ВИЗОР

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

инструкция по установке

Аннотация

Настоящий документ описывает установку и настройку Системы защиты информации (СЗИ) «Визор» версии **2016.Q2.R1** (далее - программный продукт) на одном сервере.

Документ содержит сведения о технических и программных средствах, обеспечивающих функционирование программного продукта, предпочтительную очередность установки, процедуры установки и первоначальной настройки системных и прикладных программных компонент, а также способы проверки работоспособности программного продукта, возможные аварийные ситуации и способы их устранения.

Содержание

Аннотация 1
Содержание 2
Комплект поставки 3
Содержимое поставки 3
Функциональные характеристики 4
Ограничения 5
Условия применения 6
Требования к серверной части 6
Требования к рабочему месту пользователя 7
Процедура установки 8
Предпочтительная очередность установки 8
Установка и настройка контроллера домена Active Directory Domain Controller for Windows Server 2008 8
Установка и настройка JVM 37
Установка дистрибутива 40
Проверка работоспособности 42

Комплект поставки

Номер версии: 2016.Q2.R1

Дата выпуска: 01.07.2016

Дистрибутив: 2016.Q2.R1.zip

Содержимое поставки

Компонента	Версия	Дистрибутив
JDK	8	http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html
Java SE Timezone Updater	2.0.3	http://www.oracle.com/technetwork/java/javase/downloads/tzupdater-download-513681.html
PostgreSQL	9.5.1	http://www.enterprisedb.com/products-services-training/pgbindownload
Apache HTTPD	2.4	ДИСТРИБУТИВ\Apache24
Apache ActiveMQ	5.11.1	ДИСТРИБУТИВ\ActiveMQ
WildFly AS	9.0.2	ДИСТРИБУТИВ\wildfly
Gradle	2.12	ДИСТРИБУТИВ\Gradle
cURL	7.48.0	ДИСТРИБУТИВ\curl
Служба управления идентификационными данными	6.2.0	ДИСТРИБУТИВ\modules\security-distribution-6.2.0.zip
Служба управления событиями безопасности	7.2.0	ДИСТРИБУТИВ\modules\audit-distribution-7.2.0.zip
Служба аутентификации пользователей	6.1.0	ДИСТРИБУТИВ\modules\cas-distribution-6.1.0.zip
Служба авторизации пользователей	6.1.0	ДИСТРИБУТИВ\modules\cds-distribution-6.1.0.zip
Единый центр поддержки пользователей	2.1.0	ДИСТРИБУТИВ\modules\usersupport-distribution-2.1.0.zip
Приложение смены пароля	1.0.1	ДИСТРИБУТИВ\modules\change-password-distribution-1.0.1.zip
Служба доставки уведомлений	2.1.0	ДИСТРИБУТИВ\modules\notifier-distribution-2.1.0.zip
Хранилище фотографий	3.1.0	ДИСТРИБУТИВ\modules\photo-storage-distribution-3.1.0.zip
Приложение первичного наполнения	1.0.1	ДИСТРИБУТИВ\modules\installer-distribution-1.0.1.zip

Функциональные характеристики

Управление идентификационными данными:

- учет сведений о сотрудниках с сохранением истории изменений и возможностью прикрепления документов, на основе которых произведены изменения;
- поддержка групповых операций над сотрудниками;
- автоматическая блокировка учетных записей после достижения установленного количества дней неактивности пользователя;
- управление правами доступа сотрудников к информационным ресурсам на основе ролевой модели управления доступом;
- поддержка прав доступа сотрудников на время;
- управление служебными расследованиями в отношении сотрудников;
- управление жизненным циклом ролевой модели информационных ресурсов;
- работа с электронными заявками на доступ;
- управление политикой генерации идентификаторов учетных записей;
- ведение справочников организационной структуры, должностей, званий;
- управление паролями, включая возможность определения единой политики паролей;
- автоматическая синхронизация данных с Active Directory;
- возможность конфигурированию ролевой модели доступа к службам информационной безопасности без программирования;
- экспорт отчетов.

Управление доступом к информационным ресурсам:

- идентификация и аутентификация пользователей при доступе к информационным ресурсам по идентификатору и паролю;
- предотвращение доступа не идентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;
- блокирование учетной записи пользователя при превышении установленного числа попыток доступа;
- поддержка функции однократной аутентификации (Single Sign-On);
- разграничение доступа пользователей к информационным ресурсам в зависимости от назначенных прав доступа;
- сопряжение сведений о сотруднике с учетной записью субъекта, от имени которой он осуществляет доступ к информационным ресурсам;
- поддержка ограничения доступа в соответствии с графиком доступа;
- защита сетевых коммуникаций с использованием протокола SSL;
- протоколирование успешных и неуспешных попыток доступа пользователей к информационным ресурсам;
- принудительное завершение действия сессий безопасности пользователей.

Управление событиями безопасности:

- предоставление интерфейса для протоколирования событий, связанных с действиями пользователей в информационных ресурсах, а также в рамках информационного взаимодействия между системами;
- ведение журнала зарегистрированных событий;
- управление заданиями очистки журнала от событий, потерявших актуальность;
- предоставление пользовательских интерфейсов для поиска и аудита накопленной информации;
- экспорт отчетов.

Ограничения

Программный продукт предназначен для развертывания на одном сервере в среде Microsoft Windows с дополнительной интеграцией с контроллером домена Active Directory Domain Controller.

Условия применения

Комплекс программно-технических средств программного продукта состоит из серверной части, рабочих мест пользователей и обслуживающего персонала.

Взаимодействие пользователей с программным продуктом осуществляется по технологии тонкого клиента.

Требования к серверной части

Требования к аппаратному обеспечению

Ниже представлены рекомендуемые требования к аппаратному обеспечению серверной части:

- сервер контроллера домена:
  - два процессора Pentium 4 с частотой 3 ГГц или выше;
  - 4 Гб ОЗУ;
  - 80 ГБ свободного места на жестком диске;
  - сетевой адаптер для подключения сервера к ЛВС по протоколам стека TCP/IP с полосой пропускания 1 Гбит/с;
- сервер приложений / баз данных:
  - процессор Intel Xeon ® E5-2680 2.7ГГц или аналогичный;
  - 8 Гб ОЗУ;
  - 300 ГБ свободного места на жестком диске;
  - сетевой адаптер для подключения сервера к ЛВС по протоколам стека TCP/IP с полосой пропускания 1 Гбит/с;

Вышеперечисленные средства вычислительной техники могут быть представлены виртуальными машинами с аналогичными характеристиками.

Требования к программному обеспечению

Ниже представлены рекомендуемые требования к программному обеспечению серверной части:

- сервер контроллера домена:
  - операционная система Microsoft Windows Server 2008 R2 Standard SP1, 64bit;
  - рекомендуется файловая система NTFS;
- сервер приложений / баз данных:
  - операционная система Microsoft Windows Server 2008 R2 Standard SP1, 64bit;

- комплект разработчика приложений Oracle Java Development Kit версии 8u77, 64bit;
- СУБД PostgreSQL версии 9.5.1;
- Apache HTTPD версии 9.5.1;
- Apache ActiveMQ 5.11.1;
- WildFly AS 9.0.2.

Требования к рабочему месту пользователя

Требования к аппаратному обеспечению

Ниже представлены рекомендуемые требования к аппаратному обеспечению рабочего места пользователя:

- процессор Intel i3, 2GHz или аналогичный;
- 4 Гб ОЗУ;
- 50 ГБ свободного места на жестком диске;
- сетевой адаптер для подключения рабочей станции к ЛВС по протоколам стека TCP/IP с полосой пропускания не менее 100 Мбит/с;
- графический SVGA монитор с разрешением экрана 1280x1024x24bit;
- клавиатура и мышь.

Требования к программному обеспечению

Ниже представлены рекомендуемые требования к программному обеспечению рабочего места пользователя:

- операционная система Microsoft Windows 7 и выше;
- интернет-браузер Internet Explorer версии 11 и выше, либо Google Chome версии 44 и выше, Firefox Mozilla версии 39 и выше;
- программа просмотра документации в pdf–формате Adobe Acrobat Reader версии 9.0 и выше;
- программа для работы с электронными таблицами Microsoft Office Excel 2007 и выше.

Процедура установки

Предпочтительная очередность установки

1. Установка и настройка контроллера домена домена Active Directory Domain Controller for Windows Server 2008.
2. Установка и настройка JVM.
3. Установка дистрибутива.
4. Проверка работоспособности.

Установка и настройка контроллера домена Active Directory Domain Controller for Windows Server 2008

Для установки контроллера домена Active Directory необходимо запустить «Server Manager» («Диспетчер сервера») и перейти в узел «Roles» («Роли») в правой панели консоли. Далее необходимо нажать кнопку «Add Roles» («Добавить роли») в правой панели (см. рис. 1).

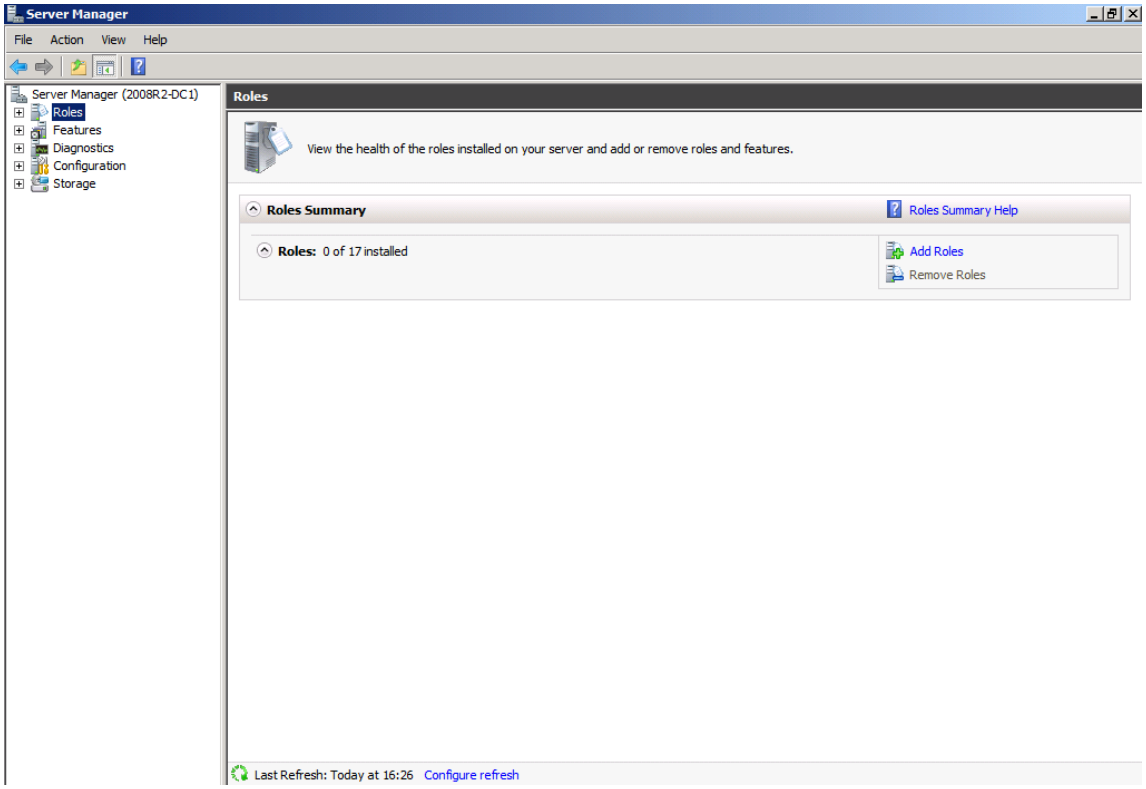

РИСУНОК 1. ДОБАВЛЕННЫЕ РОЛИ

В открывшемся окне «Add Roles» («Добавление ролей») на вкладке «Before You Begin» («Перед началом работы») приведены описания основных сведений по

установке роли с помощью диспетчера сервера. Для того что бы продолжить установку, следует нажать кнопку «Next» («Далее») (см. рис. 2).

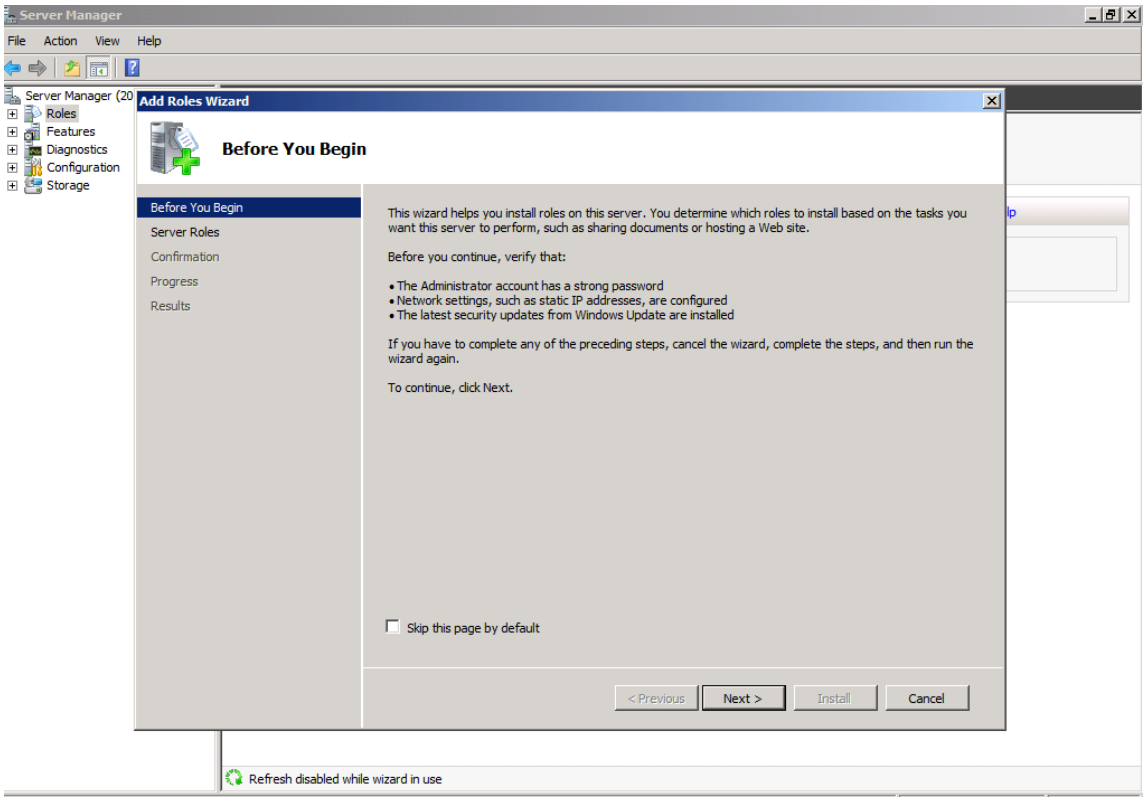

Рисунок 2. Сведения по установке роли

Затем необходимо выбрать роли сервера для установки. Другие роли сервера будут установлены позже, для начала необходимо установить роль контроллера домена (DC). Следует выбрать роль «Active Directory Domain Services», отмечая соответствующую опцию. Необходимо обратить внимание, что мастер отобразит ряд функций, которые будут установлены наряду с ролью «Active Directory Server Role». Далее следует нажать кнопку «Add Required Features» («Добавить нужные функции»), чтобы установить эти функции во время установки роли «Active Directory Server» (см. рис. 3).

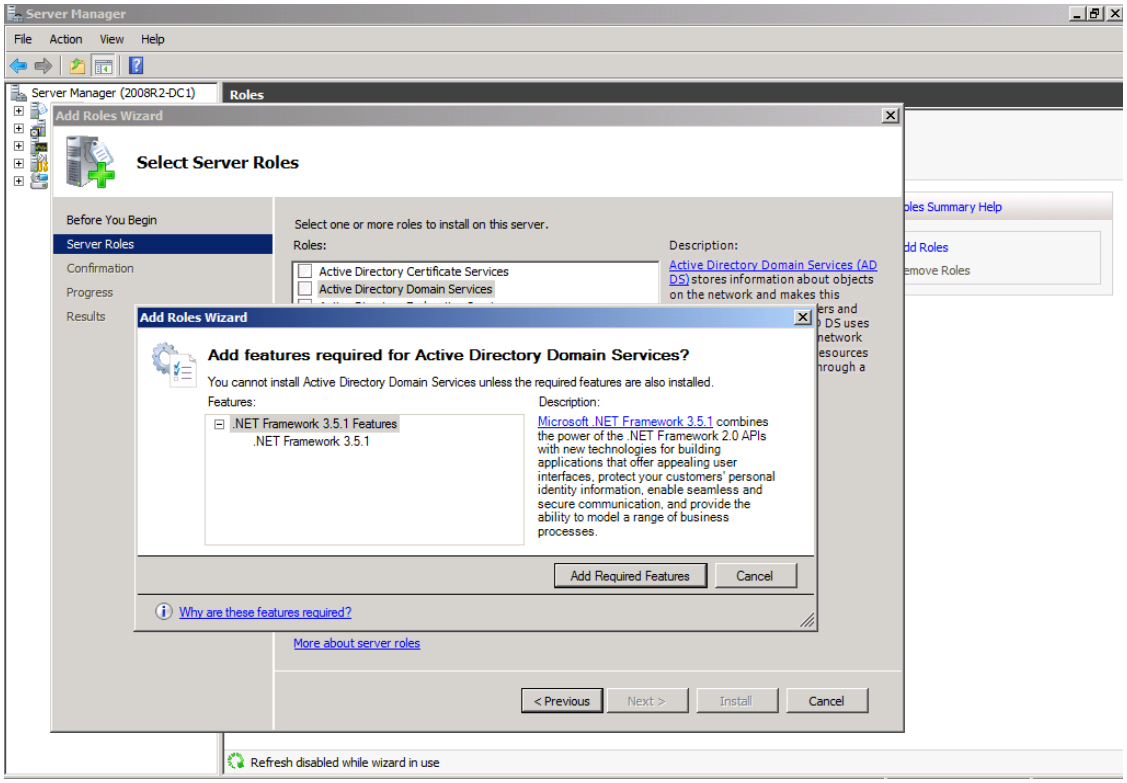

Рисунок 3. Добавление нужных функций

После выбора роли «Active Directory DC Server», отобразится информация об этой роли сервера. Необходимо обратить внимание на ряд моментов (см. рис. 4):

- для обеспечения отказоустойчивости рекомендуется установка, как минимум, двух DC в своей сети;
- установка одного DC в сети является предпосылкой сбоя;
- для корректного функционирования DC необходимо дополнительно установить DNS;
- необходимо запустить «dcpromo» после установки роли, далее не придется выполнять дополнительные шаги во время установки других ролей сервера, поскольку весь процесс установки ролей можно выполнить с помощью диспетчера сервера. Роль «Active Directory Domain Services» является единственной ролью, требующей использования двух шагов для установки;
- необходимо помнить, что во время установки роли «Active Directory Domain Services» также устанавливаются службы «DFS пространства имен», «DFS репликации и репликации файлов» – все эти службы используются службами «Active Directory Domain Services», поэтому устанавливаются автоматически.

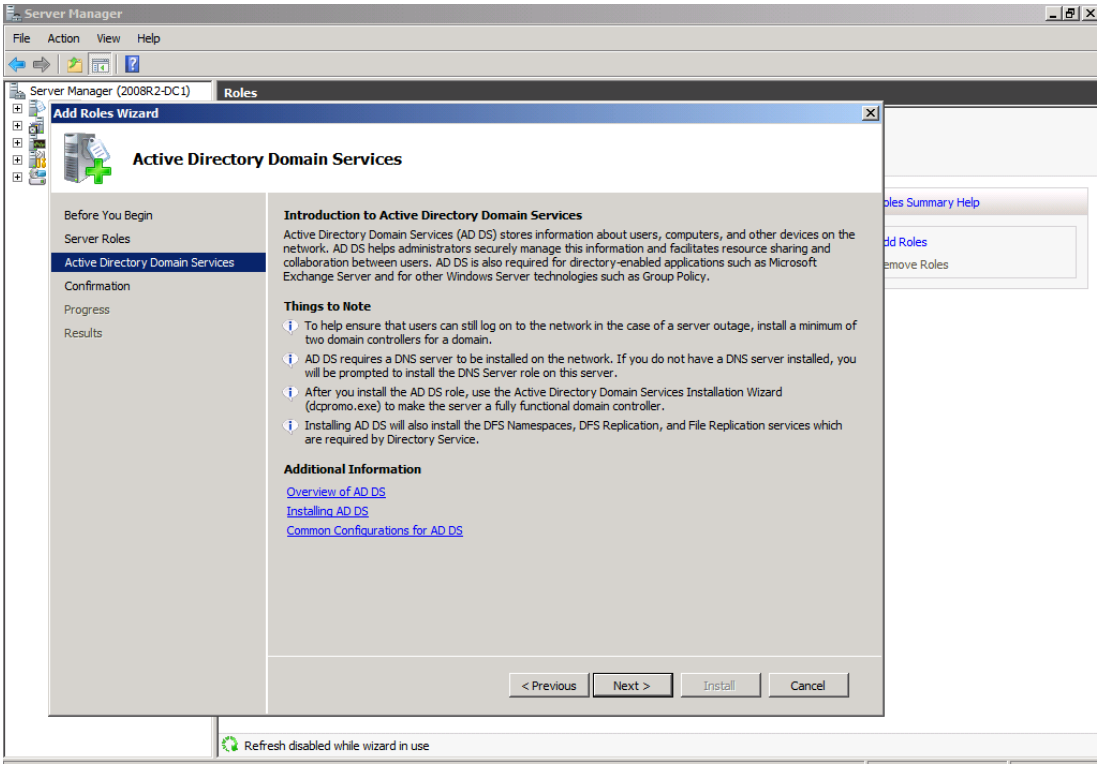

Рисунок 4. Установка служб DFS пространства имен

Далее необходимо нажать кнопку «Install» («Установить») для установки файлов, необходимых для запуска «dcpromo» (см. рис. 5).

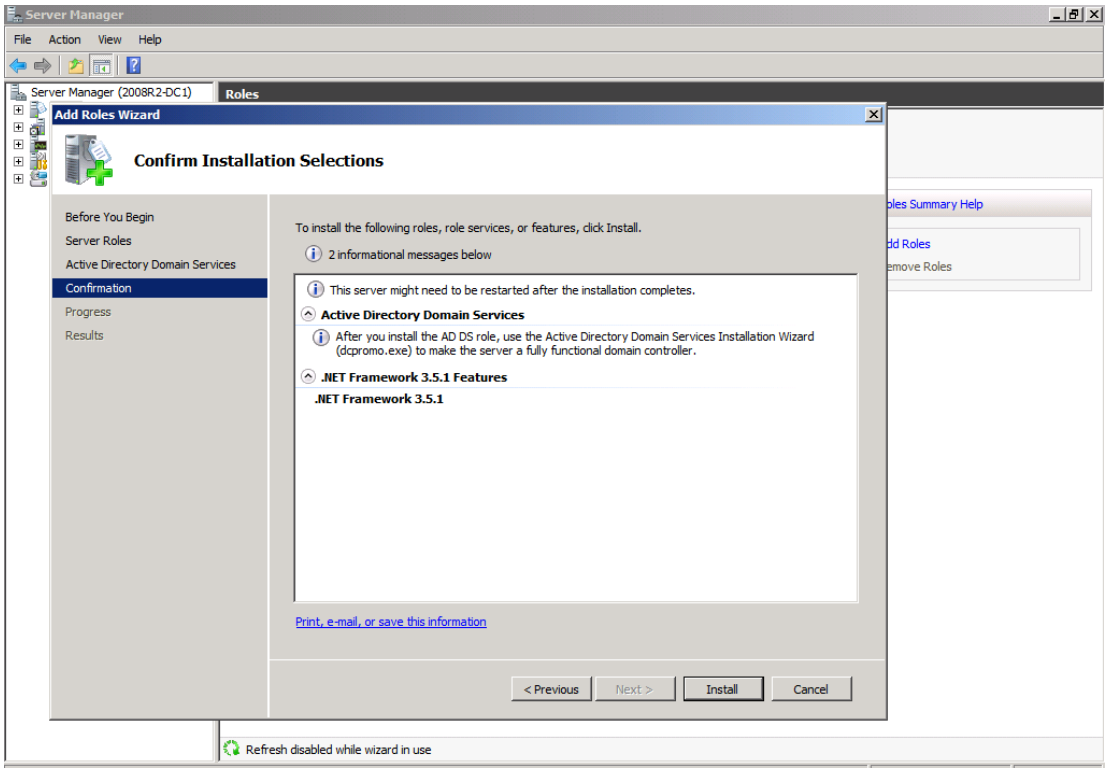

Рисунок 5. Установка файлов, необходимых для запуска «dcpromo»

После того, как установка будет завершена, следует нажать кнопку «Close» («Закрыть») (см. рис. 6).

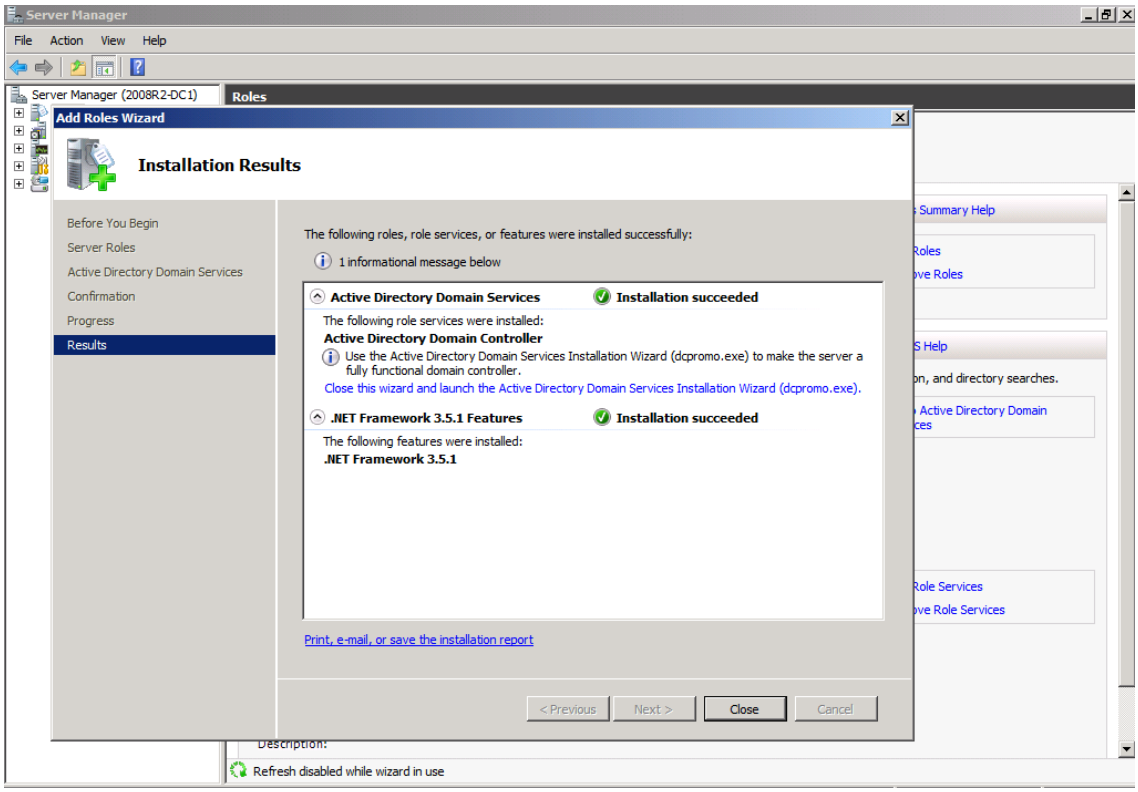

Рисунок 6. Завершение установки

Далее необходимо перейти в меню «Пуск» и в текстовом поле «Выполнить» ввести «dcpromo» (см. рис. 7).

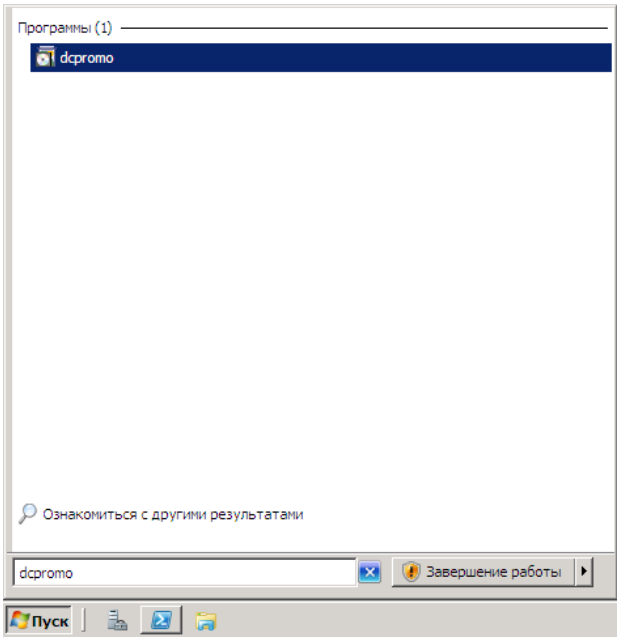

Рисунок 7. Переход в меню «Пуск» и ввод «dcpromo» в текстовом поле «Выполнить»

После этого запустится мастер «Active Directory Domain Service Installation Wizard» («Мастер установки сервисов домена»). Так как расширенные опции в этом сценарии не нужны, необходимо нажать кнопку «Next» («Далее») (см. рис. 8).

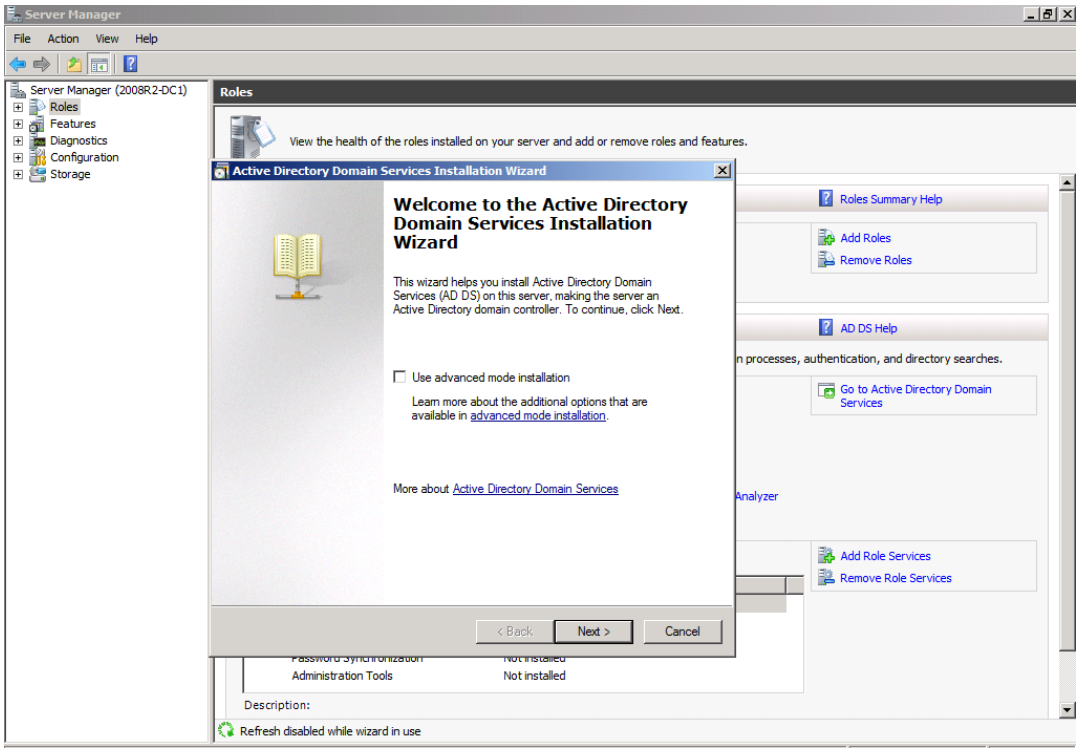

РИСУНОК 8. ЗАПУСК МАСТЕРА «ACTIVE DIRECTORY DOMAIN SERVICE INSTALLATION WIZARD»

На странице «Operating System Compatibility» («Совместимость операционной системы») будет отражено предупреждение о том, что NT и non-Microsoft SMB клиенты будут испытывать проблемы с некоторыми криптографическими алгоритмами, используемыми в Windows Server 2008 R2. Для того, что бы продолжить установку настроек следует нажать кнопку «Next» («Далее») (см. рис. 9).

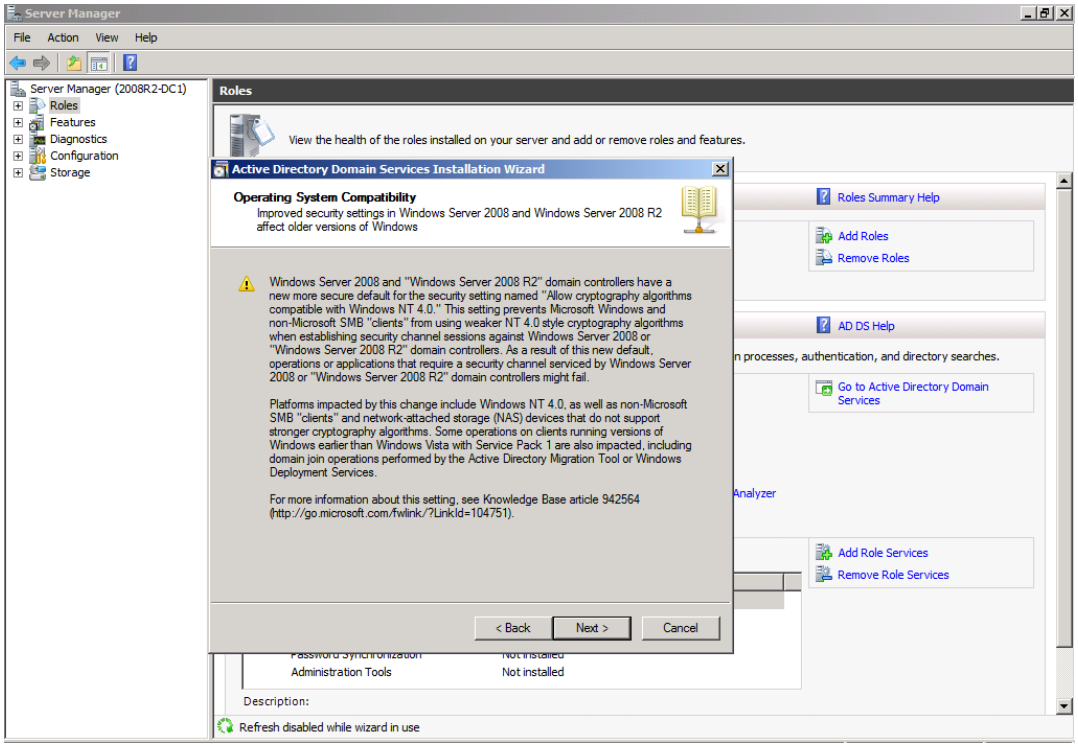

Рисунок 9. Предупреждения мастера

В открывшемся окне «Choose a Deployment Configuration» («Выбор конфигурации установки») необходимо выбрать опцию «Create a new domain in a new forest» («Создание нового домена в новом лесу») (см. рис. 10).

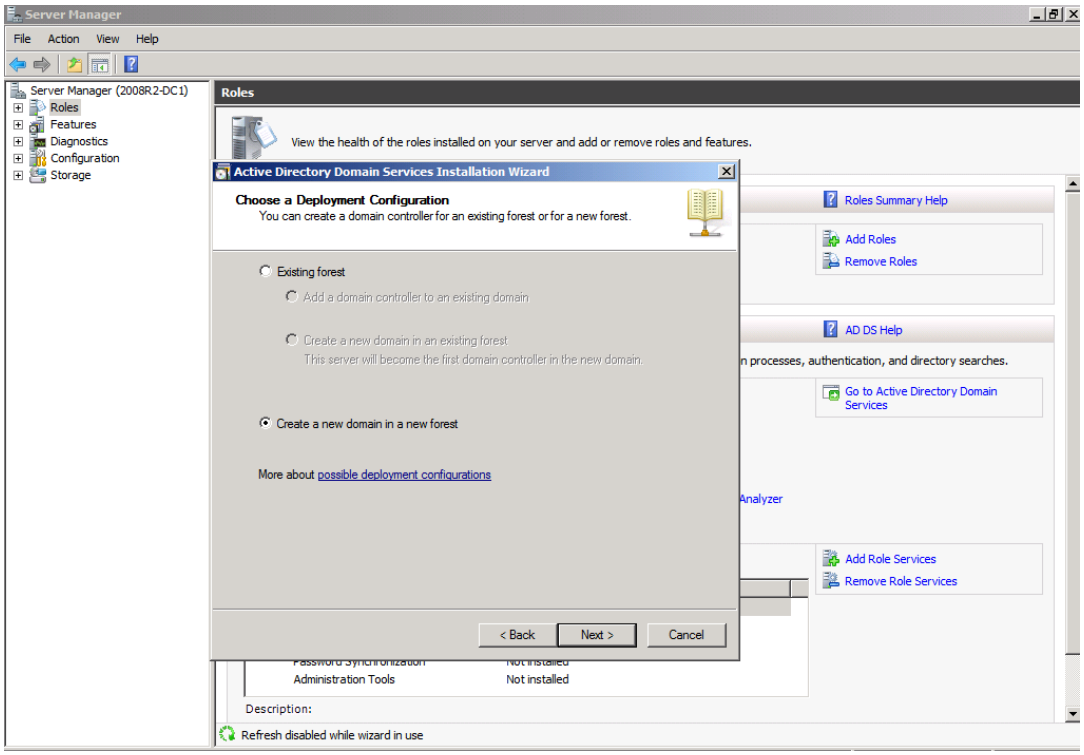

Рисунок 10. Выбор опции «Create a new domain in a new forest»

В открывшемся окне «Name the Forest Root Domain» («Имя корневого домена в лесу») необходимо ввести название домена в текстовое поле «FQDN» корневого домена в лесу. Имя домена может быть любым, но если будет выбрано имя, которое уже было зарегистрировано, то могут возникнуть проблемы раздвоения имен. После ввода имени домена необходимо нажать кнопку «Next» («Далее») (см. рис. 11).

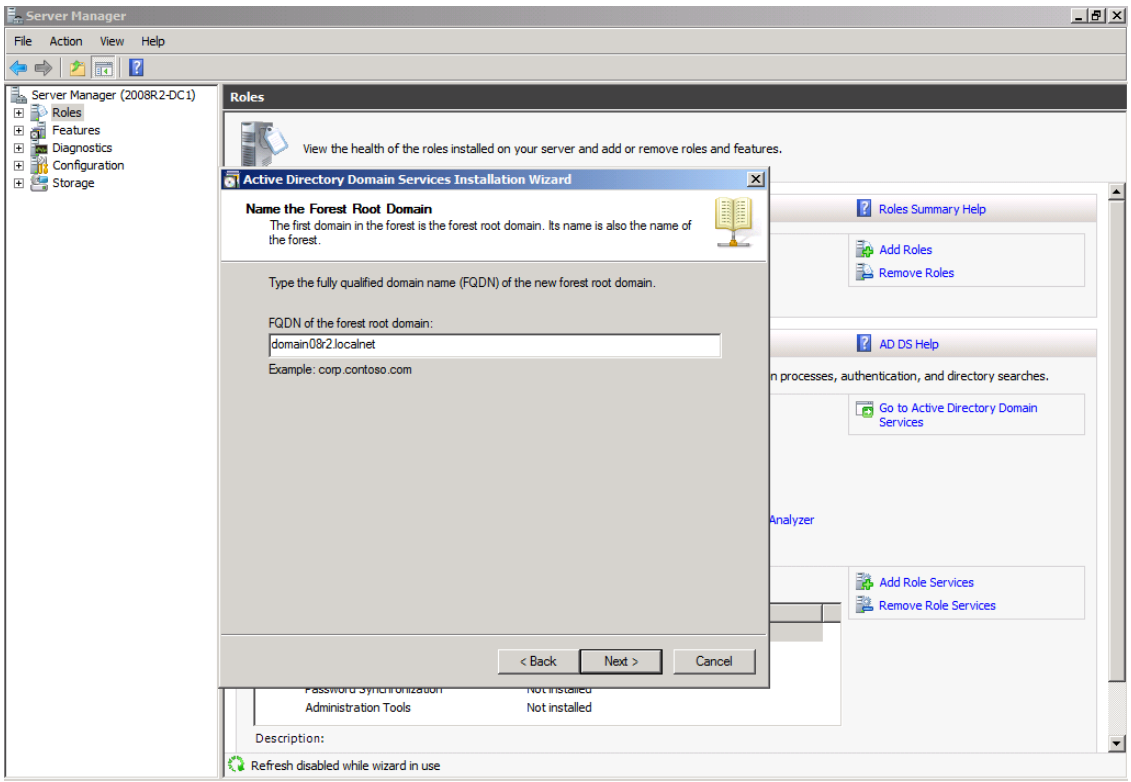

Рисунок 11. Ввод названия домена в текстовое поле FQDN

В открывшемся окне «Set Forest Functional Level» («Определение функционального уровня леса») необходимо выбрать опцию «Windows Server 2008 R2» и нажать кнопку «Next» («Далее») (см. рис. 12).

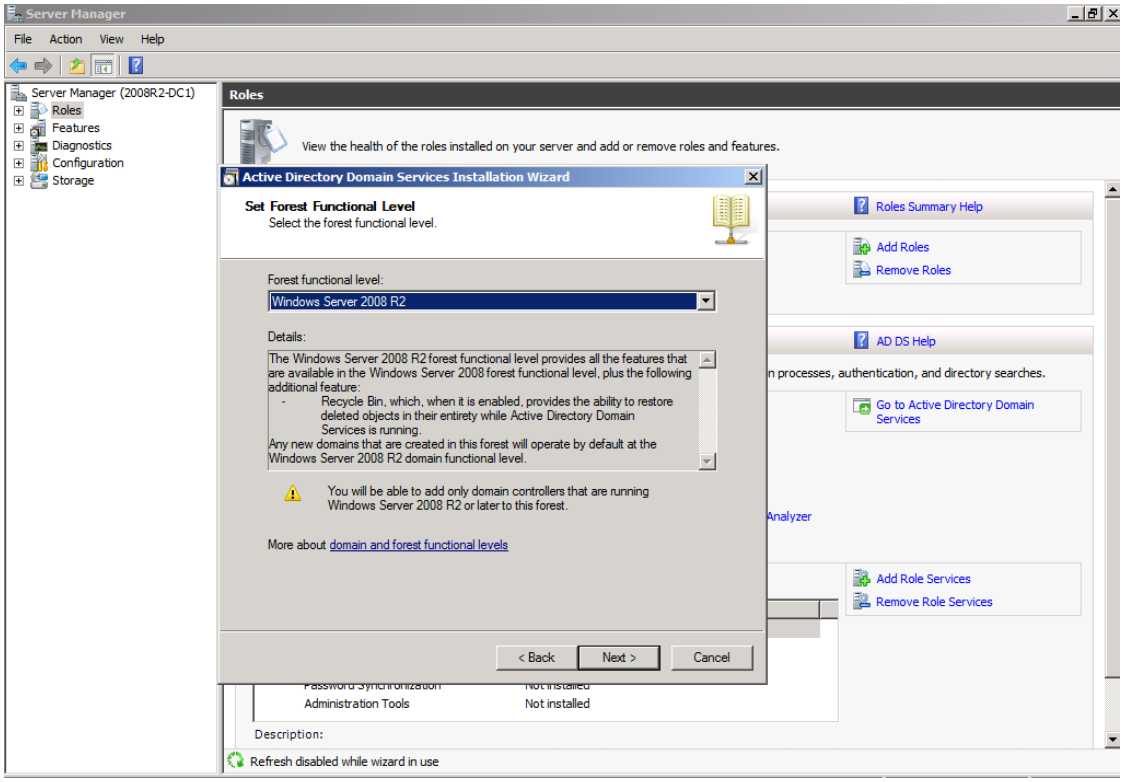

Рисунок 12. Выбор опции Windows Server 2008 R2

В окне «Additional Domain Controller Options» («Дополнительные опции контроллера домена») для выбора будет доступен «DNS сервер». Опция глобального каталога выбрана и не является опцией по выбору, так как пока что это единственный DC в этом домене, поэтому он должен быть сервером глобального каталога. Опция контроллера домена с разрешением только чтения (Read-only domain controller – RODC) не отмечена, поскольку необходимо иметь другой не-RODC в сети, чтобы включить эту опцию. Необходимо выбрать опцию DNS сервер и нажать кнопку «Next» («Далее») (см. рис. 13).

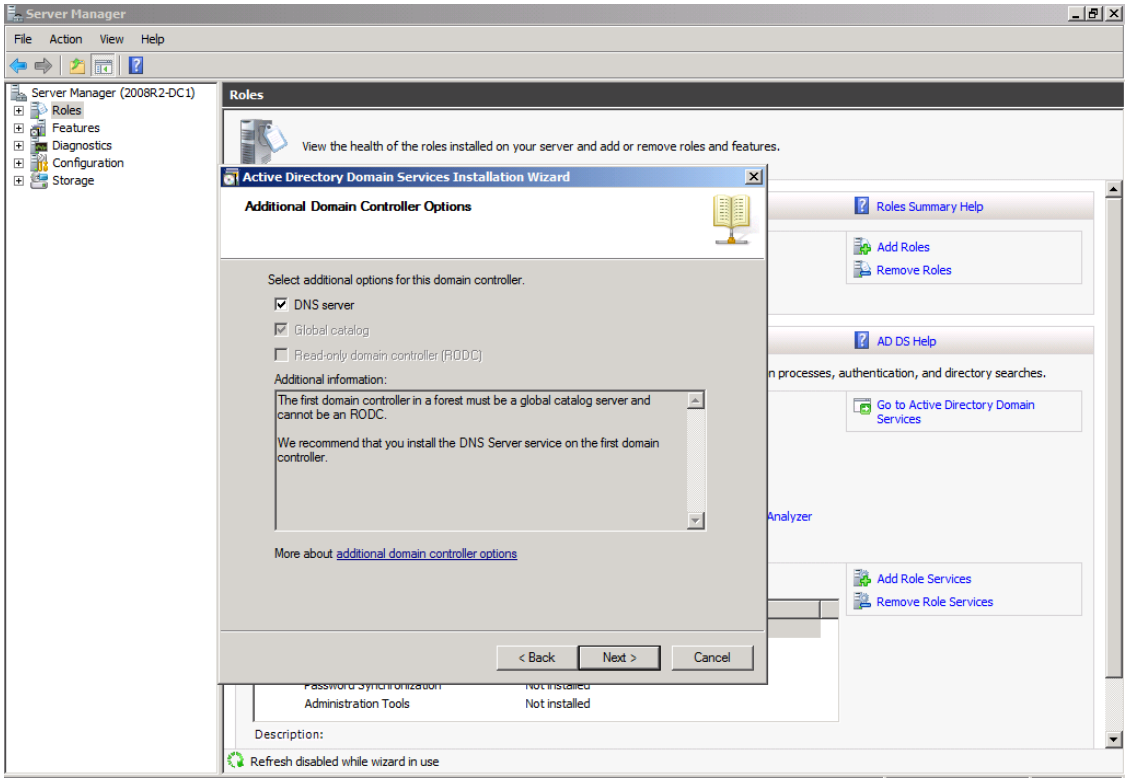

РИСУНОК 13. ВЫБОР ОПЦИИ «DNS СЕРВЕР»

Откроется диалоговое окно, информирующее о том, что невозможно создать делегирование для этого сервера DNS, поскольку полномочная родительская зона не может быть найдена или не использует Windows DNS сервер. Причина в том, что это первый DC в сети. Необходимо нажать кнопку «Yes» («Да»), чтобы продолжить настройку (см. рис. 14).

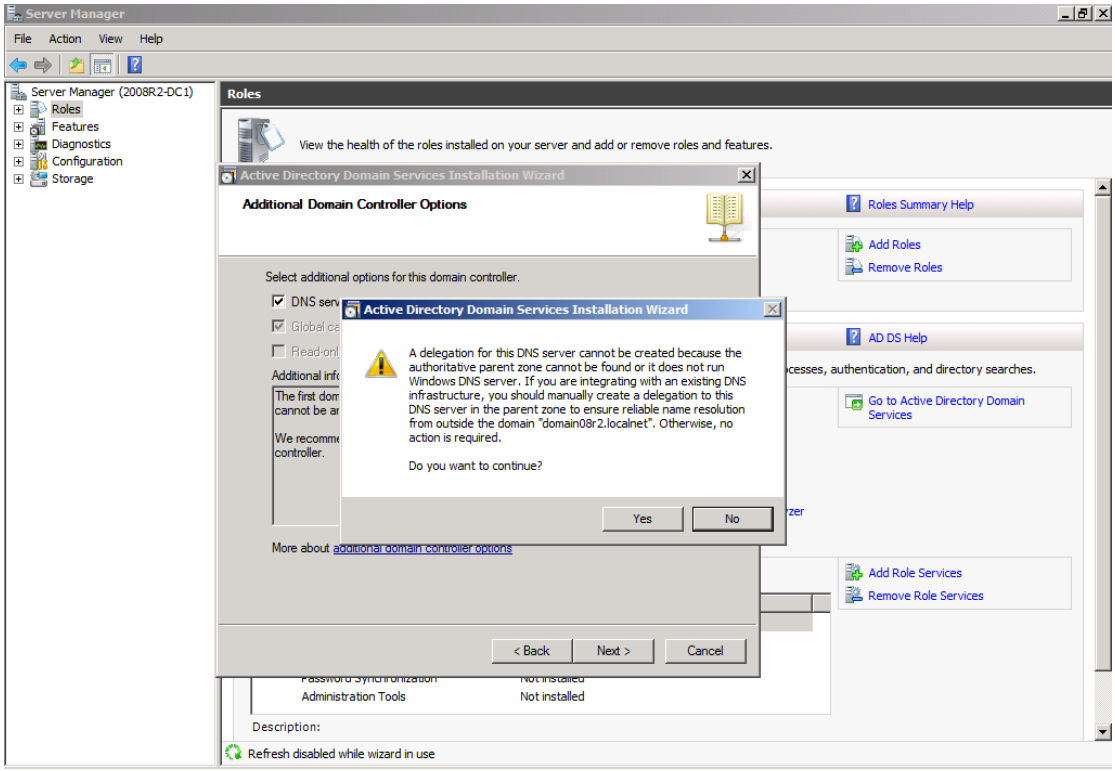

Рисунок 14. Предупреждение мастера

В открывшемся диалоговом окне необходимо оставить все настройки по умолчанию и нажать кнопку «Next» («Далее») (см. рис. 15).

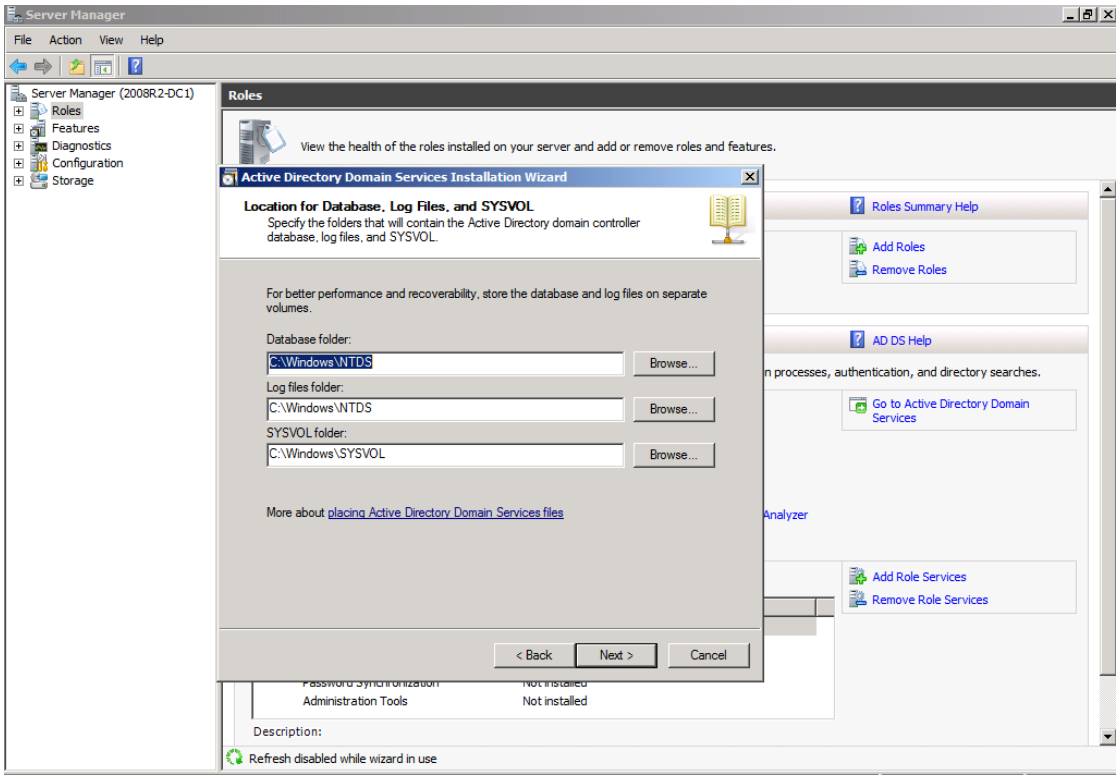

Рисунок 15. Окно выбора мест хранения информации

В открывшемся окне «Directory Service Restore Mode Administrator Password» («Служба каталогов администратора режима восстановления пароля») необходимо ввести надежный пароль в текстовые поля «Password» («Пароль») и «Confirm password» («Подтверждение пароля»), для того чтобы продолжить настройку следует нажать кнопку «Next» («Далее») (см. рис. 16).

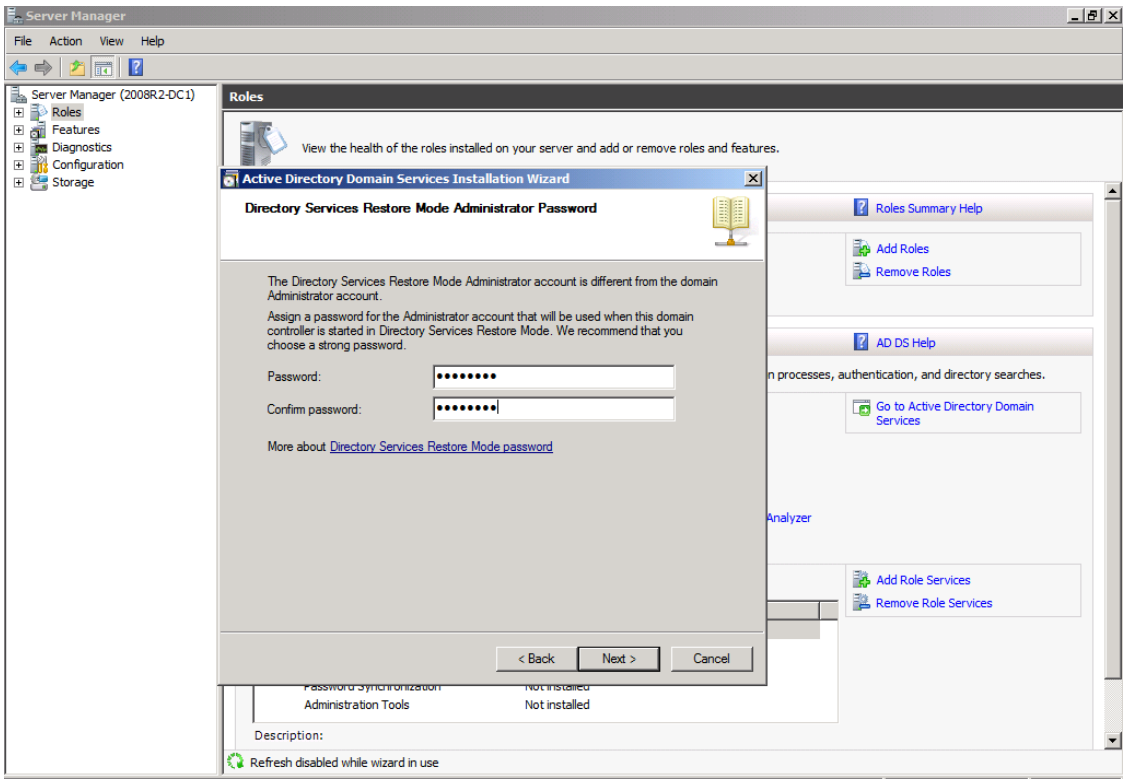

Рисунок 16. Ввод пароля

Необходимо проверить информацию в открывшемся окне «Summary» («Основная информация») и нажать кнопку «Next» («Далее») (см. рис. 17).

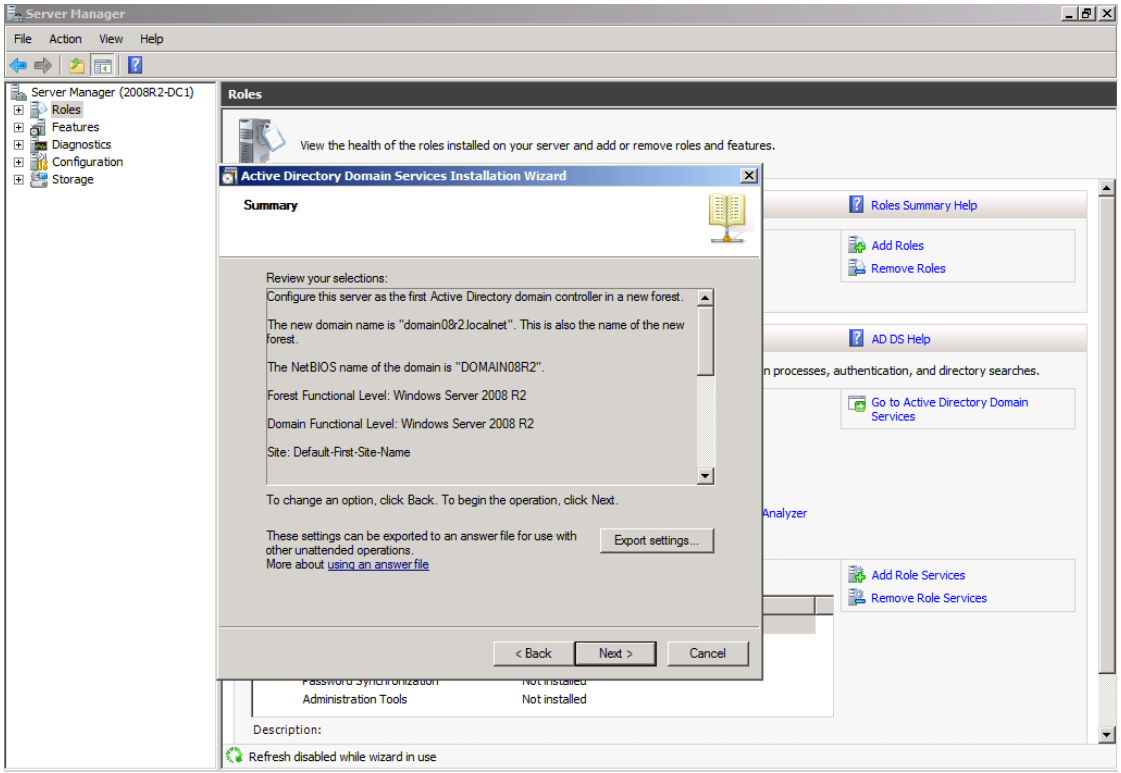

Рисунок 17. Проверка информации в окне «Summary»

Установка первого DC занимает, как правило, немного времени. Необходимо отметить опцию «Reboot on completion» («Перезагрузить по окончании») в окне «Active Directory Domain Services Installation Wizard» («Мастер установки сервисов домена»), и нажать кнопку «Cancel» чтобы машина автоматически перезагрузилась после установки DC (см. рис. 18).

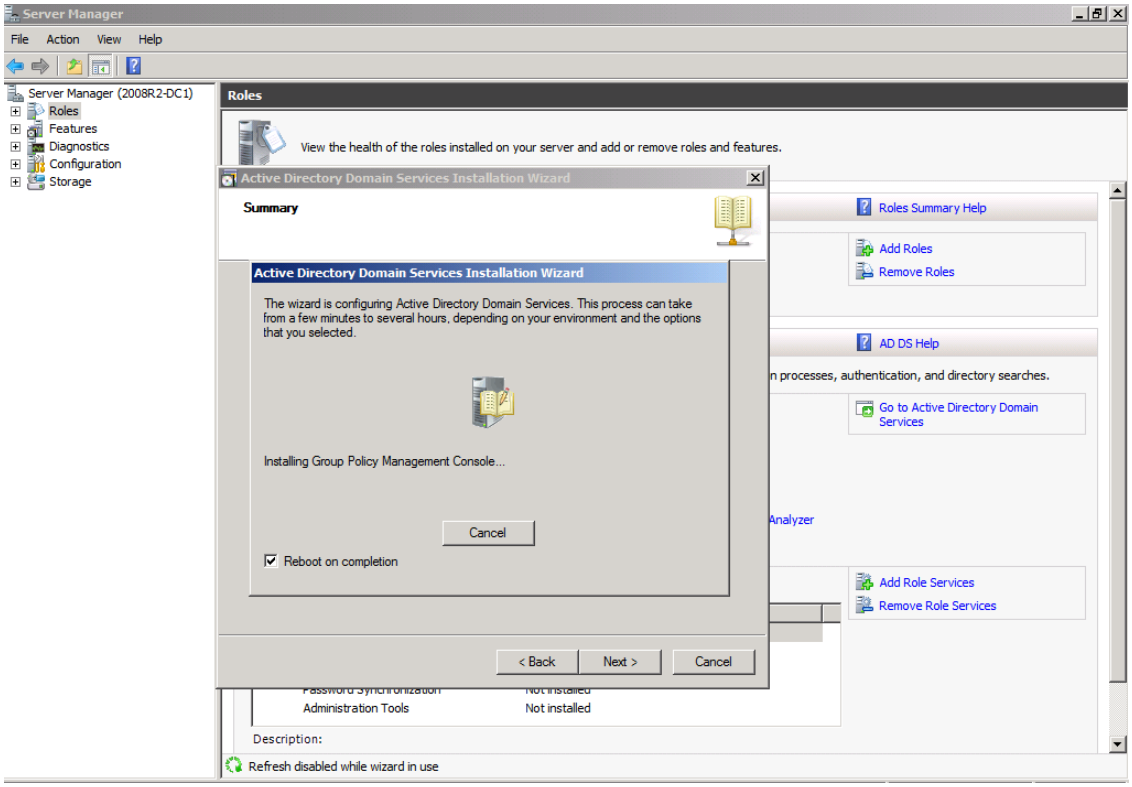

Рисунок 18. Отметка о необходимости перезагрузки

Произойдет перезагрузка сервера. Установка будет завершена после входа в систему.

Настройка ведения электронного журнала объектов

По умолчанию для клиентских систем аудит отключен, для серверных активна подкатегория «Доступ к службе каталогов Active Directory», остальные отключены. Для включения глобальной политики «Audit directory service access» («Аудит доступа к службе каталогов») необходимо вызвать «Редактор управления групповыми политиками», перейти в ветку «Параметры безопасности»/ «Локальные политики»/ «Политика аудита», где активировать политику и установить контролируемые события (успех, отказ) (см. рис.19).

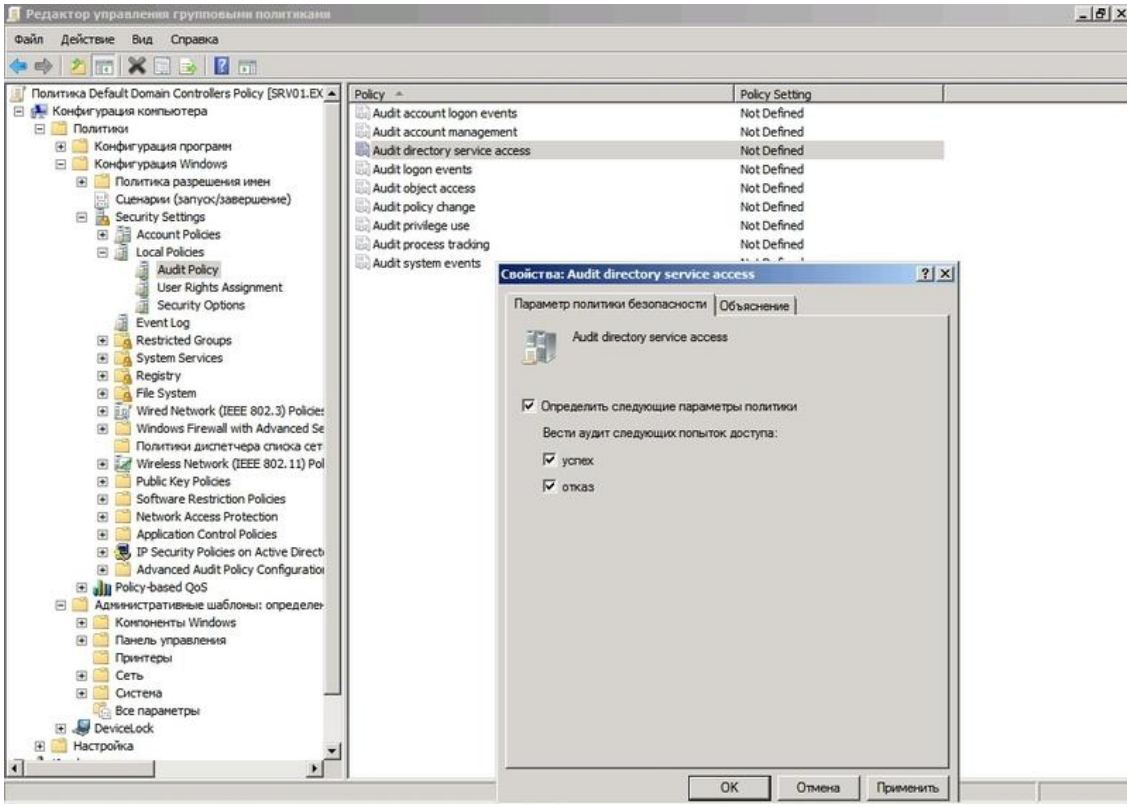

Рисунок 19. Активация политики аудита и выбор контролируемых событий

Другой вариант — использовать для настройки утилиту командной строки «auditpol» (см. рис. 20), получить полный список GAP с установленными параметрами. При помощи командной строки «auditpol» достаточно ввести команду:

```
> auditpol /list /subcategory:*
```

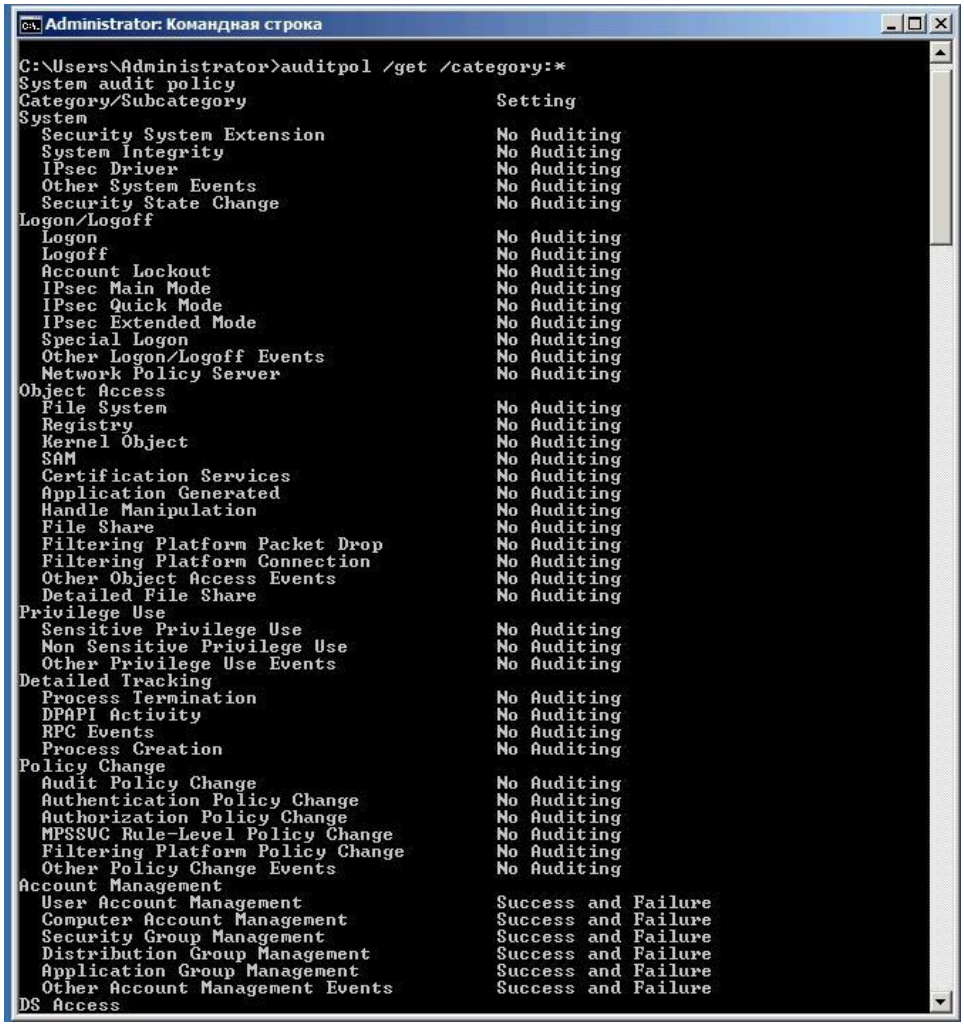

РИСУНОК 20. ВКЛЮЧЕНИЕ ПОЛИТИКИ АУДИТА ЧЕРЕЗ УТИЛИТУ КОМАНДОЙ СТРОКИ «AUDITPOL»

Активировать политику «directory service access»:

```
> auditpol /set /subcategory:"directory service changes" /success:enable
```

Обновить политику контролера домена:

```
> gpupdate
```

Подкатегория политики аудита «Доступ к службе каталогов» формирует события в журнале безопасности с кодом 4662, которые можно просмотреть при помощи консоли «Просмотр событий» («Event Viewer») вкладка «Журналы Windows – Безопасность» (см. рис. 21).

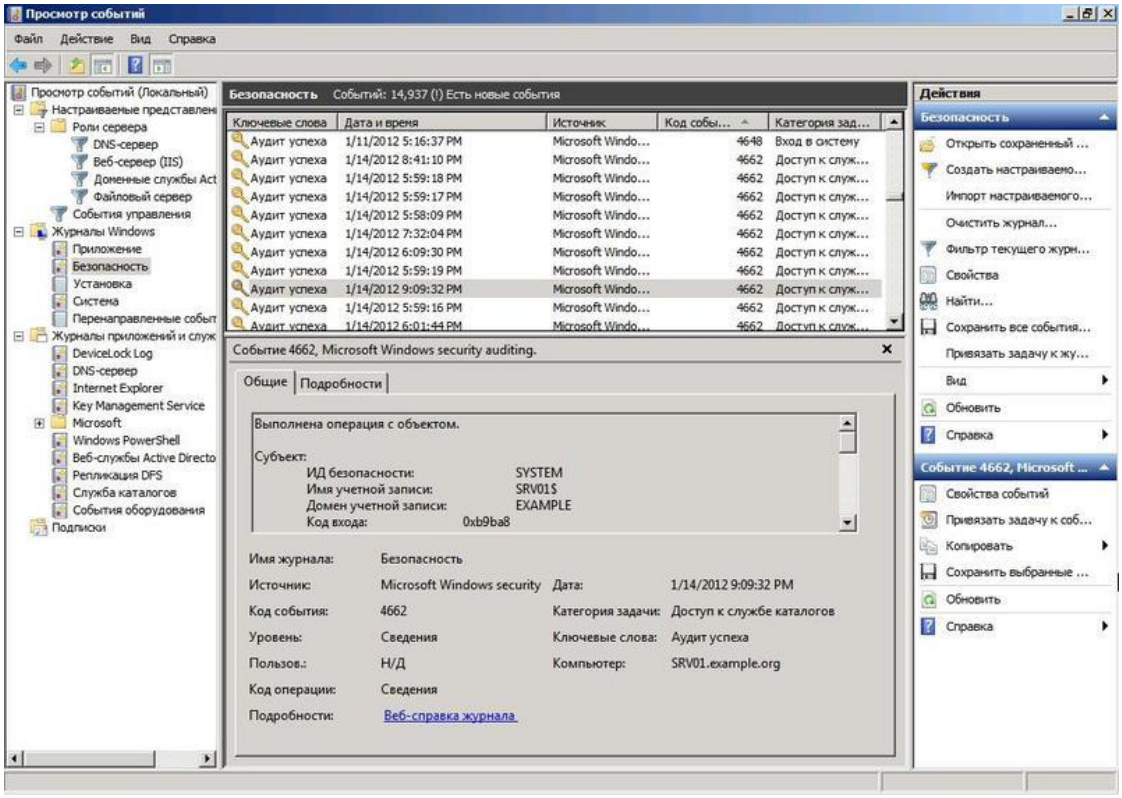

Рисунок 21. Просмотр событий

В качестве альтернативного варианта просмотра событий необходимо использовать командлет «Get-EventLog» оболочки «PowerShell» (см. рис. 22). Например:

```
PS> Get-EventLog security | ?{$_.eventid -eq 4662}
```

Командлет «Get-EventLog» может принимать 14 параметров, позволяющих отфильтровать события по определенным критериям:

- «After»;
- «AsBaseObject»;
- «AsString»;
- «Before»;
- «ComputerName»;
- «EntryType»;
- «Index»;
- «InstanceID»;
- «List»;
- «LogName»;
- «Message»;
- «Newest»;
- «Source»;
- «UserName».

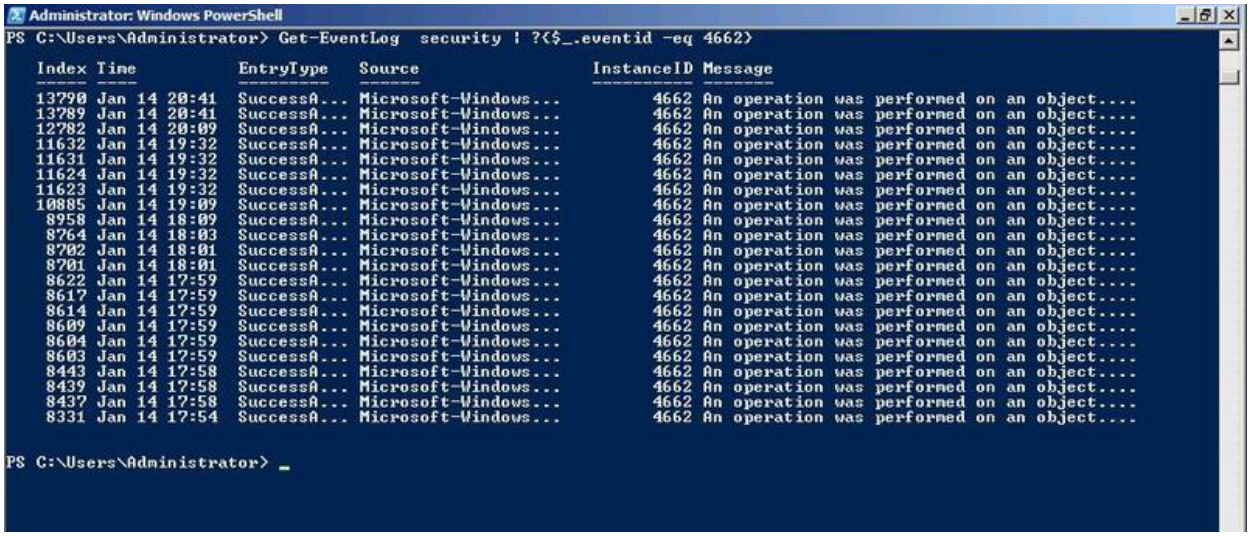

Рисунок 22. Просмотр событий с использованием оболочки PoweShell

Кроме события с кодом 4662, регистрируется ряд других событий 5136 (изменение атрибута), 5137 (создание атрибута), 5138 (отмена удаления атрибута) и 5139 (перемещение атрибута).

Для удобства отбора определенных событий в консоли «Просмотр событий» используют фильтры и настраиваемые представления, а также подписку, позволяющую собирать данные журналов и с других серверов.

В ветке «Политика аудита» также активируются следующие возможности:

- аудит входа/выхода в систему;
- аудит управления учетными записями;
- доступ к объектам;
- изменения политик и так далее.

Например, для настройки аудита доступа к объектам на примере папки с общим доступом, необходимо активировать, как описано ранее, политику «Audit object access», затем выбрать папку и вызвать меню «Свойства папки», в котором необходимо перейти в подпункт «Безопасность» и нажать кнопку «Дополнительно». Теперь в открывшемся окне «Дополнительные параметры безопасности для..» перейти во вкладку «Аудит» и нажать кнопку «Изменить» и затем «Добавить» и указать учетную запись или группу, для которой будет осуществляться аудит. Далее необходимо отметить отслеживаемые события (выполнение, чтение, создание файлов и др.) и результат (успех или отказ). При помощи списка «Применять» указать область применения политики аудита. После чего необходимо подтвердить изменения (см. рис. 23).

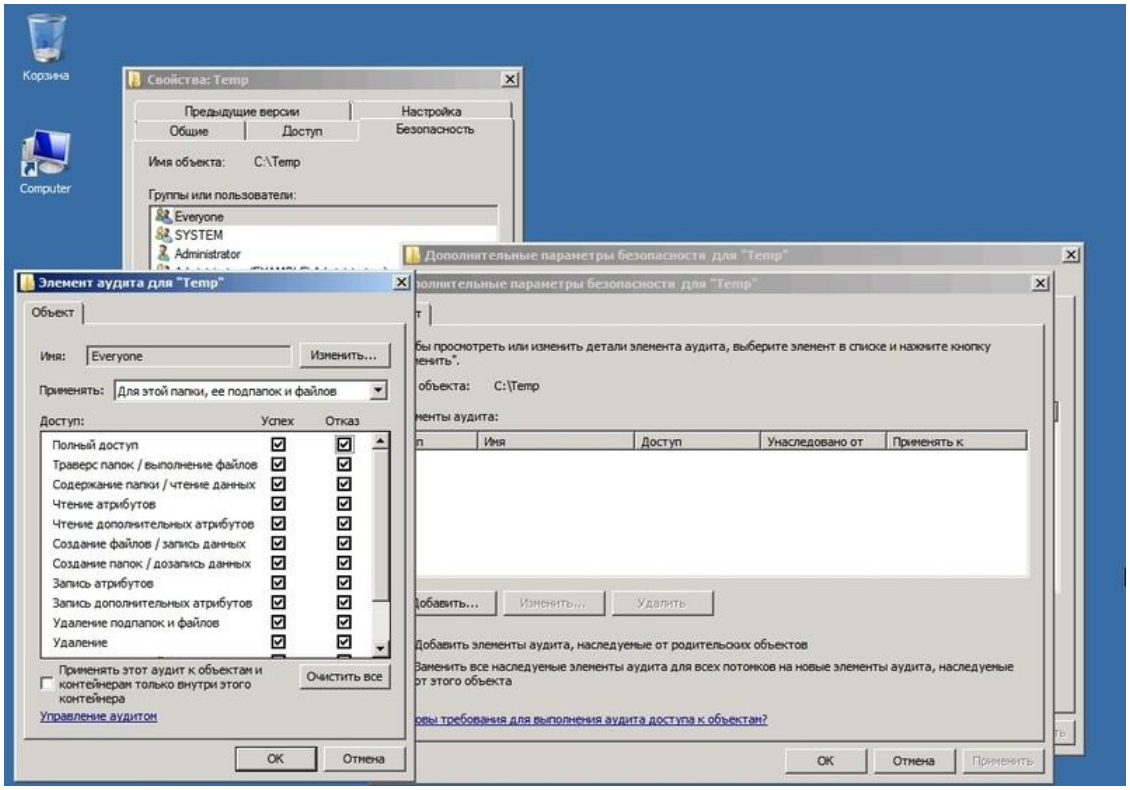

РИСУНОК 23. АУДИТ ДОСТУПА К ОБЪЕКТАМ НА ПРИМЕРЕ ПАПКИ С ОБЩИМ ДОСТУПОМ

Теперь все указанные операции будут отображаться в журнале безопасности.

Чтобы упростить настройку аудита при большом количестве объектов, следует активировать флажок «Наследование параметров от родительского объекта». При этом в поле «Унаследовано от» будет показан родительский объект, от которого взяты настройки.

Больший контроль событий, записываемых в журнал, достигается применением политики детализированного аудита (Granular Audit Policy), которая настраивается в «Параметры безопасности/Локальные политики/Advanced Audit Policy Configuration». В настройках указаны следующие 10 подпунктов (см. рис. 24):

- вход учетной записи – аудит проверки учетных данных, службы проверки подлинности «Kerberos», операции с билетами службы «Kerberos», другие события входа;
- управление учетными записями – аудит управления группами приложений, учетными записями компьютеров и пользователей, группами безопасности и распространения;
- подробное отслеживание – событий RPC и DPAPI, создания и завершения процессов;
- доступ к службе каталогов DS – аудит доступа, изменений, репликации и подробной репликации службы каталогов;

- вход/выход – аудит блокировки учетных записей, входа и выхода в систему, использования IPSec, сервера политики сети;
- доступ к объектам – аудит объектов ядра, работы с дескрипторами, событий создаваемых приложениями, служб сертификации, файловой системы, общих папок, платформой фильтрации;
- изменение политики – изменения политики аудита, проверки подлинности, авторизации, платформы фильтрации, правил службы защиты MPSSVC и другие;
- использование прав – аудит прав доступа к различным категориям данных;
- система – аудит целостности системы, изменения и расширения состояния безопасности, драйвера IPSec и других событий;
- аудит доступа к глобальным объектам – аудит файловой системы и реестра.

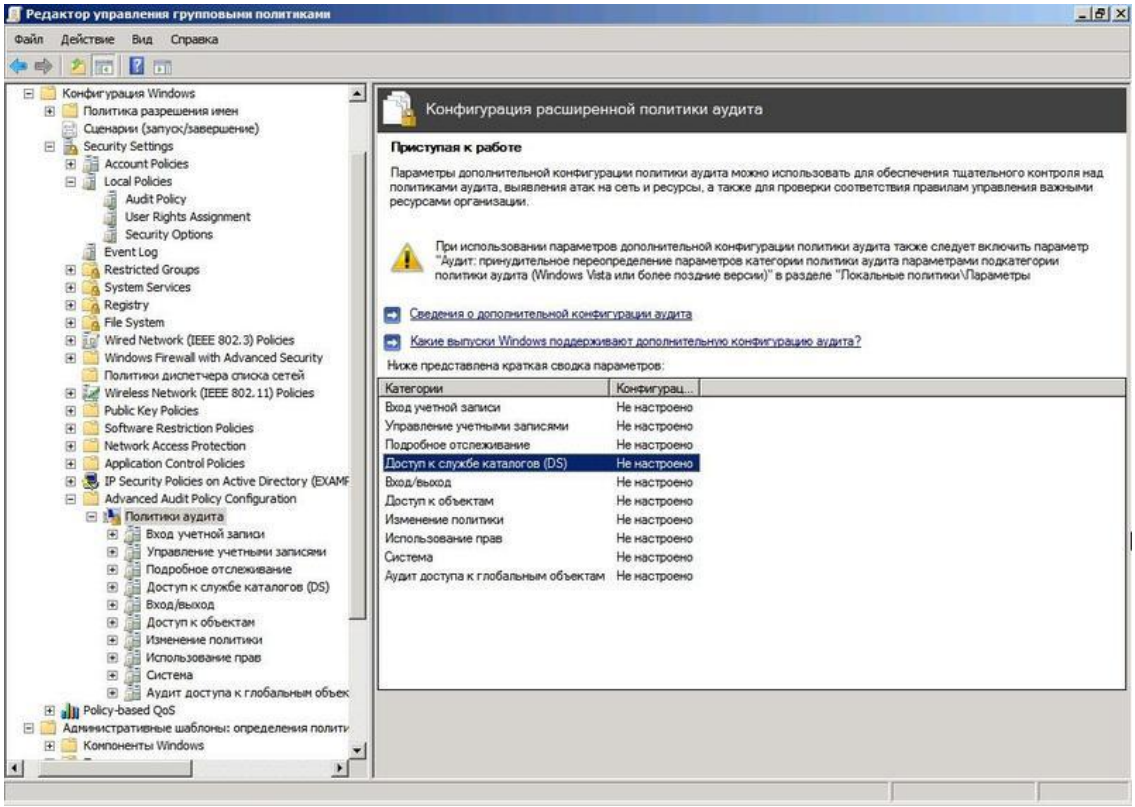

РИСУНОК 24. ДОСТУПНЫЕ НАСТРОЙКИ ADVANCED AUDIT POLICY CONFIGURATION

Настройка политики паролей

Контроль за политикой паролей пользователей (сложность пароля, минимальная длина и т.д.) является одной из важных задач для администраторов. Ниже подробно описано изменение политики паролей с помощью GPO для всех пользователей домена.

Политика паролей домена конфигурируется объектом GPO - «Default Domain Policy», которая применяется для всех компьютеров домена. Для того что бы

посмотреть или внести изменения в политику паролей, необходимо запустить оснастку «Управление групповой политикой», в иерархии найти «Default Domain Policy» (Политика домена по умолчанию), нажать на ней правой кнопкой мыши и в меню выбрать поле «Edit» («Изменить») (см. рис. 25).

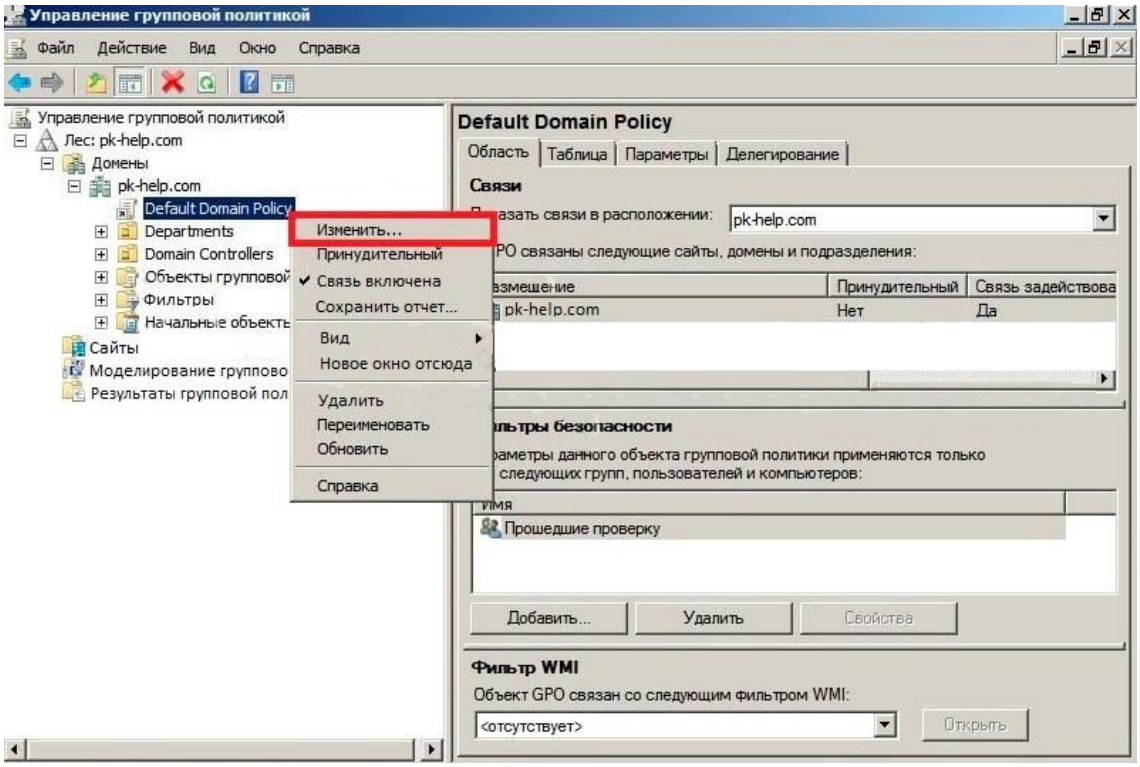

РИСУНОК 25. КОНСОЛЬ «УПРАВЛЕНИЕ ГРУППОВОЙ ПОЛИТИКОЙ»

Откроется консоль «Редактор объектов групповой политики» («Group Policy Object Editor»), в окне которой будет выбрана политика «Default Domain Policy» (см. рис. 26). Необходимо раскрыть следующие узлы:

- «Конфигурация компьютера» («ComputerConfiguration»);
- «Конфигурация Windows» («WindowsSettings»);
- «Параметры безопасности» («SecuritySettings»);
- «Политика паролей» («Account Policies»).

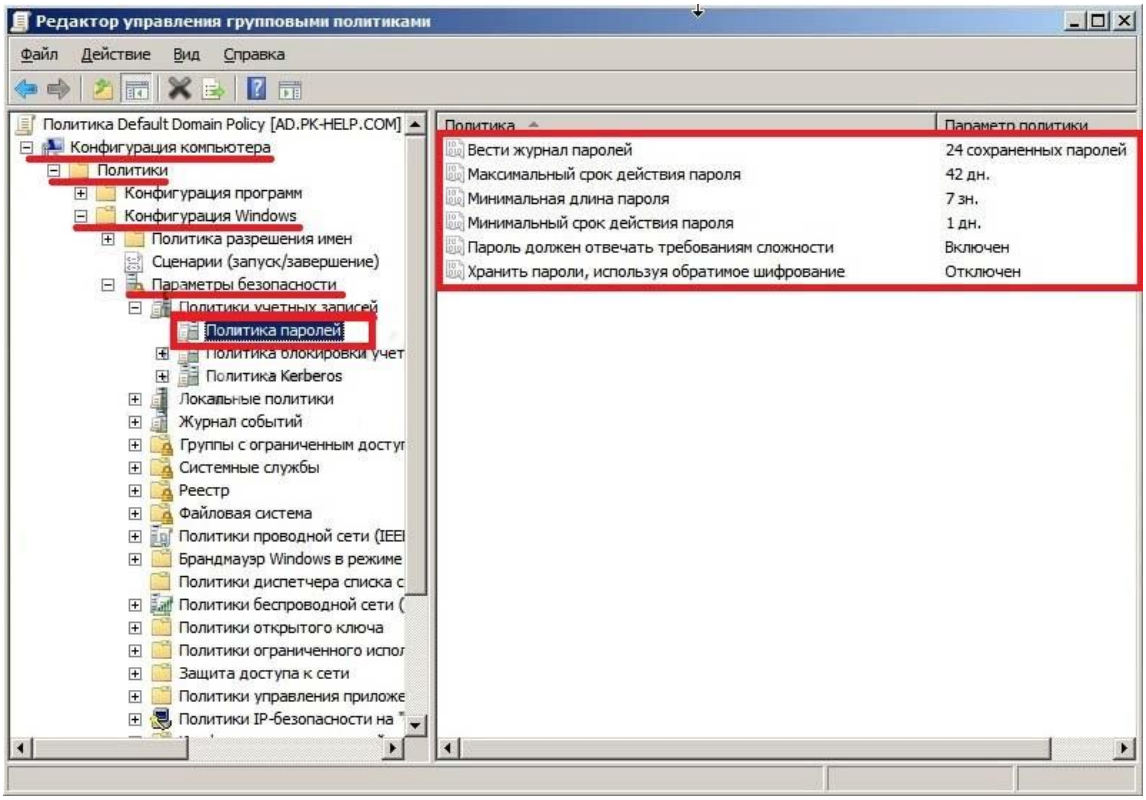

Рисунок 26. Консоль «Редактор объектов групповой политики»

В таблице 1 «Политика паролей учетной записи» представлен перечень доступных политик паролей («Password Policy»).

Таблица 1. Политика паролей учетной записи

Политика	Описание	Возмож. значения	Реком. значение
Неповторяемость паролей (Enforce Password History)	Когда политика включена, Active Directory хранит список недавно использованных паролей и не разрешает пользователю задавать пароль из этого списка. В результате, когда пользователю предлагается сменить пароль, он не может повторно ввести тот же пароль, то есть увеличить срок его действия. Эта политика включена по умолчанию, причем максимальное значение для нее равно 24.	0-24	5

Максимальный срок действия пароля (Maximum Password Age)	Эта политика определяет, когда пользователю необходимо сменить пароль. Неизменные или редко изменяемые пароли более уязвимы, и злоумышленники могут использовать их для доступа под существующей учетной записью. Значение по умолчанию — 42 дня.	1-999	60
Минимальный срок действия пароля (Minimum Password Age)	Когда пользователю необходимо сменить пароль, то, даже если включена история паролей, он может просто несколько раз изменить пароль, чтобы обойти требования и снова ввести исходный пароль. Политика «*Минимальный срок действия пароля*» предотвращает такую ситуацию, требуя, чтобы между сменами паролей проходило определенное количество дней. Конечно, администратор или сотрудник службы поддержки с соответствующими разрешениями может в любое время сменить пароль в Active Directory. Но пользователю запрещено менять пароль более одного раза в течение указанного в этом параметре периода времени	0-998	1
Минимальная длина пароля (Minimum Password Length)	Эта политика задает минимальное количество символов в пароле. По умолчанию в пароле должно быть 7 символов.	0- без пароля 1-14	5
Пароль должен отвечать требованиям сложности	Эта политика включает правила (фильтры) для новых паролей. В Windows Server 2003 требования фильтра	Включена/ Отключена	Отключена

(Passwords Must Meet Complexity Requirements)	паролей по умолчанию (passfilt.dll) следующие: ○ пароль не должен быть основан на имени учетной записи пользователя; ○ в пароле должно быть не менее 6 символов; ○ пароль должен содержать символы следующих типов (минимум три): ▪ заглавные алфавитные символы (A ... Z); ▪ строчные алфавитные символы (a ... z); ▪ арабские цифры (0...9); ▪ не алфавитно-цифровые символы (например ! $ # , %). По умолчанию в Windows Server 2003 эта политика включена		
Хранение паролей с использованием обратимого шифрования (Store passwords using reversible encryption)	Параметр указывает использовать ли операционной системой для хранения паролей обратимое шифрование.	Включена/ Отключена	Отключена

Для того что бы изменить параметр достаточно нажать на него левой кнопкой мыши и указать значение. Изменение требований к длине и сложности паролей не влияет на существующие пароли. После включения этих политик, изменения будут влиять только на новые учетные записи и изменяемые пароли.

Настройка политики блокировки учетной записи

В общем смысле блокировка учетных записей подразумевает, что после нескольких неудачных попыток входа в систему та должна решить, что злоумышленник пытается подобрать пароль, чтобы воспользоваться учетной записью, и в целях безопасности заблокировать эту учетную запись и пресечь дальнейшие попытки входа в систему. Политики блокировки учетных записей определяют предел для не авторизованных входов в систему, то есть количество

неудачных попыток за период времени и требования, выполнение которых позволит разблокировать учетную запись, — пользователю придется просто подождать или обратиться к администратору.

Политика блокировки учетной записи конфигурируется объектом GPO- «Default Domain Policy», которая применяется для всех компьютеров домена. Для того что бы посмотреть или внести изменения в политику, необходимо запустить оснастку «Управление групповой политикой», найти «Default Domain Policy», нажать на ней правой кнопкой мыши и в открывшемся меню выбрать «Изменить» («Edit») (см. рис. 3.25).

Откроется консоль «Редактор объектов групповой политики» («Group Policy Object Editor»), в окне которой будет выбрана политика «Default Domain Policy» (см. рис. 3.26). Необходимо раскрыть следующие узлы:

- «Конфигурация компьютера» («ComputerConfiguration»);
- «Конфигурация Windows» («WindowsSettings»);
- «Параметры безопасности» («SecuritySettings»);
- «Политика паролей» («Account Policies»).

В таблице 2 приведены политики блокировки учетной записи («Account Policies»).

ТАБЛИЦА 2. ПОЛИТИКИ БЛОКИРОВКИ УЧЕТНОЙ ЗАПИСИ

Политика	Описание	Возмож. значения	Реком. значение
Пороговое значение блокировки (Account Lockout Threshold)	Задает количество неудачных попыток входа в систему, влекущее блокировку учетной записи. Если указано слишком маленькое пороговое значение (например, три), учетные записи могут блокироваться из-за обычных ошибок. Если значение равно 0, учетные записи не блокируются никогда. Значение счетчика блокировки не изменяется при попытке входа в систему на заблокированных рабочих станциях	0 до 999	5
Блокировка учетной записи	Определяет период времени, который должен	0 до 99 999 минут	0

на (Account Lockout Duration)	пройти после блокировки до того, как Active Directory автоматически разблокирует учетную запись пользователя. Эта политика не включается по умолчанию, и ее полезно использовать только в сочетании с политикой «Пороговое значение блокировки» (Account Lockout Threshold). Хотя допустимыми являются значения от 0 до 99 999 минут, то есть около 10 недель, небольшие значения (от 5 до 15 минут) могут существенно снизить количество атак, причем пользователи, заблокированные по ошибке, не будут при этом испытывать серьезных неудобств. Если выбрано значение 0, пользователю следует обратиться к администратору, для разблокировки учетной записи вручную.		
Сброс счетчика блокировки через (Reset Account Lockout Counter After)	Этот параметр указывает время, которое должно пройти после неудачной попытки входа в систему до того, как значение счетчика будет сброшено до 0. Допустимые значения — от 1 до 99 999 минут, причем значение параметра должно быть меньше или равно продолжительности блокировки учетной записи	1 до 99 999	10

Для того что бы изменить параметр достаточно нажать на него правой кнопкой мыши и указать новое значение.

Настройка периода синхронизации даты последнего входа пользователя в систему

Дата последнего входа пользователя в систему в модуле ОИБ определяется по параметру Active Directory «LastLogonTimestamp». Параметр «LastLogonTimestamp» - хранит последнюю дату входа пользователя, по умолчанию обновляемую каждые 9 - 14 дней. За период актуализации параметра отвечает системный параметр - «msDS-LogonTimeSyncInterval». Чтобы дата последнего входа пользователя обновлялась каждый день необходимо указать системному параметру Active Directory «msDS-LogonTimeSyncInterval» значение равное 1.

Для того, что бы задать значение параметра «msDS-LogonTimeSyncInterval» необходимо запустить редактор интерфейсов служб Active Directory «ADSIEDIT.MSC» (перейти в меню «Пуск» и в текстовом поле «Выполнить» ввести «ADSIEDIT.MSC» (см. рис. 27)).

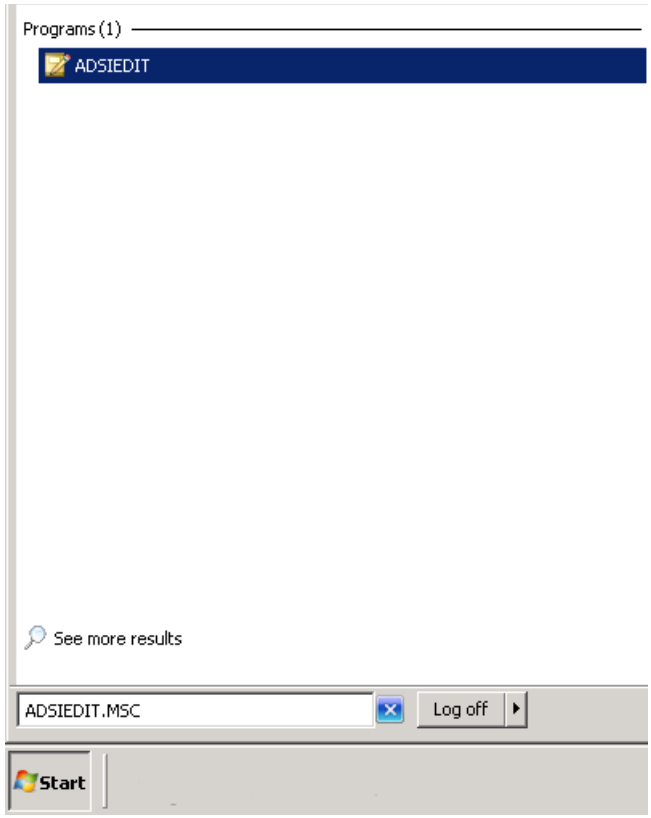

Рисунок 27. Переход в меню «Пуск» и ввод «ADSIEDIT.MSC» в текстовом поле «Выполнить»

После запуска оснастки «ADSIEDIT.MSC» найти параметр «msDS-LogonTimeSyncInterval» и задать его значение. Для этого перейти в «Настройки» («Properties») (см. рис. 28).

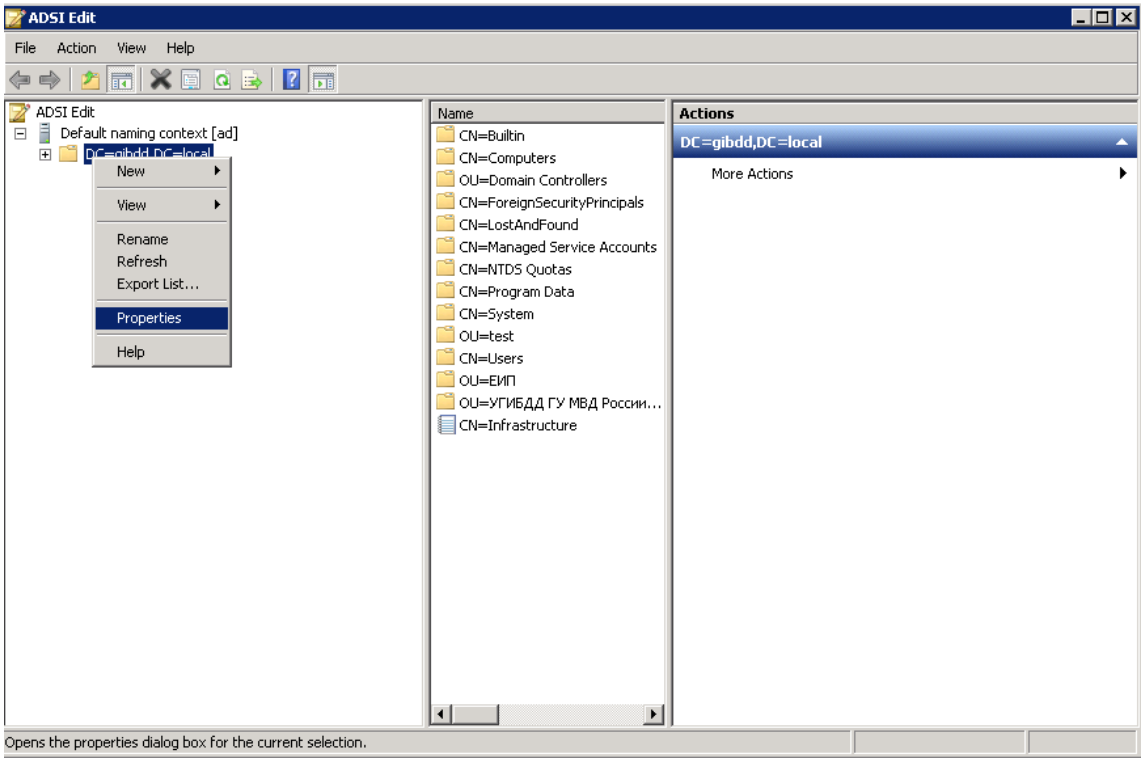

Рисунок 28. Редактор интерфейсов служб Active Directory «ADSIEDIT.MSC»

В открывшемся окне «Настройки» («Properties») указать значение параметра «msDS-LogonTimeSyncInterval» (см. рис. 29).

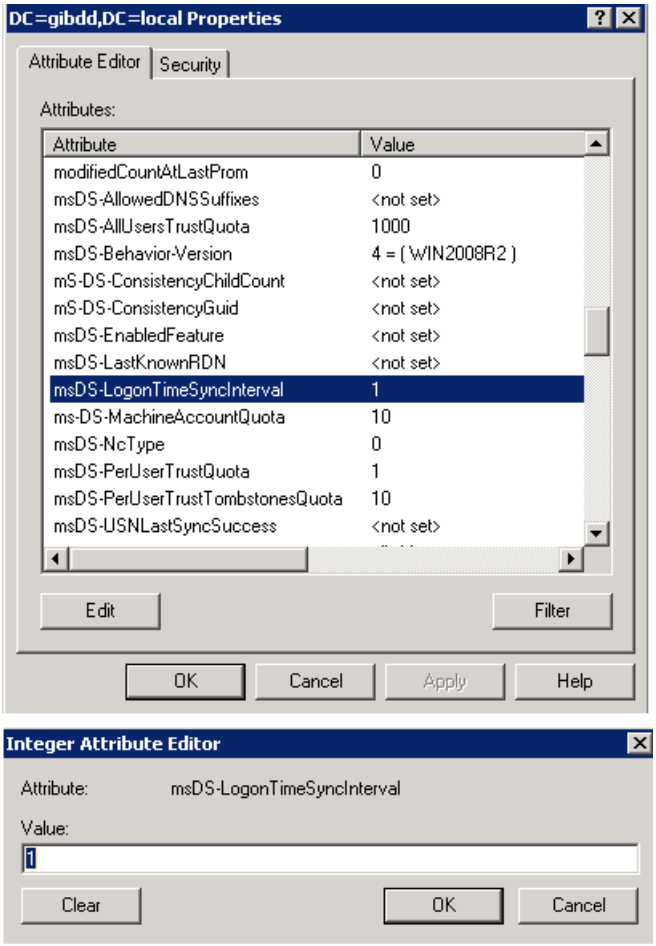

РИСУНОК 29. ЗАДАНИЕ ЗНАЧЕНИЯ ПАРАМЕТРА «MSDS-LOGONTIMESYNCINTERVAL»

Создание служебной учетной записи

Для доступа программного продукта к Active Directory требуется создать служебную учетную запись с добавлением ее в группу Domain Admins ("Администраторы домена").

Экспорт сертификата

Для экспорта сертификата из Active Directory рекомендуется воспользоваться утилитой JXplorer, дистрибутив которой можно скачать с сайта http://jxplorer.org/.

После запуска JXplorer, необходимо установить соединение с сервером LDAP (File → Connect), в открывшемся окне "Open LDAP/DSML Connection" указать настройки соединения, например:

Host	organization.ru
Port	636
Base DN	OU=Организация,DC=organization,DC=ru
Level	SSL + User + Password

User DN	CN=Ldap Manager,CN=Users,DC=organization,DC=ru
Password	5ecr3t

Подключиться к серверу, нажав на кнопку "OK".

Для того что бы извлечь сертификат, необходимо выполнить следующие действия:

- в верхней панели JXplorer перейти "Security" → "Trusted Servers and CAS";
- в открывшемся окне "Manage Your Trusteid Server Certificates" выделить сертификат, нажать на кнопку "View Certificate" (если в окне "Manage Your Trusteid Server Certificates" доступно несколько сертификатов, выбрать сертификат с именем владельца сертификата "cn=ad");
- в открывшемся окне "Certificate" перейти на вкладку "Detalis", сохранить сертификат в отдельную директорию, нажав на кнопку "Copy to file".

Установка и настройка JVM

Для функционирования программного продукта требуется JDK 8. Вы можете использовать ту, которая уже была установлена в вашу систему или можете скачать JDK с сайта Oracle по ссылке: http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html.

При установке JDK следует отказаться от установки JRE (см. рис. 30).

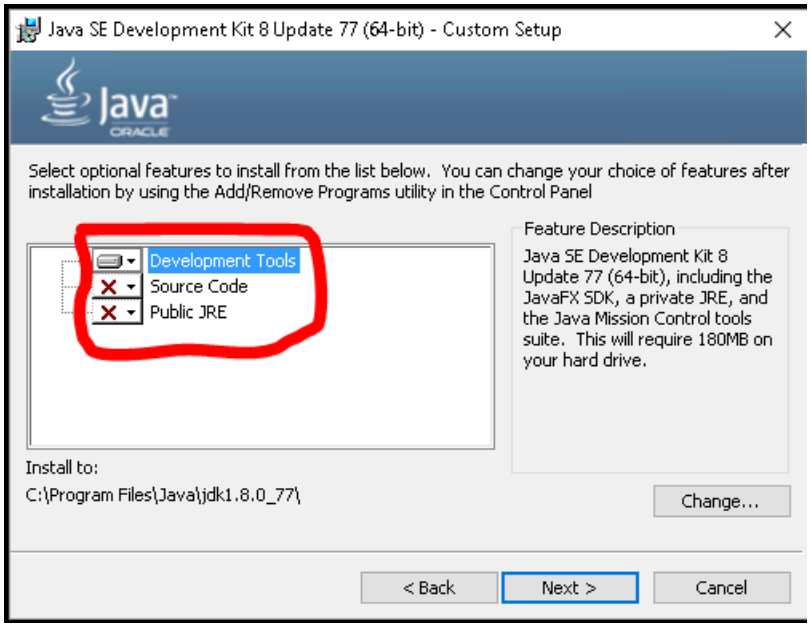

Рисунок 30. Установка JDK

Для корректной работы с часовыми поясами необходимо установить обновление Java SE Timezone Updater, скачать дистрибутив можно с сайта

Oracle http://www.oracle.com/technetwork/java/javase/downloads/tzupdater-download-513681.html.

Настройка переменной среды окружения

После установки JDK необходимо дополнительно настроить переменную окружения `JAVA_HOME`. Переменная окружения `JAVA_HOME` должна содержать путь установки JDK.

Для того, чтобы задать переменную окружения, необходимо выполнить следующие действия:

- перейти в блок "Дополнительные параметры системы" ("Пуск" → "Компьютер" → пункт контекстного меню "Свойства" → "Дополнительные параметры системы");
- в открывшемся окне "Свойства системы", на вкладке "Дополнительно" в блоке "Загрузка и восстановление" нажать на кнопку "Переменные среды".

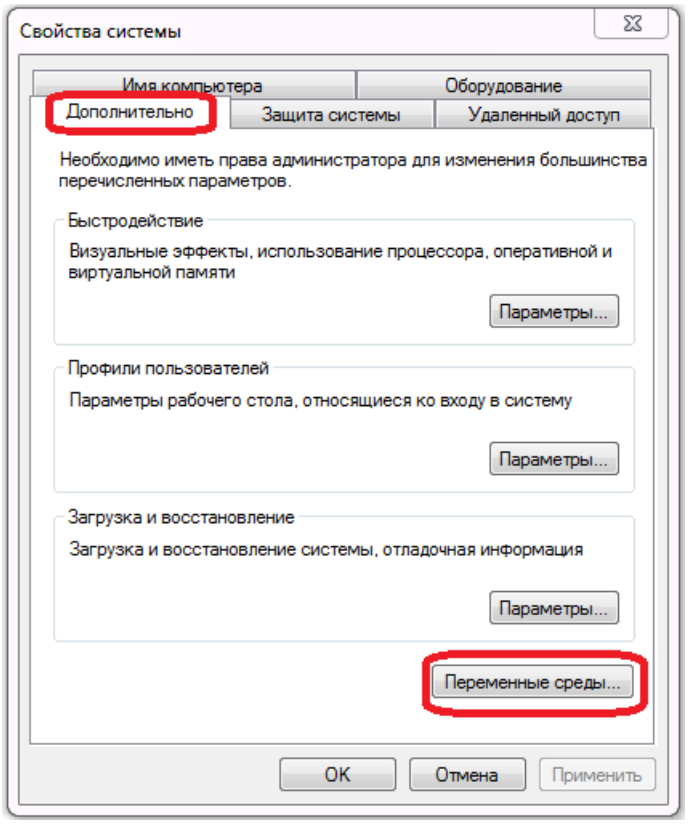

Рисунок 31. Настройка переменной окружения JAVA_HOME

В блоке "Системные переменные" задать переменную, выполнив следующие действия:

- нажать кнопку "Создать";

- в поле "Имя переменной" указать: JAVA_HOME;
- в поле "Значение переменной" указать путь до директории, в которой установлена JDK (например, C:\Program Files\Java\jdk1.8.0_77);
- сохранить изменения, последовательно нажав на кнопку "OK" в окнах "Создание системной переменой", "Переменные среды", "Свойства системы".

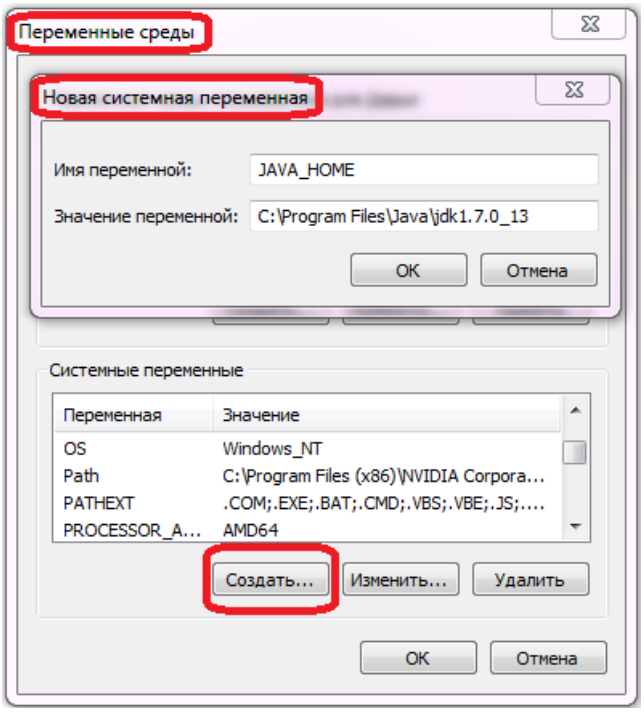

Рисунок 32. Настройка переменной окружения JAVA_HOME

Далее необходимо добавить в значение системной переменной PATH путь до исполняемого файла java.exe, для этого выполнить следующие действия (так же описание процесса настройки переменной среды окружения PATH для различных платформ Windows приведено здесь http://www.java.com/ru/download/help/path.xml):

- найти переменную PATH в окне "Переменные среды" в блоке "Системные переменные" ("Пуск" → "Компьютер" → пункт контекстного меню "Свойства" → "Дополнительные параметры системы" → в окне "Свойства системы" на вкладке "Дополнительно" нажать на кнопку "Переменные среды");
- выделить найденную переменную PATH курсором, нажать кнопку "Изменить";
- в открывшемся окне "Изменение системной переменной" поле "Значение переменной" дополнить записью о местоположении исполняемого файла:

```
;%JAVA_HOME%\bin
```

- сохранить изменения, последовательно нажав на кнопку "OK" в окнах "Изменение системной переменной", "Переменные среды", "Свойства системы".

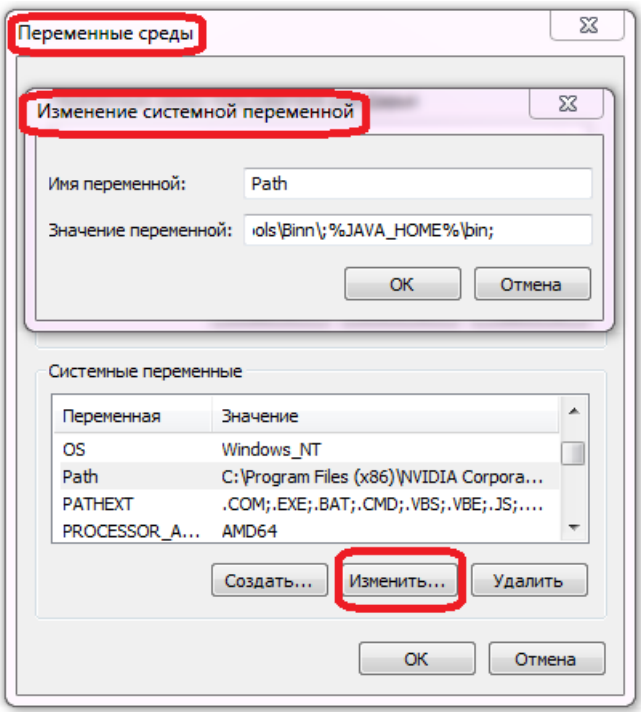

Рисунок 33. Настройка переменной окружения Path

При отсутствии элемента PATH, добавить новую переменную и указать PATH как имя переменной и местоположение исполняемого файла как значение переменной.

После того, как переменные окружения заданы, можно проверить корректность установки, выполнив в командной строке ("Пуск" → "Все программы" → "Стандартные" → "Командная строка") следующие команды:

```
echo %path% --в результате отобразится значение переменной.
echo %java home% --в результате отобразится значение переменной.
java -version --в результате отобразится номер версии установленного программного
обеспечения.
```

Установка дистрибутива

Создание рабочей директории

Для корректного функционирования программного продукта на сервере приложений требуется создать рабочую директорию C:\Runtime.

В данную директорию следует:

- распаковать содержимое дистрибутива;
- поместить сертификат Active Directory с именем **ad.crt**;
- скачать дистрибутив PostgreSQL версии 9.5.X (http://www.enterprisedb.com/products-services-training/pgbindownload) и распаковать в директорию C:\Runtime\pgsql.

Установка дистрибутива

Для запуска процесса установки программного продукта следует запустить консоль с *правами администратора* и выполнить команду:

```
cd /d C:\Runtime && install-all.cmd
```

В процессе установки дистрибутива будет запрошен свободный порт для службы Apache24 (в случае, если порт 80 уже занят), а также настройки соединения с Active Directory.

По завершении процесса установки на сервере приложений будут установлены:

- СУБД PostgreSQL 9.5.1 с:
  - *postgres/postgres* - учетная запись суперпользователя PostgreSQL;
  - *oib/oib* - учетная запись службы управления идентификационными данными;
  - *audit/audit* - учетная запись службы управления событиями безопасности;
  - *usersupport/usersupport* - учетная запись единого центр поддержки пользователей;
  - *notifier/notifier* - учетная запись службы рассылки уведомлений;
- веб-сервер Apache HTTPD 2.4;
- сервер сообщений Apache ActiveMQ 5.11.1;
- сервер приложений Wildfly 9.0.2 с инсталлированными модулями:
  - служба управления идентификационными данными;
  - служба управления событиями безопасности;
  - служба аутентификации пользователей;
  - служба авторизации пользователей;
  - единый центр поддержки пользователей;
  - приложение смены пароля;
  - служба рассылки уведомлений;
  - хранилище фотографий.

Проверка работоспособности

Проверка доступности и работоспособности *Службы управления идентификационными данными*:

Адрес	https://localhost:8282/security-admin-web
Пользователь	devadmin
Пароль	P@@ssw0rd

Проверка доступности и работоспособности *Службы управления событиями безопасности*:

Адрес	https://localhost:8282/audit/webapp/journal
Пользователь	devadmin
Пароль	P@@ssw0rd

Проверка доступности и работоспособности *Единого центра поддержки пользователей*:

Адрес	https://localhost:8282/usersupport
Пользователь	devadmin
Пароль	P@@ssw0rd

Проверка доступности и работоспособности *Приложения смены пароля*:

Адрес	https://localhost:8282/security-changepwd-web/webapp/change-password.html
Пользователь	devadmin
Пароль	P@@ssw0rd

Проверка доступности и работоспособности *Службы рассылки уведомлений*:

Адрес	https://localhost:8282/notifier
Пользователь	devadmin
Пароль	P@@ssw0rd

Проверка доступности и работоспособности *веб-сервера Apache HTTPD*:

Адрес	https://127.0.0.1/server-info
Адрес	https://127.0.0.1/server-status

Проверка доступности и работоспособности *сервера сообщений Apache ActiveMQ*:

Адрес	http://127.0.0.1:28161/admin
Пользователь	admin
Пароль	p@ssw0rd

Проверку доступности и работоспособности *СУБД PostgreSQL* можно осуществить через psql или утилиту PgAdmin.

Дополнительно следует убедиться в отсутствии ошибок в системных журналах сервера приложений Wildfly, расположенных в директории C:\Runtime\wildfly\standalone\log.