HP Universal CMDB Configuration Manager

для операционных систем Windows и Linux

Версия ПО: 9.20

Руководство по развертыванию

Дата выпуска документа: июнь 2011 г.
Дата выпуска программы: июнь 2011 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

ЧАСТЬ I: УСТАНОВКА И НАСТРОЙКА

Часть I

Установка и настройка

1

Обзор

Данная глава включает:

Компоненты

HP Universal CMDB Configuration Manager – это совместный выпуск нескольких компонентов:

- ➤ **HP Universal CMDB Foundation**

  HP Universal CMDB Foundation (UCMDB Foundation) – это база данных управления конфигурацией (CMDB) для организаций IT, позволяющая документировать, хранить, а также администрировать определения бизнес-служб и соответствующих инфраструктурных связей.

  В UCMDB Foundation реализована модель данных, управление потоком данных, а также функции моделирования данных. Кроме того, поддерживаются функции анализа воздействия, отслеживания изменений и подготовки отчетов с целью преобразования данных CMDB в понятную и практическую информацию, помогающую ответить на важные вопросы и решить насущные проблемы бизнеса.

➤ **HP Universal CMDB Configuration Manager**

HP Universal CMDB Configuration Manager (Configuration Manager) предлагает новый подход к управлению конфигурацией в разрезе топологии и перечня ЭК, контролируемый политиками. Приложение разработано специально для менеджеров конфигураций и их владельцев. Оно позволяет выполнять тщательный анализ, дополняющий данные об ЭК и топологии, доступные в UCMDB. Configuration Manager дает необходимые инструменты для быстрой настройки политик конфигурации для режимов топологии и перечня ЭК, а также автоматической оценки выполнения корпоративных стандартов.

Configuration Manager развертывается как дополнительный сервер на базе Tomcat. Он взаимодействует с UCMDB посредством широкого набора возможностей UCMDBSDK.

➤ **HP Discovery and Dependency Mapping Advanced Edition**

Программное обеспечение HP Discovery and Dependency Mapping Advanced Edition (DDMA), включающее обширный набор регулярно обновляемой информации, считается наилучшим методом сбора и поддержки данных об инфраструктуре IT для UCMDB.

➤ **HP Operations Orchestration**

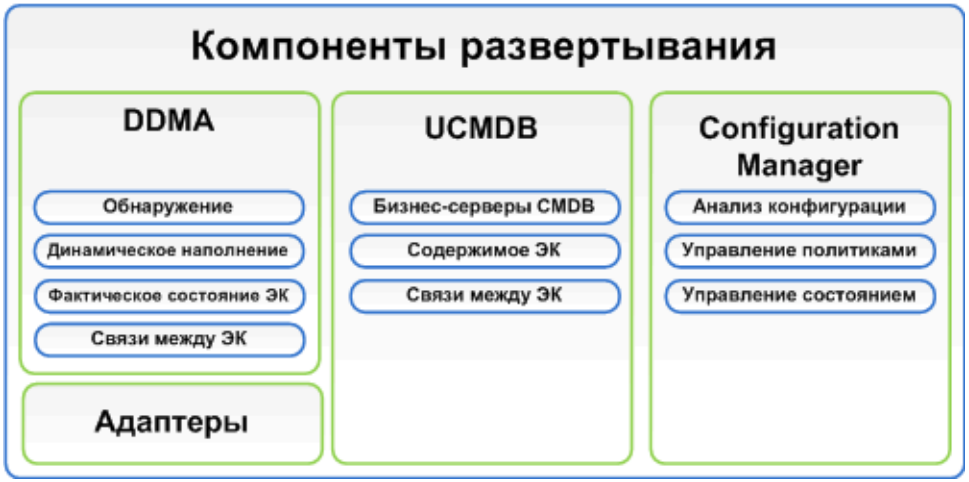
HP Operations Orchestration **(**OO) – это инструмент создания и развертывания рабочих потоков. Интуитивно-понятный интерфейс OO Studio позволяет быстро проектировать, создавать, публиковать и изменять потоки без программирования. OO Studio поддерживает взаимодействие между различными авторами благодаря системе контроля версий. Мощный встроенный отладчик позволяет тестировать потоки в различных средах, что ускоряет разработку содержимого и обеспечивает проверку потоков для стабильной и надежной работы.

Кроме того, OO Studio позволяет легко развертывать потоки. OO Studio позволяет сравнивать и приоритезировать потоки в различных средах (разработки, тестирования, промежуточной и рабочей). При этом поддерживается документирования стандартных процессов и создание структурированной документации для обеспечения соответствия нормативным требованиям.

- **Интеграция Configuration Manager с OO.**

  Configuration Manager позволяет выполнять потоки OO внутри платформы Configuration Manager. Существует два основных метода выполнения потоков OO:

  - **Интеграция процессов** – позволяет открыть RFC во внешней заявке на обслуживание, сопоставляющей определенный ЭК с конкретной политикой конфигурации.
  - **Выверка политик** – позволяет запустить поток OO для устранения проблемы в конфигурации. К примеру, виртуальной машине будет выделена дополнительная память.



Определение среды

В данном руководстве описывается процесс развертывания HP Universal CMDB Configuration Manager с различных начальных точек:

Для Configuration Manager

➤ Если установлен Configuration Manager версии 9.10

Подробнее об обновлении Configuration Manager до текущей версии см. в разделе "Обновление Configuration Manager" на стр. 39.

➤ Если Configuration Manager не установлен.

Подробнее см. в следующих разделах:

- ➤ "Установка HP Universal CMDB Configuration Manager на платформе Windows" на стр. 17
- ➤ "Установка HP Universal CMDB Configuration Manager на платформе Linux" на стр. 43

Для UCMDB

➤ Если установлена UCMDB версии до 9.03

Выполните следующие действия:

- ➤ Обновите UCMDB до версии 9.03. Подробнее см. в документе *Руководство по развертыванию HP Universal CMDB (PDF)*. Руководство можно загрузить со страницы www.hp.com/go/hpsoftwaresupport.
- ➤ Установите пакет обновлений Cumulative Update Pack 2. Его можно найти на установочном диске Configuration Manager или загрузить с вебсайта www.hp.com/go/hpsoftwaresupport.

Подробнее о настройке готовности корпоративной системы см. в разделе "Настройка базы данных или пользовательской схемы" на стр. 18.

➤ Если установлена UCMDB версии 9.03

Установите пакет обновлений Cumulative Update Pack 2. Его можно найти на установочном диске Configuration Manager или загрузить с вебсайта www.hp.com/go/hpsoftwaresupport.

Подробнее о настройке готовности корпоративной системы см. в разделе "Настройка базы данных или пользовательской схемы" на стр. 18.

➤ Если UCMDB не установлена

Попробуйте один из следующих способов:

- ➤ Установите UCMDB параллельно с Configuration Manager при помощи Диспетчера развертывания (только для систем Windows). Дополнительные сведения см. в разделе "Установка HP Universal CMDB Configuration Manager на платформе Windows" на стр. 17.
- ➤ Установите Configuration Manager на систему Linux согласно инструкциям раздела "Установка HP Universal CMDB Configuration Manager на платформе Linux" на стр. 43.

Общая информация

В данном руководстве также учитываются особые варианты развертывания UCMDB (например, система с высокой доступностью) и даются указания по изменению процесса развертывания в этих случаях.

Примечание: Поддерживается установка UCMDB и Configuration Manager на один и тот же сервер. Тем не менее, для целей масштабирования в рабочей среде HP Software рекомендует устанавливать данные компоненты на разных серверах.

Использование Configuration Manager требует настройки UCMDB в режиме консолидированной схемы и создания нового состояния UCMDB (авторизованного состояния). В обоих случаях (использование уже существующего экземпляра UCMDB или его установка при помощи Диспетчера развертывания) данные настройки выполняются в процессе развертывания автоматически.

Важно: При обращении к уже установленному экземпляру UCMDB, если его схема еще не консолидирована, консолидация крупных баз данных (более 5 млн. ЭК) может занять продолжительное время (от 20 до 60 минут).

Необходимо учесть, что при установке только Configuration Manager (т.е. с использованием уже существующего или обновленного экземпляра UCMDB) во время установки Configuration Manager сервер UCMDB должен быть запущен.

Матрица поддержки

Системные требования к серверу

ЦП	мин. 4 ядра
Память (ОЗУ)	Минимум 4 ГБ
Платформа	x64
Операционная система	Windows (64-битная) ➤ Windows 2003 Enterprise SP2 и R2 SP2 ➤ Windows 2008 Enterprise SP2 и R2 Linux ➤ Red Hat Enterprise Linux x86 (64-битная)
База данных	➤ Microsoft SQL Server 2005 SP2; 2005 режим совместимости 80 (выпуски Enterprise Edition для всех) ➤ Microsoft SQL Server 2008 ➤ Oracle 10.2.x, 11.x
Веб-сервер	➤ Microsoft IIS 7 ➤ Apache 2

HP Universal CMDB	➤ HP Universal CMDB версии 9.03 с CUP 2 (типичная вариант установки CMDB) Полный список системных требований см. в *Руководство по развертыванию HP Universal CMDB (PDF)* . **Примечание:** ➤ При развертывании сервера HP UCMDB в сочетании с Configuration Manager необходима версия Oracle Enterprise Edition, а также Oracle Partitioning. ➤ Если сервер HP Universal CMDB уже был развернут ранее с Oracle Standard Edition, и необходимо добавить в систему Configuration Manager, следует преобразовать базу данных Standard Edition в Enterprise Edition с включенной поддержкой Partitioning.
LDAP (необязательно)	➤ Active Directory ➤ SunONE 6.x
Минимальный рекомендуемый размер схемы базы данных (необязательно)	2 ГБ

Требования к клиенту

Операционная система	➤ Windows XP x86 (32-битная) ➤ Windows Vista x86 (32- и 64-битная) ➤ Windows 7 x86 (32- и 64-битная)
Веб-браузер	➤ Microsoft Internet Explorer 7.0, 8.0. ➤ Mozilla Firefox 3.x, 4

Flash Player - подключаемый модуль браузера	Flash Player версии 9 или выше **Примечание:** Flash Player можно загрузить со страницы: http://www.adobe.com/products/flashplayer/.
Разрешение экрана	➤ Минимальное: 1024x768 ➤ Рекомендуемое: 1280x1024
Качество цветопередачи	Минимум 16 бит

HP Operations Orchestration (необязательно)

HP Operations Orchestration	➤ 7.51, 9.0

2

Установка HP Universal CMDB Configuration Manager на платформе Windows

Важно: Актуальные инструкции по установке см. в сведениях о версии.

Данная глава содержит следующую информацию:

Подготовка к установке

Этот раздел включает следующие темы:

Настройка базы данных или пользовательской схемы

Примечание: Данная задача выполняется в процессе установки Configuration Manager автоматически, однако при необходимости ее можно выполнить и вручную.

Для работы с Configuration Manager необходимо создать схему базы данных. Configuration Manager и UCMDB используют различные схемы. Configuration Manager поддерживает Microsoft SQL Server и Oracle Database Server. Ниже описана процедура создания схемы базы данных для Configuration Manager. При установке UCMDB необходимо создать отдельную базу данных или схему пользователей. Дополнительные сведения см. в документе *Руководство по развертыванию HP Universal CMDB (PDF)*.

Примечание: Подробнее о системных требованиях Microsoft SQL Server и Oracle Server см. в разделе "Системные требования к серверу" на стр. 14.

Настройка базы данных

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

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

После создания базы данных один раз выполните следующую команду:

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

Подробнее 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)

Установка Configuration Manager в среде UCMDB с высокой доступностью

Для установки Configuration Manager в среде UCMDB с высокой доступностью выполните следующие действия:

1 Отключите резервный (пассивный) сервер. Подождите две минуты после отключения сервера.

2 Установите Configuration Manager версии 9.20.

a Используйте параметры хоста балансировщика нагрузки.

b Установите Configuration Manager на третий сервер (не на серверы UCMDB).

3 Проверьте работоспособность UCMDB и Configuration Manager

4 Запустите резервный (пассивный) сервер для обеспечения высокой доступности.

Примечание: Само приложение HP Universal CMDB Configuration Manager версии 9.20 не поддерживает высокую доступность.

Установка Configuration Manager

Диспетчер развертывания позволяет установить UCMDB, Configuration Manager и DDMA в различных конфигурациях (настройка выполняется на странице Выбор продуктов в мастере установки):

- Установка нового экземпляра UCMDB
- Установка нового экземпляра Configuration Manager и его подключение к новому или уже существующему экземпляру UCMDB
- Интеграция нового экземпляра Configuration Manager с существующим экземпляром OO
- Установка нескольких экземпляров DDMA

Примечание:

- Диспетчер развертывания позволяет установить на целевую машину продукты, компоненты или интеграции. При этом Диспетчер развертывания не поддерживает функции удаления, изменения продуктов, а также установки исправлений. Эти операции необходимо выполнять вручную.
- После того, как на странице выбора продуктов нажата кнопка **Далее**, вернуться и изменить конфигурацию развертывания невозможно. Если все же необходимо изменить конфигурацию развертывания, следует перезапустить Диспетчер развертывания.

Порядок установки Configuration Manager:

1. Чтобы начать установку, вставьте установочный диск Configuration Manager и найдите на нем файл **setup.exe**.
2. Двойной щелчок на файле **setup.exe** запускает Диспетчер развертывания.
3. На время установки отключите на целевой машине брандмауэр Windows. Подробнее о брандмауэре (межсетевом экране) см. в шаге 6 данной процедуры.

4 Примите условия лицензионного соглашения и нажмите **Далее**, чтобы открыть страницу выбора продуктов.

Примечание: Условия лицензии охватывают все продукты, выбранные на странице выбора продуктов в Диспетчере развертывания.

---

5 Выберите продукты, которые необходимо развернуть. Затем нажмите **Далее** для перехода на страницу выбора местоположения сервера.

На странице выбора продуктов можно указать, какие продукты следует установить, а также задать настройки, выполняемые в процессе развертывания.

a Выбор параметров установки HP Universal CMDB Foundation.

Существует два варианта установки UCMDB Foundation:

- **Подключение к существующему серверу** – в этом случае настраивается сопоставление параметров обнаружения и зависимостей между Configuration Manager и уже существующим экземпляром сервера UCMDB Foundation.

Примечание: При этом на сервере должна быть установлена UCMDB версии 9.03 с CUP 2 или более поздняя.

- **Установка нового сервера** – в этом случае выполняется установка, настройка и подключение нового сервера UCMDB Foundation, после чего к нему подключается Configuration Manager или DDMA.

b Установите флажок напротив **Configuration Manager**, чтобы установить и настроить новый экземпляр Configuration Manager.

При желании можно выбрать вариант **Подключиться к существующему экземпляру HP Operation Orchestration**. В этом случае настраивается интеграция между Configuration Manager и Operation Orchestration (для этого в Configuration Manager вносятся данные для подключения к серверу OO).

c **HP Discovery and Dependency Mapping Advanced Edition.** Данный параметр позволяет установить и настроить DDMA.

Параметр **Число экземпляров DDMA** позволяет установить сразу несколько экземпляров DDMA. При этом указанное число экземпляров DDMA подключается к одному экземпляру сервера UCMDB.

Примечание: Диспетчер развертывания позволяет установить несколько экземпляров DDMA в одной демилитаризованной зоне (DMZ). При этом Диспетчер развертывания поддерживает до 10 экземпляров зондов обнаружения в каждой развернутой системе. Если необходимо установить большее число зондов обнаружения, это можно сделать поэтапно, группами по 10.

---

6 На странице выбора местоположения серверов укажите местоположение удаленных серверов и учетные данные целевых машин для каждого выбранного продукта. Затем нажмите **Далее** для перехода на страницу настройки подключения.

Параметры развертывания

Выберите вариант развертывания в целевом местоположении. Поддерживается два варианта:

- **Развернуть на локальной машине** – продукт развертывается на машине, где установлен Диспетчер развертывания. В этом случае отключаются поля для ввода данных удаленного хоста.
- **Развернуть на следующей машине** – указывается адрес удаленного хоста и сведения о его операционной системе. При этом необходимо указать учетные данные пользователя с правами администратора на удаленном хосте.

Примечание: В имени хоста для развертывания продуктов разрешается использовать только буквы (a-z), цифры (0-9) и дефис ('-').

Необходимо указать следующие сведения об удаленном хосте:

- **Протоколы WMI и SMB** – используются для подключения к удаленной машине. Для успешного подключения Диспетчера развертывания к удаленной машине должен быть выполнен ряд условий.
  - **Служба WMI** – на удаленной машине должна быть запущена служба WMI.
  - **Служба сервера** – для работы протокола SMB на удаленной машине следует запустить службу сервера.

➤ **Брандмауэр Windows** – необходимо разрешить удаленное подключение администраторов. Выполните необходимую команду в консоли удаленной машины:

Операционная система	Команда
Windows XP Windows Server 2003 Windows Server 2003 R2	netsh firewall set service RemoteAdmin enable
Windows Vista Windows 7 Windows Server 2008 Windows Server 2008 R2	netsh advfirewall firewall set rule group="windows management instrumentation (WMI)" new enable=Yes

Проверка подключения

Нажмите **Проверка подключения**, чтобы проверить правильность введенных данных, а также проанализировать ресурсы локальной и удаленной систем.

Если проверка прошла неудачно, Диспетчер развертывания выводит сообщение со сведениями об ошибке. При нажатии на кнопку **Далее** проверка подключения выполняется автоматически.

Проверяются следующие ресурсы машины:

➤ **Платформа ОС** – проверяется, сертифицирована ли данная ОС для развертывания продуктов.

➤ **Пространство на диске** – проверяется наличие достаточного свободного пространства на диске.

➤ **Память** – проверяется наличие достаточной физической памяти.

➤ **Порты** – проверяется доступность необходимых портов.

Параметры, проверяемые в рамках проверки подключения, зависят от матрицы поддерживаемых продуктов.

Примечание: Если проверка возвращает ошибку **Unknown**, убедитесь, что на целевой машине запущены следующие службы:

- Сервер
- Windows Management Instrumentation

Перед тем, как нажать кнопку **Далее**, убедитесь, что отключена функция User Account Control (UAC). Подробнее о UAC см. по адресу http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx.

7 Настройка подключения между выбранными продуктами на странице подключений. Настройки, доступные на странице подключений, зависят от компонентов, выбранных для развертывания на странице выбора продуктов. По окончании настройки нажмите **Далее** для перехода на страницу конфигурации установки.

- Интеграция между UCMDB и Configuration Manager

  Данный раздел отображается в случае установки Configuration Manager в варианте **Подключение к существующему серверу**. Он позволяет настроить интеграцию Configuration Manager с UCMDB.

  Примечание: При этом поддерживается подключение только к экземплярам UCMDB версии 9.03 с CUP 2 или более поздней.

Укажите следующие сведения о UCMDB:

Поле	Определение
Хост/IP-адрес UCMDB	Адрес развернутого экземпляра UCMDB. ➤ Если UCMDB развернута в режиме высокой доступности, см. инструкции в разделе "Установка Configuration Manager в среде UCMDB с высокой доступностью" на стр. 19. ➤ Если UCMDB установлена на локальной машине, а Configuration Manager – на удаленной, в качестве имени локального экземпляра UCMDB следует использовать полное имя домена, а не localhost. ➤ Если у UCMDB и Configuration Manager разные имена доменов DNS, и необходима интеграция LW-SSO, в качестве имени существующего хоста UCMDB необходимо указать полное имя домена.
Протокол	Протокол HTTP или HTTPS.
Порт HTTP(S) UCMDB	По умолчанию используются номера портов **8080** для HTTP и **8443** для HTTPS.
Файл сертификата клиента	Данное поле выводится при выборе протокола HTTPS. Необходимо вручную поместить файл сертификата клиента UCMDB на целевой хост Configuration Manager и указать в соответствующем поле полный путь к нему, включая имя файла. Если UCMDB будет использовать HTTPS, необходимо обменяться ключами. В процессе проверки подключения факт обмена ключами не проверяется.

Поле	Определение
Имя клиента	В качестве имени клиента UCMDB по умолчанию используется **Default Client**. Значение имени клиента используется при настройке интеграции между UCMDB и Configuration Manager. В процессе проверки подключения данное значение не проверяется. В случае ввода неверного значения развертывание пройдет неудачно.
Порт JMX	Значение по умолчанию – **29601**.
Системный пользователь UCMDB (JMX)	Системный пользователь UCMDB (JMX) используется для активации функций JMX, например, создания пользователя интеграции в Configuration Manager и развертывания пакета Configuration Manager. Значение по умолчанию – **sysadmin**.
Системный пароль UCMDB	Пароль системного пользователя UCMDB. Значение по умолчанию – **sysadmin**.

Примечание: В Configuration Manager настроен внутренний репозиторий пользователей. Чтобы использовать в качестве репозитория пользователей внешнюю систему LDAP, необходимо внести соответствующие изменения в настройки Configuration Manager. Подробнее см. в разделе "Системные настройки" в *Руководстве пользователя HP Universal CMDB Configuration Manager*.

➤ Интеграция Configuration Manager с OO.

Данный раздел отображается при выборе варианта **Подключиться к существующему экземпляру HP Operation Orchestration**. Он позволяет настроить интеграцию Configuration Manager с OO.

Укажите следующие сведения об OO:

Поле	Определение
Версия OO	Поддерживаются версии OO 7.5 и 9.0.
Хост/IP-адрес OO	Доменное имя сервера OO.
Номер порта OO	Номер порта по умолчанию – **8443**.
Имя пользователя OO	Имя пользователя OO по умолчанию – **admin**. В OO пользователь должен быть настроен как внешний.
Пароль OO	Пароль пользователя OO по умолчанию – **admin**.

➤ Настройка DDMA

Следующие поля отображаются при выборе варианта **экземпляр Discovery and Dependency Mapping Advanced Edition**. Он позволяет настроить соединение между DDMA и UCMDB.

Укажите следующие сведения об DDMA:

Поле	Определение
Идентификатор зонда потока данных	По умолчанию используется имя хоста DDMA (поле заполняется автоматически). Данное значение можно изменить.
Использовать домен по умолчанию	Данный параметр по умолчанию включен. Он влияет на значение имени домена. Если отключить его, появляется возможность изменить значение имени домена.
Имя домена	Значение по умолчанию – **DefaultDomain**. Чтобы активировать данное поле, снимите флажок **Использовать домен по умолчанию**.

Поле	Определение
Начальный размер кучи в Мб	Начальный объем памяти, выделенный виртуальной Java-машине DDMA. Значение по умолчанию – 256 Мб.
Максимальный размер кучи в Мб	Максимальный объем памяти, выделенный виртуальной Java-машине. Значение по умолчанию – 512 Мб.

8 Укажите целевые директории для развертывания продуктов, выбранных на странице настройки установки. По окончании настройки нажмите **Далее** для перехода на страницу конфигурации базы данных.

Для каждого выбранного продукта указывается путь к директории по умолчанию. При развертывании на локальной машине доступна функция "Обзор", позволяющая выбрать другой путь к директории. Если развертывание выполняется на удаленной машине, данная функция отключена.

Примечание: Имя директории установки должно состоять только из букв (a-z), цифр (0-9) и дефисов ('-'). Использование пробелов не допускается.

---

9 На странице конфигурации базы данных указываются данные для подключения и схема базы данных для каждого продукта. По окончании настройки нажмите **Далее** для перехода на страницу конфигурации портов.

В рамках данной процедуры настраиваются следующие базы данных (схемы):

- схема UCMDB-CM
- схема UCMDB

➤ схема истории UCMDB

Поле	Определение
Хост/IP-адрес базы данных	Имя хоста сервера базы данных
Порт	MSSQL и Oracle по умолчанию используют различные порты. Для Oracle значение по умолчанию – 1521, а для MSSQL – 1433.
SID (Oracle)	Имя экземпляра базы данных Oracle.
Имя пользователя-администратора (Oracle)	Введите имя пользователя, являющегося администратором на сервере Oracle.
Пароль администратора (Oracle)	Введите пароль пользователя, являющегося администратором на сервере Oracle.
Проверка подключения	Проверка подключения к хосту целевой базы данных с указанными реквизитами.
Имя схемы (Oracle)	Введите имя схемы.
Пароль схемы (Oracle)	Введите пароль схемы. Данное поле отображается при создании новой схемы
Табличное пространство по умолчанию (Oracle)	Введите имя табличного пространства по умолчанию.
Временное табличное пространство (Oracle)	Введите имя временного табличного пространства.
Имя базы данных (MSSQL)	Введите имя схемы базы данных, которую следует использовать или создать на сервере MSSQL.
Имя пользователя базы данных (MSSQL)	Введите имя пользователя, являющегося администратором на сервере MSSQL.
Пароль базы данных (MSSQL)	Введите пароль пользователя, являющегося администратором на сервере MSSQL.

Примечание:

- ➤ В случае переполнения табличного пространства UCMDB развертывание продукта будет выполнено успешно, однако работа продуктов и компонентов будет нарушена
- ➤ Создание новой схемы UCMDB и подключение к уже существующей схеме истории UCMDB не поддерживается.
- ➤ По соображениям безопасности не поддерживается использование проверки подлинности средствами NTLM при настройке UCMDB с базой данных MSSQL, если UCMDB устанавливается удаленно. Если необходимо использовать проверку подлинности NTLM, следует устанавливать UCMDB локально.

Режим схемы

Configuration Manager требует настройки UCMDB в режиме консолидированной схемы и создания нового состояния UCMDB.

При обращении к уже установленному экземпляру UCMDB, если его схема еще не консолидирована, автоматическая консолидация крупных баз данных (более 5 млн. ЭК) может занять продолжительное время (от 20 до 60 минут).

Примечание: Oracle Real Application Cluster (RAC) и NTLM-соединения SQL Server в процессе установки не поддерживаются. Если данные соединения необходимы, следует сначала установить Configuration Manager с простым подключением к базе данных, а затем, по окончании установки, изменить соответствующие настройки продуктов. Для этого необходимо внести соответствующие изменения в файл **database.properties**. Подробнее см. в разделе "Расширенная конфигурация базы данных (для Configuration Manager)" на стр. 32.

Режим конфигурации базы данных

Для Configuration Manager и UCMDB необходимо использовать разные схемы.

Configuration Manager позволяет настроить каждую из баз данных на сервере Oracle или MSSQL.

Типы конфигурации

Поддерживается как подключение к уже имеющейся схеме, так и создание новой. При подключении к имеющейся схеме ее содержимое будет перезаписано.

Конфигурация базы данных

Данный шаг выполняется Диспетчером развертывания автоматически. Сведения о выполнении данного шага вручную см. в разделе "Настройка базы данных или пользовательской схемы" на стр. 18.

Расширенная конфигурация базы данных (для Configuration Manager)

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 баз данных Oracle и Microsoft SQL Server. Поддерживаются все функции встроенных драйверов, которые можно настроить в URL-адресе базы данных. URL-адрес находится в файле **database.properties**.

По окончании работы Диспетчера развертывания можно выполнить дополнительную настройку баз данных и схем.

Поля настройки базы данных

Поддерживаются два типа баз данных – Oracle и MSSQL. Состав полей для ввода данных зависит от выбранного типа базы.

10 Укажите порты для подключения Configuration Manager на странице настройки портов. По окончании настройки нажмите **Далее** для перехода на страницу настройки пользователей.

Configuration Manager содержит значения портов по умолчанию, которые отображаются на странице настройки портов.

Если конфигурация установленной системы не позволяет использовать какой-либо из настроенных по умолчанию портов, перед изменением его номера обратитесь к менеджеру по IT.

Поле	Определение
Порт HTTP приложения:	8180
Порт JMX HTTP	39900
Порт Tomcat	8005
Порт AJP	8009 (Apache Java Protocol)
Порт HTTPS приложения	8143
Удаленный порт JMX	39600

Нажмите кнопку **Вернуть значения по умолчанию**, чтобы установить стандартные значения номеров портов.

11 Создайте на странице настройки следующих пользователей:

- пользователя для первого входа в UCMDB-CM с правами администратора.
- пользователя интеграции в UCMDB - пользователь интеграции в UCMDB создается по требованию Configuration Manager для обеспечения интеграции между продуктами.

По окончании настройки нажмите **Далее** для перехода на страницу настройки безопасности.

12 Активируйте Global LW-SSO в новом экземпляре UCMDB и Configuration Manager на странице настройки безопасности. LW-SSO настраивается только во вновь созданных экземплярах Configuration Manager или UCMDB согласно параметрам, выбранным на странице выбора продуктов. Затем нажмите **Далее** для перехода на страницу сводки.

LW-SSO – это модульная платформа для проверки различных маркеров проверки подлинности и безопасности (напр., LW-SSO и SAML2). LW-SSO позволяет использовать информацию о проверке подлинности из различных сред в контексте систем безопасности приложений или платформ безопасности.

Конфигурация LW-SSO зависит от выбранных компонентов продуктов.

При подключении Configuration Manager к уже установленному экземпляру UCMDB или OO настройка LW-SSO выполняется только на Configuration Manager. При этом необходимо извлечь строку LW-SSO из UCMDB или OO, а затем вставить ее в поле Строка LW-SSO. Для одновременного подключения к UCMDB и OO необходимо, чтобы их строки LW-SSO совпадали.

При подключении нового экземпляра Configuration Manager к уже существующему экземпляру UCMDB в качестве имени хоста UCMDB необходимо использовать полное имя домена.

Извлечение строки LW-SSO из UCMDB:

a Откройте UCMDB и выберите в меню **Администрирование > Управление настройками инфраструктуры**.

b В столбце **Имя** найдите поле LW-SSO init string и дважды щелкните на нем кнопкой мыши.

c Скопируйте строку из поля "Текущее значение".

d Вставьте значение в поле "Строка LW-SSO" на странице настройки безопасности.

При подключении Configuration Manager к новому экземпляру UCMDB выполняется автоматическая настройка LW-SSO как в UCMDB, так и в Configuration Manager.

13 Проверьте параметры установки и настройки на странице сводки. Затем нажмите **Далее** для перехода на страницу проверки.

На странице сводки обобщаются все параметры настройки и введенные пользователем данные. При необходимости введенные данные можно изменить, нажимая кнопку "Назад" несколько раз для перехода на нужную страницу. Затем вернитесь на страницу сводки, нажимая **Далее**.

14 На данном этапе Диспетчер развертывания выполняет ряд действий для проверки наличия достаточных ресурсов на удаленной машине, правильности введенных пользователем данных, а также правильности параметров подключения к базе данных. В процессе проверки контролируется соответствие выполненных пользователем настроек известным ограничениям среды. Процесс проверки начинается автоматически. Однако если возникла необходимость вернуться на одну из страниц Диспетчера развертывания и изменить конфигурацию, затем следует нажать **Выполнить проверку** для запуска процесса проверки. Затем нажмите **Далее** для перехода на страницу развертывания.

15 На странице "Развертывание" отражается ход процесса развертывания системы. Процесс развертывания включает установку продуктов, их запуск, интеграцию и подключение к другим продуктам.

Развертывание завершается после успешного запуска всех продуктов.

Нажмите **Сведения** для просмотра хода развертывания, включая шаги, выполненные Диспетчером развертывания для каждого из выбранных продуктов.

Нажмите **Отмена**, чтобы прервать процесс развертывания после завершения текущей задачи.

Нажмите **Прервать** (доступно только после нажатия **Отмена**) для принудительной остановки текущей задачи и процесса развертывания. В результате принудительной остановки развертывания продукты могут оказаться в неопределенном состоянии.

Проверки

В таблице ниже представлен список проверок, выполняемых Диспетчером развертывания.

Проверка	Сообщение об ошибке	Описание
Проверка учетных данных	Credentials verification failed	Указаны неверные учетные данные.
		Подключение не установлено.
Проверка совместимости операционной системы	Target operating system platform is <Platform> Product <Product Name> supports the following platforms <Platform>	Целевая операционная система не входит в список сертифицированных для работы продукта.
Проверка памяти	The assigned memory (<Memory> MB) exceeds the available memory (<Memory> MB) on <Target>	На целевой машине недостаточно памяти для всех установленных продуктов.
	<Memory> MB of memory are verified to be available on <Target Machine>	Проверка пройдена успешно.
Проверка пространства на диске	assigned disk space for (<Memory> MB) exceeds available disk space (<Memory> MB) on drive <Target>	На целевой машине недостаточно дискового пространства для всех установленных продуктов.
	<Memory> MB of disk space are verified to be available on drive <Target>	Проверка пройдена успешно.
Проверка ввода всех необходимых свойств	Missing the target storage device for the product: <Target>	Не указана директория для установки продукта.

Проверка	Сообщение об ошибке	Описание
Проверка назначения машины для развертывания	No deployment machine is defined for <Product Name>	Не указаны сведения о машине, на которой необходимо развернуть продукт.
Проверка учетных данных	Credentials verification failed	Неверные данные для входа в систему.
Проверка отключения UAC	The UAC is enabled	На целевой машине включена функция UAC.
Проверка свободных портов	The required port number <Port> is already in use on <Target>	Необходимый порт на целевой машине уже занят.
Проверка наличия целевого устройства хранения данных	The target storage device <Device> does not exist on <Target>	На целевой машине отсутствует выбранное устройство хранения данных.
Проверка наличия схемы	Schema <Name> does not exist/ already exist	На целевой машине найдена/не найдена необходимая схема.
Проверка прав доступа к схеме	Validate <Permissions> schema tables user permissions existence	У пользователя базы данных недостаточно прав доступа
Проверка существования таблиц в схеме	Schema Tables <Tables> on the database: <Tables> already exist	В базе данных уже существуют таблицы схемы.
Проверка прав доступа пользователя к таблицам схемы	The database user does not have the correct permissions	У пользователя базы данных недостаточно прав доступа.

Проверка	Сообщение об ошибке	Описание
Проверка соединения с UCMDB	Connection failed. Connection to UCMDB failed, host: <Host>, username: <User name>, port: <Port>, protocol: <Protocol> due to <Error>	Проверка подключения к UCMDB с указанными настройками завершилась неудачно.
	Требуется UCMDB версии 9.03 с CUP 2 или более поздней.	Требуется UCMDB версии 9.03 с CUP 2 или более поздней.
Проверка соединения с базой данных	The host name/IP address validation failed	Не удалось подключиться у указанному хосту или IP-адресу базы данных
	The username or password validation failed	Введены неверные учетные данные пользователя.
	The port validation failed	Не удалось подключиться к указанному порту базы данных.
	The SID validation failed	Указано неверное значение SID.
Проверка установки	The product is already installed	На целевом хосте уже установлен данный продукт

Обновление Configuration Manager

Перед началом обновления автоматически выполняются следующие проверки:

- наличие подключения к серверу UCMDB.
- наличие в UCMDB пакета исправлений CUP 2.
- наличие верно указанного порта JMX.

В случае, если какая-либо из проверок не пройдена, выводится соответствующее сообщение об ошибке. Перед выполнением обновления необходимо устранить обнаруженные ошибки.

- В случае сбоя обновления из-за отсутствия соединения с UCMDB проверьте работоспособность сервера UCMDB.
- В случае сбоя обновления из-за отсутствия CUP 2 установите данный пакет исправлений согласно инструкциям, опубликованным на следующей странице: http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_UCMDB_00045
- В случае сбоя обновления из-за неверного номера порта UCMDB JMX уточните номер порта. Номер порта указывается в свойстве ucmdb.jmx.port файла **upgrade.properties**, расположенного в папке **<директория установки Configuration Manager>\utilities\Upgrade**.

Процедура обновления состоит из следующих шагов:

Примечание: Перед началом обновления проверьте работоспособность сервера UCMDB.

---

1. Создайте резервные копии схем Configuration Manager и UCMDB.
2. Найдите файл **setup-win64.msi** в папке Windows на установочном диске Configuration Manager.
3. Двойным щелчком на файле запустите Мастер установки Configuration Manager.

4. Нажмите **Далее**, чтобы открыть страницу Лицензионного соглашения с конечным пользователем.
5. Примите условия лицензии и нажмите **Далее**, чтобы открыть страницу информации о клиенте.
6. Введите сведения о себе и нажмите **Далее** для перехода на страницу выбора типа установки.
7. Выберите папку, куда следует установить Configuration Manager. Новую версию не следует устанавливать в ту же папку, что и предыдущую.

   По умолчанию Configuration Manager устанавливается в следующую директорию: **c:\hp\cnc920**. Нажмите **Далее**, чтобы оставить папку по умолчанию, либо нажмите **Обзор**, выберите другую папку и нажмите **Далее**.

   Примечание: Имя директории установки не должно содержать пробелов.

   ---

8. Нажмите **Далее** для подтверждения и начала установки.

   По окончании установки автоматически запускается Мастер послеустановочной настройки Configuration Manager.
9. Нажимайте **Далее**, пока система не предложит выполнить новую установку Configuration Manager или его обновление.
10. Выберите **Обновление** и нажмите **Далее**.
11. По окончании установки откройте файл журнала **post_installation.log** (в папке **<директория установки Configuration Manager/tmp/log**) и убедитесь, что установка прошла без ошибок.

    В случае ошибки в ходе обновления выводится соответствующее сообщение с возможностью закрыть мастер. В этом случае обратитесь в службу поддержки HP.
12. Запустите службу Configuration Manager.

Примечание: После обновления необходимо повторно выполнить настройку SSL. Дополнительные сведения см. в разделе "Повышение безопасности" на стр. 89.

3

Установка HP Universal CMDB Configuration Manager на платформе Linux

Важно: Актуальные инструкции по установке см. в сведениях о версии.

Данная глава содержит следующую информацию:

Подготовка к установке

Данный раздел также включает:

➤ "Необходимые условия" на стр. 43

➤ "Получение файла setup.bin" на стр. 44

Необходимые условия

➤ Не менее 400 Мб свободного пространства на диске

➤ Рекомендуется работающий X display

Получение файла setup.bin

Файл установки Linux (**setup.bin**) можно найти на установочном носителе или в образе ISO, доступном на вебсайте HP. Открыть файл можно несколькими способами:

➤ Смонтируйте DVD на машине с Linux:

```
$ mkdir -p /mnt/cdrom
$ mount /dev/cdrom /mnt/cdrom
```

➤ Подключите ISO-образ как блочное loopback-устройство

```
$ mkdir -p /mnt/cdrom
$ mount -o loop cnc-<version>.iso /mnt/cdrom
```

➤ Скопируйте файл **setup.bin** во временную директорию на машине с Linux.

Установка Configuration Manager

В данной задаче описывается процедура установки Configuration Manager на сервере, настройки соединения с базой данных и интеграции с UCMDB.

Если работает X display, мастер послеустановочной настройки открывается в интерфейсе пользователя. В противном случае мастер открывается в режиме консоли.

Примечание: Описанные в данном руководстве шаги относятся к режиму консоли, однако шаги для графического режима аналогичны.

Порядок установки Configuration Manager:

1 Для установки Configuration Manager в текущую директорию введите следующую команду:

```
chmod 755 setup.bin
$ /path/to/installation/kit/setup.bin
```

2 Откроется лицензионное соглашение с конечным пользователем (EULA). Примите его условия. Прокрутите экран или несколько раз нажмите пробел, пока не будет достигнут конец соглашения. Чтобы принять условия соглашения и продолжить установку, введите **yes** и нажмите **Enter**.

HP Universal CMDB Configuration Manager будет установлен в поддиректорию **cnc** внутри текущей директории.

Страница приветствия

```
<============================>
Добро пожаловать
<============================>
Welcome to the HP Universal CMDB Configuration Manager
post installation wizard.
Введите [<C>ancel] [Ne<x>t]>
```

Нажмите **Enter** для перехода на следующую страницу.

Выбор поставщика базы данных

```
<============================>
Настройка подключения к базе данных
<============================>
-------
Поставщик:
-------
  ->1 - Oracle
    2 - Microsoft
Введите номер (1 или 2) либо [<C>ancel] [Back<b>] [Ne<x>t]>
```

Нажмите **Enter**, чтобы выбрать Oracle, либо введите **2** и нажмите **Enter**, чтобы выбрать Microsoft.

Имя хоста базы данных

```
-------------
Ввод имени хоста:
-------------
        Hostname: = "localhost"
Введите новое имя хоста: либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Введите имя хоста базы данных и нажмите **Enter**. По умолчанию используется имя хоста **localhost**.

Порт базы данных

```
---------
Ввод номера порта:
---------
        Port: = "1521"
Введите новый номер порта: либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Порт по умолчанию для Oracle – 1521, а для Microsoft – 1433. Если необходимо использовать другой номер порта, введите его и нажмите **Enter**.

Имя SID/DB

```
-----------
Ввод SID/DB:
-----------
        SID/DB = "orcl"
Введите новое значение SID/DB: либо [<C>ancel] [<B>ack]
[Ne<x>t]>
```

Для Oracle в этом поле указывается SID базы данных, а для Microsoft – имя базы данных. Введите допустимое значение и нажмите **Enter**.

Имя пользователя/схемы и пароль

```
-------------
Ввод имени пользователя:
-------------
Введите имя пользователя: либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Введите имя пользователя базы данных и нажмите **Enter**.

```
Введите пароль: либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Введите пароль базы данных и нажмите **Enter**.

Проверка подключения к базе данных

```
--------
Включение тестового режима
--------
        Test = "Yes"
Выберите [<Y>es]/[<N>o] для включения режима тестирования, либо
[<C>ancel] [<B>ack] [Ne<x>t]>
```

Нажмите **Enter** для проверки подключения к базе данных.

Поскольку мастер пытается создать в схеме базы данных таблицы, настоятельно рекомендуется проверить подключение к базе данных. Чтобы не проверять подключение, введите **No** и нажмите **Enter**.

В случае успешной проверки соединения с базой данных выводится следующее сообщение:

```
success
Введите [<C>ancel] [<B>ack] [Ne<x>t]>
```

Нажмите **Enter** для продолжения. В случае ошибки при проверке соединения выводится соответствующее сообщение с предложением повторить проверку. Исправьте ошибку, повторите проверку и переходите к следующему шагу установки.

Имя хоста сервера приложений

```
<============================>
Настройка сервера приложений
<============================>
Hostname:
----
Set
----
         = "myucmdbcmhost.mydomain"
Введите имя хоста либо [<C>ancel] [Back<b>] [Ne<x>t]>
```

По умолчанию в качестве имени хоста используется фактическое имя хоста машины. В случае установки за балансировщиком нагрузки или обратным прокси-сервером укажите внешнее имя хоста.

Настройка портов сервера приложений

```
------------------
Выберите пункт Настройка портов
------------------
        Customize ports = "No"
Выберите [<Y>es]/[<N>o] для настройки портов либо [<C>ancel]
[<B>ack] [Ne<x>t]>
```

Чтобы использовать для Configuration Manager порты по умолчанию, нажмите **Enter**. Чтобы изменить номера портов, введите **Yes**, а затем нажмите **Enter**. Номера портов по умолчанию:

Имя порта	Номер порта
HTTP	8180
HTTPS	8443
Управление Tomcat	8005
AJP	8009
JMX HTTP	39900
JMX RMI	39600

При настройке портов необходимо ввести номер для каждого из перечисленных выше портов. Введите новое значение для следующих портов и нажмите **Enter**.

```
порт HTTP:
----
Set
----
         = "8180"
Введите новое значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
порт HTTPS:
----
Set
----
         = "8443"
Введите новое значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
Порт Tomcat:
----
Set
----
         = "8005"
Введите новое значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
Порт AJP:
----
Set
----
         = "8009"
Введите новое значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
Порт JMX HTTP:
----
Set
----
         = "39900"
Введите новое значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
Удаленный порт JMX:
----
Set
----
         = "39600"
Введите новое значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Начальный пользователь-администратор

```
<============================>
Реквизиты пользователя
<============================>
Начальный пользователь-администратор
Имя пользователя-администратора:
----
Set
----
Введите новое значение либо [<C>ancel] [Back<b>] [Ne<x>t]>
```

Создается учетная запись пользователя с правами администратора или суперпользователя, которая будет использоваться для первого входа в систему. Введите имя пользователя-администратора, а затем нажмите **Enter**.

```
Пароль администратора:
Введите значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Введите пароль администратора и нажмите **Enter**.

```
Подтвердить пароль:
Введите значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Для подтверждения введите пароль администратора еще раз и нажмите **Enter**.

Пользователь интеграции

```
Пользователь интеграции платформ
Имя пользователя интеграции:
----
Set
----
Введите значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Выберите имя пользователя интеграции с UCMDB. При этом в UCMDB создается соответствующая учетная запись. HP рекомендует использовать имя пользователя, из которого понятно, что оно предназначено для интеграции (например, cm_integration). Введите выбранное имя пользователя и нажмите **Enter**.

```
Пароль интеграции:
Введите значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Введите пароль пользователя интеграции и нажмите **Enter**.

```
Подтвердить пароль:
Введите значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Введите пароль пользователя интеграции еще раз и нажмите **Enter**.

Имя хоста сервера HP Universal CMDB

```
<============================>
Настройка подключения к HP UCMDB
<============================>
Hostname:
----
Set
----
         = "localhost"
Введите имя хоста либо [<C>ancel] [Back<b>] [Ne<x>t]>
```

Введите имя хоста сервера UCMDB и нажмите **Enter**. Значение, вероятно, будет отличаться от предложенного по умолчанию localhost, поскольку в рабочей среде не рекомендуется устанавливать UCMDB и Configuration Manager на одну и ту же машину.

Порт сервера HP Universal CMDB

```
Port:
----
Set
----
         = "8080"
Введите новое значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Нажмите **Enter**, чтобы принять значение по умолчанию 8080 для сервера UCMDB, либо введите номер порта и нажмите **Enter**.

Протокол сервера HP Universal CMDB

```
Протокол:
  ->1 - HTTP
    2 - HTTPS
Введите номер (1 или 2) либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Нажмите **Enter**, чтобы использовать HTTP, либо введите 2 и нажмите **Enter**, чтобы использовать HTTPS.

Примечание: Если выбран HTTPS, необходимо будет обменяться с UCMDB ключами. Дополнительные сведения см. в разделе "Повышение безопасности" на стр. 89. Ниже описана процедура настройки HTTPS с незащищенным самоподписанным сертификатом.

Клиент сервера HP Universal CMDB

```
Клиент:
----
Set
----
         = "Default Client"
Введите новое значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Нажмите **Enter**, чтобы принять имя клиента по умолчанию для сервера UCMDB, либо введите имя клиента и нажмите **Enter**.

Учетные данные системного администратора HP Universal CMDB

```
Имя пользователя-администратора:
----
Set
----
Введите значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Введите имя пользователя-администратора сервера UCMDB. Данный пользователь имеет право выполнять методы JMX на сервере UCMDB. Данная учетная запись уже существует – она не создается во время установки. Учетные данные пользователя sysadmin можно получить у администратора сервера UCMDB.

```
Пароль пользователя-администратора:
Введите значение либо [<C>ancel] [<B>ack] [Ne<x>t]>
```

Введите пароль пользователя sysadmin UCMDB и нажмите **Enter**.

Проверка подключения к серверу HP Universal CMDB

```
--------
Включение тестового режима
--------
        Test = "Yes"
Выберите [<Y>es]/[<N>o] для включения режима тестирования, либо
[<C>ancel] [<B>ack] [Ne<x>t]>
```

Нажмите **Enter** для проверки подключения к серверу UCMDB. Поскольку мастер пытается развернуть пакеты и настроить сервер UCMDB, настоятельно рекомендуется проверить подключение к серверу. Чтобы не проверять подключение, введите **No** и нажмите **Enter**.

В случае успешной проверки соединения с сервером выводится следующее сообщение:

```
success
Введите [<C>ancel] [<B>ack] [Ne<x>t]>
```

Нажмите **Enter** для продолжения. В случае ошибки при проверке соединения выводится соответствующее сообщение с предложением повторить проверку. Исправьте ошибку, повторите проверку и переходите к следующему шагу установки.

Сводка

Перед применением настроек мастер выводит сводку всех выбранных параметров:

```
<============================>
Обзор действий после установки.
<============================>
Обзор действий после установки
Пользователи
-----
Имя пользователя-администратора HP Universal CMDB Configuration
Management: admin
Имя пользователя интеграции платформ HP Universal CMDB:
cm_integration

База данных
--------
Поставщик: Oracle
Хост: mydbhost.mydomain
Порт: 1521
SID/DB: orcl
Шифровать пароль? Да
Создать объекты схемы? Да

Сервер приложений
------------------
имя хоста: myucmdbcmhost.mydomain
HTTP: 8180
HTTPS: 8443
Tomcat management: 8005
AJP: 8009
JMX HTTP: 39900
JMX remote: 39600
Отладка: 7878

Служба Windows
---------------
Служба Service Desk: Нет

Платформа HP Universal CMDB
-----
URL: http://myucmdb.mydomain:8080
Имя пользователя sysadmin: sysadmin
Клиент: Default Client

Введите [<C>ancel] [Back<b>] [Ne<x>t]>
```

Нажмите **Enter** для продолжения настройки. В процессе настройки отображается график хода выполнения. Мастер выполняет следующие задачи:

1. Создает таблицы и объекты в базе данных.
2. Заполняет базу данных значениями по умолчанию и начальными значениями.
3. Создает начального пользователя-администратора.
4. Создает пользователя интеграции на сервере UCMDB.
5. Консолидирует сервер UCMDB.
6. Создает авторизованное состояние на сервере UCMDB.
7. Разворачивает на сервере UCMDB пакеты Configuration Manager.

По окончании настройки выводится следующее сообщение:

```
<============================>
Завершение
<============================>
Мастер послеустановочной настройки завершил работу.
Введите [Finish<f>]>
```

Нажмите **Enter** для выхода из мастера.

Фоновый режим установки

Configuration Manager может устанавливаться в фоновом режиме. В этом режиме выполняется только извлечение файлов из пакета установки, без послеустановочной настройки. Для установки в фоновом режиме выполните следующую команду:

```
$ /path/to/installation/kit/setup.bin -silent
```

Запуск сервера приложений Configuration Manager

Для запуска Configuration Manager выполните следующую команду:

```
$ cd /path/to/installation/location
$ ./start-server-0.sh
```

Создав сценарий в директории **/etc/init.d**, можно автоматически запускать Configuration Managerпосле загрузки системы.

4

Вход в Configuration Manager

Данная глава содержит следующую информацию:

Доступ в Configuration Manager

Доступ в Configuration Manager осуществляется с помощью веб-браузера 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-браузеру, а также минимальных требованиях для просмотра Configuration Manager см. в разделе "Матрица поддержки" на стр. 14.

Подробнее о безопасном подключении к Configuration Manager см. в разделе "Повышение безопасности" на стр. 89.

Сведения об устранении проблем с доступом к Configuration Manager см. в разделе "Устранение неполадок" на стр. 123.

Вход в приложение Configuration Manager

1. Откройте веб-браузер и введите URL-адрес сервера Configuration Manager, например, http://<имя или IP-адрес сервера>.<имя домена>:<порт>/cnc**,** где **<имя или IP-адрес сервера>.<имя домена>** соответствует полному доменному имени (FQDN) сервера Configuration Manager, а **<порт>** – номеру порта, заданному при установке.
2. Введите имя пользователя и пароль, заданные в послеустановочном Мастере Configuration Manager.
3. Нажмите **Войти**. После выполнения входа имя пользователя будет отображаться в правом верхнем углу экрана.
4. (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** в верхней части 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>:<port>/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.

5

Дополнительные примеры использования

Данная глава содержит следующую информацию:

Перенос установленного Configuration Manager между компьютерами

Эту процедуру следует использовать в случаях, когда необходимо перенести установленный экземпляр Configuration Manager с одной машины на другую без изменения схемы базы данных и с подключением к тому же серверу UCMDB.

1. Перейдите в директорию **<директория установки Configuration Manager>\cnc\bin** и выполните следующую команду: edit-server-0.bat.
2. Запишите все обнаруженные параметры, включая номера портов (напр., порт JMX).
3. Остановите сервер Configuration Manager на исходной машине. (Если на исходной машине установлена Windows, остановите службу Configuration Manager).

4 Установите Configuration Manager на целевую машину:

- ➤ На Windows: запустите файл **setup-win64.msi** (он находится в папке **\windows** на установочном носителе).
- ➤ На Linux: следуйте инструкциям раздела "Установка Configuration Manager" на стр. 44.

5 Отмените работу открывшегося Мастера послеустановочной настройки.

6 Скопируйте все файлы из директории предыдущей установки на исходной машине в место новой установки на целевой машине.

7 На целевой машине измените имя хоста на имя целевой машины в файлах **client-config.properties** и **resources.properties** (в папке **\conf**).

Примечание. Если домен целевой машины отличается от домена исходной, измените также ссылки на домен в файле **lwssofmconf.xml**.

---

8 На целевой машине запустите файл **bin/create-windows-service.bat**, чтобы создать службу Windows. Установите флаг **-h** для просмотра доступных параметров и при необходимости используйте параметры службы с исходной машины (записанные в шаге 2). В качестве параметра имени домена используйте server-0. Со значениями по умолчанию команда будет иметь следующий вид:

c:\HP\cnc920\bin>create-windows-service.bat -j 39900 -n server-0 -r 39600

9 Запустите сервер Configuration Manager на целевой машине.

Изменение номеров портов после установки

1. Остановите сервер Configuration Manager.
2. Создайте резервную копию папки **<директория установки Configuration Manager>\servers\server-0**.
3. Удалите папку **<директория установки Configuration Manager>\servers\server-0**.
4. Запустите сценарий **create-node.bat** с флагом **-h** для просмотра доступных параметров. Передайте служебной программе необходимые номера портов.
5. На целевой машине измените номер порта на новый номер порта HTTP в файлах **client-config.properties** и **resources.properties** (в папке **\conf**).
6. Запустите сценарий **edit-server-0.bat**, который находится в папке **<директория установки Configuration Manager>\bin**.
7. (для систем Windows) В открывшемся окне свойств HP Universal CMDB Configuration Manager нажмите на закладку Java и укажите новые номера портов в настройках **jmx.http.port** и **com.sun.management.jmxremote.port**.
8. Запустите службу Configuration Manager на целевой машине.

Копирование настроек между системами

1. Откройте Configuration Manager на исходной машине. Откройте пункт меню **Система > Настройки** и нажмите кнопку **Экспорт набора конфигурации в ZIP-файл**.

   Перед экспортом можно исключить определенные части конфигурации, сняв флажки напротив соответствующих элементов конфигурации.
2. Копирование экспортированной конфигурации на целевую машину.
3. Откройте Configuration Manager на целевой машине. Откройте пункт меню **Система > Настройки** и нажмите кнопку **Импорт набора конфигурации**.

Резервное копирование и восстановление

Создание резервной копии установленного экземпляра Configuration Manager позволяет восстановить систему после любых сбоев, для чего в противном случае потребовалась бы полная переустановка системы.

Резервное копирование

Создайте резервную копию следующей информации:

- папок **conf** и **security** в директории установки Configuration Manager. Копирование папок может выполняться без остановки работы системы.
- схемы базы данных

Восстановление (система Windows)

Данную процедуру необходимо выполнять на новой системе, в которой не установлен Configuration Manager.

1. Установите Configuration Manager на целевой машине, запустив файл **setup-win64.msi** (в папке **\windows** на установочном носителе) в фоновом режиме:

   msiexec /i setup-win64.msi TARGETDIR=path\to\install\dir /passive

2. Восстановление директорий **conf** и **security**. Процедура восстановления аналогична процедуре создания резервной копии. Перезапишите директории, созданные в процессе установки (шаг 1).
3. Восстановление схемы базы данных. В случае восстановления на другой сервер баз данных необходимо указать имя нового сервера баз данных в свойстве **url** в файле **database.properties** (он находится в папке **conf**).
4. Создайте службу Windows при помощи служебной программы **create-windows-service** с флагом **-h**.
5. Запустите сервер Configuration Manager.

Восстановление (система Linux)

1. Установите Configuration Manager на целевой машине, запустив файл **setup.bin** с установочного носителя. Подробнее см. в разделе "Установка Configuration Manager" на стр. 44, однако обратите внимание, что процесс установки необходимо прервать на первом шаге мастера послеустановочной настройки. Все файлы будут установлены, однако настройка системы не будет произведена.
2. Восстановление директорий **conf** и **security**. Процедура восстановления аналогична процедуре создания резервной копии. Перезапишите директории, созданные в процессе установки (шаг 1).
3. Восстановление схемы базы данных. В случае восстановления на другой сервер баз данных необходимо указать имя нового сервера баз данных в свойстве **url** в файле **database.properties** (он находится в папке **conf**).
4. Запустите сервер Configuration Manager.

6

Расширенная настройка

Данная глава включает:

Расширенные параметры 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**.

Примечание: Установка расширенных параметров соединения в системе Linux:

- В командах следует использовать наклонные черты (/).
- Расширение сценариев необходимо изменить с **.bat** на **.sh**.

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. HP Universal CMDB 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, **а** и . 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.

Единый вход в систему (SSO)

Единый вход в Configuration Manager и UCMDB осуществляется с использованием технологии HP LWSSO. Дополнительные сведения см. в разделе "Проверка подлинности Lightweight Single Sign-On (LW-SSO) – общие сведения" на стр. 119.

Этот раздел включает следующие темы:

Включение LW-SSO между Configuration Manager и UCMDB

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 > UCMDB Foundation**). 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. Данную задачу необходимо выполнить вручную, если только она не выполнена в процессе установки Диспетчера развертывания.

Включение LW-SSO:

1. В директории установки Configuration Manager измените файл **\conf\lwssofmconf.xml**.
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-->

Примечание: Второе значение DNSDomain необходимо указать только в случае, если Configuration Manager и другое приложение находятся в разных доменах.

Удалите символ комментария в начале и введите все домены сервера (при необходимости) в элементы DNSDomain (вместо This value should be replaced by your application domain или This value should be replaced by domain of other application). Список должен включать домен сервера, введенный в шаге 3 на стр. 74.

6 Сохраните измененный файл и перезапустите сервер.

7 Запустите веб-браузер 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. 75, 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**.

Настройка LW-SSO в Operations Orchestration

При включении LW-SSO в Configuration Manager и Operations Orchestration (OO) пользователям, вошедшим в систему Configuration Manager разрешен вход в Operations Orchestration через веб-уровень без ввода имени пользователя и пароля (для системных администраторов).

Примечание:

- В описанных ниже процедурах <OO_HOME> обозначает домашнюю директорию Operations Orchestration.
- Для работы LW-SSO необходимо совпадение имен учетных записей в Operations Orchestration и Configuration Manager (пароли при этом могут быть разными).
- Кроме того, LW-SSO не может использоваться с внутренними учетными записями Operations Orchestration.

Настройка LW-SSO в Operations Orchestration:

1 Остановите службу RSCentral.

2 В **<OO_HOME>\Central\WEB-INF\applicationContext.xml** включите импорт между LWSSO_SECTION_BEGIN и LWSSO_SECTION_END, как показано ниже:

```
<!--  LWSSO_SECTION_BEGIN-->
        <import resource="CentralLWSSOBeans.xml"/>
<!--  LWSSO_SECTION_END -->
```

3 В **<OO_HOME>\Central\WEB-INF\web.xml** включите все фильтры и сопоставления между LWSSO_SECTION_BEGIN и LWSSO_SECTION_END, как показано ниже:

```
<!-- LWSSO_SECTION_BEGIN  -->

<filter>
        <filter-name>LWSSO</filter-name>
        <filter-
    class>com.iconclude.dharma.commons.util.http.DharmaFilterToBeanProx
    y
        </filter-class>
        <init-param>
            <param-name>targetBean</param-name>
            <param-value>dharma.LWSSOFilter</param-value>
        </init-param>
   ......
   </filter>
<!-- LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
   <filter-mapping>
      <filter-name>LWSSO</filter-name><url-pattern>/*</url-pattern>
   </filter-mapping>
<!--LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
    <filter-mapping>
         <filter-name>LWSSO2Acegi</filter-name><url-pattern>/*</url-pattern>
    </filter-mapping>
    <filter-mapping>
         <filter-name>dharmaLWSSOGroupsFilter</filter-name><url-
    pattern>/*</url-pattern>
         </filter-mapping>
<!--LWSSO_SECTION_END -->
```

4 В **<OO_HOME>\Central\conf\lwssofmconf.xml** измените следующие два параметра:

- domain: Доменное имя сервера OO.
- initString: Значение должно совпадать со значением initString в конфигурации LW-SSO OO (минимальная длина: 12 символов). Например, smintegrationlwsso.

Пример:

```
<webui>
<validation>
      <in-ui-lwsso>
       <lwssoValidation  id="ID000001">
            <domain>asia.hpqc.net</domain>
            <crypto cipherType="symmetricBlockCipher"
                                    engineName="AES" paddingModeName="CBC"
keySize="256"  encodingMode="Base64Url"
                                    initString=" smintlwsso "></crypto>
       </lwssoValidation>
      </in-ui-lwsso>
</validation>
<creation>
       <lwssoCreationRef id="ID000002">
            <lwssoValidationRef refid="ID000001"/>
            <expirationPeriod>600000</expirationPeriod>
       </lwssoCreationRef>
</creation>
</webui>
```

5 Чтобы конфигурация вступила в силу, перезапустите службу RSCentral.

Проверка подлинности через Диспетчер удостоверений

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

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

Данная задача включает в себя следующие действия:

➤ "Необходимые условия" на стр. 80

➤ "Настройка HP Universal CMDB Configuration Manager для работы с Диспетчером удостоверений" на стр. 80

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 при настройке 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

---

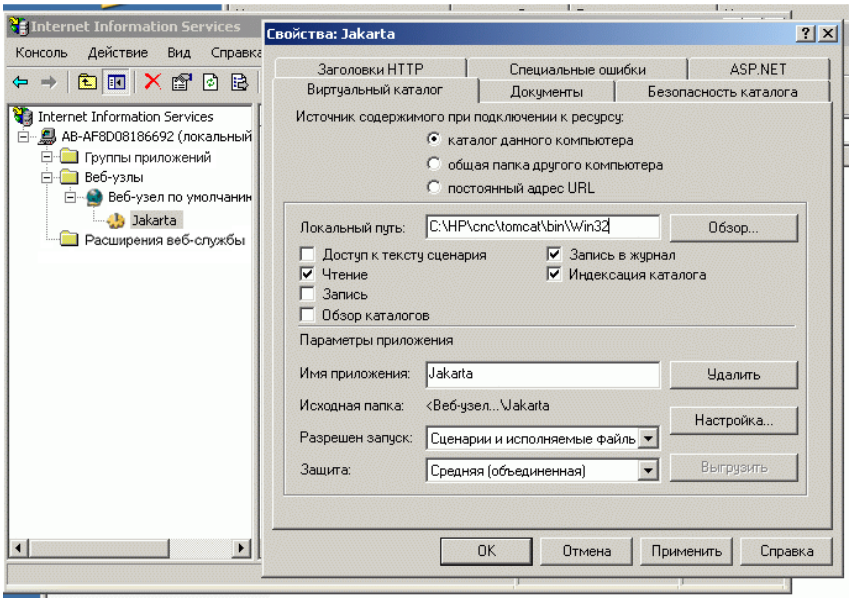
6 Создайте виртуальную директорию в соответствующем объекте вебсайта в настройках IIS.

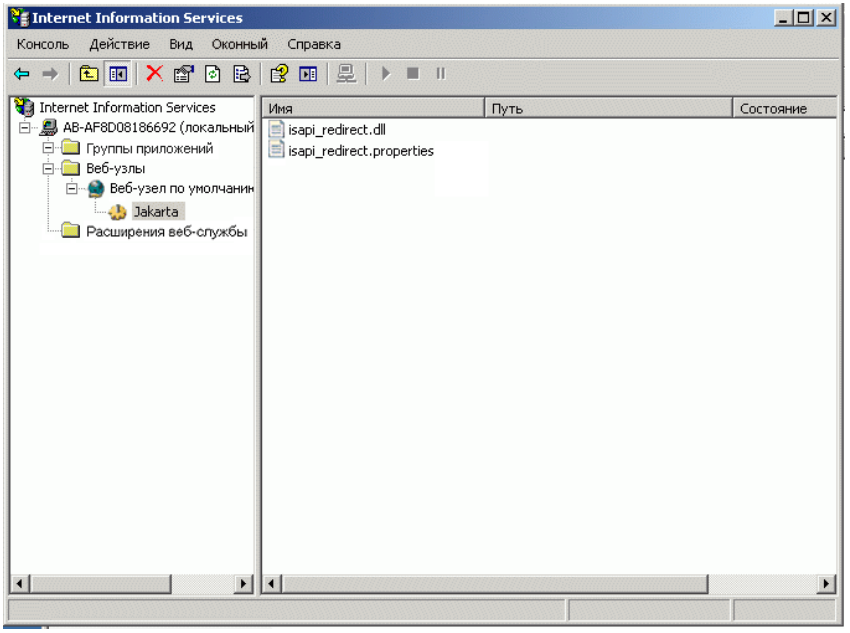
a Нажмите кнопку "Пуск" и откройте **Настройка > Панель управления >Администрирование >Менеджер Internet Information Services (IIS)**.

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:





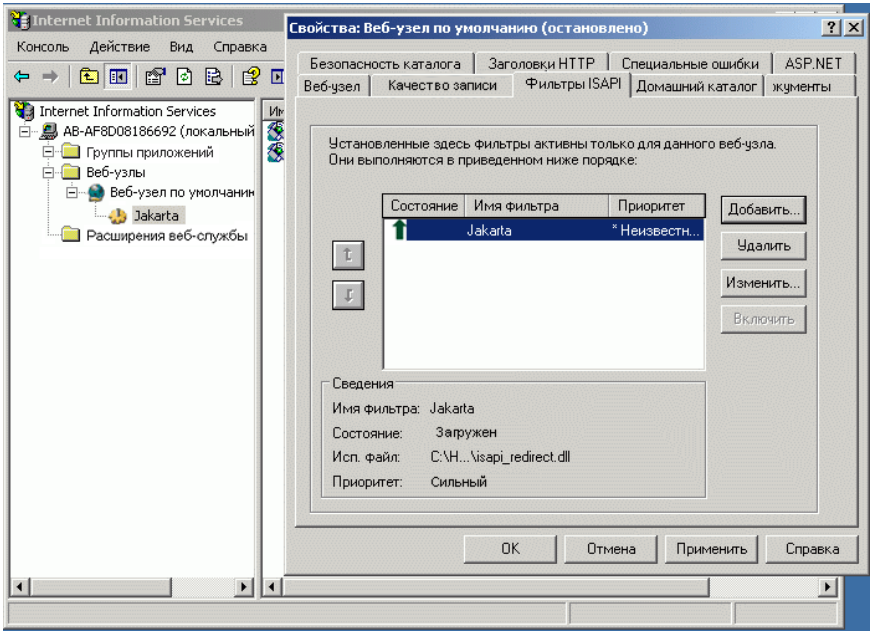
7 Добавьте **isapi_redirect.dll** как фильтр ISAPI.

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:



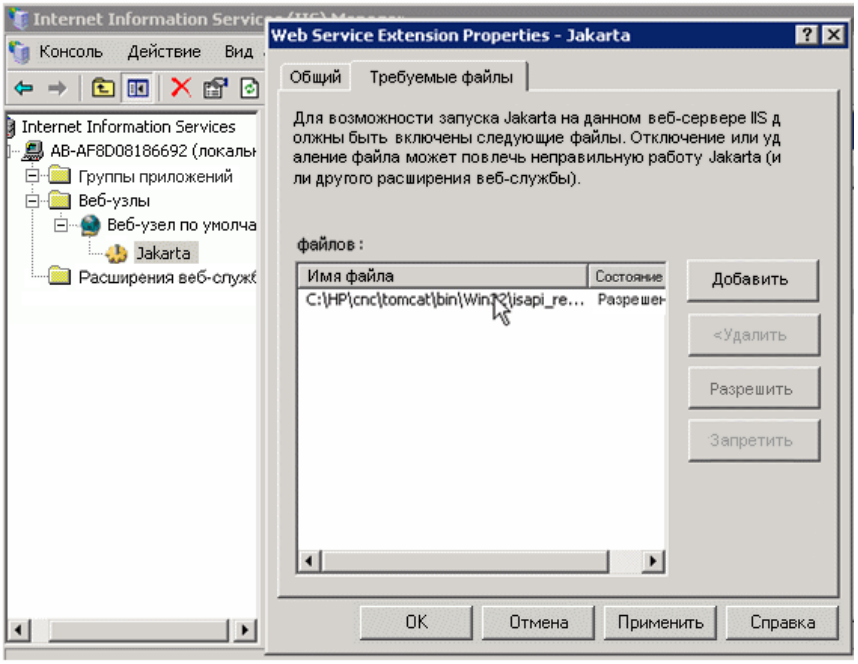
d Нажмите кнопку **Применить**.

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.

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 и IPv4. Подробнее см. в документации по операционной системе.
2. Откройте файл **client-config.properties** в папке **<директория установки Configuration Manager>/conf** и измените следующие значения:
   - Измените значение параметра **bsf.server.url** и убедитесь, что в нем используется имя хоста. Пример:

     bsf.server.url=http://mycomputer:8080/bsf

   - Измените значение параметра **bsf.server.services.url** и убедитесь, что в качестве URL-адреса Configuration Manager используется имя хоста. Пример:

     bsf.server.services.url=http://<имя хоста Configuration Manager>:<Порт Configuration Manager>/bsf

3. Откройте файл Tomcat **servers\server-0\conf\server.xml** и измените следующие значения:
   - Добавьте адрес IPv6 в ловушку SHUTDOWN, для чего допишите **address="[::]"** в следующий тег:

     <Server port="8005" shutdown="SHUTDOWN" **address="[::]"** >

   - Создайте копию коннектора HTTP. В качестве второго коннектора добавьте адрес IPv6 [::]. Пример:

```
<Connector port="8180" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
<Connector port="8180" protocol="HTTP/1.1" address="[::]"
           connectionTimeout="20000"
           redirectPort="8443" />
```

➤ Создайте копию коннектора AJP. В качестве второго коннектора добавьте адрес IPv6 [::]. Пример:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"  address="[::]" />

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

4 Добавьте на сервер переменную среды: useIPv6="true":

Откройте файл **edit_server-0.bat** в папке **<директория установки Configuration Manager>/bin**. На закладке Java добавьте в параметры следующее свойство: -DuseIPv6.

5 Перезапустите сервер.

LDAP

Настройку LDAP можно выполнить внутри Configuration Manager. Подробнее см. в разделе "Настройки системы" в *Руководстве пользователя HP Universal CMDB Configuration Manager*.

Повышение безопасности

Этот раздел включает следующие темы:

Примечание: После обновления необходимо повторно выполнить конфигурацию SSL. Дополнительные сведения см. в разделе "Обновление Configuration Manager" на стр. 39.

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 Configuration Manager 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.

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. 92.

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: **cnc920\security\encrypt_repository**, а также создайте ключ шифрования.

3 Запустите программу **bin\encrypt-password** и зашифруйте пароль. Флаг **-h** позволяет просмотреть доступные параметры.

4 Скопируйте зашифрованный пароль в файл **conf\database.properties**.

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. 91.

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.

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 7.0.

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** из папки **<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 Помещение сертификата в хранилище надежных сертификатов клиента

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

Подробнее об использовании клиентских сертификатов см. в разделе "Сертификаты клиента" на стр. 101.

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

---

4 Проверка настроек клиента

Откройте файл **client-config.properties**, расположенный в директории **conf** внутри директории установки Configuration Manager. Установите для протокола **bsf.server.url** значение **https**, а также установите номер порта **8443**.

5 Изменение файла server.xml

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

Connector port="8443"

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

keystoreFile="<tomcat.keystore file location>" (см. шаг 2 на стр. 94)
keystorePass="<пароль>"

Закомментируйте следующую строку:

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

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 Проверка настроек клиента

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

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="8443"

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

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

Закомментируйте следующую строку:

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

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.

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

Пример: java/{os name}/lib.

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**.
2. Скопируйте **hpcert.cer** в папку **<директория установки Configuration Manager>\java\bin** на сервере.
3. На сервере импортируйте сертификат ЦС 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 5 на стр. 95.
   b. Сразу после этих изменений добавьте следующие атрибуты в коннектор HTTPS:

      truststoreFile="../../java/lib/security/cacerts"
      truststorePass="изменить" />
   c. Set clientAuth="true".
5. Проверьте безопасность сервера, как описано в шаге 7 на стр. 96.

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.

1 Включите поддержку SSL на сервере, как описано в разделе "Включение SSL на сервере с самоподписанным сертификатом" на стр. 94 до шага 6 на стр. 96 или разделе "Включение SSL на сервере с сертификатом, подписанным центром сертификации" на стр. 96 до шага 5 на стр. 98.

2 Введите в веб-браузере следующий URL-адрес: http://<имя или IP-адрес сервера Configuration Manager>:8180/cnc.

Включение проверки подлинности с сертификатом клиента

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

1 Включите поддержку SSL на сервере, как описано в разделе "Включение SSL на сервере с самоподписанным сертификатом" на стр. 94.

2 Откройте следующий файл: **<Configuration Manager директория установки>\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: **<Configuration Manager директория установки>\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. 94.
- Измените **bsf.server.services.url** так, чтобы использовать HTTP, и введите изначальный номер порта HTTP.

Сертификаты клиента

Этот раздел включает следующие темы:

Информация в сертификате клиента

В данном разделе описывается информация, содержащаяся в сертификате клиента, а также процедура извлечения из сертификата идентификатора клиента.

➤ **Идентификатор пользователя**

Идентификатор пользователя – это уникальная часть информации из сертификата клиента, при помощи которой выполняется идентификация пользователя.

➤ **Базовая информация в сертификате клиента**

Базовая информация в сертификате клиента включает следующие сведения:

Поле сертификата	Описание
Version	Версия закодированного сертификата. Пример: 1 (0x1)
Serial Number	Положительное число, присвоенное сертификату органом сертификации. Пример: 0 (0x0)
Signature Algorithm	Идентификатор алгоритма, при помощи которого орган сертификации подписал сертификат. Пример: md5WithRSAEncryption
Issuer	Орган, выдавший и подписавший сертификат. Пример: CN=Issuer, C=US, ST=NY, L=New York, O=Work Organization, O=example.com

Поле сертификата	Описание
Validity	Период времени, в течение которого орган сертификации обязуется поддерживать информацию о состоянии сертификата: ➤ **Not Before**. Дата начала действия сертификата. Пример: Nov 25 04:34:49 2009 GMT ➤ **Not After**. Дата окончания действия сертификата. Пример: Nov 25 04:34:49 2010 GMT
Subject	Организация, связанная с открытым ключом, хранящимся в поле Subject Public Key.
Subject Public Key Info	Открытый ключ и сведения об алгоритме, с которым необходимо использовать данный ключ (например, RSA, DSA или Diffie-Hellman).

Подробнее см. в документе Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile:

http://tools.ietf.org/html/rfc5280

➤ **Поле Subject**

Поле Subject (также называемое различительным именем субъекта или SubjectDN) указывает на организацию, связанную с открытым ключом.

В поле Subject содержатся следующие существенные атрибуты (но могут содержаться и другие):

Атрибут субъекта	Описание атрибута субъекта	Пример
CN	Общее имя	CN=Bob BobFamily
emailAddress	Адрес электронной почты	*emailAddress=bob@example.com*
C	Страна	C=US

Атрибут субъекта	Описание атрибута субъекта	Пример
ST	Штат или провинция	ST=NY
L	Населенный пункт	L=New York
O	Организация	O=Work Organization
OU	Подразделение	OU=Managers

Для извлечения идентификатора пользователя можно использовать как поле SubjectDN целиком, так и атрибут SubjectDN.

➤ **Расширение информации в сертификате клиента**

Расширения, определенные для сертификатов X.509 v3, представляют собой методы связи дополнительных атрибутов с пользователями или открытыми ключами, а также управления отношениями между центрами сертификации. Идентификатор пользователя может содержаться в Поле Subject Alternative Name.

➤ **Поле Subject Alternative Name**

Расширение Subject Alternative Name позволяет привязать к субъекту сертификата идентификаторы. Эти идентификаторы могут дополнять или заменять собой идентификатор в поле субъекта сертификата.

В поле Subject Alternative Name могут содержаться следующие идентификаторы:

Идентификатор	Пример
otherName	Другое имя: Principal Name= *bobOtherAltName@example.com*
rfc822Name	RFC822 Name =*bobRFC822AltName@example.com*
dNSName	DNS Name=example1.com
x400Address	

Идентификатор	Пример
directoryName	Directory Address: E=*bobDirAltName@example.com*, CN=bob, OU=Gold Ballads, O=Gold Music, C=US
ediPartyName	
uniformResourceIdentifier	URL=http://example.com/
iPAddress	IP Address=192.168.7.1
registeredID	Registered ID=1.2.3.4

Для извлечения из альтернативного имени субъекта идентификатора пользователя можно использовать один из следующих идентификаторов.

Конфигурация

Configuration Manager извлекает идентификатор пользователя из сертификата клиента при помощи LW-SSO. Для настройки извлечения идентификаторов пользователей средствами LW-SSO используются следующие атрибуты обработчика сертификатов клиентов:

Для использования информации, содержащейся в сертификате клиента, необходимо настроить в Configuration Manager извлечение идентификатора пользователя.

При этом необходимо принять ряд решений:

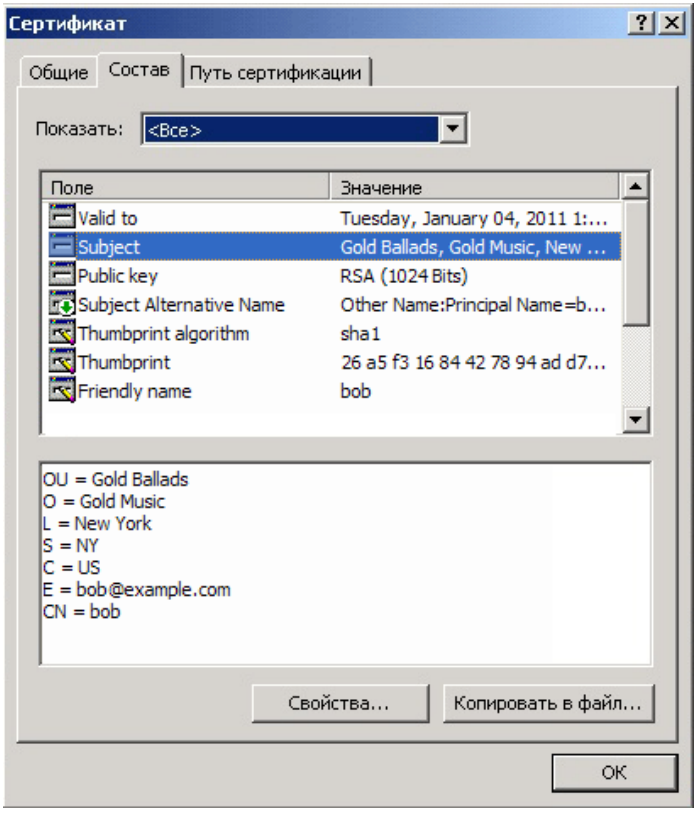
- Какое поле будет использоваться: SubjectDN или Subject Alternative Name?
- Следует ли использовать поле целиком или только его часть?
- Если используется только часть поля, необходимо указать его значение: Для поля SubjectDN необходимо указать атрибут субъекта, а для поля Subject Alternative Name – идентификатор.

Для настройки LW-SSO обработчик сертификатов клиентов использует следующие атрибуты:

Имя атрибута	Описание
enabled	Указывает, включен ли обработчик. **Важно**: Настоятельно рекомендуется установить для данного атрибута значение false и включать обработчик только в случаях, когда необходимо проверять сертификаты клиентов.
userIdentifierRetrieveField	Данный параметр указывает, в каком поле сертификата находится идентификатор пользователя. Варианты: **SubjectDN** или **SubjectAlternativeName**.
userIdentifierRetrieveMode	Параметр userIdentifierRetrieveMode указывает, является ли идентификатором пользователя все содержимое соответствующего поля либо только его часть. Варианты: **EntireField** или **FieldPart**.
userIdentifierRetrieveFieldPart	Если значение **userIdentifierRetrieveMode** равно **FieldPart**, данный параметр указывает, какая часть соответствующего поля является именем пользователя. Значение представляет собой кодовую букву, основанную на обозначениях, определенных в самом сертификате. **Примечание**: Если атрибут **userIdentifierRetrieveMode** имеет значение **FieldPart**, данный атрибут не может быть пустым. Он также не может быть пустым в случае, если атрибут **userIdentifierRetrievField** имеет значение **SubjectAlternativeName**.

Примеры

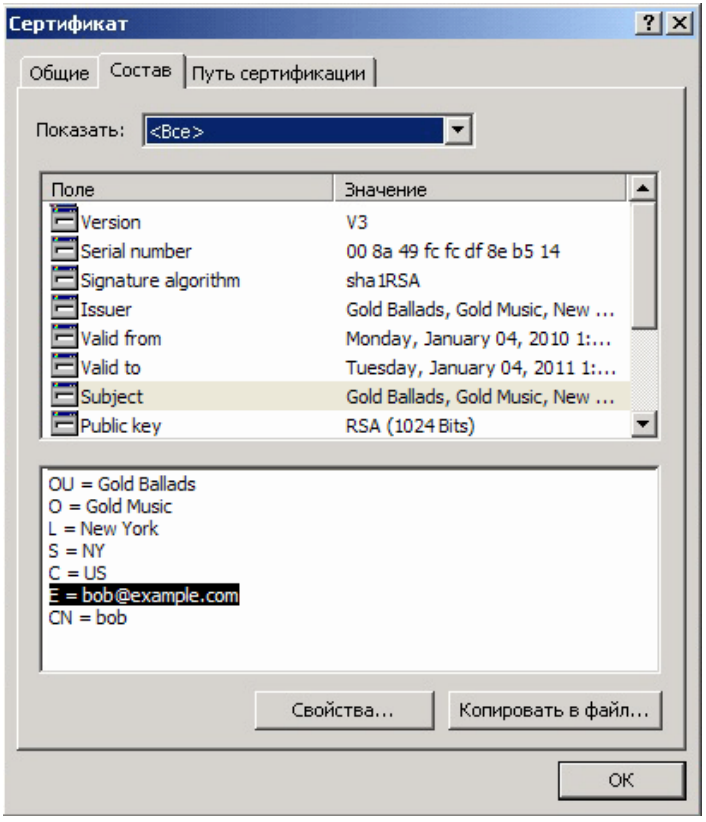
➤ **Для хранения идентификатора пользователя используется поле Subject**



В примере ниже описана процедура настройки обработчика на извлечение идентификатора пользователя из поля SubjectDN (используется поле целиком).

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="EntireField" />
```

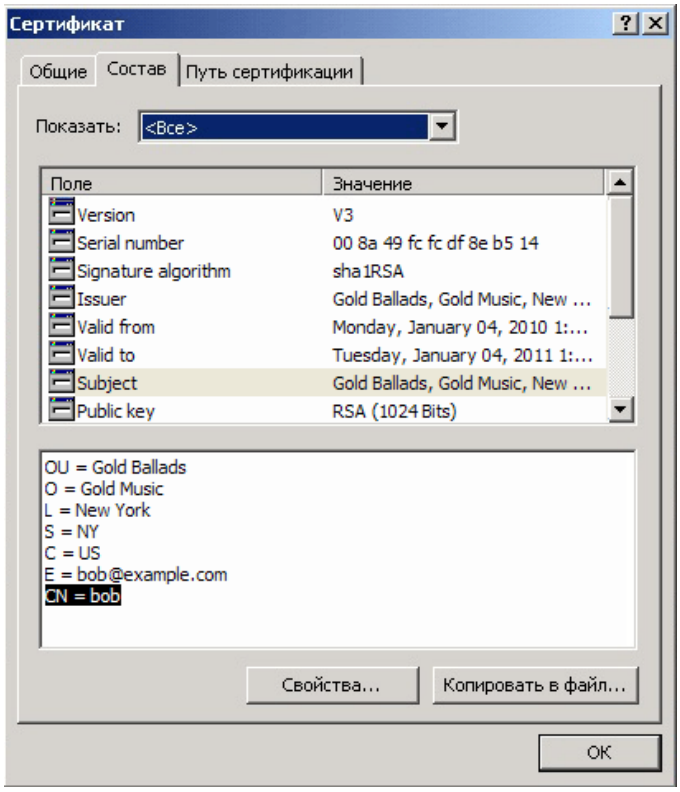
➤ **Для хранения идентификатора пользователя используется поле Email в составе Subject**



Используйте имена полей, приведенные в списке обозначений сертификата клиента. В примере ниже описана процедура настройки обработчика на извлечение идентификатора пользователя из поля Email в составе Subject:

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

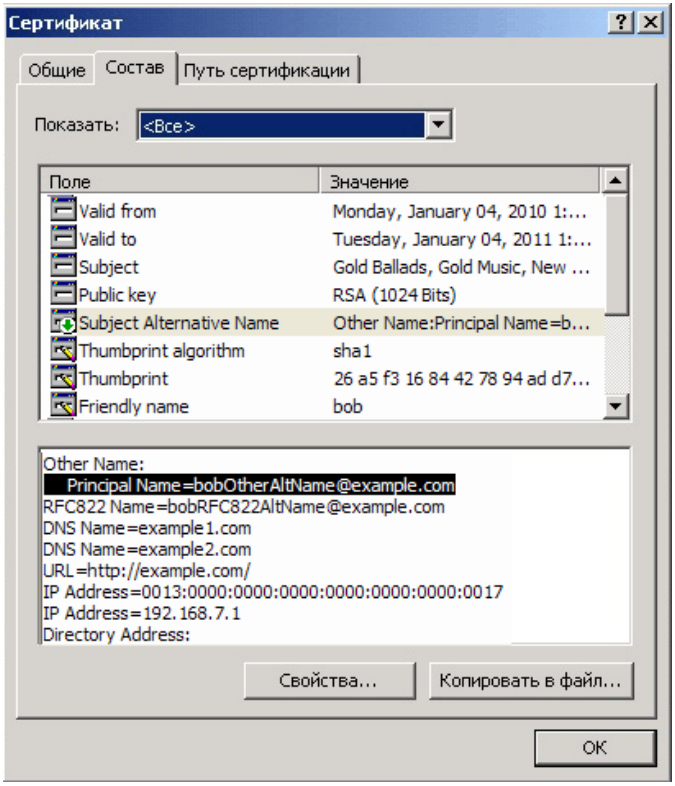
➤ **Для хранения идентификатора пользователя используется поле Command Name в составе Subject**



Используйте имена полей, приведенные в списке обозначений сертификата клиента. В примере ниже описана процедура настройки обработчика на извлечение идентификатора пользователя из поля Custom Name в составе Subject:

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

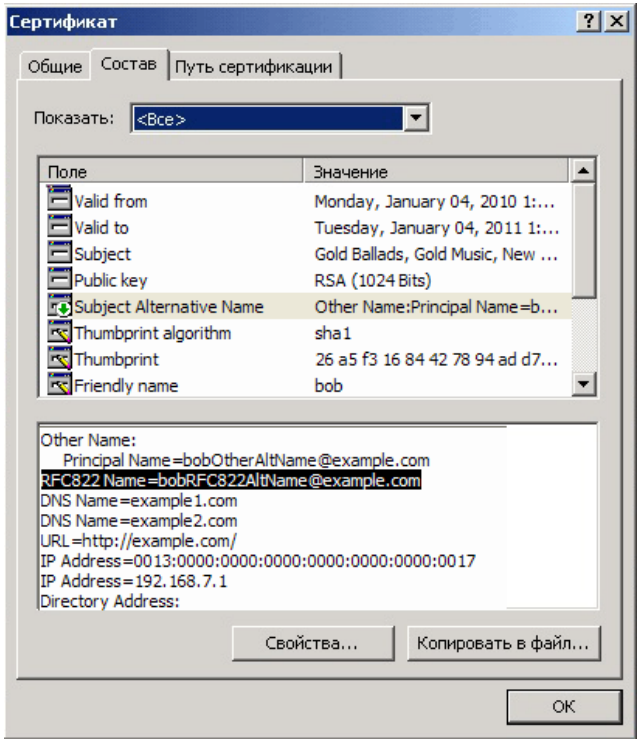
➤ **Для хранения идентификатора пользователя используется идентификатор otherName в составе поля Subject Alternative Name**



Используйте имена идентификаторов, приведенные в списке обозначений сертификата клиента. В примере ниже описана процедура настройки обработчика на извлечение идентификатора пользователя из идентификатора otherName в составе Subject Alternative Name:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

➤ **Для хранения идентификатора пользователя используется идентификатор rfc822Name в составе поля Subject Alternative Name**



Используйте имена идентификаторов, приведенные в списке обозначений сертификата клиента. В примере ниже описана процедура настройки обработчика на извлечение идентификатора пользователя из идентификатора rfc822Name в составе Subject Alternative Name:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

Настройка Configuration Manager для работы с UCMDB через SSL

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

Чтобы экспортировать сертификат сервера и импортировать его в хранилище truststore клиента, выполните следующие действия:

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

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

2. Импортируйте сертификат в хранилище truststore Configuration Manager (хранилище jre по умолчанию):

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

3. Укажите свойства соединения с UCMDB в Configuration Manager:

   Откройте пункт меню **Система > Настройки > Интеграция > UCMDB Foundation > UCMDB Foundation**. В поле "Стратегия подключения" выберите **HTTPS**, в качестве порта сервера UCMDB – порт UCMDB HTTPS, а затем измените URL-адрес доступа к UCMDB на https://<имяхоста>:8443.

4. Сохраните и активируйте настройки. Перезапустите Configuration Manager.

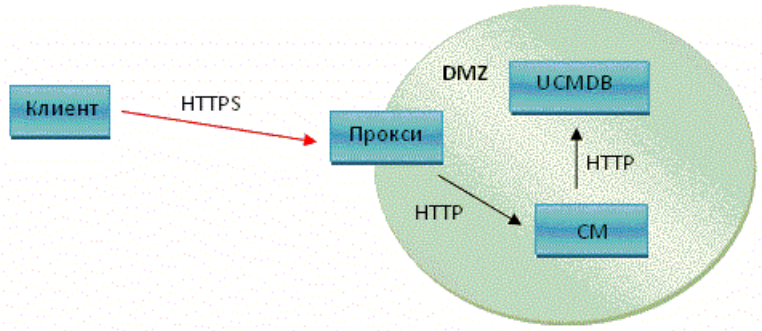
Чтобы настроить Configuration Manager для работы с другими продуктами (например, балансировщиками нагрузки) через Secure Sockets Layer (SSL), импортируйте сертификат безопасности продукта в хранилище truststore Configuration Manager (хранилище jre по умолчанию) при помощи следующей команды:

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

Обратный прокси-сервер

Если Configuration Manager и UCMDB размещаются в демилитаризованной зоне (DMZ), рекомендуется настроить работу системы с обратным прокси-сервером. Настройка осуществляется так же, как настройка работы с обратным прокси-сервером в UCMDB. Чтобы обеспечить доступ к Configuration Manager, следует сопоставить пути **/cnc** и **/bsf** с URL-адресами удаленного сервера, на котором установлен Configuration Manager.

На иллюстрации ниже представлен процесс настройки Configuration Manager для работы с обратным прокси-сервером:



К примеру, если в качестве обратного прокси-сервера используется сервер Apache, в файл **Apache2.2\conf\extra\httpd-ssl.conf** необходимо добавить следующие строки (а затем перезапустить сервер Apache):

ProxyPass /cnc http://<CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPassReverse /cnc http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPass /bsf http://< CM_HOSTNAME >:<CM_HTTP_PORT>/bsf
ProxyPassReverse /bsf http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/bsf

Процедура настройки зависит от типа обратного прокси-сервера. Подробнее см. в документации к прокси-серверу.

Настройка обратного прокси-сервера для Configuration Manager:

Внесите следующие изменения в файл **client-config.properties** в папке **<директория установки Configuration Manager>\conf**:

```
bsf.server.url=https://<proxy-server-name>:443/bsf
```

Порт HTTPS по умолчанию для прокси-сервера Apache – 443.

Часть II

Приложения

A

Ограничения емкости

В следующей таблице приведены ограничения емкости Configuration Manager.

Максимальное число представлений	100
Максимальное число политик	300
Максимальное число составных ЭК в представлении	5000
Максимальное число одновременно работающих пользователей	50
Максимальное число составных ЭК в модуле анализа конфигурации	1000

B

Проверка 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.

Сведения об устранении неполадок в LW-SSO см. в разделе "LW-SSO - устранение неполадок и ограничения" на стр. 137.

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.

C

Устранение неполадок

Данная глава включает:

Устранение неполадок и ограничения: общие сведения

Ограничения

Созданные в UCMDB типы ЭК отображаются только после выхода из Configuration Manager и повторного входа.

Устранение неполадок

Проблема. Атрибут **name** типа ЭК "узел" не считается атрибутом с отслеживанием изменений и не копируется в авторизованное состояние при авторизации ЭК. Это происходит в Configuration Manager версии 9.20 без Content Pack 9 для UCMDB.

Решение. Попробуйте один из следующих способов:

- Вручную установите для атрибута **name** отслеживание изменений в Диспетчере типов ЭК в UCMDB.
- Установите Content Pack 9.

Проблема. При запуске службы Configuration Manager выводится следующее сообщение об ошибке:

> Windows не удалось запустить HP Universal CMDB Configuration Manager на локальном компьютере. Дополнительные сведения см. в журнале событий Диспетчера системы. Если эта служба не является службой Microsoft, обратитесь к поставщику службы и сообщите ему о коде ошибки 0.

Решение. Выполните следующие действия:

1. Перейдите в директорию **<директория установки Configuration Manager>\cnc\bin** и выполните следующую команду:

   edit-server-0.bat

2. Откройте закладку Startup. В выпадающем списке Mode (внизу экрана) выберите вместо **exe jvm**.
3. Откройте закладку Shutdown. В поле Class измените последнее название с **Boostrap** на **Bootstrap**.
4. Нажмите **OK**.
5. Запустите службу.

Диспетчер развертывания - устранение неполадок и ограничения

Для устранения неполадок в Диспетчере развертывания откройте журнал предыдущей сессии, расположенный в следующей папке:

%temp%\HP\ucmdb-dm\Workspace\Sessions

Общие указания по повторному развертыванию

Во время установки следует анализировать предупреждения и ошибки, отображаемые на странице "Проверка" в Диспетчере развертывания. Для этого нажмите кнопку "Сведения" рядом с каждым из развернутых компонентов.

После выявления проблемы и нахождения решения выполните следующие шаги:

1. Удалите развернутые продукты и перезапустите машину.
2. Перезапустите Диспетчер развертывания и повторно введите все настройки.

Проблемы, вызывающие сбой при развертывании

Проблема. Ошибка с правами доступа при развертывании.

В журнале сессии зафиксирована проблема, связанная с правами доступа пользователя базы данных при создании новой схемы.

Решение. Для создания новой базы данных необходимо иметь соответствующие права доступа. Убедитесь, что для развертывания используются реквизиты пользователя, имеющего право создания табличных пространств и схем.

Проблема. Сбой конфигурации схемы/базы данных в UCMDB.

В журнале сессии есть сообщение, что Диспетчеру развертывания не удалось создать схему или базу данных.

Решение:

Примечание: Создание новой схемы UCMDB и подключение к уже существующей схеме истории UCMDB не поддерживается (независимо от типа сервера баз данных).

Проверьте, чтобы схемы UCMDB и истории UCMDB не использовали следующие типы подключения:

- схема UCMDB - Создать новую схему
- схема истории UCMDB - Подключиться к существующей схеме

Проблема. Сбой конфигурации схемы/базы данных в UCMDB.

В журнале сессии есть указание, что не удалось создать схему.

Решение. Откройте журнал сессии и найдите следующее сообщение: Ошибка SQL при выполнении оператора CREATE USER <имя схемы>

В имени схемы Oracle, задаваемом на странице настройки базы данных в Диспетчере развертывания, разрешается использовать только буквы (a-z), цифры (0-9) и дефис ('-').

Проблема. Не удается создать схему из-за недостатка пространства на диске.

Решение. Освободите пространство на диске. Это можно сделать стандартными средствами Oracle или Microsoft.

Проблема. Сбой настройки базы данных со следующей ошибкой: NT AUTHORITY\ANONYMOUS LOGON – Could not connect to database.

При выборе в качестве базы данных UCMDB сервера MSSQL с проверкой подлинности NTLM не удается настроить базу данных, что вызывает сбой развертывания.

Решение. Разверните UCMDB на машине localhost (единственное место, где поддерживается проверка подлинности NTLM).

Проблема. Сбой настройки базы данных Configuration Manager при создании новой базы данных.

На панели сведений в Диспетчере развертывания могут отображаться следующие ошибки:

> Не удалось подключиться к схеме Oracle из-за ошибки: ORA-01031: insufficient privileges

или

> Не удалось создать схему базы данных: machineName.
> Причина: ORA-01919: role 'RESOURCE' does not exist

Решение. Убедитесь, что у роли пользователя базы данных есть следующие права доступа:

- Connect
- Resource

Проблема. Не удается выполнить развертывание из-за недостатка дискового пространства на целевой машине.

Решение. Войдите в систему на целевой машине и освободите необходимое пространство:

- для развертывания UCMDB необходим 1 ГБ свободного пространства
- Configuration Manager требует 1 ГБ свободного пространства
- DDMA требует 1 ГБ свободного пространства

Примечание: В дополнение к требованиям продуктов необходимо наличие еще 1 ГБ пространства для работы с временными файлами.

Проблема. Сбой функции ping в UCMDB

Данная команда выполняется на машине Configuration Manager для проверки соединения с интерфейсом UCMDB. Откройте журнал сессии и найдите следующее сообщение:
Failed to test connection due to error: java.net.ConnectException: Connection refused: connect.

Решение:

- ➤ Убедитесь, что брандмауэр Windows не блокирует порт 8080 на целевой машине UCMDB.
- ➤ Убедитесь, что сервер UCMDB доступен с машины Configuration Manager, а также что он был успешно развернут и работоспособен.

Нет подключения к машине хоста

Проблема. Ошибка RPC Unavailable или неизвестная ошибка.

При нажатии на кнопку "Проверка подключения" возникает ошибка RPC Unavailable.

Решение. При необходимости уточните имя хоста, убедитесь, что запущены службы WMI и сервера, а также что брандмауэр Windows не блокирует доступ к интерфейсу WMI.

Отключите брандмауэр Windows или добавьте исключение, разрешающее удаленное подключение администраторов.

Для этого откройте на панели управления раздел **Брандмауэр Windows** и выберите **Правила для входящих подключений.** Включите все файлы и принтеры, правила WMI и порт 8080.

Проверка подключения пройдена неудачно

Проблема. Отказано в доступе.

Отказано в доступе из-за неверного имени пользователя или пароля, ошибки в настройках DNS, либо из-за отсутствия у пользователя, от имени которого выполняется развертывание, прав администратора на целевой машине.

Решение. Убедитесь в правильности используемых реквизитов пользователя и наличии у него прав администратора на целевой машине.

Не удалось получить доступ к приложению

Проблема. После успешного развертывания – не удалось получить доступ к приложению (UCMDB или Configuration Manager).

Решение. Проверьте наличие и работоспособность следующих служб UCMDB и Configuration Manager.

- **UCMDB_Server**
- **HPUCMDBCMoasisSNAPSHOTserver0**

Изучите журналы развертывания, расположенные в директории сессии, на предмет ошибок.

Отключена LW-SSO

Проблема. Успешное развертывание - отключены функции LW-SSO.

Решение. Убедитесь, что в UCMDB и Configuration Manager (а также в OO, если эта система используется) используются идентичные параметры LW-SSO init string и домены.

Проверьте настройки LW-SSO в продуктах следующими способами:

- Configuration Manager – Откройте файл **lwssofmconf.xml** и проверьте настройки init string и домена. Файл находится в папке **<директория установки Configuration Manager>\conf** .
- UCMDB – откройте UCMDB и выберите **Диспетчеры > Администрирование > Диспетчер настроек инфраструктуры**.

Если Configuration Manager и UCMDB расположены на машинах с разными доменами DNS, в настройках **Надежные домены** на обеих машинах должны быть указаны оба домена.

Для получения более подробной информации о развертывании Диспетчер развертывания можно запустить в режиме отладки. В режиме отладки система создает больше сведений о ходе развертывания.

Включение режима отладки:

1 После запуска Диспетчера развертывания откройте окно браузера и введите в адресную строку %temp%.

2 Перейдите в папку **hp\ucmdb-dm**.

3 Откройте в текстовом редакторе файл **ini** и добавьте в его последнюю строку следующее свойство:

–Ddebug.mode=true

4 Для запуска Диспетчера развертывания выполните файл **%temp%\HP\ucmdb-dm\ucmdb-dm.exe**.

Доступ к Configuration Manager - устранение неполадок и ограничения

Ограничения

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

Устранение неполадок

Проблема. После изменения настроек в меню **Система > Настройки** невозможно запустить сервер.

Решение. Вернуться к прежним настройкам. Выполните следующие действия:

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

<директория установки Configuration Manager>\bin\export-cs.bat <свойства базы данных> --history

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

cd <директория установки Configuration Manager>\bin export-cs.bat -p ..\conf\database.properties --history

2 Выполните следующую команду, чтобы экспортировать последний набор конфигурации:

<директория установки Configuration Manager>\bin\export-cs.bat <свойства базы данных> <ID набора конфигурации> <имя файла дампа>,

где **<ID набора конфигурации>** берется из предыдущего шага, а **<файл дампа>** – имя временного файла для сохранения набора конфигурации. К примеру, для экспорта набора конфигурации с ID **491520** в файл **mydump.zip** введите следующую команду:

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

3 Остановите службу Configuration Manager.

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

<директория установки Configuration Manager>\bin\import-cs.bat <свойства базы данных> -i <имя файла дампа> --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 пункт меню **Система > Настройки > Интеграция > UCMDB Foundation > UCMDB Foundation**, измените настройки и сохраните новый набор конфигурации. 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>\bin\encrypt-password.bat –p <password>

Команда возвращает зашифрованный пароль.

2 Скопируйте зашифрованный пароль (включая префикс {ENCRYPTED} в параметр **db.password** в файле **<директория установки Configuration Manager>\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 Configuration Manager>\servers\server-0\conf\server.xml** и изменив следующие номера портов:
  - HTTP (8180): строка 69
  - HTTPS (8443): строки 71 и 90

Проблема. Возникает ошибка "недостаточно памяти".

Решение. Выполните следующие действия, чтобы изменить параметры запуска сервера:

1 Выполните следующий пакетный файл:

<директория установки Configuration Manager>/bin/edit-server-0.bat

2 Измените следующие настройки:

-Dapplication.ms=<размер начального пула памяти>
-Dapplication.mx=<максимальный размер пула памяти>

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 разделе меню **Система > Настройки**.
- Выполните вызов JMX для запуска асинхронного анализа в соответствующем представлении.
- Откройте раздел меню **Администрирование > Политики > Политики конфигурации**. 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 > UCMDB Foundation** открывается страница входа в UCMDB.

Решение. Для доступа в UCMDB без повторного входа в систему необходимо включить единый вход. Дополнительные сведения см. в разделе "Единый вход в систему (SSO)" на стр. 73. 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 >UCMDB Foundation** не работает.

Решение. Выполните следующие действия:

1. Откройте пункт меню **Система > Настройки > Интеграции > UCMDB Foundation > UCMDB Foundation.**
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.

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 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** ко 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 ко 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 ко 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.

Устранение неполадок

Проблема: После входа в систему не создается файл-cookie LW-SSO.

- **Возможная причина:** Неверное определение непустого домена в элементе конфигурации LW-SSO.
- **Возможное решение**: Убедитесь, что домен, заданный в элементе конфигурации LW-SSO, совпадает с доменом приложения.
- **Возможная причина:** В качестве параметра для функции enableSSO передается неверный непустой домен.
- **Возможное решение**: Убедитесь, что домен, который передается в качестве параметра для функции enableSSO, совпадает с доменом приложения.
- **Возможная причина:** Доступ к приложению выполнен не с использованием полного доменного имени в URL-адресе для входа, если в конфигурации LW-SSO задан домен (например: http://192.168.12.13/WebApp).
- **Возможное решение**: Доступ к приложению должен выполняться с использованием полного доменного имени в URL-адресе для входа (например: http://myserver.companydomain.com/WebApp).

Проблема: LW-SSO не удается создать файл cookie для функции AutoCookieCreation.

- **Возможная причина:** В элементе конфигурации LW-SSO неверно определен домен.
- **Возможное решение**: Убедитесь, что домен, заданный в элементе конфигурации LW-SSO, совпадает с доменом приложения.

Проблема: Маркер LW-SSO не проходит проверку.

- **Возможная причина:** Два приложения имеют различные значения параметра шифрования initString, либо различаются другие параметры шифрования.
- **Возможное решение**: Используйте в обоих приложениях одно и то же значение initString (а также одинаковые значения всех остальных параметров шифрования в элементе создания LW-SSO).

- **Возможная причина:** Разница во времени между двумя приложениями составляет более 15 мин.
- **Возможное решение**: Все приложения, задействованные в интеграции LW-SSO, должны использовать одно время GMT с разбежкой не более 15 минут.
- **Возможная причина:** В элементе конфигурации LW-SSO указан пустой домен, и осуществляется доступ ко второму приложению на другом компьютере с тем же доменом DNS.
- **Возможное решение**: Убедитесь, что домен, заданный в элементе конфигурации LW-SSO, совпадает с доменом приложения.
- **Возможная причина:** В элементе конфигурации LW-SSO не указан домен, и осуществляется доступ ко второму приложению на другом компьютере с тем же доменом DNS.
- **Возможное решение**: Добавьте в элемент LW-SSO тот же домен, что и в настройках приложения.

Проблема: Не удается выполнить проверку маркера LW-SSO в среде с несколькими доменами

- **Возможная причина:** Неверно указан домен в элементе LW-SSO в настройках одного из приложений.
- **Возможное решение**: Домен, заданный в элементе LW-SSO конфигурации приложения, должен совпадать с фактически используемым доменом приложения.
- **Возможная причина:** В конфигурации одного из приложений неверно задан домен в настройках trustedHosts или protectedDomains.
- **Возможное решение**: Проверьте, правильно ли заданы домены в настройках trustedHosts или protectedDomains всех приложений.
- **Возможная причина:** При использовании Internet Explorer 6.x, 7.x или 8.x блокируется или отвергается сессионный файл cookie LW-SSO.
- **Возможное решение**: Добавьте все серверы LW-SSO в зону "Интранет/Надежные узлы" в Internet Explorer (Сервис> Свойства обозревателя > Безопасность > Местная интрасеть > Узлы > Дополнительно). Это позволит принимать все файлы cookie.

- **Возможная причина:** Приложения имеют различные значения параметра шифрования initString, либо различаются другие параметры шифрования.
- **Возможное решение**: Используйте во всех приложениях одно и то же значение initString (а также одинаковые значения всех остальных параметров шифрования в элементе создания LW-SSO).
- **Возможная причина:** Разница во времени между приложениями составляет более 15 мин.
- **Возможное решение**: Все приложения, задействованные в интеграции LW-SSO, должны использовать одно время GMT с разбежкой не более 15 минут.
- **Возможная причина:** Ссылка с защищенного (HTTPS) и незащищенный (HTTP) ресурс на другом домене.
- **Возможное решение**: При создании ссылок между доменами необходимо, чтобы первая ссылка вела с одного защищенного ресурса (HTTPS) на другой защищенный ресурс (HTTPS).

Поддержка IPv6 - устранение неполадок и ограничения

Ограничения

- URL-адрес не должен содержать IP-адрес.
- Операционная система должна поддерживать IPv6 и IPv4. Если адрес IPv4 не закрыт или не поддерживается, вход в Configuration Manager будет невозможен.
- После каждого изменения времени на сервере Tomcat Configuration Manager необходимо перезапустить сервер, чтобы обновить время на нем.

Устранение неполадок

Проблема. После настройки подключения UCMDB к адресу IPv6 в процессе установки пункт меню **Администрирование > UCMDB Foundation** не работает.

Решение. Выполните следующие действия:

1. Откройте пункт меню **Система > Настройки > Интеграция > UCMDB Foundation > UCMDB Foundation**.
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/ucmdb-ui/.
3. Сохраните и активируйте настройки.
4. Перезапустите Configuration Manager.

Проверка подлинности - устранение неполадок и ограничения

В этом разделе описываются известные проблемы проверки подлинности.

Проблема: При проверке подлинности для входа в приложение после перенаправления в точку проверки подлинности выдается ошибка 500.

- **Возможная причина:** Configuration Manager WAR и BSF WAR имеют различные значения параметра шифрования initString, либо различаются другие параметры шифрования.
- **Возможное решение:** Используйте в обоих приложениях одно и то же значение initString (а также одинаковые значения всех остальных параметров шифрования в элементе создания LW-SSO).

Проблема: При проверке подлинности для входа в приложение после перенаправления в точку проверки подлинности не отображается форма для входа.

Решение: При использовании Internet Explorer 6.0, 7.0 или 8.0 блокируется или отвергается сессионный файл cookie проверки подлинности Configuration Manager. Добавьте сервер Configuration Manager в зону **"Интранет/Надежные узлы"** в Internet Explorer (**Сервис> Свойства обозревателя > Безопасность > Местная интрасеть > Узлы > Дополнительно**). Это позволит принимать все файлы cookie.

Проблема: После проверки подлинности выдается ошибка 403.

- **Возможная причина:** Неверное определение домена в элементе LW-SSO конфигурации приложения.
- **Возможное решение:** Убедитесь, что домен, заданный в элементе конфигурации LW-SSO, совпадает с доменом приложения.
- **Возможная причина:** Доступ к приложению выполнен не с использованием полного доменного имени в URL-адресе для входа, если в конфигурации LW-SSO задан домен (например: http://192.168.12.13/WebApp).
- **Возможное решение:** Доступ к приложению должен выполняться с использованием полного доменного имени в URL-адресе для входа (например: http://myserver.companydomain.com/WebApp).

Проблема: После проверки подлинности отображается страница **Get Acegi User Details**.

Решение: При использовании Internet Explorer 6.0, 7.0 или 8.0 блокируется или отвергается сессионный файл cookie проверки подлинности Configuration Manager. Добавьте сервер Configuration Manager в зону **"Интранет/Надежные узлы"** в Internet Explorer (**Сервис> Свойства обозревателя > Безопасность > Местная интрасеть > Узлы > Дополнительно**). Это позволит принимать все файлы cookie.