

Дослідження Технологій Формування Інфраструктури Комп'ютерної Мережі

Володимир Саєнко

кафедра інформаційних управляючих систем
Харківський національний університет
радіоелектроніки
Харків, Україна
vladimir.sayenko@nure.ua

Роман Савченко

кафедра інформаційних управляючих систем
Харківський національний університет
радіоелектроніки
Харків, Україна
roma.savchenko.96@gmail.com

Study on Designe Technologies for Computer Network Infrastructure

Vladimir Sayenko

Information Control System department
Kharkov National University of Radioelectronics
Kharkov, Ukraine
vladimir.sayenko@nure.ua

Roman Savchenko

Information Control System department
Kharkov National University of Radioelectronics
Kharkov, Ukraine
roma.savchenko.96@gmail.com

Анотація—Розглядаються питання щодо керування конфігурацією мережі. Конфігурація сервера комп'ютерної мережі розглядається як логічна конфігурація, сформована на основі сервісів у операційній системі Windows. Всі сервіси поділяються на кілька груп: обов'язкові, звичайні, спеціальні, помилкові, додаткові, невідомі. Критерії повноти функціональності, критерії рівня сервісу, технології вибору сервісів та технологічних змін у структурі-конфігурації мережевої інфраструктурі. Цей підхід забезпечує більш ефективне рішення для управління комп'ютерними мережами.

Ключові слова—адміністрування, конфігурація, інфраструктура, комп'ютерна мережа, Windows Server, сервіси, служби, ролі.

Abstract—The questions on network Configuration Management are considered. The computer configuration is considered as a logical configuration formed on the basis of services in the Windows operating system. All services are divided on a several groups: mandatory, ordinary, special, false, additional, unknown. The criteria for completeness of functionality, service level criteria, service selection technologies and technology changes in the structure-configuration of network infrastructure. This approach provides a more effective solution for computer networks management.

Keywords—administration, configuration, infrastructure, computer network, Windows Server, services, services, roles.

I. ВСТУП

Під інфраструктурою мережі розуміють безліч взаємопов'язаних технологій і систем, які адміністратори

повинні досконально знати, щоб успішно підтримувати роботу мережі і усувати неполадки.

Інфраструктура мережі - це набір фізичних і логічних компонентів, які забезпечують зв'язок, безпеку, маршрутизацію, управління, доступ і інші обов'язкові властивості мережі [1]. Найчастіше інфраструктура мережі визначається проектом, але багато визначають зовнішні обставини і «спадковості». Наприклад, підключення до Інтернету вимагає забезпечити підтримку відповідних технологій, зокрема протоколу TCP/IP. Інші ж параметри мережі, наприклад фізична компоновка основних елементів, визначаються при проектуванні, а потім вже успадковуються пізнішими версіями мережі.

Адміністрування комп'ютерних мереж – це той вид обслуговування, без якого не може обійтися жоден сучасний офіс. Завдяки локальній мережі став можливим обмін даними між групами користувачів і програмами в онлайн режимі. Проведення комп'ютерної мережі може допомогти заощадити гроші на програмному забезпеченні. Якщо співробітникам Вашої фірми для роботи потрібне певне програмне забезпечення (ПЗ), Вам зовсім не обов'язково купувати і встановлювати програми на кожен ПК, досить встановити їх на сервер. Це стало можливим, через підвищення рівня продуктивності серверів і їх доступності для установки і налаштування під кожен тип підприємства.

Традиційні способи адміністрування мережі засновані на управлінні нею з урахуванням певних чітко регламентованих правил. Такий підхід прийнятний тільки для адміністрування невеликої мережі з обмеженою інтенсивністю трафіку. Налаштування великих



корпоративних мереж, які мають складну топологію і включають безліч окремих підмереж, істотно відрізняється в адмініструванні через безлічі додаткових мережевих параметрів в конфігурації.

Основне призначення комп'ютерної мережі - надання інформаційних послуг (сервісів). Для реалізації процедури сервісу необхідно два програмних додатки: клієнт і сервер. Всі сучасні комп'ютери мають можливість надання сервісних послуг. Вони містять компоненти-додатки, які мають категорії «служби» (сервіси) [2]. Наявність таких служб визначає інформаційну функціональність комп'ютерної мережі. Фактично склад цих служб визначає логічну конфігурацію сервера комп'ютерної мережі. Кожна зі служб споживає ресурси і впливає на статус інформаційної захищеності мережі. Отже, формування оптимальної конфігурації цих служб дозволяє оптимізувати роботу комп'ютерної мережі. Розробка відповідних методів оптимізації - актуальне завдання, особливо для операційних систем (ОС) Windows.

Логічна конфігурація може бути розглянута з різних позицій [3]. Будемо розглядати тільки структуру, утворену на основі сервісів в ОС Windows Server 2016. Всі сервіси можна розділити на кілька груп: системні обов'язкові, просто системні, системні помилкові, спеціальні обов'язкові, додаткові, невідомі.

А. Кроки аналізу:

а) а) Згідно отриманих класів першою умовою є системні обов'язкові служби, без яких завантаження ОС неможливе.

б) б) Наступна умова, виходячи з вимог користувача, вибираємо номенклатуру сервісів з групи просто системні, ті які необхідні для роботи в мережі (локальній, інтернет), та запуску необхідних системних утиліт.

с) с) З класу спеціальні обов'язкові, якщо користувач буде використовувати антивірусне програмне забезпечення, додаткове ПЗ для виконання певних завдань, додаємо відповідні сервіси.

д) д) Для функціонування додаткового обладнання сервера комп'ютерної мережі додаємо до списку необхідні сервіси з класу додаткові.

е) е) Також необхідно контролювати сервісний склад виявляючи сервіси, які можна віднести до груп системні помилкові та невідомі.

Результати проведеного аналізу показують, що при безконтрольному ставленні до складу конфігурації число невідомих сервісів згодом збільшується. Як ми бачимо кількість запущених сервісів є дуже великою, що відображається на роботі системи. Проаналізувавши та чітко визначивши які служби потрібні, а які ні, можна значно оптимізувати роботу ОС.

Отримана конфігурація є достатньою для виконання необхідних функцій і оптимізована під вирішувани задачі. Практична цінність полягає в тому, що вона збільшує

швидкість комп'ютерної системи та покращує рівень інформаційної безпеки.

Залежно від бізнес-процесів і розмірів підприємств стандартний набір служб і ролей не є оптимальним для роботи сервера комп'ютерної мережі. Так як установка додаткових компонентів використовує доступні ресурси сервера.

II. ОСНОВНІ РЕЗУЛЬТАТИ

Пропонується метод контролю стану логічної конфігурації інфраструктури комп'ютерної мережі з використанням розширеного набору сервісів за рахунок використання можливостей нових версій операційних систем Windows [4].

Чому дана задача є актуальною? З виходом нових версій операційних систем Windows Server додаються нові сервіси та служби, спрощується процес адміністрування, але не всі сервіси необхідні для процесу функціонування конкретного типу підприємства, це залежить від розмірів об'єкта (малий офіс, середній офіс, великий офіс, компанія, корпорація), вимог безпеки (слабкий, середній, високий), рівня інформатизації об'єкта. У зв'язку з цим необхідна розробка технології вибору раціонального набору сервісів в залежності від типу підприємства, що значно скоротить вартість володіння, зробить рішення більш надійним і відмовостійким, а також підвищить загальний рівень безпеки інфраструктури.

Нововведення в Windows Server 2016 пов'язані з віртуалізацією, сховищами даних і службами віддаленого робочого столу.

Велика частина нововведень в Windows Server 2016 пов'язані з безпекою. Це можливо побачити по всіх ролях і службах, а саме Shielded VM в Hyper-V, code integrity в сервері додатків і Privileged Access Management в Active Directory Domain Services.

З виходом Windows Server 2016, служба Active Directory отримала три важливих нових функцій, а саме Access Management, Azure AD Join і Microsoft Passport [5]. Це розподілена база даних і служба каталогів, яка реплікується на всі контролери домену в мережі. У базі даних Active Directory зберігається інформація про мережеві об'єкти, в тому числі про домени, комп'ютери, користувачів та інші об'єкти. Розподілена природа Active Directory дозволяє користувачам отримувати доступ до ресурсів, розташованим в будь-якій точці мережі, на основі одного входу в систему і забезпечує єдину політику адміністрування для всіх об'єктів мережі. Термін домен використовується як для позначення групи комп'ютерів в Active Directory, так і для завдання суфіксів в іменах DNS визначають ієрархію доменів [6].

Функціональність сервера Fi визначається набором сервісних програм (S1, S2, ..., Sn).

Зміна функціонального стану безпосередньо пов'язана зі зміною складу чи інформаційних властивостей сервісів (S1, S2, ..., Sn).



Логічна конфігурація комп'ютера (сервера) комп'ютерної мережі представлена набором від 1 до n сервісів (Services).

Проблема оптимізації логічної конфігурації формалізується у вигляді комплексного контролю за всіма елементами, діагностики, прийняття рішень для керування набором елементів логічної конфігурації, а саме набором сервісів.

Правильне функціонування (стабільний режим роботи) можна представити як набір сервісів, які вона підтримує, тобто

$$\text{Services} = \{\text{Service 1, Service 2, \dots, Service n}\},$$

де n – кількість сервісів (служб).

Кожен з сервісів містить певний окремий набір показників P (інформація про процеси та програми з якими працює елемент; його розмір; ресурси які він використовує; доступ до портів та його активність тощо):

$$\text{Service } i = \{P_1, P_2, \dots, P_k\},$$

де k – кількість показників.

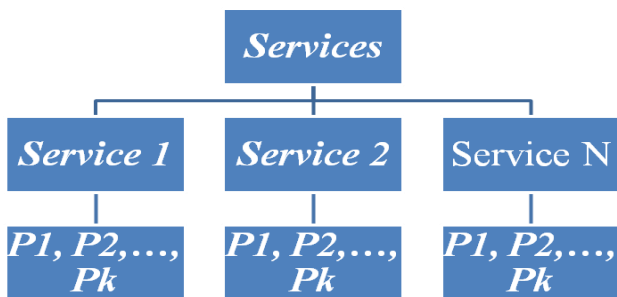


Рис. 1 – Конфігурація сервера комп'ютерної мережі.

Тоді наша задача оптимізації логічної конфігурації сервера комп'ютерної мережі набуває варіанту контролю стану окремих компонентів, в нашому випадку сервісів Service1, Service 2, ..., Service n (на основі показників P1, P2, ..., Pk), і побудови методів комплексного адміністрування, моніторингу, управління сервісами.

Метод заснований на представленні цієї конфігурації у вигляді комплексної інформаційної моделі. Модель складається з класів (груп) сервісів. Для кожного типового елемента класу вводиться опис, що відображає інформацію про процеси і додатках, з якими пов'язаний елемент; про його розмір, код і споживаних ресурсах, про порти, яке воно підтримує, про стан портів, про активність. Для кожного елемента створюється два опису: статичне (базова конфігурація) і динамічне (зміна активності). Оперативний контроль за сервісами дозволяє в будь-який момент часу дати характеристику функціонального стану комп'ютера і ступеня його фонові завантаженості. Аналогічні методи реалізовані в ProcessExplorer [2], але в ньому немає можливості провести розподіл сервісів на класи.

Наступним кроком є оптимізація конфігурації. Метод оптимізації заснований на використанні інформаційних

властивостей сервісних елементів, що стосуються їх функцій. Метод полягає в тому, що користувач формує свій набір функцій, який йому потрібен. Система автоматично пропонує відповідний мінімальний (достатній і необхідний) набір сервісів. При цьому пропонується контролювати системну цілісність.

Додатковим методом оптимізації конфігурації є реалізація контролю системних служб з перевіркою їх істинності (порівняння з еталоном), а також виявлення неправдивих системних служб. Крім того виявляються служби, які можуть бути віднесені до категорії «невідомі».

Для всіх служб пропонується також створити опис «корисних» і «небезпечних» функцій. Точно так же, як і служби за замовчуванням, додаткові служби можуть бути ризиком для безпеки. Якщо служби спроектовані для взаємодії і контролю важливих даних і файлів операційної системи, то вони можуть стати потенційним шлюзом, через який зловмисник зможе отримати цю інформацію. Опис служб дають можливість користувачеві оцінити ризик від використання даної служби, тобто показують користь від використання служби і потенційну небезпеку для всієї системи при її активності.

Підсумком запропонованих методів є сформована інфраструктура комп'ютерної мережі, яка буде достатньою для виконання необхідних функцій і, отже, оптимізована під розв'язуванні задачі. Практична цінність запропонованих методів полягає в тому, що вони сприяють підвищенню функціональності роботи комп'ютерної системи і підвищують рівень зручності експлуатації комп'ютерної мережі, а також його інформаційної безпеки.

III. ВИСНОВКИ

Розглянуто технологію формування інфраструктури комп'ютерної мережі на основі ОС Windows Server 2016. Всі необхідні сервіси в комп'ютерній мережі розгорнуті на одному сервері, що значно спрощує процес контролю за службами, а значить і адмініструванні всіх користувачів мережі. Визначено показники та критерії оцінювання повноти функціональності стану сервісної конфігурації, запропоновані нові методи контролю та оптимізації логічної конфігурації сервера комп'ютерної мережі.

ЛІТЕРАТУРА REFERENCES

- [1] Barinov, Andrei Security of the enterprise network infrastructure / Andrei Barinov. - Moscow: LAP Lambert Academic Publishing, 2016. - 513 p.
- [2] Mark E. Russinovich, Aaron Margosis. Windows Sysinternals Administrator's Reference\Microsoft Press; 1 edition (July 20, 2011) - 496 c.
- [3] A.Clemm. Network Management Fundamentals\ Cisco Systems, 2007 – 501 p.
- [4] Deytel, H., M. Operating systems. Basics and principles. T. 1 / HM Daytel, DR Chofnes. - M.: Binom, 2016. - 1024 p.
- [5] Russell, Jesse Web Server Comparison / Jesse Russell. - M.: VSD, 2017. - 310 p.
- [6] Microsoft Windows 2000, Active Directory Services. MCSE Training Course. - M.: Russian Editorial Office, 2013. - 608 p.

