УДК 004.45

Загороднюк С.П.[1], к.ф.-м.н.

Використання служби Windows Server Update Services в гетерогенних локальних обчислювальних мережах з відсутнім централізованим адмініструванням

В статті пропонується метод прозорої переадресації трафіку, що генерує служба автоматичного оновлення операційних систем Microsoft Windows, на службу Windows Software Update Services за допомогою апаратно-програмного комплекса на основі маршрутизатора Cisco ASA з підтримкою протоколу WCCP, а також програми проксі-сервера Squid з додатковим програмним модулем-переадресатором. Представлено результати тестування і впровадження апаратно-програмного комплекса в мережі Київського університету імені Тараса Шевченка.

Ключові слова: оновлення програмного забезпечення Microsoft, служба Windows Update, проксі-сервер, модуль-переадресатор.

[1] Київський національний університет імені Тараса Шевченка,03680, м. Київ, пр-т. Глушкова 4г, e-mail: kola@univ.net.ua

S. P. Zagorodniuk[1], PhD.

Using a Windows Server Update Services in heterogeneous local area networks with decentralized administration

The article presents the method of transparent redirection of traffic generated by Automatic Updates service in operating systems Microsoft Windows to the service Windows Software Update Services using hardware-software system based on Cisco ASA router with WCCP protocol support, as well as proxy server Squid with additional software redirection module. The results of the testing and implementation of hardware-software system in a network of Kyiv Taras Shevchenko National University are also present in the article.

Key Words: Microsoft software update,Windows Update service, proxy server, redirection module.

[1] Taras Shevchenko National University of Kyiv, 03680, Kyiv, Glushkova st., 4g, e-mail: kola@univ.net.ua

Статтю представив д.ф.-м.н., проф. Погорілий С.Д.

Своєчасне оновлення операційних систем (ОС) та програмних продуктів є важливим підгруттям стабільності [4] і безпеки [5] програмного забезпечення (ПЗ). Для комерційного пропрієтарного ПЗ це означає, в першу чергу, комерційний успіх від поширення ПЗ, а також зміцнення репутації його виробника. Для безкоштовного вільного ПЗ це означає довготривалість існування проекту по його розробці та підтримці, інтегрованість та сумісність його функціоналу з іншими існуючими апаратно-програмними комплексами.

Користувачі ПЗ доволі часто задають просте і очевидне, на їх погляд, запитання: чому одразу не можна розробити стабільне і безпечне ПЗ, що не потребує подальшого оновлення? На практиці виявляється, що не можна за багатьма причинами Безкоштовне ПЗ, як правило, поширюється на умовах "As Is". Розробники комерційного ПЗ мають чітко визначений обмежений час на відлагоджування ПЗ з наперед заданою функціональністю. Цей час визначається як золота середина між двома крайніми негативними випадками. Якщо час відлагоджування надто малий, то рівень стабільності і безпеки цього ПЗ буде низький, що не буде відповідати його ринковій вартості. Якщо час відлагоджування, навпаки, надто великий, то ПЗ буде представлено на ринку з великою затримкою і програє конкурентну боротьбу з ПЗ від іншого виробника. Для користувачів обох видів ПЗ - безкоштовного і комерційного, як правило, організовано зворотній зв'язок для централізованого накопичення зауважень і побажань щодо експлуатації ПЗ. З наведених тверджень випливає очевидний висновок: ПЗ повинно бути вчасно представлено і доступно для користувачів, а процес його відлагоджування повинен продовжуватись і тривати ще деякий період часу.

Всесвітньо відомі корпорації-виробники ПЗ (Microsoft, Adobe і т.п.), що мають вже сформовану стійку репутацію, дозволяють собі представляти на ринку не повністю відлагоджене ПЗ і фактично використовувати користувачів цього ПЗ як велетенську армію бета-тестерів, не сумніваючись у тому, що в результаті звернень користувачів до служби підтримки завершальний етап відлагодження ПЗ буде протікати набагато швидше і ефективніше, ніж в результатів випробовування ПЗ кадровими розробниками корпорацій.

Процес оновлення ПЗ являє собою автоматичне завантаження та встановлення пакетів оновлень. Для цього в ОС Microsoft Windows зареєстрована і постійно працює служба Automatic Updates (Windows 2000, XP, 2003) або Windows Update (Windows Vista, 7, 8, 2008, 2012). Ця служба щодоби з'єднується з загальносвітовим глобальним центром оновлень корпорації Microsoft і перевіряє наявність нових пакетів оновлень. Однак очевидно, що коли підприємство або установа має багато комп'ютерів з однотипною ОС, то важко назвати раціональним факт з'єднання кожного індивідуального комп'ютера з глобальною загальносвітовою службою оновлення і багатократне завантаження з неї однакових файлів. Саме з метою раціонального використання Інтернет-каналу підприємства корпорація Microsoft надає можливість кожному підприємству додатково налаштувати в своїй локальній мережі спеціалізовану службу - Windows Server Update Services (WSUS) [4-6]. Ця служба дозволяє багатократно скоротити зовнішній мережевий трафік, що є вкрай важливим для регіональних підрозділів і відділень підприємства. Крім того, коли WSUS тримує новий пакет оновлень, він може бути попередньо проаналізований і перевірений адміністратором на сумісність з існуючим ПЗ, що використовується на підприємстві і тільки при позитивному результаті тестування дозволені ним для встановлення на робочі станції та сервери підприємства.

Однак розгортання і налаштування лише самої служби WSUS є недостатнім для того, щоб всі комп'ютери підприємства з операційною системою Windows стали нею активно користуватись. Клієнтська частина служби WSUS операційної системи Windows, роль якої виконує вбудована в операційну систему Windows служба Windows Update / Automatic Update (WU/AU), також повинна бути додатково сконфігурована у такий спосіб, щоб запити на завантаження нових оновлень були адресовані не глобальному центру оновлень, а до розгорнутої і функціонуючої в локальній мережі підприємства службі WSUS.

Налаштування служби WU/AU на одному комп'ютері як клієнта до служби WSUS не є складним [7]. Воно полягає в явному присвоюванні URL-посилання на службу WSUS конкретному параметру локальної політики ОС Windows (рис. 1). Для англомовної ОС Windows цей параметр називається «Specify intranet Microsoft update service location» (SIMUSL).

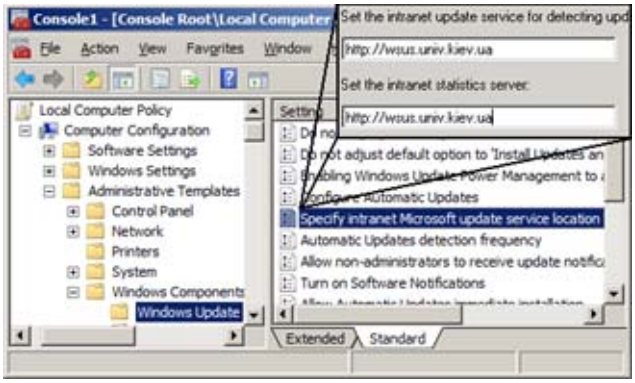

Рис. 1. Ручне налаштування служби WU/AU як клієнта до служби WSUS.

Наявність стандартного параметра SIMUSL породжує проблему централізованого масового застосування цього параметра на всіх комп'ютерах підприємства. В багатьох випадках ця проблема ефективно вирішується шляхом впровадження мережевих служб централізованої аутентифікації та застосування стандартних політик підприємства. Найбільш популярними службами серед такого ПЗ є служби каталогу Microsoft Active Directory та Novell eDirectory. Вони передбачає об'єднання всіх комп'ютерів підприємства в один каталог і примусове застосування до всіх комп'ютерів каталогу довільної кількості параметрів локальної політики, в тому числі параметра SIMUSL [4-7]. Доки комп'ютер користувача входить до каталогу, користувач не може скасувати або перевизначити параметр SIMUSL та інші параметри, налаштовані адміністратором каталогу.

Проте практика показує, що служби Microsoft Active Directory, Novell eDirectory та інші популярні служби каталогу, не зважаючи на їх очевидні переваги, дуже важко впроваджуються в наукових і академічних установах, державних

підприємствах, силових структурах тощо. По-перше, само існування служби каталогу вимагає її регулярного обслуговування і налаштування. По-друге, істотна кількість працівників в вищевказаних установах працюють на власних портативних комп'ютерах і мобільних пристроях, які неможливо в примусовому порядку ввести в каталог і застосувати на них доменні політики. В більшості випадків ситуація заходить в глухий кут: адміністратор локальної мережі налаштовує службу WSUS, а примусити учасників мережі користуватись цією службою не може. Дана стаття описує апробований і перевірений на практиці метод вирішення цієї проблеми.

Основою програмного комплекса є служба веб-проксі під керуванням популярного відкритого ПЗ «Squid» [1]. Дана програма існує понад 30 років, добре відлагоджена, стабільна і працює на всіх популярних операційних системах, в тому числі Linux та Windows. Класичний режим роботи проксі-сервера Squid передбачає ручне введення його параметрів на кожному комп'ютері підприємства. Але примусити всіх користувачів підприємства налаштувати параметри проксі-сервера є ще більш складною задачею для адміністратора служби WSUS, ніж встановити параметр локальної політики SIMUSL.

Проте проксі-сервер Squid може працювати не тільки у класичному режимі. У поєднанні з файрволами і маршрутизаторами він може працювати в режимі «прозорого» проксі [1,2]. В цьому режимі маршрутизатор не відправляє HTTP-запити користувача до HTTP-сервера в Інтернеті, а переадресовує їх проксі-серверу Squid, який може працювати або на окремому хості, або на самому маршрутизаторі.

Характерною особливістю проксі-сервера Squid є можливість розширення його функціональності за допомогою додаткових модулів-переадресаторів, які можно розробляти довільною мовою програмування. Такі модулі

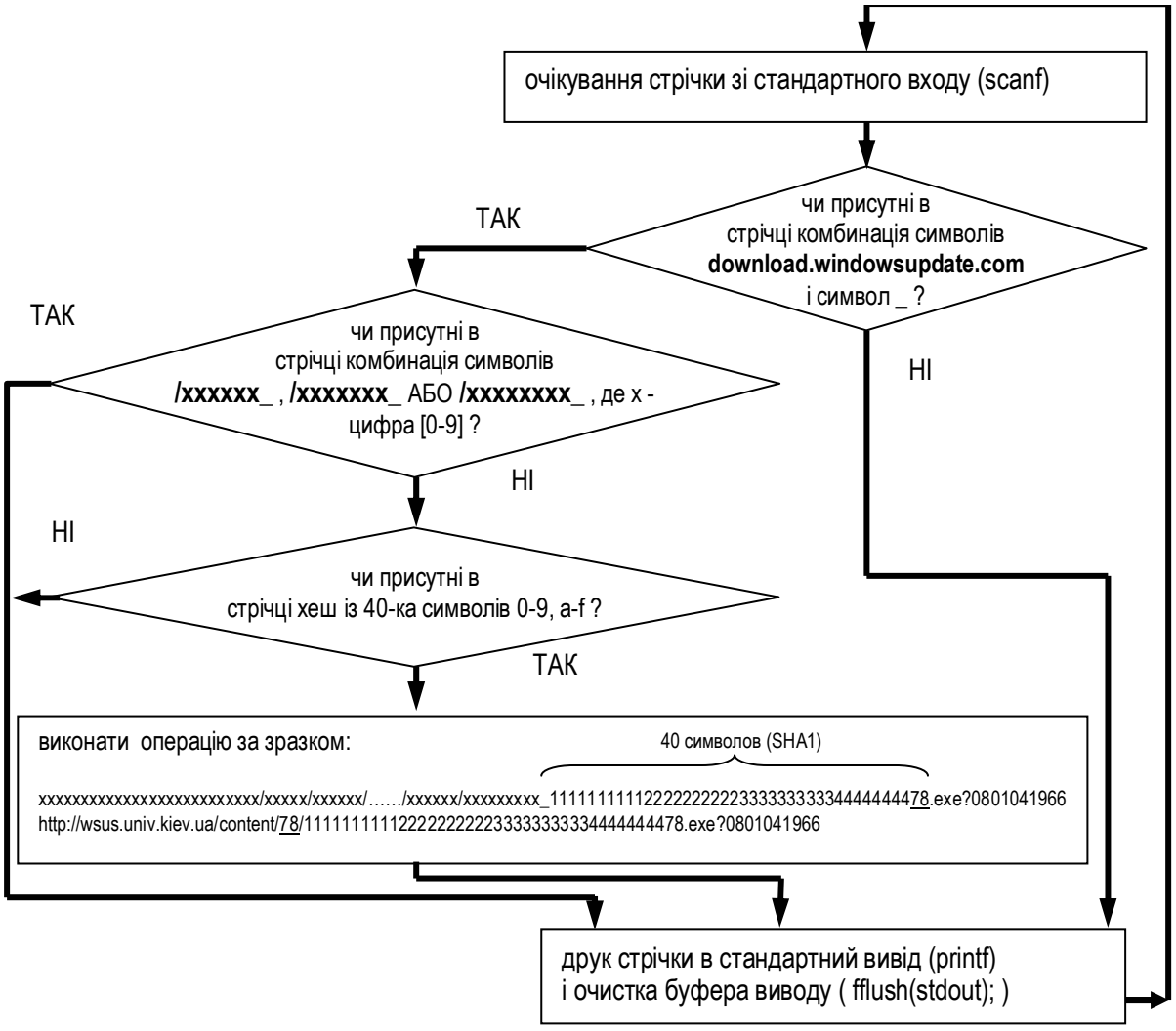

Рис. 2. Логіка роботи програми-переадресатора проксі-сервера Squid.

дозволяють проксі-серверу перед обробкою HTTP-запита клієнта попередньо модифікувати його URL-адресу і таким чином переадресувати запит на інший неоригінальний сервер, відповідь якого клієнт сприймає як «відповідь» оригінального сервера. Аналіз мережевих запитів, що генерує служба WU/AU, дозволив спроектувати та реалізувати переадресатор за блок-схемою, наведеною на рис. 2:

З метою перевірки стабільності даного модуля-переадресатора він реалізований і впроваджений в локальній мережі Київського університета імені Тараса Шевченка у складі програмного комплексу на базі популярного маршрутизатора Cisco ASA з підтримкою протокола WCCP [3]. Результат роботи модуля-переадресатора зручно продемонструвати на прикладі завантаження одного оновлення для російської версії Windows XP. Оригінальна URL-адреса цього оновлення

http://au.download.windowsupdate.com
/msdownload/update/v3-19990518/cabpool
/windowsxp-kb842773-v2-x86-
rus_56c63b12ecca0686a25385bf39f8ebc2e426d52b.exe

модифікується модулем-переадресатором і перетворюється на URL-адресу

http://wsus.univ.kiev.ua/content/2b/56c63b12ecca0686a25
385bf39f8ebc2e426d52b.exe

Модифікована URL-адреса успішно обробляється проксі-сервером, про що свідчить відповідний запис в його журналі:

10.17.1.2 TCP_MISS/200 375 GET
http://au.download.windowsupdate.com
/msdownload/update/v3-19990518/cabpool
/windowsxp-kb842773-v2-x86-
rus_56c63b12ecca0686a25385bf39f8ebc2e426d52b.exe -
DIRECT/10.25.25.200 application/octet-stream

Цей запис тлумачиться наступним чином: Компьютер з адресою 10.17.1.2 успішно (код помилки 200 означає «OK») виконав команду HTTP-GET на завантаження вказаного файла з вузла 10.25.25.200 (IP-адреса WSUS-сервера wsus.univ.kiev.ua), час виконання запиту 375 мс. В результаті роботи програмного комплексу весь трафік, що генерують служби WU/AU, не виходить за межі локальної приватної мережі університету і не навантажує його закордонний Інтернет-канал.

Висновки

1.Служба автоматичних оновлень операційних систем Microsoft Windows генерує значний закордонний Інтернет-трафік і може бути причиною повільної роботи мережі Інтернет усього підприємства або установи.

2.Служба оновлень не налаштована на явне використання проксі-серверів, а отже підтримує лише «прозорий режим» проксі-сервера.

3.Створюючи модулі-переадресатори популярного проксі-сервера Squid, можна змінювати маршрут завантаження великих файлів і таким чином суттєво знизити завантаження зовнішнього Інтернет-каналу підприємства.

Список використаних джерел

1. *Kulbir Saini.* Squid Proxy Server 3.1: Beginner's Guide. – Packt Publishing, 2011. – 332 p.
2. *Duane Wessels.* Squid: The Definitive Guide. – O'Reilly Media, 2004. – 472 p.
3. *Zach Seils, Joel Christner.* Deploying Cisco Wide Area Application Services. – Cisco Press, 2008. – 400 p.
4. *Susan Norwood.* Microsoft Windows Server Update Services 3.0 Operations Guide.– Microsoft, 2007. – 167 p. (http://www.microsoft.com/en-us/download/details.aspx?id=4813)
5. *Jeff Centimano.* Windows Server Update Services 3.0 Usability Improvements. – Microsoft, 2007.– 14 p. (http://download.microsoft.com/download/e/5/7/e578cebc-0533-4baa-bbef-f9e3f36e1976/wsus3%20usability%20improvements.doc)
6. *Susan Norwood.* Deploying Microsoft Windows Server Update Services. – Microsoft, 2007. – 154 p. (http://www.microsoft.com/en-us/download/details.aspx?id=21543)
7. Readme for Microsoft Windows Server Update Services 3.0. – Microsoft, 2007. – 28 p. (http://www.microsoft.com/en-us/download/details.aspx?id=7226)

Надійшла до редколегії 22.11.13