подлинности через Диспетчер удостоверений.

Данная задача включает в себя следующие действия:

Необходимые условия

Сервер Tomcat Configuration Manager должен быть подключен к веб-серверу (IIS или Apache), защищенному при помощи Диспетчера удостоверений через коннектор Tomcat Java (AJP13).

Инструкции по использованию коннектора Tomcat Java (AJP13) см. в документации по Tomcat Java (AJP13).

Настройка HP Universal CMDB Configuration Manager для работы с Диспетчером удостоверений

Настройка Tomcat Java (AJP13) с IIS6:

1 Настройте в Диспетчере удостоверений отсылку заголовка персонализации / обратного вызова, содержащего имя пользователя, а также запрос имени заголовка.

2 Откройте файл **<директория установки Configuration Manager>\conf\lwssofmconf.xml** и найдите раздел, начинающийся с **in-ui-identity-management**.

Пример:

```
<in-ui-identity-management enabled="false">
    <identity-management>
      <userNameHeaderName>sm-user</userNameHeaderName>
    </identity-management>
</in-ui-identity-management>
```

a Включите функцию, удалив символ комментария.

b Замените **enabled="false"** на **enabled="true"**.

c Замените **sm-user** на имя заголовка, запрошенное в шаге 1.

3 Откройте файл **<директория установки Configuration Manager>\conf\client-config.properties** и измените следующие свойства:

a Замените **bsf.server.url** на URL-адрес Диспетчера удостоверений, а порт - на порт Диспетчера удостоверений:

bsf.server.url=http://< URL-адрес Диспетчера удостоверений>:< порт Диспетчера удостоверений >/bsf

b Измените **bsf.server.services.url** на протокол HTTP и введите изначальный номер порта Configuration Manager:

bsf.server.services.url=http://<Configuration Manager URL>:< Configuration Manager Port>/bsf

Пример использования коннектора Java для настройки Диспетчера устройств для Configuration Manager с IIS6 на базе ОС Windows 2003

В данном примере описана установка и настройка коннектора Java при конфигурации управления удостоверениями для Configuration Manager с IIS6 на базе операционной системы Windows 2003.

Установка коннектора Java и его настройка для IIS6 на базе Windows 2003:

1 Загрузите последнюю версию Java Connector (напр., **djk-1.2.21**) с вебсайта Apache.

a Нажмите **http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/**.

b Выберите последнюю версию.

c Загрузите файл **isapi_redirect.dll** из директории **amd64**.

2 Сохраните файл в директории **<директория установки Configuration Manager>\tomcat\bin\win32**.

3 Создайте новый текстовый файл с именем **isapi_redirect.properties** в той же директории, что и isapi_redirect.dll.

Содержимое файла:

Файл конфигурации Jakarta ISAPI Redirector

Путь к ISAPI Redirector Extension относительно вебсайта

Это должна быть виртуальная директория с правами на исполнение

extension_uri=/jakarta/isapi_redirect.dll

Полный путь к файлу журнала ISAPI Redirector

log_file=<директория установки Configuration Manager>\servers\server-0\logs\isapi.log

Уровень журнала (debug, info, warn, error или trace)

log_level=info

Полный путь к файлу workers.properties

worker_file==<директория установки Configuration Manager>\tomcat\conf\workers.properties.minimal

Полный путь к файлу uriworkermap.properties

worker_mount_file==<директория установки Configuration Manager>\tomcat\conf\uriworkermap.properties

4 Создайте новый текстовый файл с именем **workers.properties.minimal** в **<директория установки Configuration Manager>\tomcat\conf**.

Содержимое файла:

workers.properties.minimal -

#

В данном файле содержится минимальная конфигурация jk

свойства, необходимые для

подключения к Tomcat.

#

Определение протокола worker с именем ajp13w типа ajp13

Имя и тип не обязательно

совпадают.

worker.list=ajp13w

worker.ajp13w.type=ajp13

worker.ajp13w.host=localhost

worker.ajp13w.port=8009

#END

5 Создайте новый текстовый файл с именем **uriworkermap.properties** в **<директория установки Configuration Manager>\tomcat\conf**.

Содержимое файла:

```
# uriworkermap.properties - IIS
#
# В данном файле содержатся образцы отображений, например:
# ajp13w worker, определенный в workermap.properties.minimal
# Общий синтаксис файла:
# [URL]=[Worker name]

/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

Важно: Обратите внимание, что у Configuration Manager должно быть два правила. Новый синтаксис позволяет объединить их в одно правило, например:

/cnc|/*=ajp13w

---

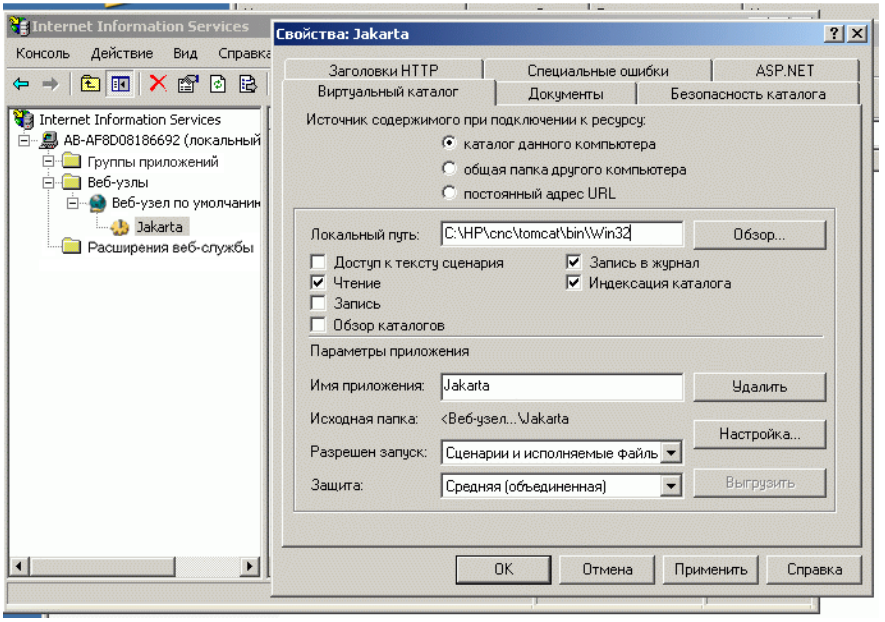
6 Создайте виртуальную директорию в соответствующем объекте вебсайта в настройках IIS.

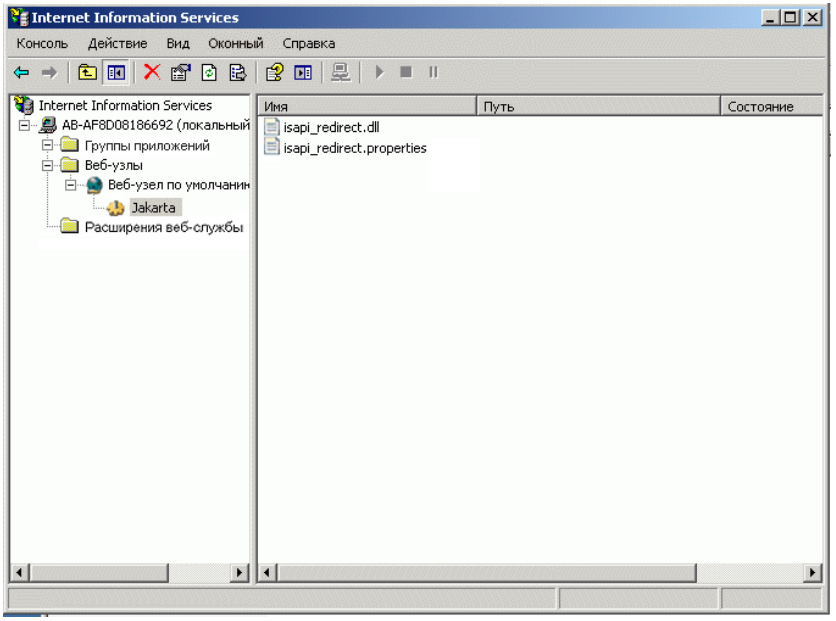
a Нажмите кнопку "Пуск" и откройте **Настройка\Панель управления\Администрирование\Менеджер Internet Information Services (IIS)**.

b На панели справа нажмите правой кнопкой на **<имя локального компьютера>\веб-узлы\<имя веб-узла>** и выберите **Создать\Виртуальную папку**.

c Присвойте директории псевдоним **Jakarta** и задайте локальный путь к директории, в которой находится isapi_redirect.dll.

Окно Менеджера выглядит следующим образом:





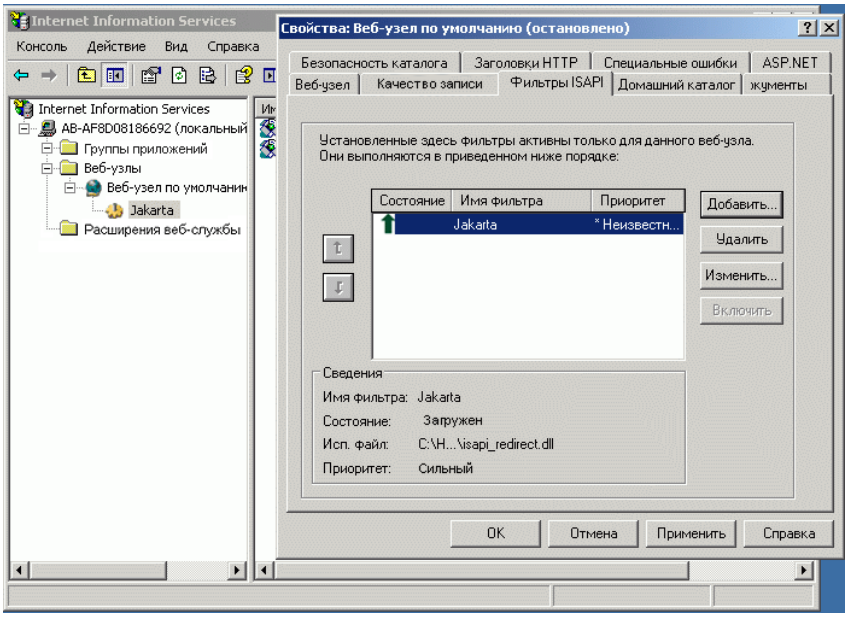
7 Добавьте **isapi_redirect.dll** как фильтр ISAPI.

a Нажмите правой кнопкой на **<имя веб-узла>** и выберите **Свойства**.

b Выберите закладку **Фильтры ISAPI** и нажмите кнопку **Добавить…**.

c Выберите имя фильтра **Jakarta** и укажите файл **isapi_redirect.dll**. Фильтр будет добавлен, но не активирован.

Окно настройки выглядит следующим образом:



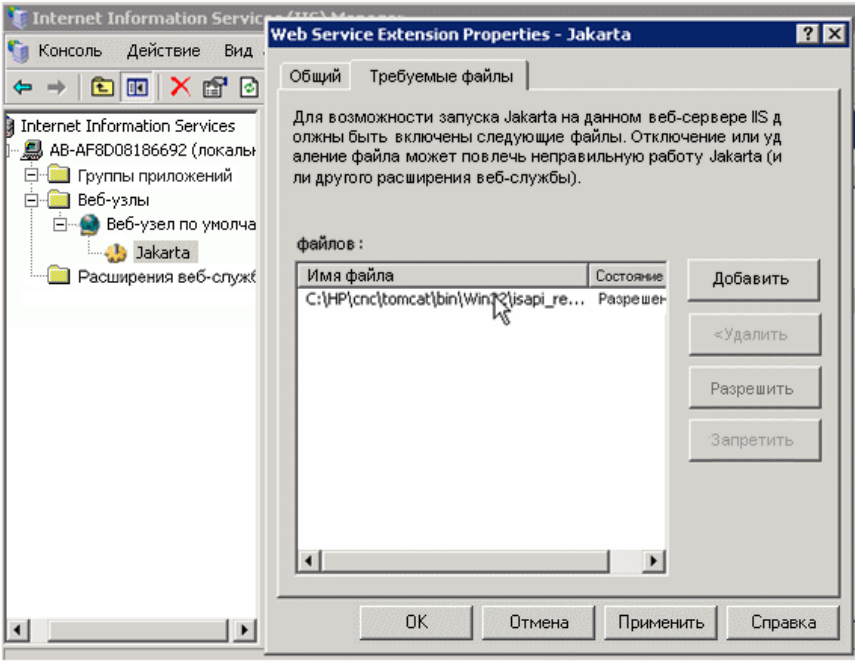
d Нажмите кнопку **Применить**.

8 Определите и разрешите новое расширение веб-службы.

a Нажмите правой кнопкой на запись **<имя локальной машины>\Расширения веб-служб** и выберите пункт меню **Добавить расширение веб-службы…**.

b Назовите новое расширение веб-службы **Jakarta** и укажите файл **isapi_redirect.dll**.

Примечание. Перед тем, как нажать кнопку **OK**, установите флажок **Разрешить расширение**.



9 Перезапустите веб-сервер IIS и войдите в приложение через веб-службу.

6

Вход в Configuration Manager

Данная глава содержит следующую информацию:

Доступ в Configuration Manager

Доступ в Configuration Manager осуществляется с помощью веб-обозревателя с любого компьютера, имеющего сетевое подключение (интранет или Интернет) к серверу Configuration Manager. Уровень доступа пользователя определяется его правами. Подробнее о предоставлении прав доступа см. в разделе "Управление пользователями" в Руководстве пользователя *HP Universal CMDB Configuration Manager*.

Дополнительные сведения о требованиях к веб-обозревателю, а также минимальных требованиях для просмотра Configuration Manager см. в разделе "Системные требования Configuration Manager" на стр. 8.

Подробнее о безопасном подключении к Configuration Manager см. в разделе "Повышение безопасности" на стр. 73.

Получение доступа к Configuration Manager

Откройте веб-браузер и введите URL-адрес сервера Configuration Manager, напр., **http://<имя сервера или IP-адрес>.<имя домена>:<порт>** где **<имя сервера или IP-адрес>.<имя домена>** соответствует полному доменному имени (FQDN) сервера Configuration Manager, а **<порт>** – номеру порта, заданному при установке.

Вход в приложение Configuration Manager

1. Введите имя пользователя и пароль, заданные в послеустановочном Мастере Configuration Manager.
2. Нажмите **Войти**. После выполнения входа имя пользователя будет отображаться в правом верхнем углу экрана.
3. (Рекомендуется) Подключитесь к серверу LDAP организации и назначьте пользователям LDAP роли администраторов, чтобы позволить администраторам Configuration Manager войти в систему. Подробнее о предоставлении прав доступа к Configuration Manager см. в разделе "Управление пользователями" в Руководстве пользователя *HP Universal CMDB Configuration Manager*.

Выход из системы

По окончании работы рекомендуется выйти из системы, чтобы предотвратить несанкционированное использование.

Для выхода из системы:

Нажмите **Выход** вверху страницы.

Примечание. По умолчанию действие сессии истекает через 30 минут.

Доступ к консоли JMX для Configuration Manager

Доступ к консоли JMX может потребоваться для устранения неисправностей или изменения некоторых настроек.

Доступ к консоли JMX:

1. Откройте консоль JMX по адресу http://<имя или IP-адрес сервера>:<порт>/cnc/jmx-console. Укажите номер порта, заданный при установке Configuration Manager.
2. Введите данные пользователя по умолчанию. Они совпадают с данными для входа в Configuration Manager.

Устранение неполадок и ограничения

Проблема. После изменения настроек в модуле "Администрирование сервера" невозможно запустить сервер.

Решение. Вернуться к прежним настройкам. Выполните следующие действия:

1. Выполните следующую команду, чтобы найти идентификатор последнего активированного набора конфигурации:

   <HP Universal CMDB Configuration Manager>\bin\export-cs.bat <свойства базы данных> --history

   где **<свойства базы данных>** можно задать путем указания файла **<директория установкиConfiguration Manager>\conf\database.properties** или задания каждого свойства базы данных. Пример:

   cd <HP Universal CMDB Configuration Manager>\bin export-cs.bat -p ..\conf\database.properties --history

2. Выполните следующую команду, чтобы экспортировать последний набор конфигурации:

   < HP Universal CMDB Configuration Manager>\bin\export-cs.bat <свойства базы данных> < ID набора конфигурации> <имя файла экспорта>

где **<ID набора конфигурации>** – это идентификатор набора конфигурации из предыдущего шага, а **<файл экспорта>** – имя временного файла, в который будут сохранены настройки. К примеру, для экспорта набора конфигурации с ID **491520** в файл **mydump.zip** введите следующую команду:

cd <директория установки HP Universal CMDB Configuration Manager>\bin export-cs.bat -p ..\conf\database.properties -i 491520 -f mydump.zip

3 Остановите службу HP Universal CMDB Configuration Manager.

4 Выполните следующую команду для импорта и активации предыдущего набора конфигурации:

< HP Universal CMDB Configuration Manager>\bin\import-cs.bat <свойства базы данных> <имя файла экспорта> --activate

Проблема. Ошибка при подключении к UCMDB.

Решение. Возможные причины:

- Сервер UCMDB не работает. Перезапустите Configuration Manager после полного включения UCMDB (убедитесь, что состояние сервера UCMDB указано как **Up**).
- Сервер UCMDB работает, однако указаны неверные реквизиты подключения Configuration Manager или URL-адрес. Запустите Configuration Manager. Откройте "Администрирование сервера", измените настройки подключения к UCMDB и сохраните новые настройки. Активируйте новые настройки и перезапустите сервер.

Проблема. Неверные настройки подключения к LDAP.

Решение. Вернуться к прежним настройкам. Задайте правильные настройки подключения к LDAP и активируйте их.

Проблема. Изменения в модели классов в UCMDB не отражаются в Configuration Manager.

Решение. Перезапустите сервер Configuration Manager.

Проблема. В журнале Configuration Manager отображается ошибка **Превышено время выполнения UCMDB**.

Решение. Данная ошибка возникает при чрезмерной нагрузке на базу данных UCMDB. Для решения данной проблемы увеличьте время выполнения следующим образом:

1 Создайте файл jdbc.properties в папке **UCMDBServer\conf**.

2 Введите следующий текст: QueryTimeout=<время в секундах>.

3 Перезапустите сервер UCMDB .

Проблема. Configuration Manager не позволяет добавить представление в список управляемых.

Решение. При добавлении представления в список управляемых в UCMDB создается новый TQL. При достижении максимально разрешенного числа активных TQL новые представления не добавляются. Увеличьте лимит активных TQL в UCMDB, изменив следующие настройки в Менеджере настроек инфраструктуры:

- Макс. число активных TQL на сервере
- Макс. число активных TQL заказчика

Проблема. Сертификат сервера HTTPS недействителен.

Решение. Возможные причины:

- Истек срок действия сертификата. Необходимо получить новый сертификат.
- Центр сертификации, подписавший сертификат, не считается надежным. Добавьте центр сертификации в список Надежных центров сертификации.

Проблема. При входе в систему через страницу входа Configuration Manager отображается ошибка входа или страница "доступ запрещен".

Решение. Возможные причины:

- Возможно, в поставщике проверки подлинности (внешнем или общем LDAP) нет пользователя с данным именем. Добавьте пользователя в систему поставщика проверки подлинности.
- Пользователь определен, однако не имеет права входить в Configuration Manager. Дайте пользователю соответствующее право доступа. Рекомендуется предоставить право входа корневой группе всех пользователей Configuration Manager.
- Данные решения также подходят в случае проблем с входом при использовании системы IDM.

Проблема. Сервер Configuration Manager не может запуститься из-за неверных реквизитов базы данных.

Решение. Если проблемы с запуском сервера начались после изменения реквизитов базы данных, возможно, реквизиты введены неверно. (**Примечание**: Послеустановочный Мастер не осуществляет автоматическую проверку введенных реквизитов. Для проверки соединения необходимо нажать в мастере кнопку **Тест**). Далее необходимо заново зашифровать пароль базы данных и ввести новые реквизиты в файле конфигурации. Выполните следующие действия:

1. Выполните следующую команду из командной строки для шифрования обновленного пароля базы данных:

   <директория установки Configuration Manager (CnC)>\bin\encrypt-password.bat –p <пароль>

   Команда возвращает зашифрованный пароль.

2. Скопируйте зашифрованный пароль (включая префикс {ENCRYPTED} в параметр **db.password** в **<директория установки CnC>\conf\database.properties**.

Проблема. При отсутствии правильного настроенного DNS для доступа к системе необходимо вводить IP-адрес. При вводе IP-адреса появляется вторая ошибка DNS.

Решение. Снова замените имя машины на IP-адрес. Пример:

Если вход осуществляется по следующему IP-адресу:
http://16.55.245.240:8180/cnc/

и возникает ошибка DNS с адресом машины, например,
http://my.example.com:8180/bsf/secure/authenicationPointURL.jsp...

замените его на:
http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

и снова запустите приложение в браузере.

Проблема. Не запускается сервер Tomcat Configuration Manager.

Решение. Попробуйте один из следующих способов:

- Запустите послеустановочный мастер и измените номера портов Configuration Manager.
- Остановите другие процессы, использующие порты Configuration Manager.
- Вручную измените номера портов в настройках Configuration Manager, отредактировав следующий файл: **<директория установки CnC>\servers\server-0\conf\server.xml** и изменив следующие номера портов:
  - HTTP (8080): строка 69
  - HTTPS (8443): строки 71 и 90

Проблема. В журнале Configuration Manager отображается ошибка из-за недостатка памяти.

Решение. Увеличьте максимальный объем памяти для Java.

Изменение объема памяти в службе Configuration Manager:

1. Перейдите в директорию **<директория установки CnC>\cnc\bin** и выполните следующую команду: edit-server-0.bat.
2. Выберите закладку **Java**.
3. Измените параметры **Начальный пул памяти (Initial memory pool)** и **Максимальный пул памяти (Maximum memory pool)**.

Изменение объема памяти в пакетном файле:

1. Перейдите в директорию **<директория установки CnC>\cnc** и откройте файл **start-server-0.bat** для редактирования
2. Найдите строку, начинающуюся с **SET JAVA_OPTS=-Dcnc.home**.
3. Найдите команды **-Xms** и **-Xmx** и измените их согласно требованиям:

   -Xms<размер начального пула памяти> -Xmx<размер максимального пула памяти>

   Пример: чтобы задать начальный пул памяти, равный 100 Мб, и максимальный пул памяти, равный 800 Мб, введите:

   -Xms100m -Xmx800m

Проблема. После нажатия **Завершить** завершение работы послеустановочного Мастера занимает много времени.

Решение. Для системы UCMDB, изначально не настроенной для работы в консолидированном режиме, операция консолидации схемы может занять продолжительное время (зависит от объема данных). Подождите 15 минут. Если прогресса нет, прервите работу Мастера и перезапустите процесс.

Проблема. Изменения ЭК в UCMDB не отражаются в Configuration Manager.

Решение. Configuration Manager выполняет процесс асинхронного автономного анализа. Возможно, процесс еще не обработал последние изменения в UCMDB. Решите проблему одним из следующих способов:

- Подождите несколько минут. По умолчанию анализ выполняется каждые 10 минут. Данный параметр можно изменить в модуле "Администрирование сервера".
- Выполните вызов JMX для запуска асинхронного анализа в соответствующем представлении.
- Откройте раздел "Администрирование политик". Нажмите кнопку **Пересчитать анализ политики**. Будет запущен асинхронный анализ для всех представлений (это может занять некоторое время). Возможно, понадобится внести искусственное изменение в одну политику и сохранить ее.

Проблема. При нажатии **Администрирование > Открыть UCMDB**, открывается страница входа в UCMDB.

Решение. Для доступа в UCMDB без повторного входа в систему необходимо включить единый вход. Дополнительные сведения см. в разделе "Включение Lightweight Single Sign-On" на стр. 20. Кроме того, убедитесь, что в системе управления пользователями UCMDB настроен пользователь, входящий в Configuration Manager.

Проблема. При настройке соединения с UCMDB в послеустановочном мастере на адрес IPv6, элемент меню **Администрирование > Открыть UCMDB** не работает.

Решение. Выполните следующие действия:

1. Откройте меню **Администрирование > Администрирование сервера > Configuration Manager > Соединение с UCMDB**.
2. Заключите IP-адрес в URL-адресе доступа к UCMDB в квадратные скобки. URL-адрес должен иметь вид: http://[x:x:x:x:x:x:x:x]:8080/.
3. Сохраните и активируйте настройки.
4. Перезапустите Configuration Manager.

При работе с Configuration Manager действуют следующие ограничения:

- После каждого изменения времени на сервере Tomcat Configuration Manager необходимо перезапустить сервер, чтобы обновить время на нем.

7

Повышение безопасности

Данная глава содержит следующую информацию:

Повышение безопасности Configuration Manager

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

Configuration Manager может быть частью защищенной архитектуры и противостоять угрозам для безопасности.

Указания по повышению безопасности описывают настройки, необходимые для повышения уровня защиты Configuration Manager.

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

Ниже описана рекомендуемая подготовка к повышению безопасности системы:

- Оцените состояние и угрозы для безопасности сети в целом, что поможет принять решение о способе интеграции Configuration Manager в сеть.
- Хорошо изучите техническую платформу и функции безопасности Configuration Manager.
- Изучите рекомендации по повышению безопасности.
- Убедитесь в полной работоспособности Configuration Manager перед началом работы по повышению безопасности.
- Выполняйте процедуры повышения безопасности по порядку в каждом разделе.

Важно!

- Описанные процедуры повышения безопасности основаны на допущении, что выполняются только шаги, перечисленные в соответствующих разделах, 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 разделах процедуры выполняются на машинах, выделенных для Configuration Manager. Использование машин для других целей помимо Configuration Manager может вызвать проблемы.
- Информация о повышении безопасности, приведенная в данном разделе, не является руководством по анализу уровня риска компьютерной системы.

Шифрование пароля базы данных

Пароль базы данных хранится в файле **<директория установки Configuration Manager>\conf\database.properties**. Механизм шифрования пароля, используемый по умолчанию, соответствует стандартам FIPS 140-2. Чтобы зашифровать пароль базы данных, установите флажок **Зашифровать пароль** на странице "Конфигурация базы данных" в послеустановочном мастере Configuration Manager.

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" на стр. 83.

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 следующие поля:
   - **engineName.** Введите название алгоритма шифрования.
   - **keySize.** Введите размер главного ключа для выбранного алгоритма шифрования.
2. Запустите сценарий **generate-keys.bat**, который создаст следующую директорию: **cnc\security\encrypt_repository**, а также ключ шифрования.
3. Повторно запустите послеустановочный мастер.

Включение SSL на сервере с самоподписанным сертификатом

В следующих разделах описана настройка в Configuration Manager поддержки проверки подлинности и шифрования с использованием SSL.

Configuration Manager использует в качестве сервера приложений Tomcat 6.0.

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** (**<директория установки Configuration Manager>\java\lib\security\tomcat.keystore**).

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 Поместите сертификат в хранилище надежных сертификатов клиента.

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

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

---

4 Проверьте настройки клиента

Откройте файл **client-config.properties**, расположенный в директории **conf** внутри **<директории установки Configuration Manager>**. Установите протокол **https** и порт **8443**.

5 Измените файл server.xml

Откройте файл **server.xml**, расположенный в директории **conf** внутри **<директории установки Configuration Manager>**. Найдите раздел, начинающийся с

Connector port="8443"

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

keystoreFile="<tomcat.keystore file location>" (см. шаг 2 на стр. 76)

keystorePass="<пароль>"

6 Перезапустите сервер

7 Проверка безопасности сервера

Для проверки безопасности сервера Configuration Manager введите в веб-браузере следующий URL-адрес: **https://<имя или IP-адрес сервера Configuration Manager>:8443/cnc**.

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

Включение SSL на сервере с сертификатом, подписанным центром сертификации

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 **tomcat.keystore** (**<директория установки Configuration Manager>\java\lib\security\tomcat.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 директорию: **<директория установки Configuration Manager>\java\lib\security**.

d Откройте командную строку и перейдите в директорию **<директория установки Configuration Manager>\bin\jre\bin**.

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

```
keytool -importkeystore -srckeystore <директория установки Configuration Manager>\conf\security\<имя файла pfx> -srcstoretype PKCS12 -destkeystore tomcat.keystore
```

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

3 Проверьте настройки клиента

Откройте следующий файл: **<директория установки Configuration Manager>\cnc\conf\client-config.properties** и убедитесь, что свойство **bsf.server.url** имеет значение **https**, а порт – **8443**.

4 Измените файл server.xml

Откройте следующий файл: **<директория установки Configuration Manager>\conf\server.xml**. Найдите раздел, начинающийся с

Connector port="8443"

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

keystoreFile="../../java/lib/security/tomcat.keystore"

keystorePass="пароль" />

5 Перезапустите сервер

6 Проверка безопасности сервера

Для проверки безопасности сервера Configuration Manager введите в веб-браузере следующий URL-адрес: **https://<имя или IP-адрес сервера Configuration Manager>:8443/cnc**.

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

Включение SSL с сертификатом клиента

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

Если сервер не считает центр сертификации надежным, импортируйте сертификат ЦС 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**.

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

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

3. На сервере импортируйте сертификат ЦС в хранилище надежных сертификатов (cacerts) при помощи утилиты keytool, введя следующую команду:

   keytool.exe -import -alias hp -file hp.cer -keystore ..\lib\security\cacerts

4 Измените файл server.xml следующим образом:

   a Внесите изменения, описанные в шаге 5 на стр. 77.

   b Сразу после этих изменений добавьте следующие строки:

   truststoreFile="../../java/lib/security/cacerts"

   truststorePass="изменить" />

   c Set clientAuth="true".

5 Проверьте безопасность сервера, как описано в шаге 7 на стр. 78.

Включение SSL только для проверки подлинности

В данной задаче описывается настройка Configuration Manager только для поддержки проверки подлинности. Это минимальный уровень безопасности, необходимый для работы с Configuration Manager.

Включение SSL для проверки подлинности:

1 Включите поддержку SSL на сервере, как описано в разделе "Включение SSL на сервере с самоподписанным сертификатом" на стр. 76 до шага 6 на стр. 78 или разделе "Включение SSL на сервере с сертификатом, подписанным центром сертификации" на стр. 78 до шага 5 на стр. 80.

2 Введите в веб-браузере следующий URL-адрес: **http://<имя или IP-адрес сервера Configuration Manager>:8080/cnc**.

Включение проверки подлинности с сертификатом клиента

В данной задаче описывается настройка Configuration Manager для проверки подлинности с сертификатом клиента.

Включение проверки подлинности с сертификатом клиента:

1 Включите поддержку SSL на сервере, как описано в разделе "Включение SSL на сервере с самоподписанным сертификатом" на стр. 76.

2 Откройте следующий файл: **<директория установки Configuration Manager>\conf\lwssofmconf.xml.** Найдите раздел, начинающийся с in-client certificate. Пример:

<in-clientCertificate userIdentifierRetrieveField="SubjectDN" userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="e" />

Включите поддержку сертификатов клиента, удалив символ комментария.

3 Выделите имя пользователя из сертификата следующим образом:

a Параметр **userIdentifierRetrieveField** указывает, в каком поле сертификата находится имя пользователя. Возможные параметры:

- **SubjectDN**
- **SubjectAlternativeName**

b Параметр **userIdentifierRetrieveMode** указывает, является ли именем пользователя все содержимое соответствующего поля либо только его часть. Возможные параметры:

- **EntireField**
- **FieldPart**

c Если значение **userIdentifierRetrieveMode** равно **FieldPart**, параметр **userIdentifierRetrieveFieldPart** указывает, какая часть соответствующего поля является именем пользователя. Значение представляет собой кодовую букву, основанную на обозначениях, определенных в самом сертификате.

4 Откройте следующий файл: **<директория установки Configuration Manager>\conf\client-config.properties** и измените следующие свойства:

- Измените **bsf.server.url** так, чтобы использовать HTTPS, и введите номер порта HTTPS, указанный в разделе "Включение SSL на сервере с самоподписанным сертификатом" на стр. 76.
- Измените **bsf.server.services.url** так, чтобы использовать HTTP, и введите изначальный номер порта HTTP.

Параметры шифрования

В следующей таблице перечислены параметры, указанные в файле **encryption.properties**, который используется для шифрования пароля базы данных. Дополнительные сведения о шифровании пароля базы данных см. в разделе "Шифрование пароля базы данных" на стр. 75.

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. 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

Параметр	Описание
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.