УДК 004.8+65.05+681.5

DOI: 10.31673/2412-9070.2022.021221

Ю. І. КАТКОВ, доктор техн. наук, доцент;
В. П. ЛИСАК, студент;
В. В. ВИШНІВСЬКИЙ, студент,
Державний університет телекомунікацій, Київ

РОЗРОБЛЕННЯ КЛАСИФІКАЦІЇ ІНСТРУМЕНТІВ СИСТЕМНОГО АДМІНІСТРУВАННЯ СЕРВЕРІВ

Стаття присвячена актуальному питанню пошуку методів застосування інструментів системного адміністрування серверів, які надають можливість керувати та обслуговувати серверну інфраструктуру хмарного середовища. Поставлено задачу: визначити класифікацію інструментів системного адміністрування серверів, потрібних для ефективного системного адміністрування серверів хмарного середовища.

Відомо, що системний адміністратор відповідає за виконання завдань щодо керування та обслуговування серверної інфраструктури, яка допомагає компанії досягти своїх бізнес-цілей. Для виконання різноманітних завдань потрібно ухвалювати рішення щодо вибору засобів адміністрування серверів із множини наявних або створення нових. Звідси виникають складнощі з вибором найбільш ефективних засобів для розв'язання завдань та опису цих інструментів. Особливо це важливо, коли настають питання навчання системних адміністраторів, тобто необхідно досягти певних цілей навчання, після завершення якого адміністратор зможе: описати функції центру адміністрування, правила ефективного використання засобів пакетів інструментів для системного адміністрування, кросплатформні інструменти адміністрування, інструменти для автоматизації виконання окремих завдань адміністрування; застосовувати різноманітні аналізатори та сніфери адміністрування, засоби віддаленого адміністрування сервера для керування серверами; визначати порядок диспетчеризації серверів; знаходити для використання спеціальне програмне забезпечення для обслуговування й налаштовування множини комп'ютерних систем і мереж моніторингу, а також різноманітних утиліт, застосунків та менеджерів для адміністрування.

Для розв'язання такого завдання запропоновано метод визначення ознак для проведення класифікації множини інструментів адміністрування через встановлення типів системних адміністраторів: адміністратор бази даних; адміністратор серверів; адміністратор мережі; адміністратор безпеки; вебадміністратор; системний інженер; інженер з надійності. Окреслено перелік груп типових завдань: адміністрування користувачів та груп користувачів; адміністрування засобів забезпечення безпеки системи; адміністрування локальних та мережних принтерів; моніторинг подій та ресурсів; архівування та відновлення даних. Запропоновано класи інструментів автоматизації задач системного адміністрування: пакети інструментів для системного адміністрування, кросплатформні інструменти адміністрування, інструменти у вигляді автоматизації окремих завдань адміністрування. Здійснено аналіз класів інструментів для системного адміністрування. Показано, що знання інструментів для системного адміністрування необхідне для усунення несправності, тестування, зв'язку та виправлення систем, потрібних для продовження роботи. За допомогою правильних інструментів робота стає менш виснажливою, оскільки багато завдань можна виконати за допомогою цих інструментів для системного адміністрування.

Ключові слова: адміністрування; інфраструктура; сервер; хмарне середовище.

ВСТУП

Відомо, що системний адміністратор (*sysadmin*, сисадмін) — це спеціаліст із підтримання в працездатному стані програмного забезпечення і комп'ютерного обладнання та будь-якої ІТ-інфраструктури загалом. До його обов'язків входить забезпечення надійного функціонування комп'ютерів та оргтехніки, мережі та програмних продуктів у компанії. Розрізняють кілька типів системних адміністраторів: *адміністратор бази даних* (*database administrator*, DBA), що обслуговує систему баз даних і відповідає за цілісність даних, а також ефективність і продуктивність системи; *адміністратор серверів*, який забезпечує ефективну роботу, підтримуючи оновлення програмного забезпечення, розробляючи та впроваджуючи нові системні структури, відстежуючи активність і безпеку функціонування сервера; *адміністратор мережі*, котрий обслуговує мережну інфраструктуру, здебільшого комутатори та маршрутизатори, і діагностує проблеми з ними або поведінку комп'ютерів, підімкнених до мереж; *адміністратор безпеки* — це спеціаліст із захисту комп'ютерів і мереж, зокрема адміністрування пристроїв безпеки, таких як брандмауери, а також консультації щодо загальних заходів безпеки; *вебадміністратор* — підтримує служби вебсервера (наприклад, Apache або IIS), які надають внутрішній або зовнішній доступ до вебсайтів та охоплюють завдання керування кількома сайтами, а також забезпечення безпеки та налаштування потрібних компонентів і програмного забезпечення; *системний інженер* — виконує регулярне технічне обслуговування апаратних та програмних засобів; *інженер із надійності сайту* — використовує програмну інженерію або програмний

підхід до керування системами, наприклад *Site Reliability Engineering* (SRE).

Загалом системне адміністрування — це комплекс робіт, які потрібно виконувати системному адміністратору з обслуговування операційної системи та загальносистемного апаратно-програмного забезпечення, спрямованого на забезпечення стабільної та безпечної роботи засобів комп'ютеризації, а саме: забезпечення штатної роботи парку комп'ютерної техніки, мережі, програмного забезпечення, забезпечення інформаційної безпеки в організації, а також виконання поточних завдань із керування користувачами.

Відомо, що кожний тип адміністрування використовує свій набір інструментів адміністрування для забезпечення ефективного виконання адміністративних функцій. Умовно для системного адміністрування характерні такі основні напрямки завдань: моніторинг вебсерверів з метою підвищення захищеності та відмовостійкості серверів; проєктування, налаштування та кластеризація високонавантажених вирішень та розподілених систем; оптимізація адміністрування вебсерверів, оновлення та налаштування програмного забезпечення, профіль, діагностика. Отже, *системний адміністратор* відповідає за виконання завдань щодо керування та обслуговування серверної інфраструктури, яка допомагає компанії досягти своїх бізнес-цілей.

Вважається, що *системний адміністратор* має бути здатний використовувати різноманітні інструменти адміністрування для роботи центру адміністрування Windows або Unix; правил ефективного використання засобів віддаленого адміністрування сервера для керування серверами (наприклад, Remote Server Administration Tools for Windows, RSAT); порядку диспетчеризації серверів; використання спеціального програмного забезпечення обслуговування й налаштовування множини комп'ютерних систем моніторингу. Природно, що для виконання такої множини завдань потрібно ухвалювати рішення щодо вибору інструментів адміністрування, а саме: засобів поточного, віддаленого адміністрування серверів, засобів диспетчеризації серверів, а також слід оперативно вирішувати поточні технічні проблеми функціонування серверів за допомогою утиліт, застосунків, менеджерів адміністрування. Сьогодні стало очевидним, що застосування інструментів системного адміністрування серверів надає великі можливості ефективно керувати та обслуговувати серверну інфраструктуру хмарного середовища. Тому головне, актуальне та своєчасне завдання сучасності для системного адміністратора полягає в організації і виконанні роботи з досягненням оптимальної продуктивності та гарантованої відмовостійкості комп'ютерних систем та служб.

Постановка завдання

Припустимо, що існує компанія, офіси якої розташовані в усьому світі. Вони надають послуги за допомогою всесвітньої мережі. Для керування всесвітньою мережею компанії створено обчислювальне середовище, що працює локально на Windows Server 2016, 2019. Для підвищення ефективності роботи компанії і досягнення своїх бізнес-цілей системному адміністратору компанії потрібно перекласти локальні сервери цієї мережі на Windows Server 2022. Тобто слід з'ясувати, в який спосіб можна застосовувати доступні інструменти адміністрування Windows Server, зокрема Windows Admin Center, засоби віддаленого адміністрування сервера, диспетчер серверів та Windows PowerShell. Крім того, звичайно, що для виконання множини завдань необхідно оперативно розв'язувати поточні технічні проблеми функціонування серверів за допомогою утиліт, застосунків, менеджерів адміністрування.

Тут постає потреба в попередньому вивченні та описі різних інструментів адміністрування, а також визначенні критеріїв вибору відповідного інструменту для певної ситуації з метою систематизації знань щодо підготовки (навчання) системних адміністраторів. Отже, систематизація знань щодо множини інструментів для системного адміністрування (класифікація інструментів системного адміністрування) необхідна для підвищення ефективності усунення несправності, тестування, зв'язку та виправлення систем, які потрібні для продовження роботи. За допомогою правильних інструментів робота стає менш виснажливою, оскільки багато завдань можна автоматизувати.

Аналіз останніх досліджень

Питання систематизації знань щодо підготовки (навчання) системних адміністраторів доволі актуальне та своєчасне. Сьогодні інтенсивно ведеться пошук у навчальних організаціях форм і методів навчання системних адміністраторів. Існує багато різноманітних навчальних організацій (шкіл, курсів, академій тощо), після закінчення яких отримують міжнародні дипломи, а також сертифікати від компаній-партнерів [1–3]. Нині такі навчальні організації надають слухачам та студентам навички, яких потребують роботодавці та сучасний бізнес — жодної сухої теорії та «води», оскільки роботодавцям потрібні не просто знання — їм потрібна компетенція в розв'язанні робочих завдань та налаштування бізнес-процесів. Але такий підхід не дає змоги майбутньому системному адміністратору самостійно вдосконалювати свої знання, уміння та навички через те, що відсутня база систематизації знань щодо підготовки (навчання) системних адміністраторів, яка дає можливість оперативно змінювати інформацію про

новітні розробки інструментів адміністрування та замінювати застаріли програмні продукти новими.

ОСНОВНА ЧАСТИНА

Системний адміністратор — одна з найскладніших професій, яка з'явилася нещодавно, але стала незамінною для стабільної налагодженої роботи адміністративних та освітніх установ, банків, виробництва, бізнесу, сфери продажів, послуг тощо. Системне адміністрування застосовується для налагодження роботи: мережі, адміністрування робочих станцій, централізованої авторизації, адміністрування соціальних мереж та поштових клієнтів, адміністрування баз даних, адміністрування різноманітних застосунків, адміністрування сайтів, адміністрування різноманітних систем (доступу та відеоспостереження, засобів IP-телефонії, профілів друк/сканування) тощо.

Завдання адміністрування можна поділити на п'ять груп:

1) адміністрування користувачів та груп користувачів, зокрема планування, створення та підтримання облікової інформації користувачів та груп;

2) адміністрування засобів забезпечення безпеки системи, що також охоплює планування і реалізацію політики;

3) адміністрування локальних та мережних принтерів, їх інсталяція, конфігурування для зручнішого використання, пошук несправностей, усунення проблем, що виникають під час друку;

4) моніторинг подій та ресурсів, включно з плануванням та реалізацією політики аудиту мережних подій для виявлення проломів у системі захисту, а також моніторинг процесів використання мережних ресурсів;

5) архівування та відновлення даних, зокрема планування і виконання регулярного резервного копіювання критичних даних, засобів оновлення та відновлення операційних систем.

Відомо, що посада системного адміністратора наявна сьогодні в усіх організаціях, де є велика комп'ютерна мережа. Звісно, що посадові обов'язки системного адміністратора полягають у забезпеченні штатної роботи парку комп'ютерної техніки, мережі та програмного забезпечення, а також інформаційної безпеки в організації і залежать від його типу: адміністратор бази даних; адміністратор серверів; адміністратор мережі; адміністратор безпеки; вебадміністратор; системний інженер; інженер з надійності сайту типу Site Reliability Engineering (SRE) [4; 5].

Зазвичай до його обов'язків належать: адміністрація серверів та їх операційних систем; налаштування міжмережного екрана (firewall) та мережної підсистеми (IP-адреси, маршрутизація тощо); відстеження атак на сервер та блокування IP-адрес атакуючих машин на міжмережному екрані; створення та видалення облікових записів користувачів; розподіл прав доступу користувачів в операційній системі; відстеження проблем безпеки у встановленому програмному забезпеченні та своєчасне його оновлення на нові версії; оновлення поточного антивірусу та антивірусних баз; моніторинг завантаження сервера та вжиття заходів щодо запобігання перенавантаженню; читання та аналіз системних журналів стосовно виявлення потенційних проблем; установлення та налаштування web-proxy сервера; додавання, видалення сайтів та зміна налаштувань вебсервера і сайтів та багато інших [6; 7]. Тому зрозуміло, що для підвищення ефективності працездатності системного адміністратора розробляється спеціальне програмне забезпечення, яке має загальну назву — інструменти системного адміністрування. Вибір будь-якого інструменту системного адміністрування залежить від поставлених завдань. Якщо для своїх завдань ви не знайшли готового рішення, завжди можна взятися за його реалізацію самостійно [8–10].

Для розуміння ефективного застосування інструментів системного адміністрування потрібно розглянути їх перелік за призначенням, виконати їх систематизацію з метою усвідомлення того, що і де застосовується, а саме: розглянути *класифікацію інструментів системного адміністрування*. Але сьогодні класифікації інструментів системного адміністрування, на жаль, не існує. Тому далі пропонується розглянути наступний підхід для створення такої класифікації.

Класифікація інструментів для системного адміністрування передбачає поділ цих інструментів на різноманітні групи засобів автоматизації різних процесів, потрібних системному адміністратору під час адміністрування. Пропонується, щоб класифікація відбивала принцип KISS (акронім для Keep it simple, stupid — Роби простіше, дурненький).

Умовно рекомендується визначити такі класи інструментів автоматизації задач системного адміністрування: пакети інструментів для системного адміністрування, кросплатформні інструменти адміністрування, інструменти як автоматизація окремих завдань адміністрування.

1. ***Пакети інструментів для системного адміністрування***. Це набір програм для адміністрування та моніторингу комп'ютерів, що мають кілька десятків безкоштовних програм, утиліт, застосунків, менеджерів усіх типів, наприклад Sysinternals Suite, Moreutils тощо. Такі пакети можуть використовуватися навіть без завантаження на локальний комп'ютер завдяки можливості спільного доступу до ресурсу в інтернеті, який

може бути підімкнений як мережний диск. Такі пакети містять кілька десятків невеликих утиліт як консольних, так і з графічним інтерфейсом, багато з яких широко відомі в середовищі системних адміністраторів і обізнаних користувачів. Умовно можна назвати такі групи програм в пакеті інструментів для системного адміністрування: утиліти моніторингу для Windows (Process Monitor), що дають змогу показувати в реальному часі активні реєстрові записи, процеси; програми, які стежать за змінами в реєстрах, типу Regmon; утиліти для моніторингу процесів, запущених в операційній системі, для усунення вірусів та шкідливих програм, типу Process Explorer; програмне забезпечення мережного монітора (firewall); програми для моніторингу серверів та доступу до мережі; програми віртуалізації; програми керування мережними збоями; програми керування центром оброблення даних і сховищем; програми створення звітів; програми віддаленого моніторингу сайтів; застосунки для мобільних засобів тощо.

2. *Кросплатформні інструменти адміністрування*. Кросплатформність (міжплатформність) — здатність програмного забезпечення працювати з кількома апаратними платформами або операційними системами. Забезпечується завдяки використанню мов програмування високого рівня, середовищ розроблення та виконання, що підтримують умовну компіляцію, компонування та виконання коду для різних платформ. Кросплатформний інструмент автоматизації завдань системного адміністрування має у своєму складі оболонку командного рядка, мову сценаріїв та середовище керування конфігурацією, що дає змогу автоматизувати такі завдання, як керування операційною системою за допомогою сценаріїв. Інструмент адміністрування працює як середовище командного рядка на стероїдах, уможливлюючи легкий пошук та перегляд сценаріїв для розв'язання різних проблем — від відшукання базової інформації про систему до виконання розширених дій. Типовим прикладом є програмне забезпечення, призначене для роботи в операційних системах Linux та Windows одночасно, скажімо, Sysinternals, PowerShell ISE, FTP-клієнт, Stitch, FactoRedis, Azure Data Studio, SQL Server Data Tools, Silverlight та ін. Задля унаочнення складу пакетів інструментів для системного адміністрування розглянемо набір груп утиліт Sysinternals.

• *Аналізатори*: AccessChk, AccessEnum, AdExplorer, AdInsight, AdRestore, Autologon, Autoruns, BgInfo, BlueScreen, CacheSet, ClockRes, Contig, Coreinfo, Ctrl2Cap, DebugView, Desktops, Disk2vhd, DiskExt, DiskMon, DiskView.

• *Використання диску* (*DU*):, EFSDump, FindLinks, Handle, Hex2dec, Junction, LDMDump, ListDLLs, LiveKd, LoadOrder, LogonSessions, MoveFile, NotMyFault, NTFSInfo, PendMoves, PipeList, PortMon, ProcDump, Process Explorer, Process Monitor, PsExec, PsFile, PsGetSid, PsKillInfo, PsList, PsLoggedOn, PsLogList, PsPasswd, PsPing, PsService, PsShutdown, PsSuspend, PsTools, RAMMap, RDCMan, RegDelNull, RegHide, RegJump.

• *Використання реєстру* (*RU*): SDelete, ShareEnum, ShellRunas, Sigcheck, Strings, Streams, TCPView, VMMap, VolumeID, WhoIs, WinObj, ZoomIt.

3. *Інструменти як автоматизація окремих завдань адміністрування* — це доволі великий перелік інструментів, що містить такі окремі групи програм адміністрування:

• *аналізатори*: повідомлень, сценаріїв керування операційними системами, інформації в журналах подій, активності системи, продуктивності мережі, візуалізації даних, причин блокування, дискового простору;

• *моніторинг процесів та дії*: інфраструктури, мережного трафіку, мережних протоколів, баз даних, віддалених завдань, резервного копіювання, архівування даних, логування, роботизації безвідмовної роботи інформаційних панелей даних;

• *автоматизація окремих завдань адміністрування*: адміністрування баз даних, усунення несправностей, клонування дисків, текстових редакторів, створення репозиторіїв (єдиного джерела вірогідної інформації), менеджер-паролів, конфігурування і трансферації, для контролювання графічних інструментів адміністрування серверів, а також для керування процесами клієнт/сервер тощо.

Розглянемо особливості побудови деяких груп інструментів у вигляді автоматизації окремих завдань адміністрування.

♦ ***Аналізатор*** — це інструмент системного адміністрування, необхідний для вимірювання продуктивності, уможливлює виконання налаштування багатьох параметрів, пов'язаних із синхронізацією, буферами і протоколами (TCP, UDP, SCTP з IPv4 і IPv6). Це інструмент моніторингу комп'ютерних систем та мереж: спостереження, контролю стану обчислювальних вузлів та служб, оповіщення адміністратора в разі, якщо деякі зі служб припиняють (або відновлюють) свою роботу. Також здійснює тестування мережі, може створювати потоки даних TCP і UDP та вимірювати пропускну здатність мережі, яка їх передає. Дає змогу користувачеві встановлювати різні параметри, котрі можуть бути застосовні для тестування мережі або для її оптимізації чи налаштування. Після виконання він активно вимірює і повідомляє про пропускну здатність, втрати, затримки, джитер тощо. Прикладами є: iPerf/JPerf /iPerf3, Nmap/Zenmap, Paessler SNMP Tester, NTOPNG для Linux, Nagios, Real-Time NetFlow

Analyzer, Kiwi Syslog Server для високошвидкісного веб-аналізу трафіку і збору потоків тощо.

Різновидом аналізатора є сніфер. ***Сніфер (Sniffer)*** або мережний аналізатор — це один із найпростіших методів моніторингу трафіку, що проходить через комп'ютерну мережу. Сніфери можуть бути апаратними чи програмними утилітами. Основна мета сніфера — забезпечити постійний моніторинг трафіку локальної чи зовнішньої мережі, тобто проаналізувати всі пакети в мережі, особливо вхідний трафік, щоб знайти будь-який об'єкт, вміст якого має шкідливий код, і в такий спосіб підвищити безпеку в організації, запобігаючи установленню будь-якого типу клієнта на будь-якому клієнтському комп'ютері. Переважно таке відстеження відповідає за аналіз потоків пакетів даних, які відправляються і приймаються між мережним обладнанням як усередині, так і зовні. Тобто сніфер використовує режим відстеження, що називається «випадковим режимом», за допомогою якого в нас з'являється можливість досліджувати всі пакети незалежно від їх призначення. Проте це може потребувати деякого часу, але це є ключем для впевненого знання того, що сніфер проходить через нашу мережу.

Існує кілька різновидів сніферів: сніфери пакетів, сніфери Wi-Fi, сніфери мережного трафіку та сніфери пакетів IP. Системні адміністратори використовують сніфінг (перехоплення та аналіз) трафіку, аби забезпечити стабільну роботу мережі (визначивши пропускну здатність); вчасно виявити вірусну активність, попередити IT-інциденти в потужних конфігураціях IT-інфраструктури. Для працездатності процесу треба підімкнути сніфер до наявної мережі за допомогою мережного адаптера. Далі потрібно запустити програмне забезпечення для реєстрації, перегляду або аналізу даних, зібраних пристроєм. Пакети даних проходять через сніфер, збираються, розпізнаються, реєструються незалежно від того, як саме було сформовано пакет і куди його було направлено. Одні з найкращих мережних аналізаторів (sniffer), доступних для Windows та Linux, це: Wireshark/Tshark, EtherApe, TCPйитр, Kismet, NetworkMiner, Microsoft Message Analyzer, WinDump, WinPcap, Capsa Network Analyzer, Netcat тощо.

♦ ***Моніторинг процесів та дії*** — важлива складова будь-якої IT-інфраструктури, що дає змогу своєчасно виявити збої та несправності, повідомити про них співробітників IT-підрозділу, а також службу технічного підтримання виробника обладнання або сервісного партнера. Системи моніторингу допомагають економити значний обсяг ресурсів, розкриваючи потенційні несправності ще до того, як вони спричинять збої в бізнес-процесах і завдадуть чималих збитків компанії в цілому. Відомо, що *моніторинг* — це налаштування автоматичних пристроїв для контролю за певними процесами. Вони відстежують стан програми та серверів, тобто як усе працює. Моніторинг дає можливість переконатися, що всі потенційні проблеми будуть виявлені та розв'язані до того, як їх побачить користувач. Наприклад, якщо моніторинг показав, що на сервері закінчується місце, буде додано додаткові сервери, щоб впоратися з навантаженням. Моніторинг потрібен для визначення часу відгуку сервера, навантаження на сервер, серверних помилок, визначення ступеня завантаження процесора, обсягу використання пам'яті, наявність ресурсу простору на диску. Головним способом моніторингу щодо стану програми та серверів є періодичні перевірки або пінг. Для цього формується завдання: сервер запитують кожні кілька хвилин і записують, чи була відповідь позитивною або негативною. Іншим способом моніторингу є застосування спеціальних інструментів, які відстежують кількість запитів до сервера та фіксують, чи були вони успішні. Такі дані, як час відгуку та завантаження процесора, також можна записувати та вивчати, щоб проаналізувати, чи є тенденції, котрі сигналізують про проблеми програми. Прикладом інструменту для моніторингу може бути AppDynamics.

Моніторинг має такі різновиди: для керування і моніторингу систем Unix та для моніторингу інфраструктури.

Керування і моніторинг систем Unix — забезпечують виконання функцій, потрібних для системного моніторингу та усунення помилок. Наприклад, такі як Monit, Netdata, Linux Dash, Glances, Monitorix, Nixstats, Cacti, Zenoss Server Monitoring, Shinken.

Моніторинг інфраструктури — забезпечує функції PagerDuty, Server Density, Pingdom і Nagios. Прикладом є Cabot.

Цінність подібних вирішень у тому, що вся їхня робота здійснюється в автоматичному режимі, без залучення системних адміністраторів, а отже, виключається фактор тимчасового проміжку від виникнення інциденту до його виявлення IT-фахівцями. Іноді трапляється, що IT-фахівці дізнаються про несправність саме тоді, коли на порозі з'являються системні інженери, які вже прибули для ремонту або заміни обладнання, або вузла, що вийшло з ладу. Відомо, що постійний контроль IT-середовища дає змогу на 66% швидше усувати проблеми та у 95% випадків зробити це з першого разу.

♦ ***Автоматизація окремих завдань адміністрування*** виконується за допомогою утиліт, програм для адміністрування, застосунків для адміністрування, менеджерів для адміністрування.

• *Утиліта* — це невелика допоміжна програма для вирішення спеціалізованих завдань із настроювання, оптимізації, покращення роботи обладнання та програмного забезпечення. Утиліти або дають доступ до прихованих параметрів і параметрів системи, або роблять процес зміни окремих налаштувань простішим, автоматизуючи його. Утиліти створюються для автоматизації різноманітних процесів, наприклад: для очищення пам'яті та реєстрів комп'ютерів та оптимізації системи (CCleaner, Wise Registry Cleaner, Registry Life, CPU-Control, BlueScreenView), підвищення швидкості роботи системи (Glary Utilities), відновлення Windows після системних збоїв (Windows Repair), для контролю за параметрами материнської плати та різноманітних карт (SpeedFan, Nvidia Inspector, AMD OverDrive), для створення завантажувальної флешки та образів системи (WinToFlash, Win Toolkit), для керування графічними параметрами (Monitor Test, ATITool, Palit-4), для автоматичної перевірки та оновлення встановлених програм (SUMo), моніторингу файлової системи, реєстру і процесів операційної системи (Process Monitor), для створення завантажувальної флешки (WinSetupFromUSB), розблокування захищених файлів і папок (Unlocker), аналізу поточних процесів у комп'ютері (System Explorer), для створення дистрибутивів (nLite), для автоматичного перемикання розкладки мови і перепризначення клавіш (Punto Switcher, Mapkeyboard).

• *Програми для адміністрування в IT-галузі* — це програми, за допомогою яких здійснюється обслуговування та адміністрування комп'ютера, і призначені вони насамперед для системних адміністраторів та досвідчених користувачів. Такі програми створюються для автоматизації різноманітних процесів, наприклад: для очищення дисків від сміття (ACleaner), для автоматичного усування системних помилок (Wise PC 1stAid), для створення завантажувальної флешки (Rufus, UNetbootin), форматування USB нагромаджувачів (USB Disk Storage Format Tool), проведення тестів оперативної пам'яті (Memtest86+), для очищення реєстру (Regcleaner), виправлення помилок DLL (DLL-Files Fixer), для роботи редактора реєстру (Reg Organizer), для створення безпечної мережі зашифрованого потоку даних OpenVPN тощо.

• *Застосунок для адміністрування в IT-галузі* — це прикладний комп'ютерний сервіс, який має набір певних функцій і є одним із компонентів програмного забезпечення. Простіше кажучи, це програма, яка виконує деякі дії, щоб полегшити життя користувачеві або вирішити ту чи іншу проблему. Такі застосунки створюються для автоматизації різноманітних процесів, наприклад: для аналізу і прискорення роботи Windows (HeavyLoad), для повного видалення програм із системи (Advanced Uninstaller Pro), для виправлення помилок у реєстрі Windows (Registry Recycler), для оптимізації реєстру й очищення Windows (Eusing Cleaner), для швидкого копіювання і переміщення файлів (UltraCopier).

• *Менеджер для адміністрування в IT-галузі* — це комп'ютерна програма, що надає інтерфейс користувача для роботи із системою, здатна здійснювати контроль над усім, що запущено на персональному комп'ютері, надаючи різноманітний інструментарій для додаткового налаштування комп'ютера. Менеджер дає змогу виконувати основні операції, а саме: створення, відкриття/програвання/перегляд, редагування, переміщення, перейменування, копіювання, видалення, зміна атрибутів та властивостей, пошук файлів та призначення прав. Крім основних функцій, багато менеджерів охоплюють низку додаткових можливостей, скажімо роботу з мережею (через FTP, NFS тощо), резервне копіювання, керування принтерами та ін. Наприклад є такі менеджери: для керування процесами, автозавантаженням, драйверами (AnVir Task Manager), для оновлень програмного забезпечення для Windows (Soft4Boost Update Checker), автозапуску програм Windows (Autoruns), поточних процесів Windows (Process Explorer) тощо.

Важливо зауважити, що адміністрування здійснюється за такими напрямками діяльності: усунення несправностей, моніторинг статистичних даних, моніторинг мережного трафіку, працездатність баз даних, керування віддаленими завданнями на мережних засобах, резервне копіювання, здійснення логування, конфігурація і трансферизація, керування терміналами і текстовими редакторами, контролювання серверів, керування процесами зовнішніх пристроїв за схемою клієнт/сервер.

1. ***Адміністрування для усунення несправностей*** — це технічні засоби та утиліти для керування, діагностики, усунення несправностей та моніторингу всього середовища Microsoft Windows. Умовно можна назвати такі групи утиліт: утиліти моніторингу для Windows, що дають змогу показувати в реальному часі активні реєстрові записи, процеси, такі як Process Monitor; програми, які стежать за змінами в реєстрах, наприклад Regmon; утиліти моніторингу процесів, запущених в операційній системі для усунення вірусів та шкідливих програм, наприклад Process Explorer.

2. ***Адміністрування моніторингу статистичних даних*** — спостереження в часі за показниками заданих параметрів процесів. Тут розділяємо окремі компоненти: моніторинг з оповіщеннями та статистика за показниками. Це інструменти, які безперервно контролюють сервер. Його осно-

вне завдання — попередити, коли сервер вийде з ладу через будь-які невідповідності. Прикладами є Better Uptime, Webmin для Unix-подібних систем. А також графічний інструмент адміністрування серверів Linux на основі браузера — надають доступ до сервера з браузера і дозволяють виконувати повсякденні завдання з адміністрування (Cockpit, Netdata).

3. ***Адміністрування моніторингу мережного трафіку*** — дає можливість аналізувати активність у мережі на детальному рівні, відстежувати стан мережі та відслідковувати проблеми, що виникають з часом, наприклад, WireShark, OpenNMS/OpenNMS Horizon/OpenNMS Meridian, LibreNMS, Munin, Observium.

4. ***Адміністрування працездатності баз даних*** — організовується встановленням, налаштуванням та технічним супроводом баз даних. Адміністрування баз даних є функцією керування та підтримання програмного забезпечення систем керування базами даних (СКБД). Основні програмні засоби СКБД, такі як Oracle, IBM DB2 і Microsoft SQL Server, потребують постійного керування. А отже, корпорації, що використовують програмне забезпечення СКБД, часто наймають спеціалістів з інформаційних технологій, яких називають адміністраторами баз даних. Наприклад, SQL Server Management Studio, Plus і Oracle Enterprise Manager/Grid Control. Quest Software, Embarcadero Technologies.

5. ***Адміністрування віддалених завдань*** — це керування ролями, рольовими службами та компонентами віддаленого сервера, періодичне оновлення програмного забезпечення, контроль доступу до ресурсів, внесення змін до конфігурації. Послуги віддаленого адміністрування охоплюють:

- *адміністрування вебсервера:* встановлення, настроювання та обслуговування програмного забезпечення вебсерверів хостингової компанії. Послуги такого виду використовуються в основному для клієнтів, які розміщують сайти своєї та дружніх компаній, інтернет-системи на власних серверах чи придбаних віртуальних серверах хостингів. Це можуть бути держустанови, вузи, комерційні освітні установи, комерційні підприємства з будь-яким напрямом діяльності;
- *адміністрування баз даних:* установлення, налаштування та обслуговування баз даних. Ця послуга може бути корисна організаціям, автоматизація бізнес-процесів яких створена в межах свого технопарку з наявністю 2–3 серверів;
- *адміністрування мережі:* розроблення та обслуговування мереж із застосуванням знань у галузі мережних протоколів та їх реалізації, маршрутизації, реалізації віртуальних приватних мереж, систем білінгу, активного мережного обладнання;
- а*дміністрування мережної безпеки:* широкий спектр аналізу проблем інформаційної безпеки із застосуванням знань у протоколах шифрування та автентифікації та їх практичному застосуванні, плануванні інфраструктури відкритих ключів, систем контролю доступу (брандмауери, проксі-сервери, смарт-картки), інцидентному аналізі, резервному копіюванні, завданнях аудиту та організації політик безпеки. Поширеними та популярними програмами виступають, наприклад, Windows Remote Desktop, UltraVNC, Apple Remote Desktop, Remote Office Manager та ін.

6. ***Адміністрування резервного копіювання*** — дає можливість автоматизувати збереження даних, каталогів у сховищі системи контролю, відстежує зміни під час установлення або оновлення пакетів. Об'єкти резервного копіювання — це дані або сукупність даних, з яких можна створити резервну копію. Приклади об'єктів: файли або теки, дані прикладних програм, дані операційної системи чи сама ОС (наприклад, Windows System State або AIX System Backup), образи віртуальних машин та дисків віртуальних машин, файлові системи тощо.

7. ***Логування*** — збір або агрегація логів, допомагає виявити джерела багатьох проблем, конфлікти в конфігураційних файлах, відстежити події, завдяки логам знайдені помилки можна швидко виправити. Логування — це запис усього того, що відбувається в застосунку. Лог — текстовий файл, який містить інформацію про дії програмного забезпечення або користувачів, і зберігається на комп'ютері або сервері. Логування може здійснюватись через запис у файл або базу даних. Розробники створюють логування, щоб визначити, що відбувається із застосунком «під капотом». Це особливо корисно в програмах, які викликають кілька серверів або баз даних. Логування допомагає виявляти помилки (баги) під час тестування системи повідомлень, документує процес передавання повідомлення різними каналами, що дає змогу відстежувати повідомлення цими каналами. Тому повідомлення логів мають бути зручними і надавати корисну інформацію, тобто в логах є повідомлення про те, що відбувся збій, і в якій частині коду це сталося. Інша корисна тактика для логування – це дати кожній події окремий унікальний ідентифікатор. Він буде асоціюватися з усім, що трапляється з цією подією, і ви можете відслідковувати його переходи з однієї частини програми до іншої. Ось кілька типових випадків, у яких застосовуються логи: адміністратор шукає причини виникнення технічних проблем, збоїв у пристрої або операційній системі та недоступності сайту; розробник проводить дебаг, тобто шукає, локалізує та усуває помилки; SEO-фахівці збирають статистику відвідуваності, оцінюють якість

цільового трафіку; адміністратор інтернет-магазину відстежує історію взаємодії з платіжними системами та дані про зміни в замовленнях.

Типи логів. Існують різні рівні та різні подробиці логування. Коли помилку складно відтворити, використовують дуже докладні логи; якщо це не потрібно, збирають лише ключову інформацію. Для роботи з логами та пошуком інформації у великих текстових даних використовують спеціалізовані інструменти. Для зручної роботи з логами їх поділяють на типи, що допомагає швидше відшукувати потрібні та вибирати правильні інструменти для роботи з ними. Наприклад, виокремлюють такі:

• *системні логи*, тобто, які пов'язані із системними подіями;

• *серверні логи*, що реєструють звернення до сервера і виниклі при цьому помилки;

• *логи баз даних*, що фіксують запити до баз даних;

• *поштові логи*, що стосуються вхідних/вихідних листів та відстежують помилки, через які листи не було доставлено;

• *логи авторизації*;

• *логи автентифікації*;

• *логи застосунків*, установлених на цих операційних системах.

Також логи можна типізувати за ступенем їх важливості:

• Fatal/critical error — те, що потрібно терміново виправити;

• Not critical error — помилки, які впливають на користувача;

• Warning — попередження, те, на що потрібно звернути увагу;

• Initial information — інформація про виклики API сервісу, запити в БД, виклики інших сервісів.

Цікавим вирішенням логування є рішення ELK (*Elasticsearch*, *Logstash* і *Kibana*). Логи всіх інформаційних систем, підімкнених до послуги Managed IT, зберігаються в розподіленому сховищі з урахуванням рішення ELK. Механізм збору логів такий: *Logstash* збирає логи та переносить їх у сховище, *Elasticsearch* допомагає знайти потрібні рядки в цих логах, а *Kibana* візуалізує їх. Усі три компоненти розроблено на основі відкритого коду, завдяки чому їх можна модифікувати за потребами компанії: *Logstash* — застосунок для роботи з великими обсягами даних, збирає інформацію з різних джерел та переводить її у зручний формат; *Elasticsearch* — система для пошуку інформації, яка допомагає швидко знайти потрібні рядки у файлах схову; *Kibana* — плагін візуалізації даних та аналітики в Elasticsearch, що допомагає обробляти інформацію, знаходити в ній закономірності та слабкі місця.

8. ***Конфігурація і трансфери*** — забезпечують виконання різноманітних дій щодо автоматизації процесів, спрощують SSH-з'єднання, виконання команд і пошук даних.

• *Конфігурація сценаріїв*, яка описує кроки роботи сценаріїв користувачів, передбачає синтаксис мови, зазначає команди керування тестовим сценарієм, порядок формування тестового сценарію тощо. Наприклад, *Конфігурація Windows* — містить два вкладені розділи: сценарії та параметри безпеки; *EndPoint* — це конфігурація для підімкнення до сервісу-джерела або приймача даних, це адреса, на яку надсилаються повідомлення, а також може містити інформацію про те, які дані братимуть участь у трансфері та як вони мають бути оброблені в процесі перенесення.

• *Трансфери* (*Transfer*) — допомагають переносити дані між СКБД, об'єктними сховищами або брокерами повідомлень. Розрізняють *Data Transfer* та *Call Transfer*. *Data Transfer* — сервіс дає змогу скоротити час на процес міграції та мінімізувати простоювання під час перемикання на нову базу даних. Він налаштовується через стандартні інтерфейси Cloud. Сервіс підходить для створення постійної бази репліки. Перенесення схеми бази даних із джерела на приймач автоматизовано. *Call Transfer* — це процедура передавання виклику третьому абонентові, коли спочатку активне з'єднання переводиться в режим утримання, після чого здійснюється з'єднання з іншим абонентом, а потім відбувається перемикання на абонента, що викликає (утримуване з'єднання). Цей вид обслуговування відрізняється від послуги типу call forwarding тим, що зміна напрямку виклику відбувається лише після встановлення з'єднання.

Доступні два методи застосування Call Transfer: *Consult transfer* та *Blind transfer*. *Consult transfer* — консультативний трансфер, що дає змогу безпосередньо перед перекладом розмовляти з абонентом, на якого буде переведено виклик. Після того як ви набрали номер іншої сторони, потрібно дочекатися відповіді, а потім натиснути вдруге клавішу *Transfer*. Дзвінок буде переведено, а вас буде відімкнено від розмови. Цей вид трансферу потребує другої лінії або конфігурації dual-line. *Blind transfer* — сліпий трансфер, що негайно переводить дзвінок після натискання клавіші Transfer та набору номера. Цей вид трансферу працює із single-line конфігурацією. Налаштування трансферу відбувається за допомогою команди transfer-system: тут можливий трансфер типу: full-blind, full-consult та local-consult. Прикладами є: Netmiko на різних платформах, Tftpd32 server, FileZilla, WinSCP, SolarWinds SFTP/SCP Server та ін.

9. ***Термінали і текстові редактори*** — забезпечують зручність роботи з текстом за допомогою

текстових редакторів. Наприклад, Notepad++/ UltraEdit/Sublime Text, Cygwin для Linux-колекція інструментів GNU і Open Source, PuTTY.

10. ***Керування процесами клієнт/сервер*** — дає можливість користувачам керувати низкою процесів в UNIX-подібних операційних системах. Прикладом є Supervisord.

ВИСНОВКИ

1. Запропонований підхід пошуку методів застосування інструментів системного адміністрування серверів, які надають можливість ефективно керувати та обслуговувати серверну інфраструктуру хмарного середовища і дає можливість розв'язувати поставлене завдання: визначення класифікації інструментів системного адміністрування серверів, потрібних для ефективного системного адміністрування серверів хмарного середовища.

2. Даний підхід дає змогу організувати підготовку системних адміністраторів щодо вибору засобів адміністрування серверів із множини наявних або створення нових. Особливо це важливо, коли виникають питання навчання системних адміністраторів, тобто потрібно досягти певних цілей навчання, після завершення якого адміністратор зможе: описати функції центру адміністрування, правила ефективного використання засобів пакетів інструментів для системного адміністрування; застосовувати кросплатформні інструменти адміністрування, кваліфіковано використовувати інструменти для автоматизації виконання окремих завдань адміністрування; застосовувати різноманітні аналізатори та сніфери адміністрування, засоби віддаленого адміністрування сервера для керування серверами; визначати порядок диспетчеризації серверів; знаходити для використання спеціальне програмне забезпечення для обслуговування й налаштовування множини комп'ютерних систем і мереж моніторингу, а також застосовувати різноманітні утиліти, застосунки та менеджери для адміністрування.

3. Запропоновано метод визначення ознак для проведення класифікації множини інструментів адміністрування через визначення типів системних адміністраторів: адміністратор бази даних, адміністратор серверів, адміністратор мережі, адміністратор безпеки, вебадміністратор, системний інженер, інженер із надійності.

4. Визначено перелік груп типових завдань: адміністрування користувачів та груп користувачів; адміністрування засобів забезпечення безпеки системи; адміністрування локальних та мережних принтерів; моніторинг подій та ресурсів; архівування та відновлення даних.

5. Досліджено класи інструментів автоматизації завдань системного адміністрування: пакети інструментів для системного адміністрування, кросплатформні інструменти адміністрування, інструменти як автоматизація окремих завдань адміністрування. Здійснений аналіз класів інструментів для системного адміністрування засвідчив, що знання інструментів для системного адміністрування необхідне для усунення несправностей, тестування, зв'язку та виправлення систем, потрібних для продовження роботи. Завдяки правильним інструментам робота стає менш виснажливою, оскільки багато завдань можна виконати за допомогою цих інструментів для системного адміністрування.

Список використаної літератури

1. ***Chalup S. R., Limoncelli T. A., Hogan C. J.*** *The Practice of System and Network Administration // Wesley Professional Length. July 2017. 1056 p.*

2. ***Kralicek E.*** *The Accidental SysAdmin Handbook: A Primer for Early Level IT Professionals 1-st ed. 2016. 256 p.*

3. ***UNIX*** *and Linux System Administration Handbook, 5th Edition / E. Nemeth, G. Snyder, T. R. Hein, [et al.] // Addison-Wesley Professional. Aug 8, 2017.*

4. ***Hanna K. T.*** *System administrator (sysadmin). 2021 [Електронний ресурс]. URL:*

https://www.techtarget.com/searchnetworking/definition/system-administrator (дата звернення: 20.03.2022).

5. ***What*** *is a Systems Administrator? [Електронний ресурс]. URL:*

https://www.computersciencedegreehub.com/faq/what-is-a-systems-administrator (дата звернення: 20.03.2022).

6. ***System*** *Administrator job description [Електроний ресурс]. URL:*

https://resources.workable.com/system-administrator-job-description (дата звернення: 22.03.2022).

7. ***Сисадмін*** *— це хто? Вивчаємо професію. Функціональні обов'язки системного адміністратора. Системний адміністратор: що він робить [Електронний ресурс]. URL:*

https://olympsb.ru/uk/sisadmin---eto-kto-izuchaem-professiyu-funkcionalnye-obyazannosti-sistemnogo.html (дата звернення: 22.03.2022).

8. ***Sysinternals*** *Utilities Index [Електронний ресурс]. URL:*

https://docs.microsoft.com/en-us/sysinternals/downloads// (дата звернення: 22.03.2022).

9. ***40+*** *інструментів для адміністратора ПК [Електронний ресурс]. URL:*

https://winsoft.com.ua/windows/sistema/administruvannia (дата звернення: 22.03.2022).

10. ***Утилиты*** *Microsoft Sysinternals [Електронний ресурс]. URL:*

https://ab57.ru/syssuite.html (дата звернення: 22.03.2022).

*11. **Sysinternals** Suite [Електронний ресурс]. URL: https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite (дата звернення: 22.03.2022).*

Yu. I. Katkov, V. P. Lysak, V. V. Vyshnivskyi

DEVELOPMENT OF INSTRUMENT CLASSIFICATION SYSTEM ADMINISTRATION OF SERVERS

The article is devoted to the topical issue of searching for methods of application of server system administration tools that provide the ability to manage and maintain the server infrastructure of the cloud environment. The task is to determine the classification of system administration tools that are necessary for effective system administration of cloud servers.

It is known that the system administrator is responsible for managing and maintaining the server infrastructure that helps the company achieve its business goals. To perform a variety of tasks, you need to decide on the choice of server administration tools from a variety of existing or new ones. This raises difficulties in selecting the most effective means of solving problems and describing these administrative tools for study due to the lack of defined criteria for selecting the appropriate tool for the relevant administrative situation. This is especially important when there are issues of training system administrators, i.e. it is necessary to achieve certain learning objectives, after which the administrator will be able to: describe the functions of the administration center; rules for effective use of toolkits for system administration, cross-platform administration tools, tools for automation of individual administration tasks; use various analyzers and administration sniffers, remote server administration tools to manage servers; determine the order of server scheduling; to find special software for maintenance and configuration of many computer systems and monitoring networks, as well as various utilities, applications and administrators for administration.

To solve this problem, the article proposes a method for determining the characteristics for the classification of many administration tools by determining the types of system administrators: database administrator; server administrator; network administrator; security administrator; web administrator; systems engineer; reliability engineer. The list of groups of typical tasks is defined: administration of users and groups of users; administration of system security tools; administration of local and network printers; event and resource monitoring; data archiving and recovery. Classes of tools of automation of tasks of system administration are offered: packages of tools for system administration, cross-platform tools of administration, tools in the form of automation of separate tasks of administration. The analysis of classes of tools for system administration is carried out. It is shown that knowledge of system administration tools is necessary to troubleshoot, test, communicate, and fix systems that are required to continue. With the right tools, the work becomes less tedious, as many tasks can be performed with these system administration tools.

Keywords: administration; infrastructure; server; cloud environment.