DOI 10.31891/2307-5732-2020-289-5-95-100
УДК 681.3

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

ТЕСТУВАННЯ ТА ФОРМУВАННЯ ЗВІТУ ПРО ВПРОВАДЖЕННЯ ГІБРИДНОЇ ІНФРАСТРУКТУРИ

В статті розглянуто і досліджуються прогнозовані результати формування гібридної інфраструктури. Перед початком перенесення даних, необхідно переконатися, що інфраструктура після попередніх налаштувань працює нормально. Для цього необхідно провести ряд тестів, які дозволять виявити будь-які збої на різних ділянках. Першочергові тести проводяться на глобальному рівні і перевіряють, чи нормально налаштовані федеративні довірчі відносини між локальною організацією Exchange Server і хмарної службою Exchange Online. В результаті дослідження було виявлено, що деякі об'єкти хмарної частини, коли до них треба звертатись, мають іншу систему ідентифікаторів, ніж аналогічні об'єкти в локальній системі. У локальній інфраструктурі до них посилаються за ім'ям, в той час як у хмарній за ID-кодом. Тому, в цьому випадку треба робити додатковий запит, який виявить ID-об'єкт за його назвою. Під час написання ряду кодів для міграції даних запропоновано застосування різних підходів до управлінню об'єктами в наземній і хмарній частинах, що запобігає використанню одних і тих же методів для систем одного типу.

Ключові слова: система для міграції, гібридна інфраструктура, хмарні сервіси, Exchange Server, центр обробки даних (ЦОД), політики безпеки.

V. MIKHALEVSKYI, G. MIKHALEVSKA
Khmelnitsky National University

TESTING AND FORMATION OF A REPORT ON THE IMPLEMENTATION OF HYBRID INFRASTRUCTURE

The article considers and investigates the projected results of the hybrid infrastructure formation. Before starting the data transfer, you need to make sure that the infrastructure works properly after the previous settings. To do this, you must perform the series of tests that will detect any failures in different areas. Priority tests are performed globally to verify that the federated trust between the on-premises Exchange Server organization and the Exchange Online cloud service is properly established.

As a result of the research, it was found that some objects in the cloud part, when they need to be accessed, have a different system of identifiers than similar objects in the local system. In the local infrastructure they are referred to by the name, while in the cloud infrastructure by the ID. Therefore, in this case, you need to make an additional query that will find the ID-object by its name. When writing a number of codes for data migration, it is proposed to use different approaches to the management of objects in the ground and cloud parts, which prevents the use of the same methods for systems of the same type. Microsoft Exchange exports the data collected during the infrastructure analysis, as well as the data of system users, to files on external media in the form of CSV files to be used by other modules and in the form of TXT or HTML for a spreadsheet that is analyzed by staff. During the transferring data to cloud storage, most companies pay special attention to how security policies will be applied to cloud resources. The main task of this testing stage is to establish that all security parameters exported from the local infrastructure has been imported into the cloud infrastructure successfully and applied at different levels stably. The most important series include tests: related to testing traffic rules and information leakage protection policies; designed to test security policies; tests of policies that affect the client connection.

This type of system allows many large companies to avoid the problems associated with the process of migrating global local infrastructure settings to the cloud environment and to improve the data analysis process with subsequent automatic management of data migration in an IT environment with complex network infrastructure.

Keywords: migration system, hybrid infrastructure, cloud services, Exchange Server, data processing center, data security policies.

Вступ. На сьогоднішній день не існує реалізації повного переносу налаштувань локальної інфраструктури Exchange Server у хмарну. Дані користувачів можливо мігрувати різними методами і протоколами. Є багато різних аспектів, які потрібні сучасним підприємствам. Наприклад, існує велика потреба в переносі налаштувань безпеки, пов'язаних із захистом інформації. Також немає рішення, яке могло би проаналізувати існуючу топологію організації Exchange Server і, завдяки отриманій інформації, перебудувало б переміщення даних користувачів [1]. Наразі існує виключно система інвентаризації, запропонована самою корпорацією Microsoft (RAP as a Service), а також такими компаніями, як Quest, які пропонують інвентаризацію всієї топології.

Перед тим, як почнеться перенесення даних, необхідно переконатися, що інфраструктура після попередніх налаштувань працює нормально. Для цього необхідно провести ряд тестів, які дозволять виявити будь-які збої на різних ділянках.

Виклад основного матеріалу. Дані, які зібрані під час аналізу інфраструктури, а також дані користувачів системи, Microsoft Exchange експортує до файлів на зовнішньому носії у вигляді CSV-файлів, які будуть використовуватись іншими модулями, та у вигляді TXT або HTML для табличного звіту, який аналізується персоналом. Під час передавання даних в хмарні сховища більшість компанії особливу увагу приділяють тому, як будуть застосовуватися політики безпеки на хмарні ресурси. Основне завдання даного етапу тестування встановити, що всі експортовані з локальної інфраструктури параметри безпеки імпортувалися в хмарну інфраструктуру успішно і стабільно застосовуються на різних рівнях. До найважливіших серій відносяться тести: пов'язані з тестуванням транспортних правил і політикам захисту від витоку інформації; призначені для тестування політик безпеки; тести політик, що впливають на клієнтське підключення [2].

Тестування та формування звіту про впровадження гібридної інфраструктури. Першочергові тести проводяться на глобальному рівні і перевіряють чи нормально налаштовані федеративні довірчі відносини між локальною організацією Exchange Server і хмарної службою Exchange Online.

Першим тестом перевіряється нормально налаштовано федерація і чи може локальний Exchange Server отримати токен від Microsoft Federation Gateway, який відповідає за аутентифікацію і видачу посвідчень всім організаціям Exchange Server в світі. Дана перевірка здійснюється в PowerShell наступним рядком:

Test-FederationTrust -UserIdentity "USER_ID" -verbose

Результатом даної команди має бути 6 різних тестів, які повідомлять нас про стан (нормальне функціонування - success). Перш, ніж пройти всі тести необхідно створити ряд тестових поштових скриньок умовно з іменами LocalTestUser1 і LocalTestUser2 з основними поштовими суфіксами поштової організації. Також необхідно створити дві тестових поштові скриньки, які перебувають в Office 365 з іменами O365TestUser1 і O365TestUser2. Після того, як всі умови для тестів створені можна починати їх виконувати [3].

Тестування міграції даних. Для того щоб переконатися, що дані в майбутньому будуть нормально переміщатися між локальною та хмарною інфраструктурами необхідно виконати два тести.

1) Тест на те, що локальна інфраструктура нормально опублікована і до неї нормально зможуть підключатися служби Office 365, для того щоб можна було переміщати дані. Для цього необхідно відвідати портал компанії Microsoft “Microsoft connectivity analyzer”: https://testconnectivity.microsoft.com/ (Рис. 1).

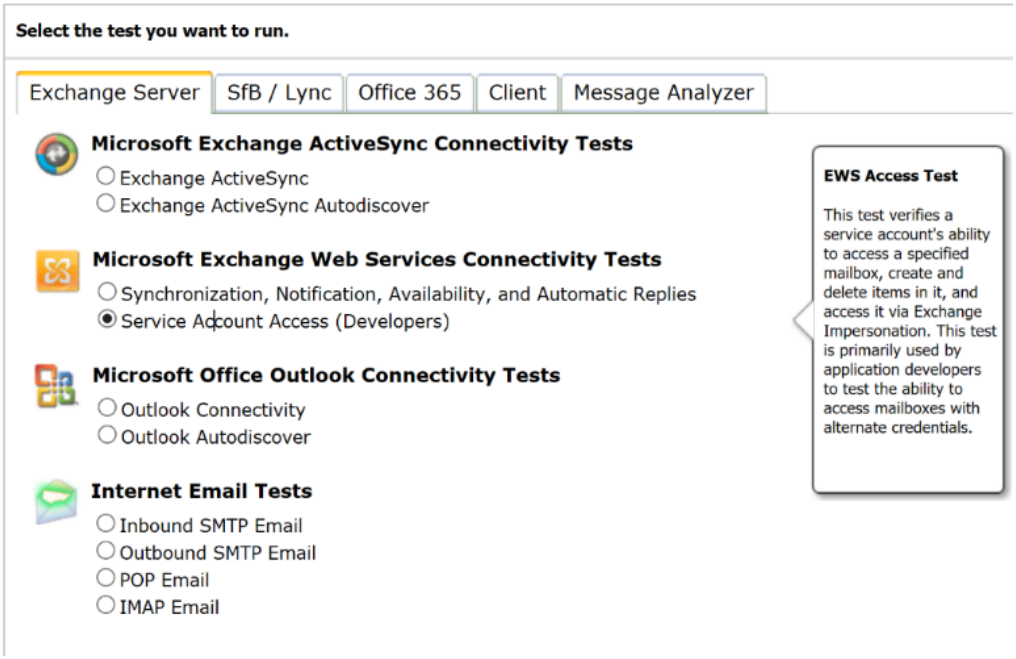

Рис. 1. Інтерфейс Microsoft Connectivity Analyzer

На цьому додатку вибираємо пункт, який протестує коректність налаштувань WEB-сервісів, що опубліковані в інтернет. Цим тестом необхідно перевірити всі сервіси, які компанія опублікувала в інтернет.

2) Тест для перевірки працездатності гібридної інфраструктури Exchange Server, тобто, тестове переміщення заздалегідь приготованих поштових скриньок з локальної інфраструктури в хмарну з подальшим тестування підключення клієнтської частиною.

Тестування клієнтської частини. Наступним тестом є перевірка того, що користувачі (власники поштових скриньок), що знаходяться в локальній інфраструктурі Exchange Server можуть отримати доступ до ресурсів користувачів, що знаходяться в Exchange Online (наприклад, календарі).

Особливу увагу в гібридної інфраструктурі Exchange Server слід приділити службі Autodiscover. Саме від неї залежить те, наскільки успішно користувачі, чиї поштові скриньки знаходяться в хмарній службі, зможуть автоматично бути перенаправлені на точку підключення Office365. А при наявності федеративної служби аутентифікації, також буде здійснено процес підключення до скриньки без запиту аутентифікаційних даних (Single-Sigh-On). Вводяться дані по тестовому обліковому запису, з поштовою скринькою в хмарі, а потім робиться безпосередньо сам тест [3, 4]:

Test-OutlookWebServices -Identity:Office365TestUser1@<domain>.com -MailboxCredential $cred -AutoDiscoverServer <FQDN_CEPBEPA_Exchange>

Також в процесі даного тесту перевіряються служби: Autodiscover; Availability Service; Outlook Anywhere; Offline Address Book.

Тестування транспортного функціоналу. Тестування транспортної конфігурації проводиться на кількох рівнях в залежності від, конфігурації, яку застосували в процесі настройки гібридної інфраструктури. Умовно всі тести діляться на наступні категорії.

- Тестування внутрішньої комунікації (відправляються листи з локального поштового ящика в хмарний і навпаки). Таким чином можна перевірити правильність налаштувань для транспортної комунікації між різними частинами гібридної інфраструктури Exchange Server.

- Тестування пошти для зовнішніх одержувачів. Відправляються два повідомлення до зовнішнього світу (одне з поштової скриньки, розташованої в локальній частині, а інше з хмарної частини гібридної інфраструктури). Мета даного тесту - перевірити правильність маршрутів і руху вихідної пошти. Під час проведення даного тесту потрібно уважно стежити, щоб на листи не застосовувалися будь-які транспортні правила або політики захисту інформації, які можуть блокувати повідомлення або змінювати його маршрут.

- Тестування вхідної пошти, що надійшла із зовнішніх систем. Для успішного виконання даного тесту необхідно відправити листа із зовнішніх поштових систем (можна використовувати безкоштовні тестові сервіси такі як outlook.com) на дві тестові поштові скриньки із гібридною організації підприємства (один одержувач з хмарної інфраструктури, другий з локальної). Мета даного тесту перевірити правильність проходження із зовнішнього світу по заздалегідь прописаному маршруту. Під час виконання тесту необхідно переконатися, що на листи не будуть застосовуватися будь-які транспортні правила або політики захисту від витоку інформації.

- Тест на можливість підключення внутрішніх ресурсів (таких як сканери або системи оповіщення) в разі перенесення відповідних конекторів (Receive Connector) з локальної інфраструктури у хмарну.

У всіх випадках можна користуватися як сторонніми утилітами, так і вбудованими командами і утилітами Windows, такими як Telnet.exe або ж командлетом Send-SMTPMail, який вбудований в стандартну поставку середовища PowerShell його останні версії.

Тестування функціоналу елементів безпеки. Під час передавання даних в хмарні сховища більшість компанії особливу увагу приділяють тому, як будуть застосовуватися політики безпеки на хмарні ресурси. Основне завдання даного етапу тестування встановити, що всі експортовані з локальної інфраструктури параметри безпеки імпортувалися в хмарну інфраструктуру успішно і стійко застосовуються на різних рівнях.

Перша серія тестів пов'язана з тестуванням транспортних правил і політикам зашиті від витоку інформації. Для цього необхідно проаналізувати звіт, згенерований на етапі оцінки інфраструктури та створити листи, які підпадали б під ті чи інші правила. Особливу увагу приділяють тому, що параметри безпеки в хмарної і локальної частинах гібридної інфраструктури діють на транспортні компоненти абсолютно незалежно. А отже, проведення тестів обов'язково, щоб не отримати ефект дублювання, який виникає, наприклад, при застосуванні правил архівування.

Друга серія тестів призначена для тестування політик безпеки, які відносяться до безпеки зберігання даних, такі як InPlace Hold Policies або ж Retention Policies. Для цього необхідно по черзі застосувати дані політик на тестовий обліковий запис, що знаходиться в хмарній частині і перевірити правильність застосування тих чи інших налаштувань.

Третьою серією тестів, які необхідно перевірити, є тести політик, що впливають на клієнтське підключення. До даних налаштувань можна віднести політики доступу до WEB-інтерфейсу (Outlook Web Application) або політики захисту даних на мобільних пристроях. Політики мають бути по черзі протестовані на тестовому поштовому ящику, розташованому в хмарній частині гібридної інфраструктури.

Перенесення даних користувачів в хмарну інфраструктуру згідно з потребами підприємства. Останнім етапом впровадження гібридної інфраструктури Exchange Server є фактичне перенесення даних в хмарну інфраструктуру з подальшим застосуванням на переміщені дані всіх політик та налаштувань, які застосовувалися на них в локальній інфраструктурі. Для досягнення цієї мети попередньо експортуються налаштування з кожної поштової скриньки і зберігаються у файли з шаблонними іменами.

Переведення поштових скриньок до хмарної інфраструктури. Найвідповідальнішим етапом при побудові гібридної інфраструктури є фактичне переміщення даних з локальної частини інфраструктури в хмарну. Перенесення даних може здійснюватися як на елементарному рівні (перенесення окремої поштової скриньки), так і на масовому - коли створюється завдання для переміщення поштових скриньок у великій кількості. І в тому, і в іншому випадку завдання створюється і управляється з боку хмарної частини.

Саме з хмарної інфраструктури здійснюється під'єднання до локальної інфраструктури через WEB-сервіси, опубліковані у зовнішній світ. Щоб хмарна служба могла під'єднатись до локальної з боку хмарних сервісів, адміністративним персоналом створюється спеціальний об'єкт «Migration Endpoint», який зберігає інформацію про те, до якого з опублікованих у зовнішній світ серверів під'єднатись, а також який обліковий запис і пароль до нього використовувати для здійснення під’єднання. Далі, коли фактично здійснюється міграція даних, адміністратор вказує який Migrationendpoint використовувати для міграції у випадку, коли налаштовано більше одного об'єкта такого класу. Такий підхід недостатньо зручний, так як адміністративний персонал, повинен вручну розібратися – які поштові скриньки через який канал під'єднання мають переміщуватись, рисунок 2.

Щоб вирішити це завдання, була розроблена система, яка аналізує стан і розташування поштових скриньок користувачів в реальному часі і самостійно визначає, через який WEB сервіс повинна бути здійснена міграція кожної поштової скриньки, після чого динамічно формуються завдання на міграцію, в яких всі поштові скриньки згруповані по WEB-сервісу, через який повинна здійснюватися ця міграція.

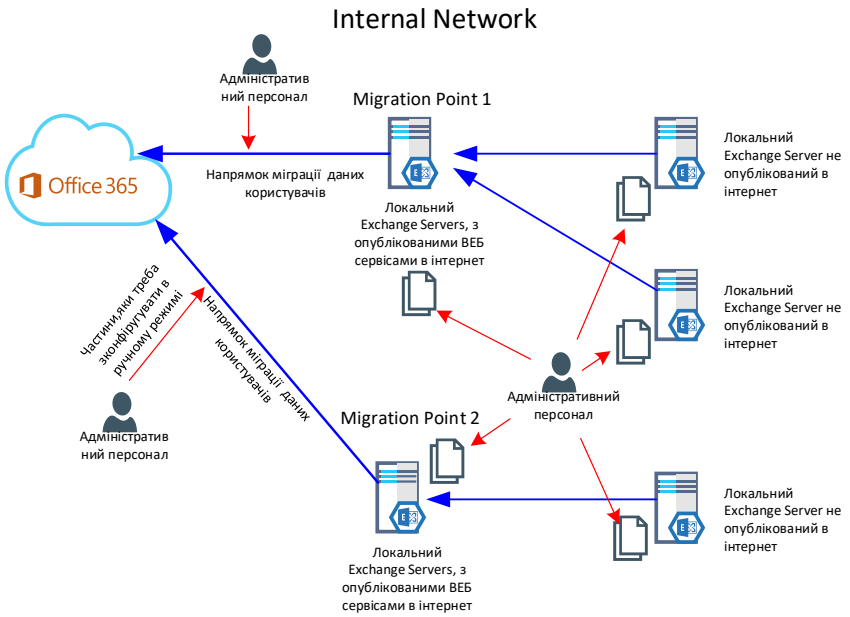

Рис. 2. Переміщення поштових скриньок в стандартному режимі

Такий підхід дозволяє ефективно використовувати всі інтернет-канали передачі даних, оптимізувати мережевий потік у внутрішній інфраструктурі, а також значно скоротити час міграції даних, так як міграція проводитися в кілька потоків, рисунок 3.

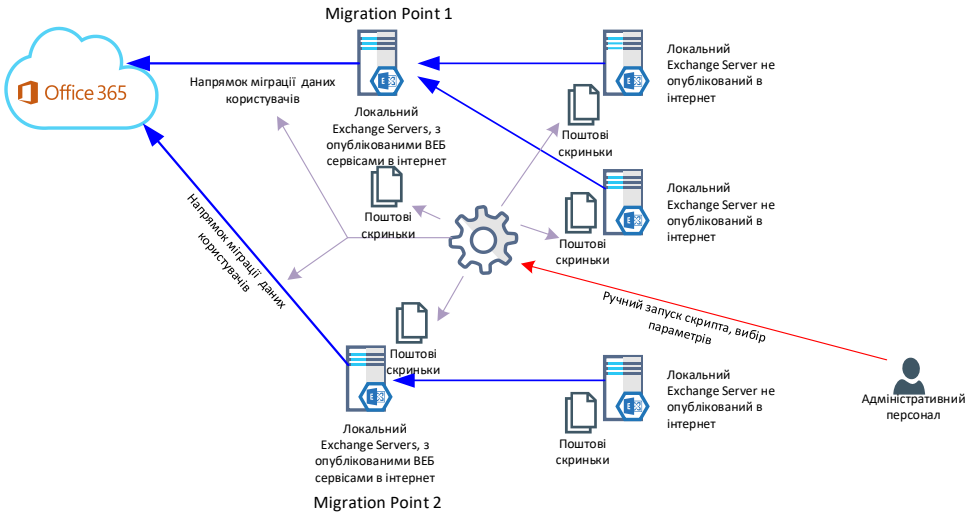

Рис. 3. Переміщення поштових скриньок в динамічному

При побудові даного рішення був обраний наступний алгоритми.

- Всі Сайти Активного Каталогу, в яких є сервери організації Exchange Server, зв'язуються із зовнішнім WEB-сервісом, через який повинна йти міграція поштових скриньок з даного сайту.

- Автоматична генерація об'єктів Migrationendpoint, по кожному WEB-сервісу. При цьому система автоматично перевіряє, чи не був Migrationendpoint раніше зареєстрований, щоб не створювати дублікати (перевірка перевіряється на ім'я WEB-сервісу, що гарантує унікальність).

- Коли необхідно відправити велику кількість даних, запускається скрипт, в якому вказується посилання на файл, який містить список всіх e-mail адресів поштових скриньок, які потрібно надіслати. Даний скрипт автоматично перевіряє поточне місцезнаходження кожної поштової скриньки, після чого маркує цю поштову скриньку інформацією про те, через який WEB-сервіс дані повинні мігрувати. Коли маркування всіх скриньок завершилось, всі скриньки групуються по іменах WEB-сервісів, щоб сформувати завдання (Migration Batch) з міграцією через конкретний Migration Endpoint. Скриньки можуть бути з різних сайтів AD, але адміністративний персонал завдяки ПЗ не повинен займатися вивченням того, через який WEB-сервіс відправляти конкретний пул поштових скриньок.

Відновлення політик та налаштувань на переміщені дані. Останнім етапом в автоматичній міграції є фінальна конфігурація поштових скриньок. Ще однією проблемою, пов'язаною з міграцією в хмарні сервіси, є застосування на них політик і налаштувань таких самих, які застосовувалися до поштової

скриньки в локальній інфраструктурі. Однак, при побудові гібридної інфраструктури політики та інші параметри (як правило, це дані, які Exchange Server зберігає в розділі Configuration служби Активного Каталогу) не переносяться в хмарну інфраструктуру. З цією метою виконуються скрипти, які повністю експортують всі налаштування локальної організації. Після цього всі дані, що визначають політики та конфігурації, імпортуються в хмарну частину гібридної інфраструктури. Також виконується скрипт, який експортує інформацію про те, які політики застосовуються на поштові скриньки. Після закінчення міграції можна запустити скрипт, який дозволяє з файлу із інформацією про зміни всіх поштових скриньок отримати необхідну інформацію, яка застосовувалася на поштову скриньку до його міграції та застосувати ті ж налаштування, але вже в хмарній інфраструктурі [1, 4]. Слід зауважити, що в локальній інфраструктурі всі зв'язки будуються по іменах, в той час, як в хмарної всі зв'язки побудовано по GUID (Global Unique Identity), що вимагає зробити додатковий крок при застосуванні налаштувань - з'ясувати, який GUID у політики, яку необхідно застосувати на поштову скриньку, після чого оперувати даними атрибутом. Даний підхід дозволяє відразу після переміщення будь-якої кількості поштових скриньок брати в обробку перелік переміщених поштових скриньок і застосовувати на них всі налаштування, не витрачаючи ресурси і час на аналіз і виявлення поштових скриньок, які мають некоректні налаштування:

```
$Root = "C:\ExchaData\"
$ExpPath = "C:\ExchaData\Export\"
$Config = "C:\ExchaData\Config\"
$MBXFile = $Root+'MBXs.CSV'
$MbxPolicyFile = $ExpPath +'MBXPolicy.csv'
$CASPolicyFile = $ExpPath+'MbxCASPolicy.csv'
$MBXs = Import-Csv $MBXFile
$MBXPolicies = Import-Csv -Path $MbxPolicyFile
$CASPolicies = Import-Csv -Path $CASPolicyFile
$cred1 = Get-Credential -Message "Enter Credentials of Admin Exchange Online"
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $cred1 -Authentication Basic -AllowRedirection
Import-PSSession $Session -DisableNameChecking
foreach ($MBX in $MBXs){
  $email=$MBX.Email
  $UsrMbxPol = $MBXPolicies | where PrimarySmtpAddress -EQ $email
  $strRetPol = " -RetentionPolicy $UsrMbxPol.RetentionPolicy "
  $strAddrtPol = " -AddressBookPolicy $UsrMbxPol.AddressBookPolicy "
  $strRolePol = " -RoleAssignmentPolicy $UsrMbxPol.RoleAssignmentPolicy "
  $UserCasPol = $CASPolicies | where PrimarySmtpAddress -EQ $email
  $StrActSyncPol = " -ActiveSyncMailboxPolicy $UserCasPol.ActiveSyncMailboxPolicy "
  $StrActSyncDef = " -ActiveSyncMailboxPolicyIsDefaulted $UserCasPol.ActiveSyncMailboxPolicyIsDefaulted "
  $StrOwaPol = " -OwaMailboxPolicy $UserCasPol.OwaMailboxPolicy "
  Set-Mailbox $email $strRetPol $strAddrtPol $strRolePol
  Set-CasMailbox $email $StrActSyncPol $StrActSyncDef $StrOwaPol
  }
}
```

Після застосування скрипта поштові скриньки користувачів, перерахованих у файлі, потрапляють під дію політик ідентично тому, як було в локальній частині організації Exchange Server.

Висновки. Для того, щоб протестувати працездатність системи, побудовано тестову інфраструктуру Exchange Server у хмарній інфраструктурі Microsoft Azure. У тестовому середовищі створено інфраструктуру із двох доменних контролерів (модуляція двох сайтів), які було розташовано у різних підмережах. На одному з доменних контролерів встановлено ПЗ Microsoft ADConnect, яке дозволяє синхронізувати користувачів Активного Каталогу до Активного Каталогу Azure. Було збудовано два сервери Exchange Server, які знаходились також на різних сайтах. Також розгорнуто додатковий Exchange Server в демілітаризованій підмережі, який виконував функцію розмежувального сервера (Edge).

Для можливості створення гібридної інфраструктури необхідно мати DNS-зону, яку сервіси Office 365 можуть перевірити (необхідна при створенні гібридної інфраструктури). Для цього, наприклад, можна придбати зону it-infrastructures.net на європейському реєстраторі доменних імен. Також, для можливості установлення гібридної інфраструктури необхідно на серверах, що опубліковані в інтернет, встановити сертифікати для того, щоб сервіси Office 365 могли встановити HTTPS-канал до «локальної» інфраструктури. Після цього на одному з серверів встановлюється модуль роботи з Azure Active Directory (MSOL). На цьому ж сервері розгортаються і створюються скрипти для модулів автоматизованої системи.

Система значно скорочує час проектів і кількість персоналу, задіяного в крупних проектах. Система проходить більшість стадій проекту і генерує вихідні проекти автоматично, що є економічно доцільним.

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. -210c.
3. Meloski V. Mastering Microsoft Exchange Server 2016, 2nd Edition / Meloski V., Wright B., Svidergol B., Clifton - Sybex, 2016. – 761 с.
4. Office 365 migration performance and best practices [Електронний ресурс]. – Режим доступу: https://docs.microsoft.com/en-us/exchange/mailbox-migration/office-365-migration-best-practices

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. -210p.
3. Meloski V. Mastering Microsoft Exchange Server 2016, 2nd Edition / Meloski V., Wright B., Svidergol B., Clifton - Sybex, 2016. – 761 p.
4. Office 365 migration performance and best practices [Electronic resource]. – Access mode: https://docs.microsoft.com/en-us/exchange/mailbox-migration/office-365-migration-best-practices

Надійшла / Paper received : 02.11.2020 р. Надрукована/Printed :27.11.2020 р.