



ГЛАВА 31

Управление исправлениями

Управление исправлениями было процессом снижения до минимума уязвимостей организации за счет управления и развертывания обновлений программного обеспечения. С течением временем оно переместилось на поддержку обновлений компонентов и продукта в целом. Обновления могут развертываться и управляться с помощью нескольких продуктов и инструментов; примером может служить System Center Configuration Manager (Диспетчер конфигурации системного центра). В этой главе мы сосредоточим внимание на комплекте инструментов, встроенном в инфраструктуру Windows Server 2012 R2, и рассмотрим предлагаемые им возможности. В современном мире информационных технологий, основами которого являются Интернет и сотрудничество, внесение изменений в программное обеспечение стало повседневной задачей. Частота, с которой вы развертываете и проверяете актуальность обновлений, может означать разницу между тратой выходных на восстановление скомпрометированных или разрушенных систем и проведением их в кругу семьи или друзей.

Обновление программного обеспечения выглядит как бесконечный процесс, и если только вы не предпочитаете лично подходить к каждому компьютеру для установки обновлений, то вам понадобятся инструменты, которые помогут справиться с этой работой. Помимо инструментов необходим также надежный процесс управления исправлениями. Вам нужно знать, применимо ли каждое обновление к компьютерам в сети, совместимо ли оно с существующими приложениями и насколько срочно следует развертывать данное обновление.

В настоящей главе мы обсудим установку и конфигурирование роли Windows Server Update Services для Windows Server 2012 R2 и расскажем, что должно приниматься во внимание при развертывании этого процесса управления исправлениями. Кроме того, мы проанализируем обновления безопасности и подробно рассмотрим службу обновления сервера Windows (Windows Server Update Services — WSUS), которая теперь интегрирована в операционную систему в виде серверной роли. Вдобавок мы объясним, как перейти от WSUS версии Windows Server 2008 R2 к WSUS версии Windows Server 2012 R2. Наконец, мы представим обзор доступных командлетов PowerShell.

В этой главе вы изучите следующие темы:

- ♦ использование автоматических обновлений Windows (Windows Automatic Updates) для проверки наличия новых обновлений на компьютере, работающем под управлением Windows 8;
- ♦ применение автономной программы установки обновлений Windows (Windows Update Standalone Installer) для молчаливой установки обновления безопасности;
- ♦ идентификация четырех фаз управления исправлениями.

Что нового в Windows Server Update Services версии Windows Server 2012 R2

Служба Windows Server Update Services (WSUS) теперь интегрирована в Windows Server 2012 R2. Эта новая роль позволяет администраторам использовать диспетчер серверов для конфигурирования и управления обновлениями; в новую версию WSUS включены те же возможности генерации отчетов и обновления состояния, что и ранее, а также несколько новых средств и модификаций предыдущей функциональности.

Новые возможности WSUS v6 в Windows Server 2012 R2

В версию WSUS v6 было добавлено несколько новых возможностей, базовый перечень которых приведен ниже.

- ♦ Службы можно добавлять или удалять с помощью диспетчера серверов.
- ♦ Доступны командлеты PowerShell для управления десятком наиболее важных задач в службе WSUS.
- ♦ Для обеспечения дополнительной безопасности добавлена возможность хеширования SHA256.
- ♦ Обеспечивается разделение клиента и сервера. Версии агента обновления Windows (Windows Update Agent — WUA) могут поставляться независимо от WSUS.

Требования к программному обеспечению для серверов и клиентов WSUS

Прежде чем устанавливать WSUS в существующей среде, вы должны удостовериться в том, что сервер (серверы) и клиенты WSUS удовлетворяют минимальным требованиям к программному обеспечению.

На серверах WSUS должно быть установлено, как минимум, следующее программное обеспечение:

- ♦ операционная система Windows Server 2012 R2;
- ♦ службы Internet Information Services (IIS);
- ♦ инфраструктура .NET Framework 4.0 или более новая версия;
- ♦ если вы используете отдельный сервер базы данных, то должны иметь компьютер, на котором функционирует SQL Server 2012 R2 либо SQL Server 2008 R2 с пакетом обновлений SP1 или более новая версия.

Конечные точки WSUS должны быть основаны на версии 7.8 агента Windows Update Agent (WUAgent 7.8). Клиенты WSUS должны работать под управлением одной из перечисленных далее операционных систем:

- ◆ Windows 8
- ◆ Windows RT
- ◆ Windows 7
- ◆ Windows Server 2008 R2
- ◆ Windows Server 2008
- ◆ Windows Server 2003 с пакетом обновлений SP1
- ◆ Windows Vista

Ниже приведен список баз данных, поддерживаемых WSUS:

- ◆ Windows Internal Database (WID)
- ◆ Microsoft SQL Server 2012 R2 Standard Edition
- ◆ Microsoft SQL Server 2012 R2 Enterprise Edition
- ◆ Microsoft SQL Server 2012 R2 Express Edition
- ◆ Microsoft SQL Server 2008 R2 SP1 Standard Edition
- ◆ Microsoft SQL Server 2008 R2 SP1 Enterprise Edition
- ◆ Microsoft SQL Server 2008 R2 SP 1 Express Edition

Предельный размер базы данных в SQL Server Express 2012 и SQL Server Express 2008 R2 составляет 10 Гбайт; для многих сред его может оказаться достаточно, но это ограничение очень важно учитывать при определении подходящего предельного размера для вашей системы. Размышления по поводу размера всегда должны начинаться с числа клиентов, которое вы собираетесь поддерживать, и количества платформ.

Сценарии развертывания

Версия WSUS в Windows Server 2012 R2 была изменена так, чтобы сценарии развертывания фокусировались не столько на размере предприятия, сколько на требованиях в отношении емкости и местоположения. Три основных вариантами развертывания являются одиночный сервер WSUS, несколько серверов WSUS и отключенный сервер WSUS. Для организаций средних и крупных размеров или сложной инфраструктуры вы должны подумать о применении какого-то продукта из семейства System Center (www.microsoft.com/systemcenter).

Сценарий с развертыванием единственного экземпляра предполагает использование одного главного сервера WSUS, который синхронизируется непосредственно со службой Microsoft Update. Клиенты WSUS могут быть разбросаны по разным географическим регионам, но все они находятся за одним и тем же брандмауэром (рис. 31.1).

Многие организации средних и крупных размеров эксплуатируют многосерверную инфраструктуру, которая состоит из нескольких серверов WSUS, обслуживающих множество географически распределенных клиентов. Один сервер WSUS может синхронизироваться с другим (рис. 31.2) или они могут получать обновления от Microsoft Update по отдельности.

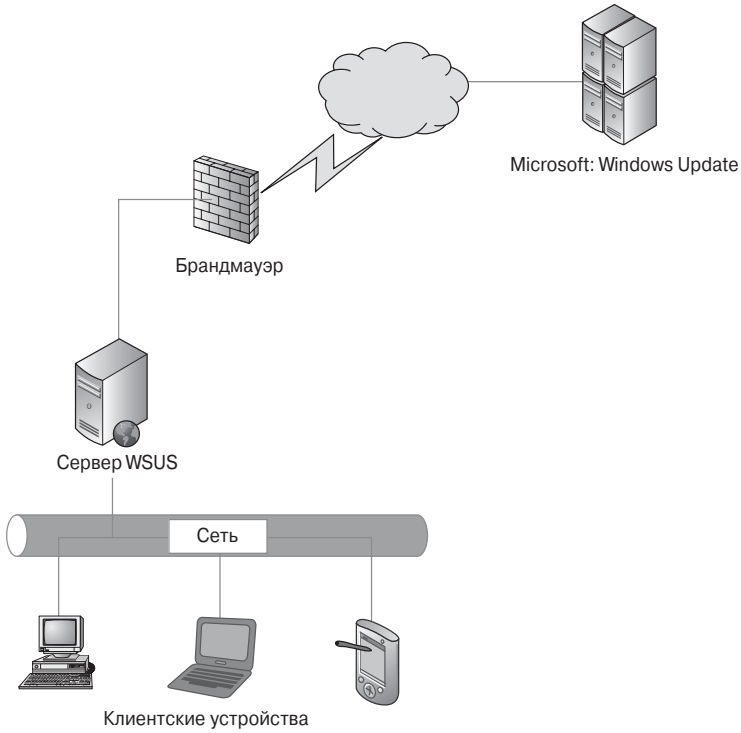


Рис. 31.1. Развертывание с одиночным сервером WSUS

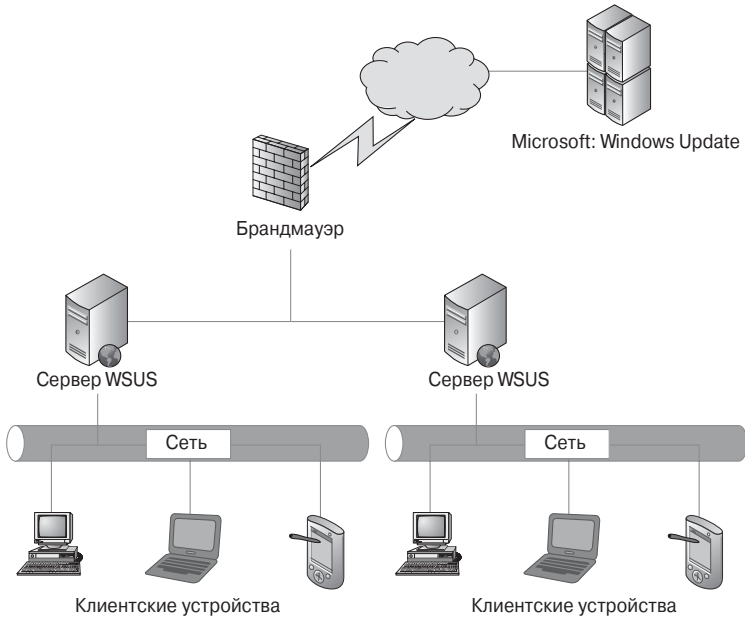


Рис. 31.2. Развертывание с несколькими серверами WSUS, в котором один сервер WSUS синхронизируется с другим

В этой конфигурации только один сервер виден из Интернета, а остальные настроены как нижестоящие серверы, которые должны синхронизироваться с первым сервером. Преимущество наличия единственного сервера, синхронизирующегося с Microsoft Update, заключается в том, что другие серверы WSUS из Интернета не видны.

Сценарий с отключенной инфраструктурой предназначен для компьютеров, которым не разрешен доступ в Интернет или которые располагают только ограниченным доступом к нему. Получать обновления для компьютеров, подключенных к такой изолированной сети, можно путем настройки в этой отключенной сети сервера WSUS. После обработки всех исправлений для производственной сети их можно экспортировать на устройства наподобие USB-дисков. Ниже описаны базовые шаги этого процесса.

1. Экспортируйте исправления из консоли WSUS на USB-диск. Для их экспорта необходимо воспользоваться командой `WSUTIL.exe`.
2. Импортируйте исправления на отключенный сервер WSUS.
3. Настройте расписание и разверните исправления.

Как только исправления будут экспортированы, их можно импортировать на отключенный сервер WSUS, как показано на рис. 31.3, а развертывание может производиться на основе расписания для этого сервера WSUS.

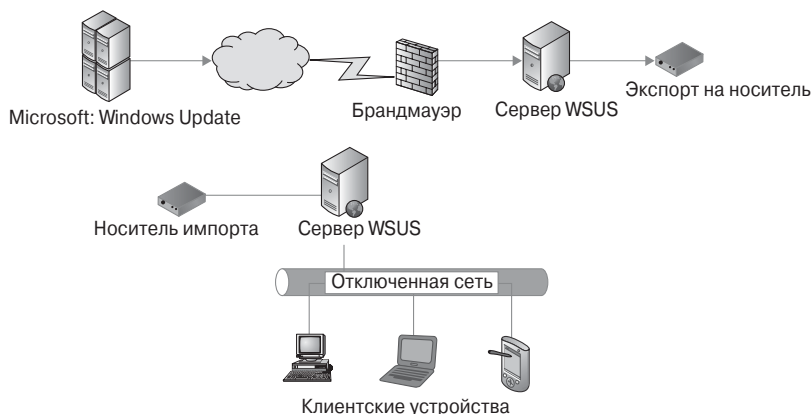


Рис. 31.3. Развертывание с отключенным сервером WSUS

Построение сложных иерархий с использованием WSUS

В зависимости от типа развертывания сервера и нужд организации существуют дополнительные преимущества применения новой версии Windows Server. Это помогает минимизировать развертывания серверного оборудования (или виртуальные развертывания), требуемые для управления средой. Используя возможности Windows Server 2012 R2 и WSUS, вы можете сконфигурировать автономный (Autonomous) режим, режим реплики (Replica), а также настроить клиентов в филиалах и блуждающих клиентов.

Автономный режим, обычно называемый распределенным режимом, является стандартным вариантом установки для WSUS. В этой конфигурации (показанной на рис. 31.4) вышестоящий сервер используется для обмена обновлениями с одним или несколькими нижестоящими серверами, и за счет внедрения средств управления доступом вы можете предоставить локальным администраторам возможность управления собственными средами.

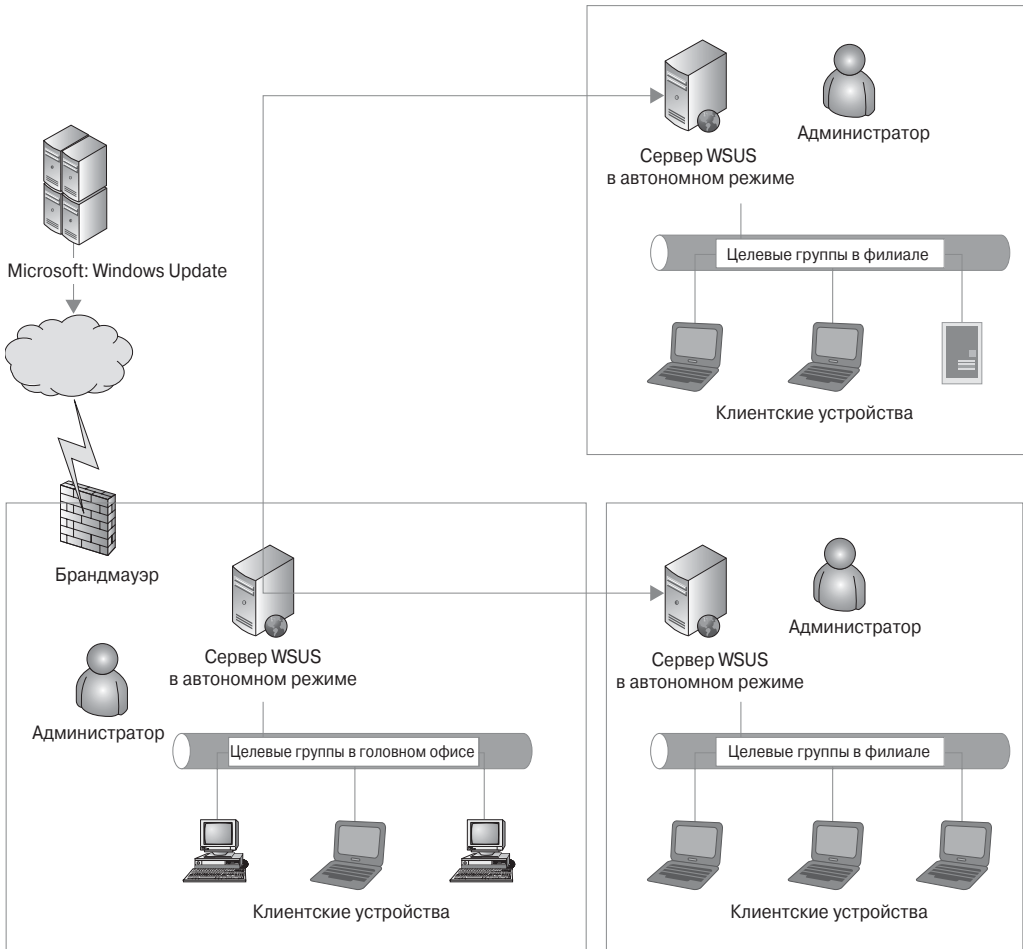


Рис. 31.4. Автономный режим в многосайтовой среде

Режим реплики (рис. 31.5) представляет собой проектное решение с централизованным администрированием и позволяет вышестоящему серверу обмениваться своими обновлениями, клиентскими группами и другими компонентами с нижестоящими серверами.

Серверы реплики — это просто нижестоящие серверы, которые управляются посредством главного вышестоящего сервера. Такая конфигурация оказывается самой удобной, когда центральный ИТ-отдел управляет обновлениями в сценарии с несколькими сайтами или офисами филиалов.

Офисы филиалов — один из новейших сценариев, введенных в Windows Server 2012 R2. В этой конфигурации используется средство BranchCache, доступное в Windows Server 2012 R2 (<http://tinyurl.com/BranchCache>). С помощью средств BranchCache и Branch Office, реализованных в Windows, можно сократить нагрузку на канал WAN и улучшить показатель времени реакции системы.

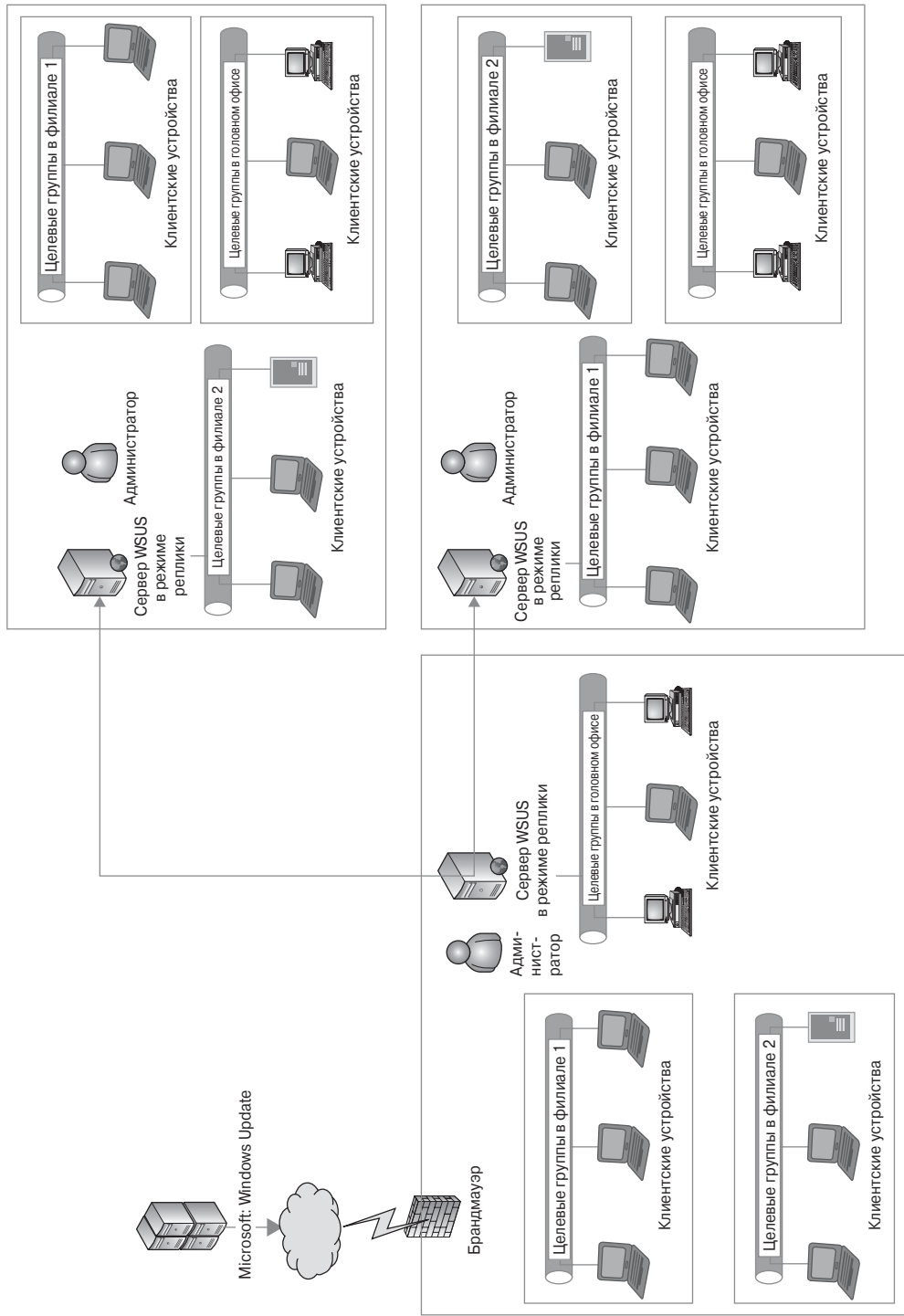


Рис. 31.5. Режим реплики в сценарии с несколькими офисами филиалов

Установка и конфигурирование управления исправлениями

Установка обновлений на компьютерах в сети вашей организации критически важна для обеспечения безопасности этой сети и оптимального функционирования клиентских компьютеров организации. Распространение обновлений требует планирования и тестирования, гарантирующего успешную их установку. В Microsoft рекомендуют применять поэтапный подход к управлению исправлениями; каждый этап подробно обсуждается на веб-сайте Microsoft TechNet по ссылке:

<https://technet.microsoft.com/en-us/library/cc700845.aspx>

Установка роли WSUS в Windows Server 2012 R2

Одним из новых средств Windows Server 2012 R2 является возможность установки серверной роли с автоматическим добавлением всех обязательных компонентов как части процесса установки. В предыдущих версиях Windows Server многие роли и компоненты приходилось конфигурировать как отдельные задачи.

Чтобы установить роль WSUS в Windows Server 2012 R2, выполните следующие шаги.

1. Откройте управляющую панель диспетчера серверов и щелкните на ссылке Add roles and features (Добавить роли и компоненты), как показано на рис. 31.6.
2. Войдите в систему компьютера с использованием учетной записи из локальной группы Administrators или администратора домена.
3. Запустите диспетчер серверов (по умолчанию в Windows Server 2012 R2 он запускается автоматически).

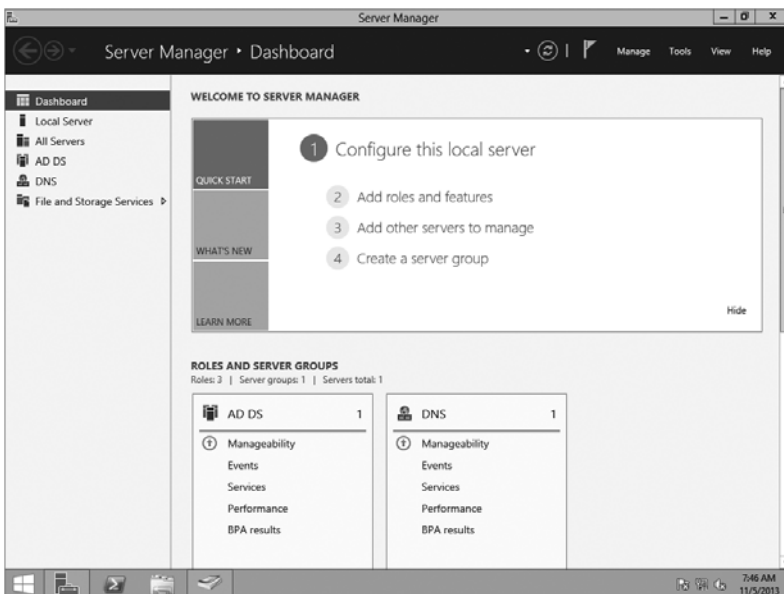


Рис. 31.6. Добавление ролей в Windows Server 2012 R2

4. В разделе Configure this local server (Конфигурировать этот локальный сервер) щелкните на ссылке Add Roles and Features.
5. На экране Before You Begin (Прежде чем начать) щелкните на кнопке Next (Далее).
6. Выберите переключатель Role-Based or Feature-Based installation (Установка на основе ролей или на основе компонентов) для типа установки и щелкните на кнопке Next.
7. На экране Select Destination Server (Выбор сервера назначения) оставьте выбранным ваш сервер, как предлагается по умолчанию, и щелкните на кнопке Next.

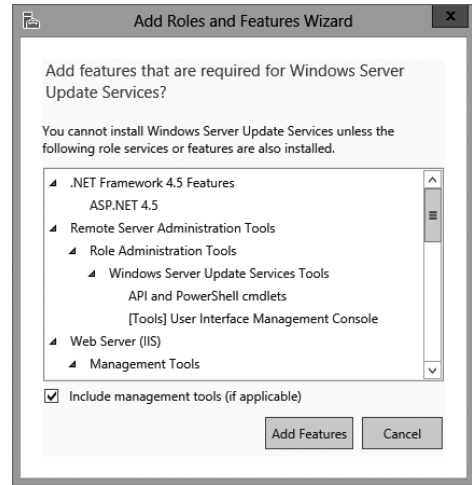


Рис. 31.7. Обязательные компоненты для Windows Server Update Services

8. Выполните прокрутку вниз до роли Windows Server Update Services, отметьте флажок рядом с ней и щелкните на кнопке Next.
9. Для продолжения установки будет предложено добавить дополнительные компоненты, как показано на рис. 31.7.
10. Щелкните на кнопке Add Features (Добавить компоненты). Вы заметите, что компонент Web Server (IIS) также выбран; щелкните на кнопке Next.

Откроется экран Features (Компоненты) с заранее отмеченными флажками для следующих компонентов:

- Remote Server Administration Tools (Инструменты дистанционного администрирования серверов)
 - Windows Internal Database (Внутренняя база данных Windows)
 - Windows Process Activation (Активация процессов Windows)
11. Просмотрите выбранные параметры и щелкните на кнопке Next.
 12. Откроется экран Windows Server Update Services (Службы обновления сервера Windows); щелкните на кнопке Next.

В разделе Role Services (Службы роли) по умолчанию отмечены флажки WID Database (Windows Internal Database) (База данных WID (внутренняя база данных Windows)) и WSUS Services (Службы WSUS). Кнопка Database (База данных) предусмотрена на тот случай, если вы намерены использовать базу данных SQL на другом сервере; она предоставит дополнительные параметры.

13. Оставьте все без изменений и щелкните на кнопке Next.

Следующий экран позволяет выбрать местоположение файлов Windows Update (если вы решили сделать их доступными локально); в рассматриваемом примере снимите отметку с этого флажка. Тем самым вы получаете возможность сохранить все обновления на сервере Microsoft Update и применять их, когда это необходимо.

14. После снятия отметки с флажка *Store updates in the following location* (Сохранять обновления в следующем месте) щелкните на кнопке *Next*.
15. Откроется экран *Web Server Role (IIS)*; щелкните на кнопке *Next*.

После этого отобразится экран *Role Services* (Службы роли), где будут заранее выбраны перечисленные ниже флажки.

- *Common HTTP Features* (Общие компоненты HTTP):
 - *Default Document* (Стандартный документ)
 - *Static Content* (Статическое содержимое)
 - *Performance* (Производительность):
 - *Dynamic Content Compression* (Динамическое сжатие содержимого)
 - *Security* (Безопасность):
 - *Request Filtering* (Фильтрация запросов)
 - *Windows Authentication* (Аутентификация Windows)
 - *Application Development* (Разработка приложений):
 - *.NET Extensibility 4.5* (.NET Extensibility 4.5)
 - *ASP.NET 4.5*
 - *ISAPI Extensions* (Расширения ISAPI)
 - *ISAPI Filters* (Фильтры ISAPI)
 - *Management Tools* (Инструменты управления):
 - *IIS Management Console* (Консоль управления IIS)
 - *IIS 6 Management Compatibility* (Совместимость с управлением IIS 6)
 - *IIS 6 Metabase Compatibility* (Совместимость с метабазой IIS 6)
16. Просмотрите выбранные параметры и щелкните на кнопке *Next*.
 17. Подтвердите выбранные параметры установки и щелкните на кнопке *Install* (Установить).

Операционная система *Windows Server 2012 R2* позволяет выбирать и экспортировать любые настройки конфигурации, сделанные в ходе установки ролей и компонентов (рис. 31.8). Вы найдете ссылку *Export configuration settings* (Экспортировать настройки конфигурации) в нижней части экрана очень удобной, когда вы создаете множество идентичных конфигураций серверов или настроили специфичную конфигурацию и хотите ее сохранить.

Конфигурирование WSUS для развертывания

После завершения установки серверной роли *WSUS* вы можете запустить службу *Windows Server Update Services* из начального экрана (рис. 31.9) и приступить к конфигурированию.

Чтобы начать конфигурирование сервера *WSUS*, необходимо настроить обновления, требуемые для вашей среды. После открытия консоли *Update Services* запустится мастер конфигурирования службы обновления сервера *Windows* (*Windows Server Update Services Configuration Wizard*), который проведет через последовательность шагов по настройке параметров обновлений для последующего развертывания.

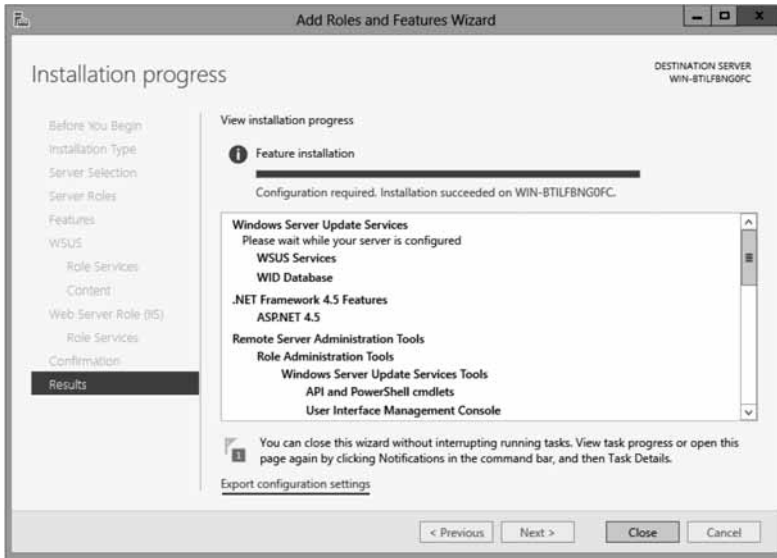


Рис. 31.8. Экспорт настроек конфигурации

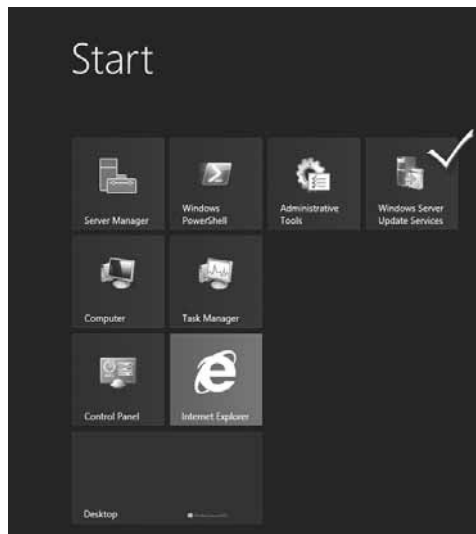


Рис. 31.9. Доступ к службе Windows Server Update Services на начальном экране

Первым экраном мастера является Before You Begin (Прежде чем начать); до начала процесса вы должны удостовериться в том, что удовлетворены перечисленные ниже условия.

- ◆ Сконфигурирован ли брандмауэр сервера на разрешение клиентам доступа к серверу?
- ◆ Может ли этот компьютер подключиться к вышестоящему серверу (такому как Microsoft Update)?

- ◆ Располагаете ли вы пользовательскими учетными данными для прокси-сервера, если в этом есть необходимость?

Убедившись в том, что эти условия выполнены, можете переходить к следующим действиям.

1. Приступите к начальному конфигурированию Windows Update Services, щелкнув на кнопке Next (Далее).

Вам будет предложено присоединиться к программе по улучшению Microsoft Update (Microsoft Update Improvement Program); при желании можете оставить соответствующий флажок отмеченным.

2. Для продолжения щелкните на кнопке Next.

Вам понадобится выбрать вышестоящий сервер, и вы задействуете на нем Microsoft Update, если это самый первый сервер. Любые дополнительные серверы, которые вы добавите впоследствии, могут ссылаться на этот сервер для синхронизации с ним. В нашем примере мы будем применять Microsoft Update в качестве партнера синхронизации.

3. Примите настройки, предложенные по умолчанию, и щелкните на кнопке Next.

4. Укажите прокси-сервер. Если в организации используется прокси-сервер, заполните все обязательные поля, как показано в примере на рис. 31.10, и щелкните на кнопке Next.

Теперь вы подключитесь к вышестоящему серверу, чтобы можно было начать получение доступных обновлений продуктов, языков и других типов обновлений для вашего сервера обновлений.

5. Чтобы начать этот процесс, щелкните на кнопке Start Connecting (Начать подключение), представленной на рис. 31.11. Процесс подключения к вышестоящему серверу в первый раз может занять несколько минут.

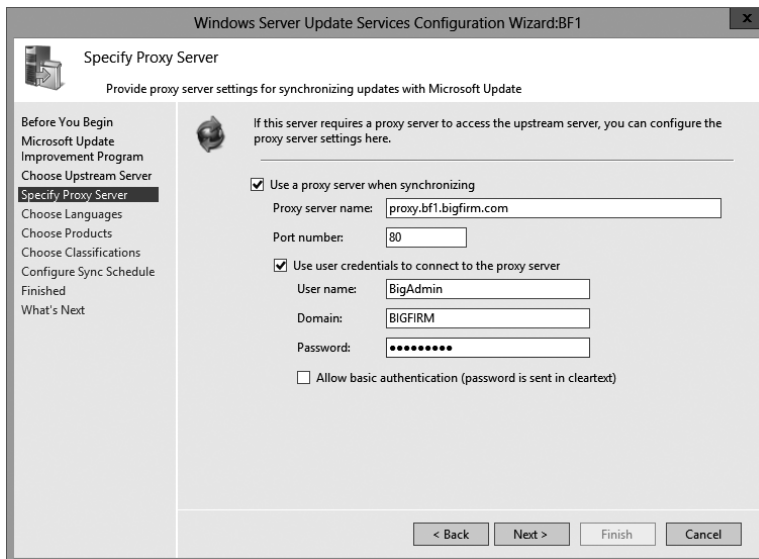


Рис. 31.10. Конфигурирование прокси-сервера

6. Когда этот процесс завершится, щелкните на кнопке Next.

На экране Product Updates (Обновления продуктов) будет приведен список всех продуктов, доступных на вашем вышестоящем сервере. Вы можете выбрать целый продукт или конкретную его версию.

7. В этом примере мы отметили флажки только для Office 2013 и всех версий Silverlight (рис. 31.12). Выберите желаемые продукты и щелкните на кнопке Next.

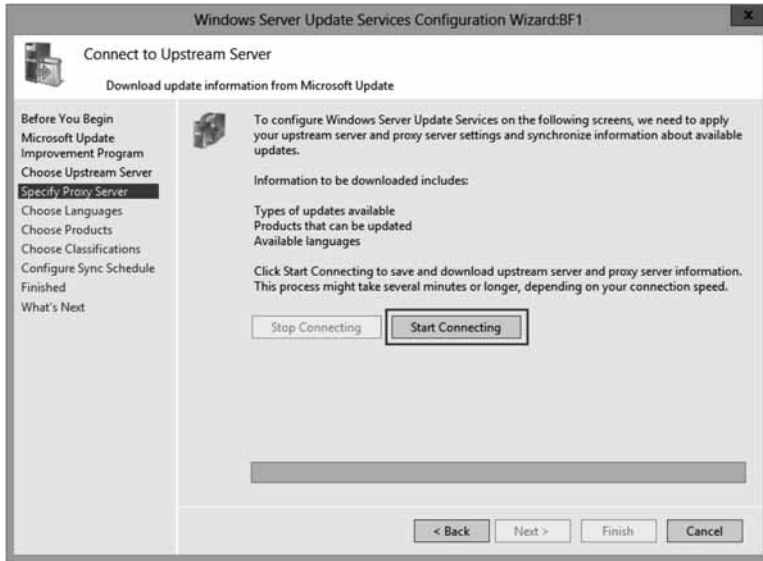


Рис. 31.11. Подключение к вышестоящему серверу

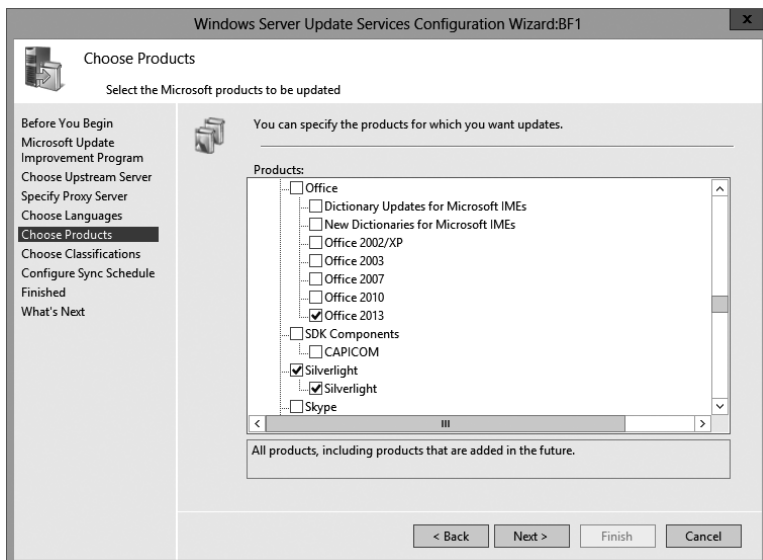


Рис. 31.12. Выбор продуктов для обновления

Далее понадобится выбрать классификации ваших обновлений для синхронизации. Перечень простирается от важных обновлений (Critical Updates) до обычных обновлений (Updates), как показано на рис. 31.13.

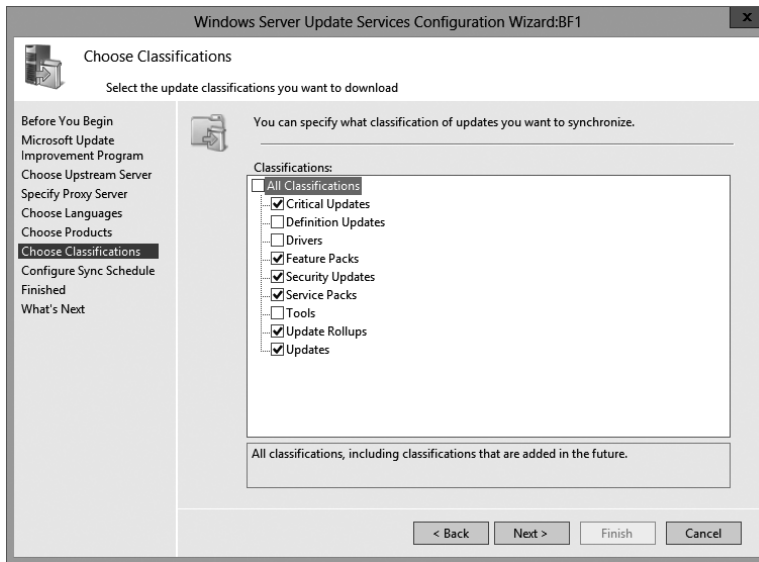


Рис. 31.13. Выбор классификаций обновления

8. Сделав нужный выбор, щелкните на кнопке Next.

Следующий экран позволяет настроить расписание синхронизации. Здесь есть два варианта: первым является ручная синхронизация, которую можно выполнять посредством консоли службы обновления, а вторым — автоматическая синхронизация в определенный день и время. (За день можно также выполнять несколько синхронизаций.)

9. Установив расписание синхронизации, щелкните на кнопке Next.

10. В завершение вы можете инициировать начальную синхронизацию, отметив соответствующий флажок, и щелкнуть на кнопке Finish (Готово).

В качестве альтернативы можете щелкнуть на кнопке Next и перейти на экран What's Next (Что дальше), где можно задать дополнительные параметры конфигурации, такие как SSL, и назначить компьютеры для обновления с помощью групповой политики (подробнее об этом речь пойдет в следующем разделе).

Обновления Windows начнут синхронизироваться с сервером Microsoft Update и заполнять консоль Update Services.

Прежде чем приступить к развертыванию обновлений и конфигурированию объектов групповой политики (GPO), давайте рассмотрим несколько других параметров в этой консоли, которые должны приниматься во внимание на завершающих шагах конфигурирования. Первым параметром, на который мы хотим взглянуть, являются компьютеры. Каким образом вы хотите добавлять свои устройства к WSUS? Открыв раздел Options (Параметры) консоли Update Services (рис. 31.14), вы можете выбрать объект Computers (Компьютеры); это позволит либо использовать консоль Update

Services для распределения компьютеров по группам, либо применять для назначения компьютеров групповую политику (или настройки реестра).

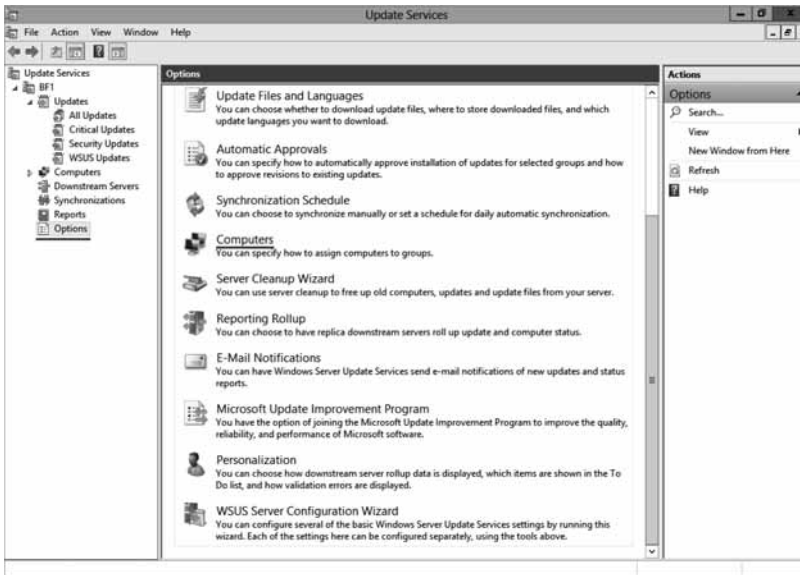


Рис. 31.14. Параметры консоли Update Services

В разделе Synchronizations (Синхронизации) вы должны проверить успешность синхронизации, но если она не началась, можете запустить ее вручную, щелкнув на элементе Synchronize Now (Синхронизировать сейчас) в панели Actions (Действия). Дополнительные детали приведены на рис. 31.15.

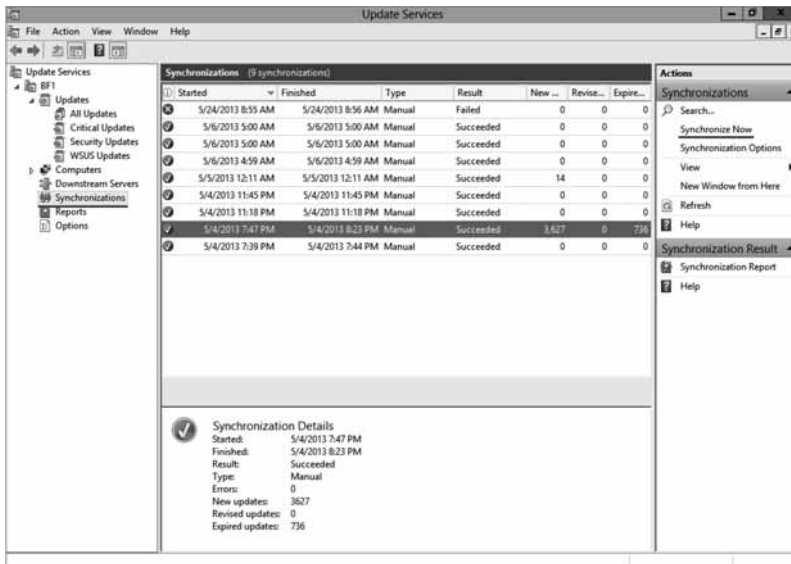


Рис. 31.15. Консоль Update Services, параметры синхронизации и задачи

Развертывание обновлений и миграция для WSUS

Чтобы получать обновления WSUS, у вас должна функционировать одна из следующих операционных систем: Windows 8, Windows 7, Windows Server 2012 R2, Windows Server 2008 R2, Windows Vista, Windows Server 2008 или Windows Server 2003. Также поддерживается Windows 8 RT, но с ограниченными возможностями.

Конфигурирование групповой политики для Windows Update

Использование объектов групповой политики (GPO) является наиболее распространенным и рекомендуемым подходом к управлению Windows Server Update Services. В этом разделе вы сконфигурируете параметры, необходимые для того, чтобы вытолкнуть обновления Windows с помощью объекта GPO. Для этого примера мы создаем совершенно новый объект GPO и применяем его к организационной единице Workstations (Рабочие станции) в Active Directory. Этот вновь созданный объект GPO называется BigFirmUpdates (рис. 31.16). Чтобы сконфигурировать настройки автоматического обновления Windows, выполните перечисленные ниже шаги.

1. Щелкните правой кнопкой мыши на объекте GPO и выберите в контекстном меню пункт Edit (Редактировать), чтобы открыть редактор управления групповыми политиками (Group Policy Management Editor), как показано на рис. 31.17.

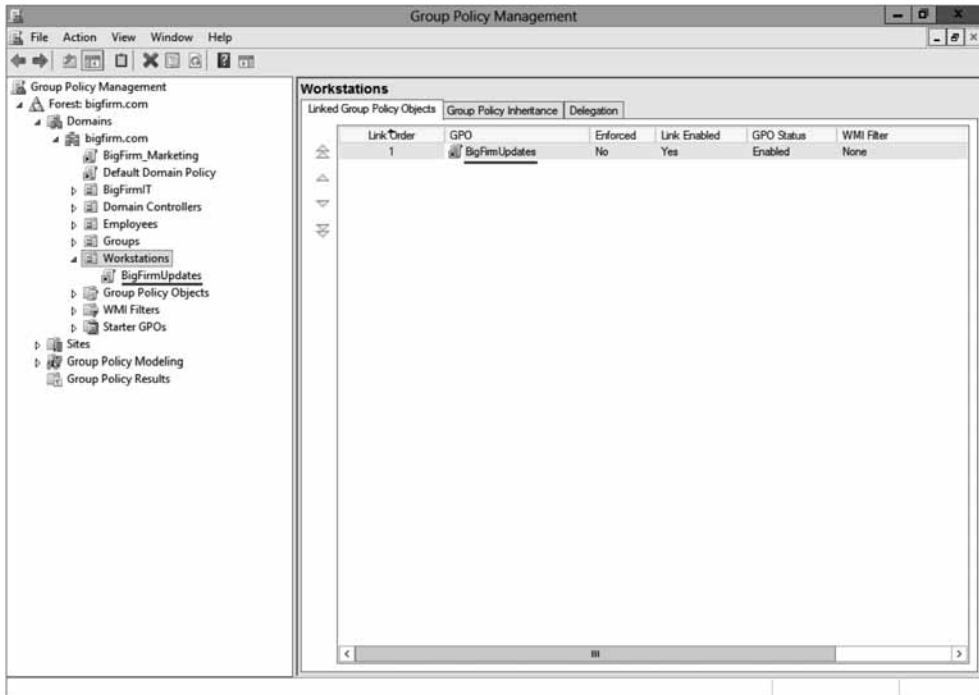


Рис. 31.16. Консоль Group Policy Management

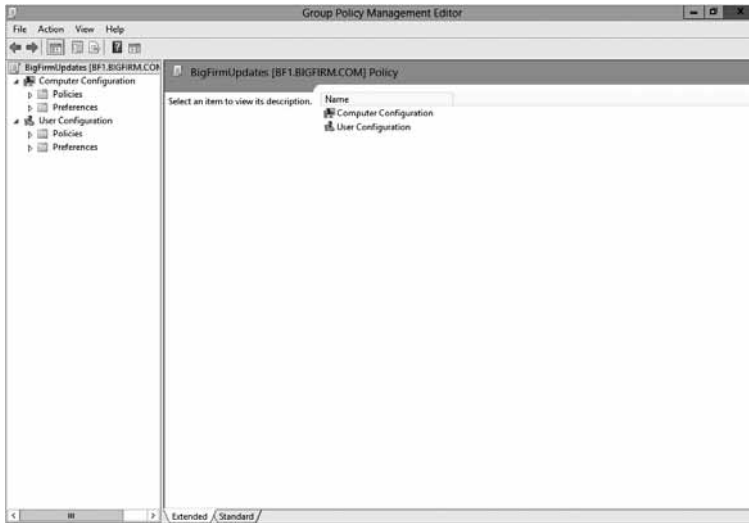


Рис. 31.17. Редактор Group Policy Management Editor

2. В редакторе Group Policy Management Editor перейдите в папку Computer Configuration \ Administrative Templates \ Windows Components \ Windows Update (Конфигурация компьютера \ Административные шаблоны \ Компоненты Windows \ Обновление Windows).
3. Дважды щелкните на настройке Configure Automatic Updates (Конфигурировать автоматические обновления), показанной на рис. 31.18, и выберите для нее переключатель Enabled (Включить).

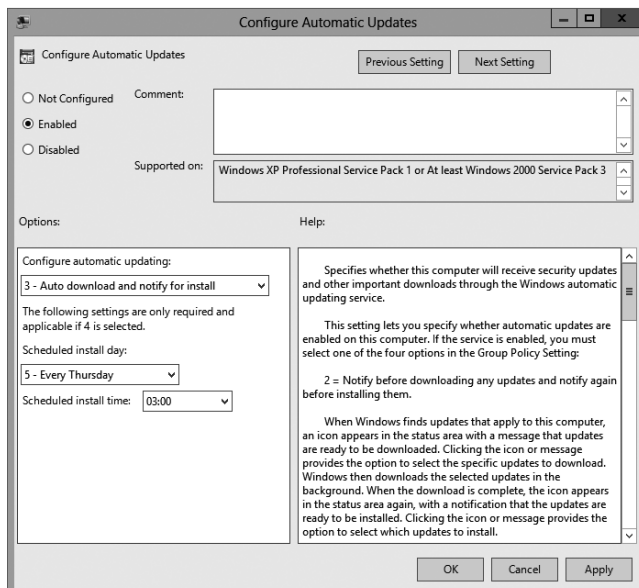


Рис. 31.18. Конфигурирование автоматических обновлений

- а. В поле со списком Configure automatic updating (Конфигурировать автоматическое обновление) выберите подходящий вариант из числа доступных: Notify for download and notify for install (Уведомления о загрузке и установке), Auto download and notify for install (Автоматическая загрузка и уведомление об установке), Auto download and schedule the install (Автоматическая загрузка и установка по расписанию), Allow local admin to choose setting (Локальный администратор может менять параметр).
 - б. Если вы выбрали вариант Auto download and schedule the install, то должны указать день и время установки по расписанию.
4. Выберите настройку Specify intranet Microsoft update service location (Указать размещение службы обновлений Microsoft в интрасети). Здесь вам предстоит указать клиентам WSUS на сервер WSUS.
 - а. Выберите переключатель Enabled (Включить).
 - б. В полях Set the intranet update service for detecting updates (Укажите службу обновлений в интрасети для поиска обновлений) и Set the intranet statistics server (Укажите сервер статистики в интрасети) введите имя сервера WSUS, как показано на рис. 31.19.
 - в. Щелкните на кнопке ОК.
- Все это условия, которые обеспечат выталкивание обновлений на ваши клиентские устройства и использование только что созданной инфраструктуры WSUS.

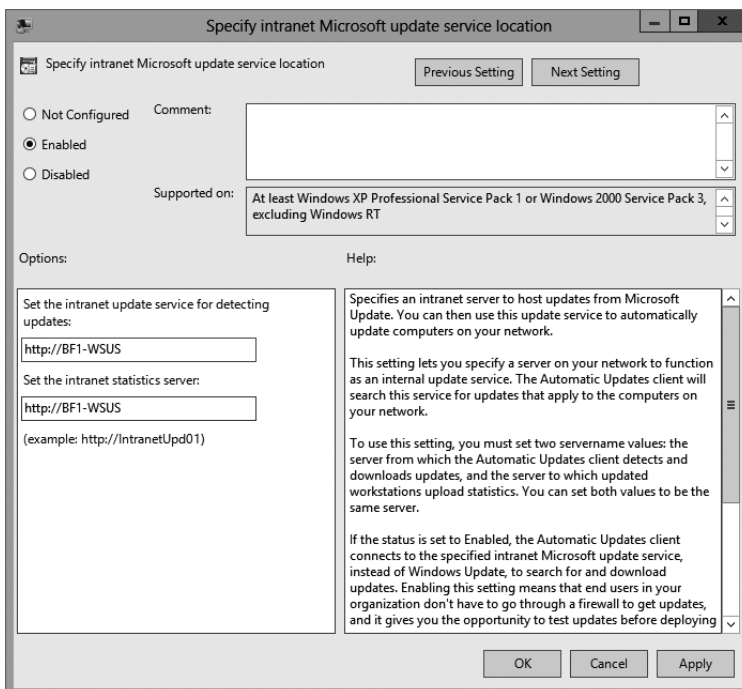


Рис. 31.19. Конфигурирование сервера WSUS

В разделе Windows Update редактора Group Policy Object Editor (рис. 31.20) легко заметить несколько других настроек, которые помогают существенно повысить эффективность администрирования и применения Windows Update. Они предоставляют возможность изменять график автоматических обновлений, включать выбор целей на клиентской стороне и отключать отображение на клиентах параметра установки обновлений, когда они доступны.

Конфигурирование клиентов для обновлений Windows

В этом разделе мы расскажем о конфигурировании и проверке того, что компьютер Windows 8 (по имени WIN8CLIENT), получает обновления из нашего сервера WSUS версии Windows Server 2012 R2. Настройка на клиентской стороне очень проста и требует только наличия самих обновлений или конфигурирования объекта GPO для получения этих обновлений. Если вы провели модернизацию до нового сервера Windows Server 2012 R2, то останется лишь модифицировать объекты GPO из предыдущего раздела.

Вообще говоря, внесение изменений в объекты GPO является единственной серьезной задачей для конфигурирования клиентов на получение обновлений из нового сервера WSUS. Ниже мы раскроем некоторые основы проверки и гарантии того, что клиент получает свои обновления и нацелен на правильный сервер.

Обновление групповой политики, которое происходит после указания клиентам нового сервера WSUS, может занять от 90 до 120 минут. Стандартное обновление объекта GPO занимает 90 минут.

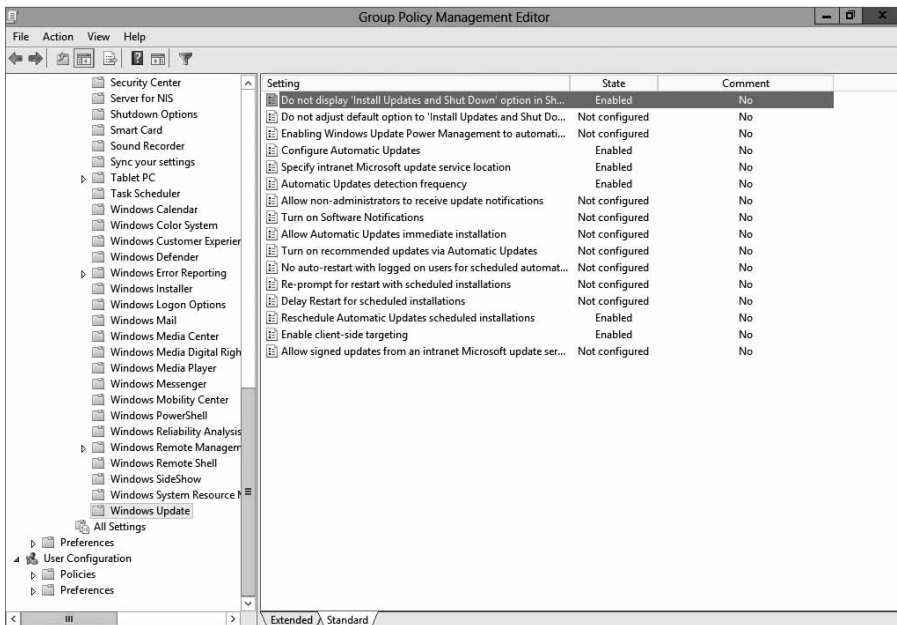


Рис. 31.20. Дополнительные настройки групповой политики Windows Update

Если вы хотите протестировать клиент, выполните следующие шаги.

1. На клиентском компьютере Windows откройте окно командной строки.
2. Введите команду `wuaclt.exe /detectnow /reportnow`.

Это приведет к немедленному переходу клиента на сервер WSUS, проверке доступности его обновлений и выдаче отчета, по сути, подтверждающего их существование.

Чтобы проверить наличие ошибок или проблем с локальным клиентом, вы можете запустить средство Event Viewer локальной системы и перейти в нем к узлу \ Applications and Services Logs \ Microsoft \ Windows \ Windows Update Client \ (\ Журналы приложений и служб \ Microsoft \ Windows \ Клиент обновлений Windows \). Здесь вы увидите информационные сообщения, сообщения об ошибках и предупреждения клиентской системы, касающиеся обновлений (рис. 31.21).

Вдобавок вы всегда можете открыть инструмент Windows Update (Центр обновления Windows) из панели управления на клиенте и проверить, получает ли клиентский компьютер обновления. Средство Windows Update отобразит, когда выполнялись самые последние проверки наличия обновлений, укажет, какие обновления были установлены и как производится управление обновлениями (рис. 31.22).

В следующем разделе собираемся перейти от клиентских настроек к обзору процесса миграции вашей текущей реализации WSUS в Windows Server 2012 R2 и встроенной роли для Windows Server Update Services.

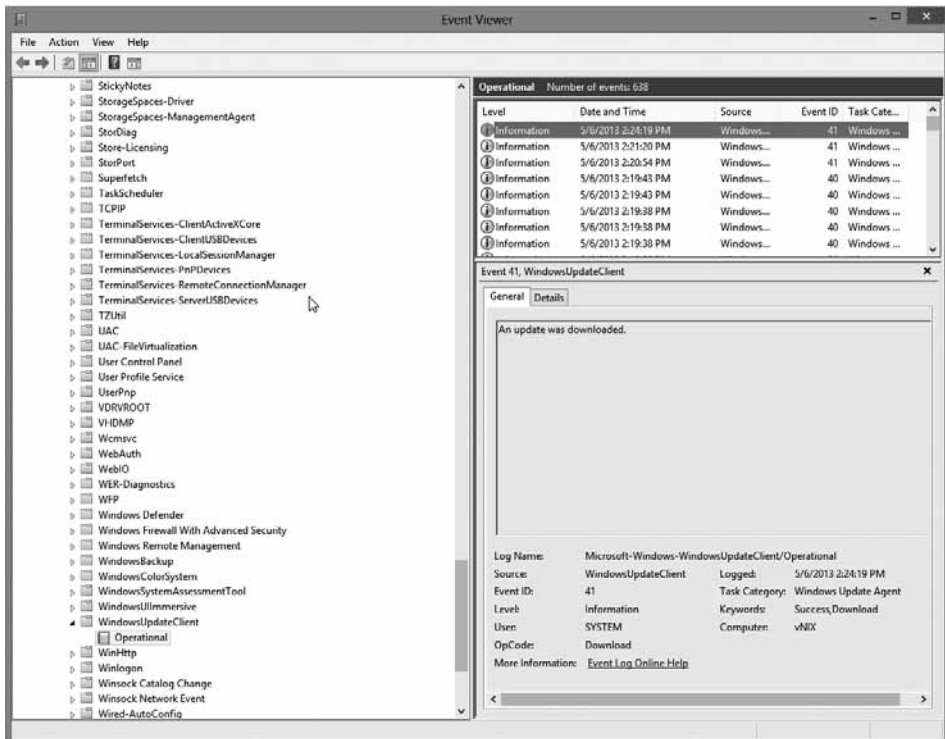


Рис. 31.21. Журнал Windows Applications and Services для обновлений клиентской стороны

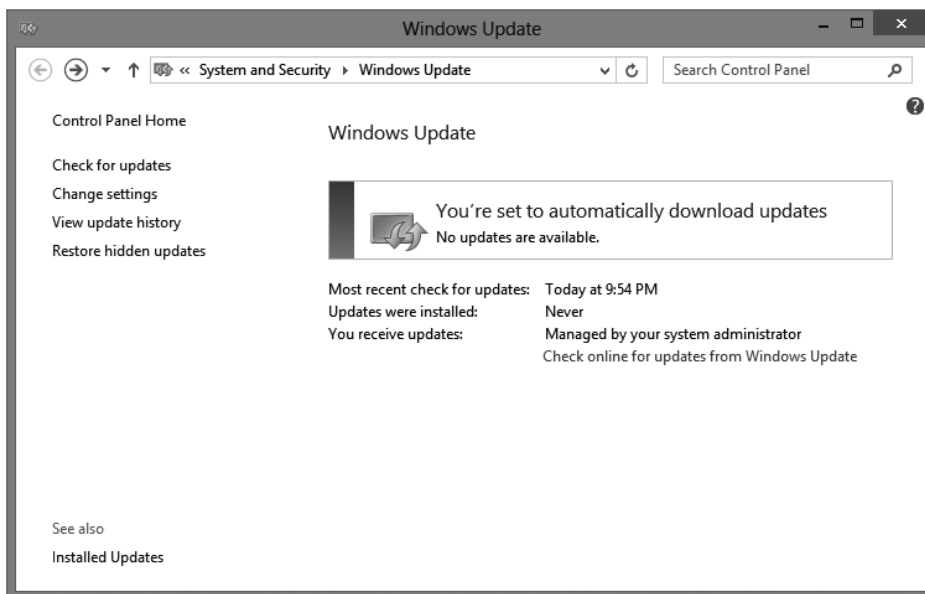


Рис. 31.22. Инструмент Windows Update в Windows 8

Миграция из WSUS 3.0 на Windows Server 2012 R2

Служба WSUS 3.0 упакована как автономный модуль установки, доступный в центре загрузки Microsoft (Microsoft Download Center), тогда как служба WSUS v6 (или WSUS 4.0, как иногда на нее ссылаются) представляет собой встроенную роль в Windows Server 2012 R2. В этом разделе вы узнаете, каким образом перейти от текущей установки WSUS 3.0 к новой встроенной платформе Windows Server 2012 R2.

В Microsoft предоставили четырехэтапный процесс для выполнения миграции из существующей реализации WSUS на новый целевой сервер, функционирующий под управлением Windows Server 2012 R2. Описание этого процесса можно найти в TechNet по ссылке:

<https://technet.microsoft.com/ru-ru/library/hh852339.aspx>

Прежде чем выполнять любой переход в производственной среде, понадобится принять во внимание множество разных факторов. Наличие достоверной исходной информации и перечня всех имеющихся серверов уступает по своей значимости лишь знанию вами всех возможных сценариев перехода.

Редакции Windows Server 2012 R2 Standard и Datacenter поддерживаются в качестве целевых серверов; возможен также переход с физической операционной системы на виртуальную. Модернизация будет поддерживать переход от SQL или Windows Internal Database (WID) как составную часть этого процесса миграции. Вдобавок можно переходить от WID к SQL Server.

Процесс перехода от службы WSUS 3.0 SP2 на инфраструктуру WSUS в Windows Server 2012 R2 требует определенных усилий, и очень важно иметь план резервного копирования/отката, если что-то не заработает, как ожидалось. При запуске процесса миграции, прежде всего, необходимо переместить все обновления WSUS

со старого исходного сервера на новый целевой сервер Windows Server 2012 R2. Использование инструментов вроде XCopy или Robocopy является жизнеспособным вариантом, но гораздо важнее понимать командлеты и управление с помощью PowerShell. Применение PowerShell для переноса таких объектов, как двоичные файлы, более подробно объясняется здесь:

<https://technet.microsoft.com/ru-ru/library/hh852349.aspx>

Создание резервной копии базы данных WSUS

Прежде чем приниматься за решение серьезной задачи миграции, вы должны позаботиться о создании резервной копии конфигурации, примененных исправлений и баз данных. Перед выполнением любых крупных задач модернизации или миграции, понадобится протестировать процесс резервного копирования и восстановления.

Частью рекомендуемой стратегии миграции является резервное копирование базы данных WSUS 3.0 SP2 и последующее восстановление этих данных на новом целевом сервере. После восстановления базы данных WSUS 3.0 SP2 на новом сервере WSUS v6 в Windows Server 2012 R2 процесс переноса должен завершиться успешно и вам не придется решать проблемы с утраченными отчетами, совместимостью данных или отменой примененных ранее исправлений.

Резервные копии информации и базы данных WSUS будут зависеть от типа выполняемого резервного копирования. Существует один процесс для резервного копирования и восстановления Windows Internal Database и другая последовательность действий, если в качестве сервера базы данных используется SQL Server. Создание резервной копии базы данных SQL Server описано по ссылке:

<https://technet.microsoft.com/ru-ru/library/ms175477.aspx>

Базу данных WID можно просмотреть в проводнике объектов (Object Explorer); после того как вы раскроете узлы баз данных, она будет обозначаться во всех экземплярах как SUSDB.

За дополнительной информацией о создании резервных копий WSUS и пошаговым руководством по этому процессу обращайтесь по ссылке:

<http://tinyurl.com/c31widbackup>

Дополнительные соображения

Помимо разработки плана резервного копирования для новой среды WSUS и подтверждения того, что все клиенты в организации получают обновления от нового сервера WSUS на основе Windows Server 2012 R2, вам необходимо разработать исчерпывающую документацию по всем настройкам, определенным для вашей организации. Уделите время включению сценариев PowerShell, приведению ссылок на любые компоненты и перечислению предварительных условий.

Как вы видели во многих приведенных ранее примерах, основными соображениями являются интенсивное использование PowerShell и количество новых процессов, выполняемых в его командной строке. Удостоверьтесь в том, что располагаете четким планом тестирования и списком задач в той или иной форме, что поможет создать контрольные точки на всем пути миграции.

Еще одно важное соображение касается построения собственного плана миграции и документации, чтобы иметь определенный процесс с указанием всех основных предварительных условий и диаграммы существующей инфраструктуры. Наличие такой документации становится исключительно полезным, если в будущем вам понадобится перейти на более крупный сервер или вы решили перейти с WID на SQL.

Операционное управление и инструменты

Клиентские компьютеры используют для получения обновлений WSUS клиент автоматического обновления Windows и могут быть сконфигурированы с применением объекта групповой политики. Объект GPO резко сокращает административные накладные расходы, поскольку один такой объект можно однократно развернуть на всех компьютерах в среде Active Directory. Конфигурирование автоматического обновления Windows посредством GPO производится с помощью редактора объекта групповой политики (Group Policy Object Editor).

PowerShell и WSUS

Управлять всеми аспектами WSUS можно посредством PowerShell, который предоставляет великолепный набор инструментов, ориентированных на повседневное управление обновлениями. Замечательным примером того, что можно делать с помощью этих инструментов, а также функций PowerShell в WSUS является возможность перехода от установки роли WSUS на сервере Windows Server 2012 R2, как показано здесь:

```
... \Install-WSUSServ.ps1 -ComputerName BF1 -StoreUpdatesLocally  
-ContectDirectory "E:\Packages\WSUS" -InstallDatabasePatch "E:\"  
-CreateDatabase -Verbose
```

к управлению клиентом и настройками реестра с помощью командлетов `Get-WSUSClientSettings` и `Set-ClientWSUSSettings`. Получить более подробную информацию о любом из этих командлетов можно по команде `Get-Help` или в Интернете. По ссылке <http://tinyurl.com/c3lpswsus> доступна отличная статья по управлению WSUS и PowerShell.

Обновление с учетом кластеров

В Windows Server 2012 R2 предлагается новый компонент, который называется обновлением с учетом кластеров (Cluster-Aware Updating — CAU). Этот компонент позволяет обновлять кластеры без потери доступности в рамках окна обновлений. Когда компонент CAU запускается внутри окна обновлений, он переводит первый узел в режим обслуживания и передает рабочую нагрузку другим серверам в кластере, пока выполняется установка обновлений и при необходимости перезагрузка. После того как первый узел возвращается в рабочее состояние, CAU выводит данный сервер из режима обслуживания, возвращает ему исходные роли и переходит к следующему узлу. Например, при наличии кластера из двух узлов все роли или серверы из узла 1 будут перенесены в узел 2. После внесения исправлений в узел 1 и его перезагрузки он вернется к исполнению своих исходных ролей, а затем примет роли, размещенные в узле 2. Узел 2 будет переведен в режим обслуживания и перенесет свои серверы в узел 1.

ДОПОЛНИТЕЛЬНЫЕ ИНСТРУМЕНТЫ УПРАВЛЕНИЯ ИСПРАВЛЕНИЯМИ, ПРЕДОСТАВЛЯЕМЫЕ MICROSOFT

Хотя в этом разделе внимание было сосредоточено на WSUS, доступно еще несколько инструментов производства Microsoft, которые могут содействовать в управлении обновлениями внутри организации.

- **Microsoft Update** (Центр обновления Microsoft). Компонент Microsoft Update теперь включен в панель управления и позволяет просматривать текущие настройки, выяснять, когда применяются обновления, и видеть действие, которое предпринимается при обнаружении обновлений.
- **Microsoft Update Catalog** (Каталог центра обновления Microsoft). Все файлы, доступные в Microsoft Update, имеются и в Microsoft Update Catalog, в том числе драйверы, исправления, безопасность и другие обновления продуктов Microsoft. Важной особенностью Microsoft Update Catalog является возможность добавления нескольких в корзину и загрузки их всех за раз. Каталог центра обновления Microsoft находится по ссылке <http://catalog.update.microsoft.com>.
- **Командлеты PowerShell для службы Windows Server Update Services**. В Windows Server 2012 R2 доступна обширная библиотека командлетов PowerShell, которые применяются для решения общих и повторяющихся задач внутри инфраструктуры WSUS. С полным списком этих командлетов PowerShell можно ознакомиться в TechNet (<http://tinyurl.com/c31pscmdlets>). Возможность управления компонентами и классификациями исправлений из PowerShell позволяет дополнительно автоматизировать процесс управления многосерверными инфраструктурами и оказывать более тонкое влияние на процесс обновления (например, запрещать применение определенного исправления к конкретному развертыванию).
- **Инструменты для поддержки безопасности Microsoft**. В клиентах Windows Server 2012 R2 и Windows 8 вместо MBSA (Microsoft Baseline Security Analyzer — анализатор базовых уровней безопасности Microsoft) используются инструменты оценки безопасности (Security Assessment Tools), которые обеспечивают поддержку Windows 7, Windows Server 2008, Windows XP, Windows Vista и Windows Server 2008 R2.

Доступно несколько инструментов: Microsoft Security Assessment Tool 4.0, Microsoft Baseline Security Analyzer 2.2 и Microsoft Security Compliance Manager. Все эти инструменты и дополнительные сведения о них можно найти на веб-сайте Microsoft.

- **Блог центра реагирования на проблемы безопасности Microsoft**. Центр реагирования на проблемы безопасности Microsoft (Microsoft Security Response Center — MSRC) предназначен для выдачи обновлений безопасности для продуктов Microsoft. Этот сайт также предоставляет сводки о проблемах, которые еще не решены, но изучаются. Блог MSRC можно использовать для получения текущей информации. Он доступен по ссылке <http://blogs.technet.com/b/msrc/>.
Отслеживание этой группы в Твиттере (@MSFTSecResponse) позволит быть в курсе актуальных обновлений.

Инструменты Cluster-Aware Updating можно устанавливать на компьютерах Windows Server 2012 R2 и Windows 8. После установки инструментов вы конфигурируете нужный сценарий CAU; примеры таких сценариев можно найти по ссылке <http://tinyurl.com/c31cluster>.

В руководствах по сценариям Cluster-Aware Updating вы заметите, что компонент CAU работает в двух основных режимах.

- ◆ **Самообновление.** Эта конфигурация выполняется на узле кластера, который вы хотите обновить. Вам понадобится только настроить расписание обновления и позволить CAU обновить кластер.
- ◆ **Дистанционное обновление.** Вы запускаете CAU из автономного сервера или клиента, не входящего в кластер, например, из настольного компьютера Windows 8 с установленными инструментами CAU. Затем вы подключаетесь к нужному кластеру и обновляете его согласно расписанию.

В ходе установки и управления компонентом Cluster-Aware Updating вы обнаружите набор командлетов PowerShell, которые помогут выяснить, готов ли сервер, запустить необходимый процесс и проверить общее состояние кластеров. Выбрав подходящий метод применения компонента CAU, а также установив расписание, вы получите в свое распоряжение расширенные возможности Windows Server 2012 R2 и новую роль WSUS v6.

Диспетчер конфигурации системного центра

Диспетчер конфигурации системного центра (System Center Configuration Manager — SCCM) — это инструмент централизованного управления, построенный на основе комплекта программного обеспечения System Center (Системный центр) от Microsoft. В число основных областей внимания SCCM входит управление клиентами (серверами и рабочими станциями), применение исправлений, защита конечных точек, развертывание приложений и автоматизированная доставка операционных систем.

Анализ самой последней версии этого продукта, SCCM 2012 SP1, можно найти по ссылке:

<https://www.microsoft.com/ru-ru/server-cloud/products/system-center-2012-r2-configuration-manager/default.aspx>

Диспетчер конфигурации системного центра предлагает более широкие возможности генерирования отчетов и поддержания совместимости по сравнению с WSUS. Для любой средней и крупной организации обычно рекомендуется использовать SCCM в качестве основного инструмента применения исправлений. Ниже перечислены некоторые дополнительные преимущества внедрения SCCM.

- ◆ Возможность централизованного отката исправления, которое уже было развернуто.
- ◆ Оценка совместимости, позволяющая выполнять поиск программного обеспечения или обновлений, которые необходимы для обеспечения совместимости.
- ◆ Один унифицированный клиент: вы можете использовать клиент SCCM для установки обновлений, управления или регулировки обновлений и существенного упрощения единичных развертываний.
- ◆ Усовершенствованные отчеты и возможность определять подписки, которые помогают оценивать совместимость.

- ◆ Возможность определения окон обслуживания для выталкивания исправлений; использование групповой политики обеспечивает только строгий подход в стиле “все или ничего” к применению исправлений в системах. С помощью SCCM и окон обслуживания вы можете вносить исправления в подгруппы компьютеров только на протяжении определенных часов.
- ◆ Издатель обновлений системного центра (System Center Update Publisher) позволяет собирать загрузочные файлы исправлений от Adobe, Java и производителей оборудования. Эти исправления легко интегрируются в развертывание и расписание.
- ◆ Автономное обслуживание позволяет обновлять файл WIM (Windows Image File Format — файловый формат для образа Windows) после его сохранения, избавляя от необходимости развертывать и обновлять образ вручную. Это гарантирует, что образы развертывания ОС всегда развертываются с самыми последними исправлениями.

Резюме

Используйте Windows Automatic Updates для проверки наличия новых обновлений на компьютере, работающем под управлением Windows 8. Компонент Windows Automatic Updates входит в состав панели управления и применяется для проверки наличия на сайте Microsoft Update любых обновлений для вашего компьютера.

Контрольный вопрос. Воспользуйтесь Windows Automatic Updates на компьютере Windows 8, чтобы проверить наличие для него доступных обновлений.

Применяйте Windows Update Standalone Installer для молчаливой установки обновлений безопасности. Инструмент Windows Update Standalone Installer применяется для установки обновлений безопасности во всех операционных системах Windows, начиная с Windows Vista и Windows Server 2008.

Контрольный вопрос. Установите в молчаливом режиме обновление безопасности и отложите требуемую перезагрузку с использованием Windows Update Standalone Installer.

Идентифицируйте четыре фазы управления исправлениями. Согласно рекомендациям Microsoft, существуют четыре фазы при планировании стратегии управления исправлениями.

Контрольный вопрос. Какое из перечисленных ниже действий не имеет отношения к четырем фазам управления исправлениями?

1. Идентификация
2. Поиск и устранение проблем
3. Оценка и планирование
4. Оценка
5. Развертывание