УДК 681.3
DOI 10.31891/2307-5732-2020-285-3-8

В. Ц. МІХАЛЕВСЬКИЙ, Г. І. МІХАЛЕВСЬКА
Хмельницький національний університет

АСПЕКТИ МІГРАЦІЇ ДАНИХ З ЛОКАЛЬНИХ ЦЕНТРІВ ОБРОБКИ ДО ГІБРИДНОЇ ІНФРАСТРУКТУРИ

У статті розглядаються аспекти міграції даних, що первинно знаходяться в локальних центрах обробки даних, до гібридної інфраструктури. Процес міграції передбачає систему заходів, серед яких розробка автоматизованої системи для синхронізації даних користувачів і врахування особливостей інфраструктури Exchange Server. Така система має проводити інвентаризацію існуючого середовища, робити звіти та конфігурувати компоненти, які приймають участь у міграціях користувачів. Система має відновити всі налаштування користувача, які існували до міграції. Після створення гібридної інфраструктури налаштовуються елементи на глобальному рівні, які будуть застосовані до різних підсистем і поштових скриньок користувачів. Важливими аспектами міграції також є корегування архітектури під специфічні умови підприємства та дослідження списку варіантів проходження пошти в гібридній інфраструктурі (харному середовищі). На дизайн і майбутню конфігурацію гібридної інфраструктури впливають безпосередньо аспекти клієнтського доступу, так як міграція залежно від наземної архітектури може проводитися через один ЦОД або через декілька ЦОДів.

Ключові слова: аспекти міграції даних, автоматизована система, клієнтський доступ, система для міграції, гібридна інфраструктура, хмарні сервіси, Exchange Server, Office 365, центр обробки даних (ЦОД).

V. MIKHALEVSKYI, G. MIKHALEVSKA
Khmelnytskyi National University

ASPECTS OF DATA MIGRATION FROM LOCAL PROCESSING CENTERS TO HYBRID INFRASTRUCTURE

The article considers aspects of data migration, which are initially located in local data centers (LDCs), to the hybrid infrastructure. The migration process involves a system of activities, including the development of an automated system for synchronizing the user data and considering the features of the Exchange Server infrastructure. Such a system should conduct the inventory of the existing environment, make reports and configure the components, involved in user migration. The system must restore all user's settings that existed before the migration. The transport part of the system is analyzed by obtaining data on the components of mail traffic, the application rules of certain actions to mail that moves from sender to recipient, and the rules for collecting information about correspondence and archiving in the archive mailbox. An important aspect of preparing for data migration is the collecting information about how the organization stores all user data and whether there are any policies related to deleting obsolete data. During collecting data about an Exchange Server organization, one of the most important steps is to gather information about how users can connect to the current environment. An important aspect is to test the AutoDiscover service, which is required to configure clients and can be used by Office 365 to connect the enterprise Exchange Server. Because many security aspects are not transferred to the cloud infrastructure during the hybrid configuration and in the process of moving users' mailboxes, migration must be performed manually. The Exchange Server mail system also contains a number of additional elements that cannot be attributed to any standard modules, such as client access, transport or data storage, but still are required data synchronization with the cloud application. After creating a hybrid infrastructure, items are configured (imported) globally, which further will be applied to various subsystems and user mailboxes. Important aspects of migration are also the adjustment of the architecture to the specific conditions of the enterprise and the study of the list of options for the passage of mail in a hybrid infrastructure (good environment). The design and future configuration of the hybrid infrastructure is directly influenced by aspects of client access, as migration depending on the terrestrial architecture can be performed through one (main) data center or through several data centers. The proposed migration system allows many large companies to avoid the complex process of migrating global local infrastructure to the cloud and improves enterprise-level data analysis with automatic data migration management in IT environment with a complex network infrastructure.

Keywords: data migration aspects, automated system, client access, migration system, hybrid infrastructure, cloud services, Exchange Server, Office 365, data center.

Постановка проблеми. На даний час хмарні сервіси все частіше використовуються для потреб підприємств та збереження даних [1]. Тому тема коректної міграції даних з локальних центрів обробки до провайдерів хмарних обчислень є актуальною. Потрібно оцінити існуючу інформаційну систему [2], проаналізувати дані та безпосередньо їхню міграцію в хмарні системи.

Важливим аспектом є побудова найкращого шляху міграції у середовищах, коли компанія має багато офісів, розташованих по всій планеті, де кожний має свої інтернет-канали різної якості. Також необхідно застосувати всі налаштування та параметри, що були в локальному ЦОДі, бо за довгі роки підприємство виробляє велику кількість правил, політик, які добре працювали в локальній інфраструктурі, а після міграції даних їх потрібно перетворювати, а потім визначати відповідні налаштування.

Аспект підготовки до міграції даних полягає в тому, щоб зібрати інформацію про те, як організація зберігає всю інформацію користувачів і чи є які-небудь політики, пов'язані з видаленням застарілих даних. Крім цього, існує велика потреба в переносі налаштувань безпеки, пов'язаних із захистом інформації.

Формулювання цілей статті (Постановка завдання). Для зниження навантаження на працівників та визначення економічної доцільним з точки зору витрат на процес міграції даних необхідно описати всю систему міграції та визначити найважливіші її аспекти. Система має бути такою, що враховуватиме потреби підприємства при інтеграції з Office 365, буде пропонувати і впроваджувати зміни для визначення оптимального шляху потоку даних та планувати перенос даних до хмарної частини. Основним критерієм має бути рішення для процесу міграції з урахуванням сучасного підходу в IT-проектах. Для гібридної інфраструктури Exchange Server, яка є наслідком інтеграції корпоративної системи з хмарним сервісом

Office 365, сформулювати рішення, що допомагають перенести фактичні дані користувачів різних видів з локальних центрів у кінцеву інфраструктуру.

Виклад основного матеріалу. Під час міграції даних від локальних центрів до хмарних сервісів необхідно брати до уваги велику кількість вимог, таких як транспортна служба, служби зберігання даних, авторизації і служби доступу до даних, календарі і адресні книги, а також служби безпеки і захисту корпоративних даних. При цьому, необхідно враховувати мережеву інфраструктуру, тому що це може вплинути безпосередньо на період та час міграції, а також інші додаткові дії, що необхідні для забезпечення міграції.

Аналіз транспортної системи. Транспортна частина, зазвичай, вимагає докладної інвентаризації, оскільки у великих організаціях має бути організовано нестандартизований доступ по протоколу SMTP: а) поверхові сканери або сервери моніторингу, які надсилають повідомлення; б) надсилання пошти на спеціальні вузли, які відповідають за пересилання пошти або обмін поштою з партнерами із примусовою аутентифікацією серверів за сертифікатами; в) застосування правил до повідомлень, які переміщуються всередині організації, виходять за межі організації або надходять від зовнішньої організації.

Щоб оцінити всі аспекти транспортної системи, необхідно отримати дані про такі компоненти:

1) **Send connectors** – компонент відправки пошти, інформація отримують на рівні організації [6]. Зазвичай поштовий трафік не потребує особливих змін під час налаштування гібридної інфраструктури, але у випадку специфічної конфігурації відправлення пошти до партнерів деякі сполучні лінії (конектори) доведеться експортувати з наявної організації Exchange Server, після створення нових сполучних ліній у хмарі та застосування до них налаштування з експортованих даних. Щоб отримати всю інформацію по Send connectors, необхідно виконати такий запит:

```
$ExpPath = "C:\ExchaData\Export\"
$SendConExpPath = $ExpPath + 'SendConnectors.csv'
$SendConnectors = Get-SendConnector
$SendConnectors | select Identity, Name, AddressSpaces, IgnoreSTARTTLS, RequireOorg, RequireTLS,
SmartHostAuthMechanism, SmartHostsString, TlsAuthLevel, TlsCertificateName, TlsDomain | export:
foreach ($sendConnector in $SendConnectors) {
...$TempName = $SendConnector.name
...$Addressspaces = $sendconnector.addressspaces
...$FileName=$ExpPath+'_SEND_'+$tempName+'.csv'
...$addressspaces | Export-Csv -Path $fileName -NoTypeInformation
……}
$SendConnectors | ft Name, addressspaces, requiretls
```

Результатом буде файл з даними в форматі, як зазначено в таблиці 1.

Таблиця 1

Формат даних, представлений по Send Connector

Name	Address Space	Require TLS
Internet	{SMTP:*;2}	False
Lotus Notes	SMTP:domino.testvg.it-infrastructures.net	False
…	…	…

В результаті цього запиту у вказаному каталозі буде файл, який містить відомості про всі Send connectors, а також список файлів, що відповідають назві конкретних конекторів, що містять простори імен, які обслуговує даний конектор;

2) **Receive connectors** – компонент, відповідальний за отримання пошти, інформація має бути доступна для зчитування з кожного сервера, який має транспортну роль (застосовне до старих версій Exchange Server) [6]. Отримані об'єкти повинні бути проаналізовані, щоб визначити, чи конектор створено по замовчуванню і чи не було ніяких змін в ньому, після чого все те, що не відповідає налаштуванням по замовчуванню, експортувати, щоб потім мати можливість проаналізувати і, за потреби, застосувати до конекторів, створених у хмарній службі. Щоб отримати всю інформацію по всіх Receive connectors, необхідно виконати запит, результатом якого буде список з іменами, що відповідають іменам серверів, які будуть містити докладні конфігурації всіх конекторів на даному сервері, а також зведений файл зі зведеною таблицею для звіту;

3) **Transport rules** – транспортні правила, які застосовують певні дії до пошти, яка переміщується від відправника до одержувача [4]. Інформація про правила транспортування зчитується на глобальному рівні організації, а також на EDGE-серверах, розташованих в мережі периметра. Зауважимо, що правила транспортування не переміщуються до хмарної служби і вони повинні бути експортовані з наявної організації Exchange Server, піддаватись аналізу, а потім імпортуватися до хмарної організації;

4) **Journal rules** – правила, призначені для збору відомостей про листування та архівування в архівній поштовій скриньці. Ці правила конфігуруються як на глобальному рівні для певних груп користувачів, так і на рівні баз даних поштових скриньок. На цьому етапі необхідно експортувати інформацію з глобального рівня для подальшого аналізу та імпорту до хмарної організації, оскільки існуючі засоби міграції не дають можливості мігрувати цей тип інформації [6]. З цього моменту всі елементи, які

відносяться до транспортної підсистеми, зберігаються в каталозі для експорту в файловій системі у форматі CSV (Coma Separated Value). Там же знаходяться звіти, які мають розширення TXT.

Аналіз даних користувачів поштової системи. Етап збору інформації про дані користувачів включає в собі не лише збір статистичних даних поштових скриньок користувачів, а й відомості про ресурсні поштові скриньки і спільні папки. Крім усього іншого, необхідно зібрати інформацію про те, як компанія керує інформацією користувачів, та яким є підхід до застарілої інформації.

Для того, щоб зібрати загальну статистику про обсяг даних користувачів першим етапом необхідно з'ясувати, які бази даних існують в організації і як вони розподіляються по IT-інфраструктурі всередині організації. Для цього ми можемо використовувати стандартний запит по базах даних і визначаємо додатковий параметр, який вказує на якому сервері бази даних активні. Після отримання інформації про розподіл баз даних, маємо змогу запустити циклічний запит для пошуку поштових скриньок в кожній базі даних і збору статистичних даних по них. Такий підхід дозволить зробити звіт, який відображає не тільки інформацію про конкретну поштову скриньку, але і отримати зведені відомості по кожному з Центрів Обробки Даних відносно загального обсягу інформації. На підставі отриманої інформації, буде легко обчислити, скільки часу знадобиться для міграції даних користувачів і як міграцію цих даних поділити на етапи [4]. Як наслідок, маємо змогу проаналізувати, в якому сайті Активного каталогу (Active Directory – AD) знаходиться кожна поштова скринька. Цей звіт буде корисним в майбутньому, якщо міграцію поштових скриньок заплановано проводити не через один ЦОД, а паралельно через декілька ЦОДів.

Ще один аспект підготовки до міграції даних полягає в тому, щоб зібрати інформацію про те, як організація зберігає всю інформацію користувачів і чи є які-небудь політики, пов'язані з видаленням застарілих даних (наприклад, поштові повідомлення старше 5 років). Це питання слід уточнити, оскільки елементи конфігурації не переносяться автоматично до хмарної служби. Для досягнення цієї мети нам потрібно вивантажити з конфігурації Exchange Server інформацію про всі елементи Retention Tag, а також інформацію про те, з якими елементи Retention Policy вони пов'язані.

Зібрані дані можливо буде спершу відтворити у хмарній інфраструктурі, а після міграції користувачів також можна застосувати до вже перенесених поштових скриньок. Останнім у цьому сценарії залишилось ідентифікувати і визначити на якого користувача які політики збереження даних застосовуються.

Другою немаловажною частиною аналізу збережених даних є Спільні папки. У багатьох організаціях вони є рудиментом старої інфраструктури, коли організація мала змогу зберігати там корпоративні документи, щоб забезпечити швидкий пошук необхідних даних, а також організувати порівняно недорогий і надійний інструмент автоматичної реплікації даних між різними відділеннями (офісами). В останніх версіях Exchange Server реплікації даних більше не підтримується, але дані, які організація може зберігати в спільних папках, можуть бути використані, а обсяг даних може бути критично великим [2].

Для того, щоб підготуватися до міграції спільних папок в хмарну інфраструктуру, необхідно також проаналізувати, який обсяг даних у якому ЦОД зберігається. Для цього потрібно зібрати статистичні дані про обсяги поштових скриньок, призначених для зберігання даних спільних папок (Public Folder Mailboxes) та ідентифікувати їх в ЦОД. Слід зазначити, що коли ми аналізуємо Спільні папки, необхідно також проаналізувати наявність обмежень по кожній з папок та з'ясувати, чи є у будь-якої з папок поштова адреса, яка асоціюється з нею. Результати, отримані на даному етапі, необхідно буде звірити пізніше, після міграції Спільних папок, що є критичним для багатьох організацій.

Аналіз клієнтського доступу до системи. Під час збирання даних про організацію Exchange Server одним з найважливіших етапів є збір даних про те, як користувачі можуть підключатися до поточного оточення. На сьогодні Exchange Server пропонує наступні варіанти підключення:

– MAPI – Mail Application Program Interface, який є протоколом, що інкапсульовано до протоколу HTTPS і працює по порту TCP-443. Даний протокол є найбільш бажаним, оскільки він є найлегшим та функціональним водночас. Однак він підтримується лише останніми версіями Outlook;

– Outlook Anywhere, або як його ще раніше називали, RPC over HTTPS. За функціоналом він такий самий як і попередній протокол, хоча значно важчий і повільніший за рахунок того, що він використовує ще один рівень інкапсуляції. Протокол верхнього рівня MAPI інкапсулювався в RPC (раніше рідний протокол Exchange Server), після чого інкапсулювався в HTTPS, задіявши вбудовану у Windows службу RPC-Proxy (RPC over HTTPS Feature). Даний протокол завершує використання в нових версіях Exchange Server та існує лише для підтримки старих клієнтів Outlook. Протокол також працює по порту TCP-443;

– допоміжним протоколом для роботи клієнта Outlook є протокол завантаження Оффлайнової Адресної Книги – OAB (Offline Address Book). Даний протокол просто дозволяє клієнту скачати групу файлів, які є кешем адресної книги на випадок недоступності Інтернет (порт TCP-443);

– Active Sync – протокол, призначений для підключення та роботи з Exchange Server з мобільних пристроїв. Цей протокол дозволяє мобільним пристроям працювати з поштою, календарями, адресною книгою, особистими правилами і, звичайно, працювати з Спільними папками. Протокол також дозволяє керувати мобільними пристроями та застосовувати політику безпеки для них, щоб мати змогу захистити корпоративну інформацію на мобільних пристроях. Цей протокол працює, як і попередні протоколи, поверх протоколу HTTPS, а, отже, покладається на порт TCP-443;

– протокол EWS (Exchange Web Services) — це універсальний інтерфейс підключення до Exchange Server для розробників та сторонніх додатків, наприклад, Skype For Business Server використовує його для

отримання інформації про одержувачів Exchange Server. Він також використовується клієнтами Outlook для отримання інформації про зайнятість тих чи інших ділянок зібрання (Free/Busy) і отримувати випливаючі підказки Mail Tips. Протокол працює як розширення протоколу HTTPS;

– для тих користувачів, які не мають поштового клієнта, є протокол, який дозволяє підключати і працювати з поштою через звичайний браузер – Outlook Web Application (OWA). Цей протокол дозволяє користувачеві не тільки повноцінно працювати з усіма функціями поштової скриньки, але і робити це без Інтернету – оффлайнова робота (підтримується не всіма браузерами);

– нестандартними протоколами підключення до Exchange Server є протоколи POP3 та IMAP4. Обидва протоколи вкрай лімітовані по функціоналу і є вразливі з точки зору безпеки. Протоколи використовують для безпечного підключення портів TCP 995 та 993 відповідно. Дані протоколи призначені виключно для отримання поштових повідомлень і відправки повідомлень. Вимагається протокол SMTP, який для клієнтів працює на стандартному TCP порті 587. За умовчанням, ці протоколи вимкнено, і, якщо вони використовуються організацією, вони повинні бути ввімкнені в Office 365 і налаштовані відповідно (наприклад, для того, щоб деякі пріоритетні додатки мали можливість завантажити пошту з Exchange Server);

– для автоматичного налаштування поштових клієнтів використовується протокол AutoDiscover, який дозволяє клієнту отримати параметри підключення до Exchange Server, що значно спрощує налаштування клієнтської частини. Даний протокол працює так само поверх HTTPS та підтримується всіма клієнтами Outlook та значною кількістю Мобільних клієнтів, працюючими за протоколом ActiveSync.

При оцінюванні інфраструктури Exchange Server необхідно зняти параметри та налаштування зі всіх протоколів, тому що: а) частина протоколів не переноситься, як наприклад POP3 та IMAP4; б) частина протоколів використовується хмарним сервісом для підключення до Exchange Server організації (протокол EWS) [6]; в) протокол OWA потребує ще і ретельного перенесення політик, застосованих до WEB додатків, призначених для браузерів.

Параметри всіх протоколів та пов'язаних з ними об'єктів мають бути експортовані, а також оформлені у вигляді табличних звітів для подальшого аналізу, після чого багато отриманих даних будуть доступні як параметри підключення до мережі Exchange Online для організації Exchange Server, а також у якості параметрів конфігурації для клієнтів PO3 та IMAP4, які, як відомо, не мігрують в Office 365.

Збір інформації про підключення починається із зібрання інформації про протоколи, які можуть використовувати Office 365 для підключення до внутрішньої інфраструктури Exchange Server. Для цього необхідно збирати параметри таких протоколів, як MAPI та Outlook Anywhere, але передумовою є те, що протокол повинен мати можливість зовнішнього з'єднання із сервером Exchange Server. Таким чином, аналізуємо лише ті протоколи, де параметр External URL не має пустого значення. Якщо цей параметр містить пусте значення, це означає, що підключення до цього сервера із зовнішнього світу неможливе. Результати також повинні бути проаналізовані на предмет того, на яких сайтах Active Directory знаходяться сервери, відповідальні за обслуговування даних з'єднань. Такий підхід дозволить в подальшому визначити, які поштові скриньки і через які сервери зручніше мігрувати до Office 365 (якщо організація має більше одного підключення до Exchange Server з Інтернету).

Всі протоколи працюють на захищеному каналі HTTPS. Таким чином, для ініціалізації безпечного підключення потрібен цифровий сертифікат. Для того, щоб Office 365 мав змогу прийняти цей сертифікат для встановлення безпечного з'єднання, цей сертифікат має відповідати низці вимог [4, 6]: а) сертифікат повинен бути виданий комерційним центром сертифікації, якому довіряють сервери у ЦОДах Microsoft; б) поле Subject або Subject Alternative Name (SAN) має містити ім'я, яке відповідає Fully Qualified Domain Name (FQDN), ім'я сервера із зовнішнього атрибуту External URL, який було видобуто на попередньому кроці; в) одна з цілей сертифікату повинна бути Server Authentication; г) сертифікат має бути дійсним з точки зору терміну служби; д) сертифікат не повинен бути відкликаний центром сертифікації, що його видав. Тому, щоб отримати всі зазначені відомості, необхідно отримати параметри сертифіката з кожного можливого зовнішнього підключення та зберегти його як звіт.

Важливим аспектом є перевірка служби Autodiscover, яка потрібна для налаштування клієнтів і може використовуватись Office 365 для підключення до корпоративного Exchange Server. Для того, щоб отримати параметри цієї служби необхідно так само, як і на попередніх кроках, вивантажити параметри Autodiscover і відповідні сертифікати з їх параметрами.

Аналіз елементів безпеки. Exchange Server, як і багато інших продуктів, містять ряд компонентів, відповідальних за безпеку. Головна мета компонентів безпеки є: а) захист даних користувача від видалення; б) захист корпоративних і персональних даних від витоку; в) захист доступу до поштової системи від зовнішнього світу через веб-інтерфейс; г) захист інформації на мобільних пристроях; д) захист Exchange Server від змін конфігурації. Практично всі перераховані аспекти безпеки не переносяться до хмарної інфраструктури під час гібридної конфігурації та в процесі переміщення поштових скриньок користувачів, і тому міграція має виконуватися вручну. Першим елементом безпеки є In-Place Hold Policy, який дозволяє на корпоративному рівні визначати, в яких поштових скриньках повинні утримуватись дані, за якими критеріями і на який період. Цей елемент потрібен для організацій, які мають сумніви в тому, що працівник може видалити всю інформацію зі своєї поштової скриньки перед тим, як буде звільнений. Використовуючи ж дані політики, служба безпеки може позначити всі або деякі повідомлення відповідно до певних критеріїв і вказати, що після видалення користувачем повідомлення буде зберігатися протягом деякого часу або

нескінченно довго. Цей лист буде доступний людині з відповідними дозволами. Далі експортують усіх користувачів з інформацією про те, яким чином у них встановлена пошта на утримання.

Наступний елемент безпеки в Exchange Server є Data Los Prevention (DLP) Policies (Політики захисту витоку інформації) [5, 6]. Цей елемент є частиною транспортної системи і здатний аналізувати повідомлення не тільки під час переїзду, але і в процесі введення повідомлення в Outlook, повідомивши користувачеві, що він планує відправити лист з контентом, який являє собою секретну інформацію. Варто також зауважити, що ці політики можуть містити як регулярні вирази, налаштовані адміністратором, так і зразки документів, які система сама розкладе на набір регулярних виразів, а потім виконає порівняння з вкладенням на його «подібність» з вираженням у відсотковому співвідношенні. Особливу увагу треба звернути на те, що політики DLP самі по собі є контейнером для правил транспортування а, отже, працювати безпосередньо з ними не видається можливим, але вони можуть бути експортовані як набір правил у файлі XML.

Слід також зазначити, що ці політики можуть містити різноманітні словники та підказки, які також повинні бути експортовані і збережені в файлах, які можуть бути імпортовані в хмарну інфраструктуру.

На етапі аналізу доступу до Exchange Server через WEB-інтерфейс необхідно проаналізувати та експортувати політики захисту WEB-додатків (Outlook Web Application Policy). Дані політики визначають, які дії можуть виконувати користувачі, підключившись до Exchange Server за допомогою браузера WEB-інтерфейсу. Також за допомогою даних політик можна визначити, з яким типом корпоративних даних може працювати користувач. Елемент безпеки на Exchange, що відповідає за захист даних на мобільних пристроях, називається політикою мобільних пристроїв. Цей елемент керує тим, які дані завантажити на мобільний пристрій, і які функції пристрою доступні для кінцевого користувача (наприклад, заборона пересилки повідомлень, заборона передачі даних через Bluetooth або відмова в доступі до вбудованої камери, щоб запобігти можливості зробити знімок з корпоративних моніторів або документів). Для того, щоб зняти подібний елемент необхідно виконати скрипт, який експортує детальну інформації про політики з усіма параметрами, а також виконає експорт всіх користувачів з інформацією про те, яка політика на них застосовується.

Аналіз інших елементів. Поштова система Exchange Server також містить ряд додаткових елементів, які не можна віднести до будь-яких стандартних модулів, таких як клієнтський доступ, транспорт або ж зберігання даних, однак все одно вимагають синхронізації даних з хмарним додатком.

До таких елементів можна віднести: а) адресні списки; б) офлайново адресні книги; в) політики адресних книг; г) динамічні групи; д) адресні списки. Дані елементи або не переносяться в хмарну інфраструктуру, або взагалі не існують, як у випадку з динамічними групами розсилки. Отже, всі зазначені елементи повинні бути експортовані для подальшого аналізу і розуміння, що можна буде просто імпортувати в Office 365, а що доведеться замінювати альтернативними рішеннями за допомогою скрипта [6].

```
$ExpPath = "C:\ExchaData\Export\"
$DYNRep = $ExpPath+'DYN_GROUPS.csv'
Get-DynamicDistributionGroup | Select ALias, Dysplayname, Notes, RecipientFilter, RecipientFilter |
Export-Csv -Path $DYNRep -NoTypeInformation
```

Динамічні групи залишаються для дослідження внутрішньою службою фахівців, так як повного аналогу даного об'єкта в хмарній частини інфраструктури не існує. Єдиним аналогом можуть бути групи Office 365. Однак цей об'єкт не є прямим аналогом і визначення динамічності не відповідають локальним (наприклад, в хмарній інфраструктурі немає такого поняття як Organizational Units), а, отже, необхідно провести ручне дослідження.

Адресні списки, так само, як офлайнові адресні книги є виключно об'єктом окремої Exchange організації. В гібридній інфраструктурі по суті співіснує дві і більше організації, не маючи загального Активного каталогу (Активний Каталог з локальної організації синхронізує дані в хмарну службу каталогів Azure Active Directory). Такі об'єкти як адресні списки не синхронізуються, так як в локальній інфраструктурі їх визначення знаходиться в розділі Configuration Активного Каталогу. Даний розділ навіть не синхронізується і, більш того, за замовчуванням робота з ними заблокована. Єдиною, що є майже однаковою, то це Глобальна Адресна Книга (GAL). Це пов'язано з тим, що її визначення і в локальній, і в хмарної службі просте – «відображати всіх отримувачів Exchange Server». Таким чином, якщо вона синхронізує всі облікові записи користувачів з локального AD в Хмарний, то і GAL буде однаковою. Адресні списки зберігають в собі визначення запитів, які дозволяють вибрати з Глобальної Адресної Книги деяку кількість отримувачів (за якимось критеріями). Однак, і в хмарній, і в локальній організаціях Exchange Server є ряд стандартних адресних списків, які створюються за замовчуванням. Тому експорт скриптом повинен виключати таки адресні списки. Такий скрипт аналізує експортований адресний список на сумісність з Office 365 і, якщо даний адресний список несумісний, він інформує про це оператора і експортує визначення даного адресного списку в окремий файл.

Офлайнова адресна книга необхідна користувачам, які працюють на клієнті Outlook і програмному пакеті Microsoft Office Suite. Основне призначення даного об'єкта полягає в тому, щоб користувач міг використовувати адресну книгу підприємства в той час, коли немає з'єднання з Exchange Server. За замовчуванням в Exchange Server створюється офлайнова книга за замовчуванням "Default Offline Address Book" і, якщо організація невелика, то нею всі можуть користуватися, так як вона не буде великого розміру. Однак, якщо в організації Exchange зберігаються дані про тисячі користувачів з фотографіями та сертифікатами для шифрування пошти, розмір такої книги може займати кілька гігабайт**.** З метою

зменшення розміру обсягу переданих і збережених даних на клієнтських робочих станціях створюють додаткові офлайнові адресні книги, які зберігають інформацію тільки про деяких одержувачів (наприклад, з даного регіону). З цього випливає, що необхідно відтворити всі офлайнові адресні книги організації в хмарній інфраструктурі, після чого застосувати їх на переміщені в хмару поштові скриньки, відповідно до їх налаштувань в локальній інфраструктурі.

Політики адресних книг є останнім елементом, який пов'язаний з адресними списками. Даний тип об'єкту дозволяє зв'язати воєдино різні типи даних, такі як адресні списки, офлайнові адресні книги, списки переговорних кімнат і застосувати до профілю користувача, тим самим ми можемо визначити, які адреси користувач зможе бачити онлайн, а які в офлайн. Повноцінне перенесення потребує експорту даних політик, а також інформації про те, на які поштові скриньки вони застосовуються. Наостанок, необхідно експортувати інформацію про поточний стан інфраструктури Exchange Server. Щоб отримати таку інформацію можна звернутися до вбудованого API, який дозволяє з'ясувати як інформацію верхнього рівня, так і детальну інформацію щодо кожного компонента кожної підсистеми на найнижчому рівні. В даному випадку виникає завдання витягти тільки інформацію верхнього рівня і при аналізі, якщо буде потрібно, розслідувати проблемні причини на більш низьких рівнях, виконавши звернення до того ж інтерфейсу за допомогою скрипта. Після того, як дані об'єкти були експортовані, їх необхідно вивчити на предмет критичних помилок, з'ясувати, до яких компонентів належать дані помилки і виконати усунення несправності. Після того, як всі несправності будуть усунені, можна переходити до наступної стадії проекту – створення гібридної інфраструктури.

Формування звіту про знайдені елементи інфраструктури поштової організації. По закінченню обробки інфраструктури Exchange Server, в обумовленому каталозі буде збережено два типи даних: 1) дані, експортовані з поточної інфраструктури, які необхідно буде імпортувати в хмарну інфраструктуру. Звіт про дані у вигляді набору таблиць, який можна проаналізувати і зробити свої корективи; 2) дані, які будуть містити статистику за обсягом призначених для користувача даних з поділом по Центрах обробки даних. Звіт про стан всієї інфраструктури (верхній рівень). Після формування всіх даних можна переходити до наступного етапу – обліку потреб підприємства в умовах майбутньої гібридної конфігурації.

Після того, як вся інвентаризація проведена, а дані з поточної конфігурації Exchange Server експортовані, можна встановлювати первинне налаштування гібридної інфраструктури і переносити елементи поточної конфігурації, щоб до моменту перенесення призначених для користувача даних інфраструктура була в робочому стані.

Первинна конфігурація гібридної інфраструктури виконується в двох основних режимах.

1. Для швидкого перенесення призначених для користувача даних в хмару. У цьому випадку між локальною організацією Exchange Server і хмарною службою Office 365 налаштовується виключно рух пошти. Федеративних довірчих відносин між організаціями не встановлюється. Така конфігурація підходить виключно під підприємств малого бізнесу.

2. Для великих підприємств необхідно встановлювати повноцінні федеративні довірчі відношення. У цьому випадку встановлюється не тільки рух повідомлень між локальною організацією Exchange Server і хмарною службою Office 365, але і встановлюється довірче відношення між визначеним Exchange Server, якого опубліковано в інтернет, і хмарною інфраструктурою на рівні служби EWS. Таким чином, хмарний сервіс зможе комунікувати з локальною організацією Exchange Server через WEB API, завдяки чому користувачі, що знаходяться в хмарному сервісі, можуть перевіряти стан зайнятості в календарях користувачів, чиї поштові скриньки знаходяться в локальній інфраструктурі і навпаки. Так само, саме через цю федерацію встановлюється делегування дозволів на загальні поштові скриньки з обох частин гібридної інфраструктури.

Компанія Microsoft надає можливість налаштування первинної гібридної інфраструктури виключно за допомогою Hybrid Configurations Wizard (HCW), зразок інтерфейсу відображено на рисунку 1, який досить простий у використанні: а) необхідно зробити попереднє налаштування синхронізації AD для всіх користувачів, які мають поштові скриньки, а також облікові записи всіх ресурсних поштових скриньок і груп розсилки, які використовуються Exchange Server; б) обов'язково на сервері, який буде використовуватися для прямої федерації, повинен бути встановлений комерційний сертифікат для можливості ініціювати HTTPS-з'єднання.

Перенесення елементів конфігурації в хмарну частину гібридної інфраструктури. Після того як ми створили гібридну інфраструктуру, необхідно спочатку налаштувати (імпортувати) елементи на глобальному рівні, які потім будуть застосовані до різних підсистем і поштових скриньок користувачів. Перед початком імпортування необхідно встановити підключення із середовища PowerShell до Exchange Online, як зазначено нижче [4, 6]:

```
$UserCredential = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange –ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic –
AllowRedirection
Import-PSSession $Session -DisableNameChecking
```

Далі можна створювати елементи.

Рис. 1. Зразок інтерфейсу конфігурування гібридної інфраструктури

Transport Rules. У першій частині транспортні правила були експортовані як колекція об'єктів. Завдяки тому, що хмарний Exchange Server має практично таку ж архітектуру, отже, і інтерфейс управління в середовищі PowerShell, збережені дані можна імпортувати в Exchange Online. Однак, слід враховувати, що деякі правила можуть і не імпортуватися. Подібна ситуація може виникнути в результаті того, що всередині транспортного правила використовується посилання на абсолютний ідентифікатор об'єкта, який був в локальному Exchange Server. Прикладами з такими посиланнями можуть послужити правила із застосуванням шаблонів безпеки RMS (Right Management System). Справа в тому, що локальний Exchange Server використовує посилання на шаблон локальної служби RMS, в той час як Exchange Online посилається на Хмарний аналог даної служби. Коли виникає подібна ситуація, транспортні правила, що містять дані посилання, висвітлять помилку при імпорті. Відповідальний за міграцію фахівець повинен буде спершу в Office 365 налаштувати службу RMS, включаючи шаблони, після чого відтворити правило вручну.

Journal Rules. Цей тип об'єктів, як і попередній клас об'єктів, імпортується із збереженого файлу з колекцією. Єдиним обмеженням, яке може викликати помилку при імпорті, є посилання на поштову скриньку, призначену для зберігання архівів, яка розташована в Exchange Online. У відповідності з поточними правилами, поштова скринька для зберігання архівів корпоративного листування не повинна розташовуватись в Office 365 і в безкоштовній поштовій службі Microsoft Outlook®. Якщо ж поштова скриньку для архівів буде перебувати в локальному Exchange Server помилки не буде. Імпорт проводитися так само, як і попередній об'єкт.

Retention Policies and Retention Tags. Якщо в локальній інфраструктурі використовувалися політики видалення повідомлень і підприємство бажає, щоб ці ж політики застосовувалися для поштових скриньок, які повинні будуть переміститися в Exchange Online, то в цьому випадку дані політики та їх складові об'єкти необхідно відтворити в хмарному сервісі. Для цього спочатку необхідно імпортувати скриптом визначення всіх об'єктів класу Retention Policy Tag [6].

Після того, як всі теги відтворено, необхідно відтворити політики і пов'язати їх з тегами, які були в локальній конфігурації. Для цього імена файлів зі списком тегів використовуємо як ім'я політики, а вміст тих же файлів використовуємо як посилання на теги, які вже створені (імена файлів починаються зі стандартного префікса, який був заданий при імпорті, а отже, всі файли з налаштуваннями політик можуть бути ідентифіковані) [6]. Надалі, коли користувачів буде мігровано в хмарний сервіс, ми зможемо прив'язати політики до відповідних поштових скриньок.

Перенесення допоміжних елементів конфігурації. Опціональним кроком після того, як основні елементи безпеки імпортовані в хмарну частина гібридної організації Exchange Server, може бути імпорт елементів, пов'язаних з адресними книгами. Якщо компанії дані елементи необхідно імпортувати, то перед імпортом необхідно виконати ряд додаткових кроків, пов'язаних з тим, що за замовчуванням робота з адресними книгами заблокована (навіть глобальний адміністратор не має повноважень управляти адресними книгами). Щоб включити доступ в консолі управління Exchange Server (Online) необхідно додати до Менеджмент Групи «Organization Management» роль «Address Lists», після чого перезавантажити консоль PowerShell:

$UserCredential = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange –ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential –
Authentication Basic -AllowRedirection
Import-PSSession $Session
New-ManagementRoleAssignment -Role "Address Lists" -SecurityGroup "Organization Management"

Після перезавантаження консолі і підключення до управління Exchange Online, необхідно виконати ще одну команду, яка включає управління адресними списками:

Set-TransportConfig -AddressBookPolicyRoutingEnabled $true

З цього моменту можливо управляти адресними списками.

Імпорт адресних списків проводиться з файлу, який попередньо було експортовано. Адресні списки, які не сумісні за своїми формами з форматом Office 365, експортуються в окремий файл. Списки, які готові для імпорту, зберігаються в іншому файлі і запуск скрипта для імпорту зробить всі необхідні дії. Після імпорту адресних списків можна здійснювати **імпорт офлайнових адресних книг**, які було створено додатково до основної офлайнової адресної книги. **Політика адресних книг** є останнім класом об'єктів, який імпортується в хмарну інфраструктуру. Він пов'язує адресні списки, офлайнові адресні книги, списки приміщень і глобальні адресні книги в єдину політику, яка згодом застосовується до поштової скриньки користувача. Після цієї події базова інфраструктура Exchange Server Online стала відповідати критеріям локальної організації, так як в ній створено всі об'єкти, на які надалі будуть посилатися призначені для користувача дані. З цього моменту можна починати виконувати більш тонкі налаштування.

Корегування архітектури під специфічні умови підприємства. Коли вся інформація про поточну інфраструктуру зібрана, настає другий етап в процесі побудови гібридної інфраструктури. Його завданням є зібрати всю інформацію про те, як підприємство хоче, щоб гібридна інфраструктура працювала: як рухалася пошта, які аспекти безпеки повинні враховуватися, і які елементи поточної інфраструктури повинні переноситися в хмару, а які ні. Для цього нам необхідно зібрати ряд заявок з підприємства, які згодом вплинуть на конфігурацію гібридної інфраструктури.

Аспекти, що впливають на транспортні елементи. Першим і найголовнішим аспектом при побудові гібридної інфраструктури є транспортна частина. Якщо в наземній інфраструктурі Exchange Server пошта могла приходити через один сервер або через кілька серверів, то в гібридній інфраструктурі список варіантів розширюється і підприємство повинно вибрати варіант із врахуванням всіх переваг і недоліків.

Варіант для вхідної пошти 1. Пошта централізовано приходить в Office 365, обробляється хмарною системою боротьби з небажаною поштою, антивірусною системою, після чого, пошта призначена для поштових скриньок, що знаходяться в Office 365 доставляється до одержувача, а пошта призначена для одержувачів в наземній частині організації Exchange Server доставляється на заздалегідь визначений сервер, після якого почнеться стандартна маршрутизація, властива для Exchange Server (рис. 2).

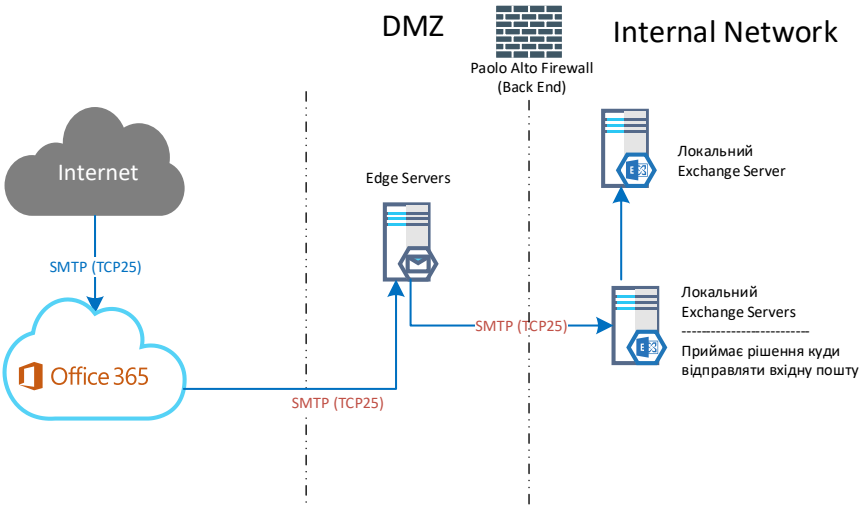

Рис. 2. Вхідна пошта через O365

Цей сценарій являє собою збалансованість між безпекою та ефективністю з точки зору навантаження на сервери, що знаходяться в локальному центрі обробки даних: а) пошта перевіряється найсвіжішими антивірусними сигнатурами; б) на локальні сервери приходить вже очищена пошта, що значно знижує навантаження на процесорні потужності; в) навантаження на мережеву інфраструктуру значно знижується, тому що навантаження з прийому всієї пошти покладається на хмарну інфраструктуру, а локальна буде навантажувати тільки тієї поштою, яка залишилася в локальних серверах.

В даному випадку підприємство повинно визначитися тільки з одним параметром: через які сервери (або в якийсь центр обробки даних) буде надходити пошта з хмарної інфраструктури в локальну. Решта значення не має. На довершення необхідно переконфігурувати MX-записи по всіх поштових доменах – вони в подальшому повинні будуть вказувати на поштову службу Office 365 – Exchange Online, яка буде знаходитися в зоні mail.protection.outlook.com.

Варіант вхідної пошти 2. Вся пошта організації, що надходить на локальні поштові сервери (все залишається без змін), локально обробляється системами боротьби з небажаною поштою, а також системами боротьби зі шкідливим ПЗ. Після цього пошта, призначена для локальних одержувачів, відправляється в поштові скриньки, а пошта, призначена для одержувачів, чиї поштові скриньки знаходяться в Office 365, перенаправляється в хмару відповідальними за дану комунікацію серверами. Там дана пошта перевіряється ще раз службами боротьби з шкідливим ПЗ (служби боротьби з небажаною поштою в даному випадку не будуть задіяні, так як пошта була відправлена з довіреної системи), і після цього доставляється в поштові скриньки.

Перевагами даної конфігурації можуть бути наступні: а) вся вхідна пошта перевіряється карантинними системами того провайдера, якого забажає менеджмент підприємства; б) вся вхідна пошта обов'язково проходить через локальні системи, а значить, інформація про всі листи буде зберігається в локальних файлах відстеження. Дана конфігурація може бути найважливішим критерієм при ухваленні рішення про те, як пошта повинна переміщатися з боку служби безпеки; в) побічним же ефектом даної конфігурації є те, що локальні сервери надлишково навантажуються, як з точки зору процесорних потужностей, так і з точки зору мережевої інфраструктури. Ще одним прихованим недоліком такої конфігурації є надмірне використання інформації на жорстких дисках, так як Exchange Server при проходженні пошти до його транспортної підсистеми зберігає пошту в своїх поштових чергах певний термін (за замовчуванням два дні) на випадок збою, як система відмовостійкості (пошта може бути затребувана тією системою, куди була відправлена, але з якихось причин загублена). Таким чином, даний варіант з точки зору продуктивності менш ефективний, але дозволяє серйозно поліпшити транспортну систему з точки зору безпеки. Єдиним параметром, який організації потрібно визначити в цьому варіанті: які сервери будуть відповідальними за обмін поштою з Office 365.

Варіант вхідної пошти 3. Вся пошта організації надходить в Office 365. Там відбувається перевірка пошти, як і в першому варіанті, але після цього вся, без винятку, пошта пересилається в локальну організацію Exchange Server, де пошта перевіряється ще раз додатковими службами, відповідальними за боротьбу з небажаною поштою та шкідливим ПЗ. Після цього пошта, призначена для локальних одержувачів, доставляється прямо в їх поштові скриньки, а пошта, призначена для одержувачів, чиї поштові скриньки знаходяться в Office 365, знову відправляється до хмарної інфраструктури. Там транспортна підсистема визначить, що повідомлення отримано із довіреної системи і доставить прямо в поштову скриньку одержувача без додаткових перевірок. Даний варіант має наступні характеристики:

а) основні атаки з інтернет на транспортні служби жодним чином не стосуються локальних серверів;

б) пошта перевіряється як хмарними, так і наземними службами, що дозволяє зробити систему вкрай захищеною з точки зору загроз, пов'язаних з передачею небажаного контенту;

в) пошта, як і в другому варіанті, проходить обов'язково через локальну транспортну систему, а отже, залишає слід в файлах трасування, що є великою перевагою з точки зору служби безпеки, що займається розслідуваннями, пов'язаними з витоком інформації та ін;

г) локальна система менше навантажується на рівні процесорних потужностей і дискової підсистеми, так як більша частина небажаної пошти буде відфільтрована на етапі проходження через «фільтри» Office 365.

Єдиним недоліком даної конфігурації є те, що буде навантажуватися транспортна система, через те, що пошта, призначена для одержувачів в Office 365, буде робити фактично петлю, що відіб'ється на продуктивності самої системи.

При виборі даної конфігурації підприємство повинно визначити, через які сервери з якого центру обробки даних буде проходити пошта під час комунікації з Office 365. Також необхідно буде, як і в першому варіанті, налаштувати MX-запис таким чином, щоб він вказував на сервери служби Exchange Online Protection, які знаходяться в зоні mail.protection.outlook.com.

Щодо **вихідної пошти,** то вона також може мати три конфігурації, проте вони відрізняються від конфігурацій, пов'язаних із вхідною поштою [2].

Варіант вихідної пошти 1. Сценарієм руху вихідної пошти за замовчуванням є сценарій, при якому вся локальна пошта продовжує відправлятися в зовнішній світ так само, як і до налаштування гібридної інфраструктури: відправка йде з локальних серверів. Пошта, яка відправляється з поштових скриньок, що знаходяться в хмарній інфраструктурі, буде йти безпосередньо зі служби Exchange Online. Єдиною дією в даній конфігурації, яку потрібно зробити, – налаштувати корпоративну службу DNS, щоб у всіх поштових доменах SPF-запис вказував не лише на локальні сервери, але і на службу Exchange Online Protection, з якої тепер теж будуть відправлятися корпоративні листи. Плюсами даної конфігурації є те, що вона вимагає мінімальних налаштувань.

Однак, якщо в компанії стоїть питання конфігурації захисту від витоку інформації, то цю систему доведеться налаштовувати як в хмарі, так і в локальній інфраструктурі (паралельно), що збільшує навантаження на обслуговування даної системи (збільшення вартості), а також збільшує ризик того, що при внесенні змін до однієї частини (наприклад, хмарної), точно такі ж зміни забудуть внести в локальній частині або зроблять з помилками (порушується цілісність конфігурації), що може призвести до інцидентів, пов'язаних з безпекою.

Варіант вихідної пошти 2. Вся вихідна пошта відправляється виключно через Office 365. У цьому випадку в локальній організації Exchange Server необхідно поміняти налаштування основного конектора, відповідального за відправку пошти в Office 365, таким чином, щоб він відповідав не тільки за пересилку пошти по доменному суфіксу «onmicrosoft.com» і «mail.onmicrosoft.com», а й додати простір імен «*». На додачу, в кожній з поштових зон DNS необхідно додати або виправити (якщо така вже існує) SPF-записи на такі, які будуть запропоновані в Office 365 (рис. 3).

Ця конфігурація зручна з наступних причин:

а) з точки мінімізації навантаження на локальні ресурси вся пошта відправляється з локальної організації в хмарну, де буде проводитися аналіз на предмет витоку інформації і так далі;

б) управління захистом від витоку інформації проводиться централізовано.

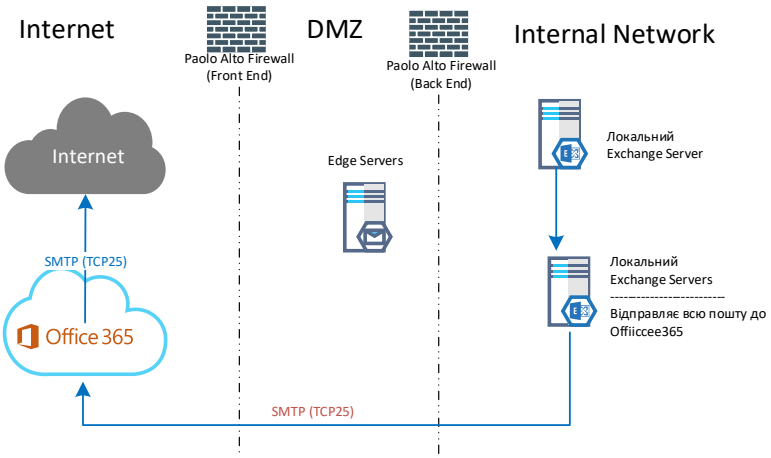

Рис. 3. Вихідна пошта системи через сервери О365

Варіант вихідної пошти 3. Вся вихідна пошта відправляється в локальну інфраструктуру і, після всіх перевірок на предмет захисту від витоку інформації, відправляється до зовнішнього світу. Дана конфігурація вимагає зробити єдине налаштування в Office 365 – налаштувати конектор, який відповідає за відправку пошти у зовнішній світ, таким чином, щоб він більше не перенаправляв пошту прямо, а відправляв її в локальну інфраструктуру Exchange Server. Дана конфігурація має наступні переваги: а) вся пошта, яка проходить через локальну інфраструктуру, буде залишати інформацію про листи в локальних файлах відстеження; б) система захисту від витоку інформації не обмежується тільки тією, яка вбудована в Exchange Server. При даній конфігурації служба безпеки може використовувати і сторонні служби захисту від витоку інформації. Саме так в більшості великих фінансових і урядових компаній і роблять.

Аспекти клієнтського доступу, які впливають на дизайн і майбутню конфігурацію гібридної інфраструктури. Якщо в організації один ЦОД з єдиним каналом в інтернет, тоді маємо єдиний сценарій міграції призначених для користувача даних. Але якщо в компанії кілька ЦОДів, доступні наступні варіанти для міграції:

1) через єдиний (основний) центр обробки даних. Підприємство самостійно приймає рішення щодо того, який ЦОД буде основним, і далі вся міграція буде йти через нього. Даний тип міграції, за замовчуванням легко налаштовується з боку управління Office 365;

2) через кілька ЦОД. У цьому випадку підприємство приймає рішення, що дані користувача повинні переноситися в Office 365 таким чином, щоб дані з одного ЦОДу ні в якому разі не мігрували через сервери іншого, при наявності клієнтського доступу з інтернету. Даний сценарій зручний, насамперед тим, що передачу даних можна вести в кілька потоків (при передачі даних компанія Microsoft обмежує пропускну здатність смуги з одного ЦОД), рис. 4.

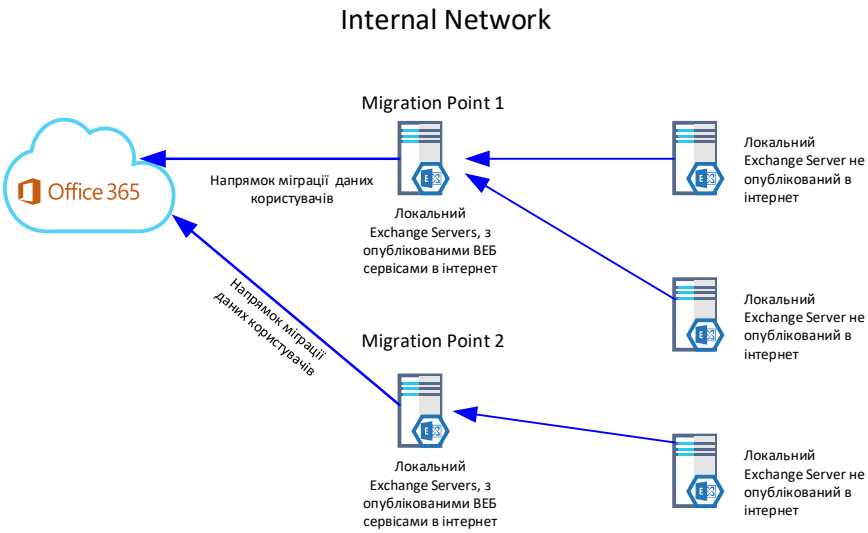

Рис. 4. Міграція даних через різні ЦОД (варіант «2»)

Отже, на даному етапі необхідно визначитися, яким чином компанії потрібно мігрувати дані і через які центри обробки даних. Для цього необхідно виконати подвійний запит: а) визначити, який режим міграції планується використовувати (1 або 2) і, якщо вибирається сценарій «2», приступаємо до конфігурації гібридної інфраструктури під формат, в якому поштові скриньки зможуть переноситися через різні ЦОД з інтелектуальною обробкою того, яким шляхом вони повинні переміщуватись; б) з'ясувати, через який ЦОД буде вестися міграція в разі варіанта «1». Якщо ж буде обраний варіант «2», то тоді в процесі

міграції система сама повинна встановити локацію поштових скриньок і визначити, через який ЦОД їх зручніше мігрувати (на підставі служби Autodiscover). Алгоритм конфігурації, наступний.

1. Здійснюється запит для отримання інформації про всі сайти активного каталогу, в яких є, як мінімум, один Exchange Server і результати запиту формують колекцію сайтів Exchange Server, які також нумеруються.

2. Здійснюється запит по всіх WEB-сервісах всередині локальної поштової організації, щоб отримати тільки ті сервіси, в яких встановлені такі параметри зовнішнього підключення (ExternalUrl). Даний параметр додається в колекцію всіх доступних для організації зовнішніх WEB-підключень. Всі елементи нумеруються.

3. Відповідальний співробітник складає підстановку того, дані з якого AD-сайту, через яке зовнішнє підключення підприємства мають переміщатися. Дана інформація зберігається в спеціальному файлі.

4. Наявність і контент конфігураційного файлу перевіряється при кожному запуску конфігураційного скрипта, який перевіряє його вміст і відображає те, що було вже раніше налаштовано, а якщо файл порожній або відсутній, то просто переконфігуровує його знову.

У разі, якщо підприємство використовує версії Exchange 2010 або 2013, рекомендується створити окремий сайт AD на одну IP-адресу і встановити в ньому додатково Exchange Server, після чого опублікувати його в зовнішній світ і здійснювати міграцію через нього.

Висновки. В процесі розробки системи було взято підхід, який супроводжує всі проекти, пов'язані з міграцією. Тобто, модулі, які запускаються, відповідають тим чи іншим фазам проектної діяльності.

Перший основний компонент відповідає стадії «оцінка даних» системи, яку планують мігрувати. Всі дані, які збираються під час аналізу інфраструктури, а також дані користувачів системи Microsoft Exchange експортуються до файлів на зовнішньому носії у вигляді CSV-файлів, які будуть використовуватись іншими модулями, та у вигляді TXT (можливо, у HTML) для табличного звіту, який може розглядатись персоналом. Модуль обробки даних запускається після того, як збір даних завершено. Модуль збирає інформацію з CSV-файлів і публікує ці дані до хмарної частини гібридної інфраструктури. Також система вміє сама створювати канали передачі даних (Migration Endpoints) та керувати потоками міграційних даних (Migration Batch).

Література

1. Риз Дж. Облачные вычисления / Джордж Риз. – СПб : БХВ Петербург, 2011. – 288 с.

2. Banerjee B. Microsoft Exchange Server PowerShell Essentials / Banerjee B. – Packt Publishing, 2016. – 210 p.

3. Catrinescu V. Essential PowerShell for Office 365: Managing and Automating Skills for Improved Productivity / Catrinescu V. – Paperback, 2018. – 234 p.

4. Kegg D. Microsoft Office 365 Administration Inside Out (Includes Current Book Service), 2nd Edition / Kegg D., Guilmette A., Mandich L., Fisher E. – MicrosoftPress, 2017. – 1040 p.

5. Stanek W. Microsoft Exchange Server 2013 Pocket Consultant Databases, Services, & Management / Stanek W. – The Microsoft Press, 2013. – 384 p.

6. Connect to Office 365 PowerShell. URL: https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell

References

1. Reese G. Cloud computing / George Reese. – SPb : BHV Petersburg, 2011. – 288 p.

2. Banerjee B. Microsoft Exchange Server PowerShell Essentials / Banerjee B. – Packt Publishing, 2016. – 210 p.

3. Catrinescu V. Essential PowerShell for Office 365: Managing and Automating Skills for Improved Productivity / Catrinescu V. – Paperback, 2018. – 234 p.

4. Kegg D. Microsoft Office 365 Administration Inside Out (Includes Current Book Service), 2nd Edition / Kegg D., Guilmette A., Mandich L., Fisher E. – MicrosoftPress, 2017. – 1040 p.

5. Stanek W. Microsoft Exchange Server 2013 Pocket Consultant Databases, Services, & Management / Stanek W. – The Microsoft Press, 2013. – 384 p.

6. Connect to Office 365 PowerShell. URL: https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell

Надійшла / Paper received: 11.04.2020 Надрукована / Paper Printed : 03.06.2020