ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Методика інтеграції сервісів Microsoft 365 та Azure Active Directory з метою забезпечення єдиної системи аутентифікації в локальних та хмарних сервісах Microsoft»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерні системи та мережі
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Дмитро ГЕРАСИМЕНКО
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав:
здобувач вищої освіти Дмитро ГЕРАСИМЕНКО
група КСДМ-61

Керівник: В'ячеслав ЧЕРЕВИК
науковий ступінь, вчене звання к.т.н., доцент

Рецензент:
науковий ступінь, вчене звання
_____
Ім'я, ПРІЗВИЩЕ

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти Магістр

Спеціальність 123 «Комп'ютерна інженерія»

Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
«_____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Герасименко Дмитру Олександровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Методика інтеграції сервісів Microsoft 365 та Azure Active Directory з метою забезпечення єдиної системи аутентифікації в локальних та хмарних сервісах Microsoft

керівник кваліфікаційної роботи В'ячеслав ЧЕРЕВИК к.т.н., професор,
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145

2. Строк подання кваліфікаційної роботи «28» грудня 2023р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література Microsoft, вимоги до середовища інтеграції Azure AD Connect, параметри синхронізації даних каталогівActive Directory.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Дослідження методу інтеграції технології Azure AD Connect
2. Реалізація технології у віртуальному середовищі
3. Оцінка корисних якостей системи єдиної аутентифікації у порівнянні зі звичайною системою

5. Перелік графічного матеріалу: *презентація*

1. Мета, об'єкт та предмет дослідження
2. Актуальність дослідження

3. Active Directory
4. Azure Active Directory
5. Тенант Azure AD
6. Azure AD Connect
7. Передумови інтеграції
8. Тестове середовище
9. Налаштування синхронізації хешів паролів
10. Синхронізація даних між AD та Azure AD
11. Azure AD Connect Synchronization Service Manager
12. Self Service Password Reset
13. Single Sign-On на основі пароля
14. Password writeback
15. Переваги використання налаштованої системи
16. Майбутні напрямки розвитку
17. Висновки

6. Дата видачі завдання«19» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	19.10-24.10.23	
2	Вивчення матеріалів для реалізації технології Azure AD Connect	24.10-30.11.23	
3	Дослідження хмарних сервісів	30.11-02.12.23	
4	Аналіз особливостей інтеграції технології у робоче середовище	02.12-04.12.23	
6	Реалізація і тестування технології синхронізації даних автентифікації локальних та хмарних сервісів	04.12-15.12.23	
7	Оформлення роботи: вступ, висновки, реферат	15.12-26.12.23	
8	Розробка демонстраційних матеріалів	26.12-27.12.23	

Здобувач вищої освіти _____ Дмитро ГЕРАСИМЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ В'ячеслав ЧЕРЕВИК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 83 стор., 1 табл., 22 рис., 31 джерел.

Мета роботи – інтеграція та налаштування сервісів Microsoft 365 та Azure Active Directory з метою забезпечення єдиної системи аутентифікації в локальних та хмарних сервісах Microsoft.

Об'єкт дослідження – технологія синхронізації локального лісу Active Directory з хмарним сервісом Azure Active Directory.

Предмет дослідження – система аутентифікації локальних та хмарних сервісів Microsoft.

Короткий зміст роботи: У роботі досліджено та реалізовано інтеграцію сервісів Microsoft 365 та Azure Active Directory з метою створення єдиної системи аутентифікації в локальних та хмарних сервісах Microsoft. Робота включає аналіз теоретичних основ інтеграції, розробку та детальний опис експериментального дослідження з використанням віртуального середовища. Результати експерименту підтверджують ефективність технології та її позитивний вплив на безпеку та ефективність роботи корпоративних інфраструктур. У висновках надано узагальнення результатів та вказано напрямки подальших досліджень у цій області..

КЛЮЧОВІ СЛОВА: ACTIVE DIRECTORY, ХМАРНІ СЕРВІСИ, AZURE AD CONNECT, ENTRA ID, AZURE AD, АВТЕНТИФІКАЦІЯ, MICROSOFT 365.

ABSTRACT

Text part of the master's qualification work: 83 pages, 22 pictures, 1 table, 31 sources.

The aim of the study is to integrate Microsoft 365 and Azure Active Directory services to establish a unified authentication system for both local and cloud-based Microsoft services.

The object of the research is the technology of synchronizing the local Active Directory forest with the cloud service Azure Active Directory.

The subject of the research is the authentication system of local and cloud-based Microsoft services.

Summary of the work: The paper explores and implements the integration of Microsoft 365 and Azure Active Directory services to create a unified authentication system for local and cloud-based Microsoft services. The work includes an analysis of the theoretical foundations of integration, the development, and detailed description of experimental research using a virtual environment. The results of the experiment confirm the effectiveness of the technology and its positive impact on the security and efficiency of corporate infrastructures. The conclusions provide a summary of the results and indicate directions for further research in this area.

KEYWORDS: ACTIVE DIRECTORY, CLOUD SERVICES, AZURE AD CONNECT, ENTRA ID, AZURE AD, AUTHENTICATION, MICROSOFT 365.

ЗМІСТ

ВСТУП

В умовах стрімкого розвитку технологій та широкого застосування хмарних сервісів, забезпечення єдиної системи аутентифікації та управління ідентичністю стає необхідністю для сучасних організацій. Методика інтеграції сервісів Microsoft 365 та Azure Active Directory (Azure AD) виходить за межі звичайних підходів, надаючи комплексне рішення для забезпечення безпеки та ефективності використання IT-ресурсів.

Основні завдання інтеграції включають:

– синхронізація ідентичності: Azure AD Connect не лише забезпечує стабільну синхронізацію користувачів та об'єктів, але й впроваджує механізми для управління атрибутами та розширеними можливостями синхронізації;

– єдиний вхід (Single Sign-On): інтеграція дозволяє налаштовувати не лише базовий один вхід, але й реалізовувати його на різних рівнях, забезпечуючи зручність та безпеки доступу до ресурсів;

– управління паролями та безпекою: автоматизоване управління політиками паролів та моніторинг їх безпеки вносять вагомий внесок у захист ідентичності користувачів;

– розширені функції безпеки: інтеграція використовує передові методи безпеки, такі як адаптивна аутентифікація, що аналізує контекст робочого процесу для ефективного контролю доступу;

Ця методика є не лише технічним рішенням, але і стратегічним кроком для підвищення конкурентоспроможності та гнучкості організації в умовах постійних змін технологічного середовища. Інтеграція сервісів Microsoft 365 та Azure AD через Azure AD Connect може запропонувати новий стандарт для управління ідентичністю та безпекою, створюючи стійку та інноваційну основу для подальшого розвитку IT-інфраструктури.

РОЗДІЛ 1 ЛОКАЛЬНІ ТА ХМАРНІ СЛУЖБИ КАТАЛОГІВ ACTIVE DIRECTORY

1.1 Active Directory

Active Directory (AD) – це служба каталогів, розроблена компанією Microsoft для доменних мереж Windows. Операційні системи Windows Server включають її як набір процесів і служб. Спочатку Active Directory використовувалася лише для централізованого керування доменами. Зрештою, вона стала загальною назвою для різних служб, пов'язаних з ідентифікацією, що базуються на каталогах.

Контролер домену – це сервер, на якому виконується роль служби домену Active Directory (AD DS). Він автентифікує та авторизує всіх користувачів і комп'ютери в мережі доменного типу Windows, призначає і застосовує політики безпеки для всіх комп'ютерів, а також встановлює або оновлює програмне забезпечення. Наприклад, коли користувач входить до комп'ютера, який є частиною домену Windows, Active Directory перевіряє введені ім'я користувача та пароль і визначає, чи є користувач системним адміністратором, чи ні. Крім того, вона дозволяє керувати та зберігати інформацію, забезпечує механізми автентифікації та авторизації, а також встановлює основу для розгортання інших пов'язаних служб: Служби сертифікатів, Служби федерації Active Directory, Полегшені служби каталогів та Служби керування правами.

1.2 Структура Active Directory

Active Directory – це служба, що складається з бази даних і виконуваного коду. Вона відповідає за керування запитами та обслуговування бази даних. Агент системи каталогів – це виконувана частина, набір служб і процесів Windows, які працюють в Windows 2000 і пізніших версіях. Доступ до об'єктів в базах даних Active Directory можливий через різні інтерфейси, такі як LDAP, ADSI, API обміну повідомленнями і служби диспетчера облікових записів безпеки.

Структура Active Directory складається з інформації про об'єкти, класифіковані за двома категоріями: ресурси і принципи безпеки (які включають облікові записи користувачів або комп'ютерів і групи). Кожному принципу безпеки присвоюється унікальний ідентифікатор безпеки (SID). Об'єкт може представляти собою користувача, комп'ютер, принтер або групу, разом з його атрибутами. Кожен об'єкт має унікальне ім'я, а його визначення – це набір характеристик та інформації за схемою, яка визначає місце зберігання в Active Directory.

Адміністратори можуть розширювати або змінювати схему за допомогою об'єкта схеми, коли це необхідно. Однак, оскільки кожен об'єкт схеми є невід'ємною частиною визначення об'єктів Active Directory, їх деактивація або зміна може кардинально змінити або зірвати розгортання каталогу. Зміна схеми автоматично впливає на всю систему, а нові об'єкти не можна видалити, їх можна лише деактивувати.

У мережі Active Directory структура, що містить об'єкти, має різні рівні: ліс, дерево і домен. Домени в розгортанні містять об'єкти, що зберігаються в єдиній реплікованій базі даних, а структура імен DNS ідентифікує їхні домени, тобто простір імен. Домен – це логічна група мережевих об'єктів, таких як комп'ютери, користувачі та пристрої, які мають спільний доступ до однієї бази даних Active Directory.

З іншого боку, дерево – це сукупність доменів та імен, пов'язаних транзитивною ієрархією довіри. Ліс – це сукупність дерев зі стандартним глобальним каталогом, схемою каталогів, логічною структурою та конфігурацією каталогів. Ліс являє собою кордон, який обмежує доступ до користувачів, комп'ютерів, груп та інших об'єктів.

Об'єкти, що зберігаються в домені, можуть бути згруповані в організаційні одиниці (Organization Units, далі OU). OU можуть надавати домену ієрархію, полегшувати його адміністрування і можуть нагадувати структуру організації в управлінському або географічному плані. OU можуть містити інші OU – у цьому випадку домени є контейнерами. Microsoft рекомендує використовувати OU, а не

домени для структуризації та спрощення впровадження політик і адміністрування. OU є рекомендованим рівнем для застосування групових політик, які є об'єктами Active Directory, формально названими об'єктами групової політики (GPO), хоча політики також можуть застосовуватися до доменів або сайтів. OU – це рівень, на якому зазвичай делегуються адміністративні повноваження, але делегування також може здійснюватися для окремих об'єктів або атрибутів.

Організаційні одиниці не мають окремого простору імен. Як наслідок, для сумісності із застарілими реалізаціями NetBios, облікові записи користувачів з однаковими іменами sAMAccountName не допускаються в одному домені, навіть якщо об'єкти облікових записів знаходяться в різних організаційних одиницях. Це пов'язано з тим, що sAMAccountName, атрибут об'єкта користувача, має бути унікальним у межах одного домену. Однак два користувачі у різних OU можуть мати однакове спільне ім'я (CN), ім'я, під яким вони зберігаються у самому каталозі, наприклад, "user1.kyiv.domain" і "user1.kharkiv.domain", де "kyiv" і "kharkiv" – це OU.

Загалом, причиною відсутності дозволу на дублювання імен через ієрархічне розміщення каталогів є те, що Microsoft в першу чергу покладається на принципи NetBIOS, який є методом управління мережевими об'єктами з плоским простором імен, який для програмного забезпечення Microsoft сягає корінням у Windows NT 3.1 та MS-DOS LAN Manager. Дозвіл на дублювання імен об'єктів у каталозі або повна відмова від використання імен NetBIOS унеможливить зворотну сумісність із застарілим програмним забезпеченням та обладнанням. Однак, заборона дублювання імен об'єктів у такий спосіб є порушенням специфікацій LDAP RFC, на яких, як передбачається, базується Active Directory.

Обхідними шляхами є додавання цифри в кінці імені користувача. Альтернативи включають створення окремої системи ідентифікації унікальних ідентифікаційних номерів користувачів для використання в якості імен облікових записів замість реальних імен людей, а також надання користувачам можливості призначати бажану послідовність слів в рамках прийнятної політики використання.

Оскільки дублікати імен користувачів не можуть існувати в межах одного домену, генерація імен облікових записів становить значну проблему для великих організацій, які не можуть бути легко розділені на окремі домени, наприклад, для учнів державних шкіл або студентів університетів, які повинні мати можливість користуватися будь-яким комп'ютером у мережі.

Сайти – це фізичні (а не логічні) групи, визначені однією або кількома IP-підмережами. AD також визначає з'єднання, розрізняючи низькошвидкісні (наприклад, WAN, VPN) і високошвидкісні (наприклад, LAN) з'єднання. Визначення сайтів не залежать від структури домену та OU і є спільними для всього лісу. Сайти відіграють вирішальну роль в управлінні мережевим трафіком, створеним реплікацією, і спрямовують клієнтів до найближчих контролерів доменів (DC).

Інформація Active Directory фізично зберігається на одному або декількох однорангових контролерах домену, замінюючи модель NT PDC/BDC. Кожен DC має копію Active Directory. Приєднані до Active Directory сервери, які не є контролерами домену, називаються серверами-членами. У розділі домену група об'єктів діє як копії контролерів домену, налаштовані як глобальні каталоги. Ці сервери глобальних каталогів пропонують повний список усіх об'єктів, розташованих у лісі.

Сервери Global Direcrory (GD) реплікують усі об'єкти з усіх доменів до себе, забезпечуючи повний перелік об'єктів у лісі. Однак, щоб мінімізувати трафік реплікації і зберегти базу даних глобального каталогу невеликою, реплікуються лише вибрані атрибути кожного об'єкта, які називаються частковим набором атрибутів (Partial Attribute Set, PAS). PAS можна змінювати, модифікуючи схему і позначаючи об'єкти для реплікації в GC. У старших версіях Windows для зв'язку використовувався протокол NetBIOS. Active Directory повністю інтегрована з DNS і вимагає TCP/IP-DNS. Для повноцінної роботи сервер DNS повинен підтримувати записи ресурсів SRV, також відомі як службові записи.

1.3 Microsoft Azure

Microsoft Azure (далі Microsoft Entra) – це загальнодоступна платформа хмарних обчислень від Microsoft. Вона надає широкий спектр хмарних сервісів, включаючи обчислення, аналітику, зберігання та мережу. Користувачі можуть вибирати з цих служб для розробки та масштабування нових додатків або запуску існуючих додатків у загальнодоступній хмарі.

Платформа Entra має на меті допомогти бізнесу впоратися з викликами та досягти своїх організаційних цілей. Вона пропонує інструменти, які підтримують усі галузі, включно з електронною комерцією та фінансами і сумісна з технологіями з відкритим вихідним кодом. Це дає користувачам гнучкість у використанні інструментів і технологій, яким вони надають перевагу. Крім того, Entra пропонує чотири різні форми хмарних обчислень: інфраструктура як послуга (IaaS), платформа як послуга (PaaS), програмне забезпечення як послуга (SaaS) і безсерверні функції.

Microsoft Entra складається з великої кількості різноманітних ресурсів і служб, варіанти її використання надзвичайно різноманітні. Запуск віртуальних машин або контейнерів у хмарі – одне з найпопулярніших застосувань Microsoft Entra. Ці обчислювальні ресурси можуть містити компоненти інфраструктури, такі як:

- сервери системи доменних імен (DNS);
- служби Windows Server, такі як Internet Information Services (IIS);
- мережеві служби;
- програми сторонніх розробників.

Корпорація Microsoft також підтримує використання сторонніх операційних систем, таких як Linux.

Microsoft Entra також широко використовується як платформа для розміщення баз даних у хмарі. Microsoft пропонує безсерверні реляційні бази даних, такі як Entra SQL, та нереляційні бази даних, такі як NoSQL.

Крім того, платформа часто використовується для резервного копіювання та

аварійного відновлення. Багато організацій використовують Entra для архівного зберігання даних, щоб задовольнити свої вимоги до довгострокового зберігання даних або аварійного відновлення (DR).

Корпорація Microsoft поділяє хмарні служби Entra на 20 різних категорій. Кожна категорія може включати численні конкретні екземпляри або типи служб.

Служби обчислення дають змогу користувачеві розгортати віртуальні машини, контейнери й пакетні завдання та керувати ними, а також підтримувати віддалений доступ до програм. Обчислювальні ресурси, створені в хмарі Entra ID, можна налаштувати на публічні або приватні IP-адреси, залежно від того, чи повинен ресурс бути доступним для зовнішнього світу.

Мобільні продукти допомагають розробникам створювати хмарні додатки для мобільних пристроїв, надаючи сервіси сповіщень, підтримку бекенд-задач, інструменти для побудови прикладних програмних інтерфейсів (API) та можливість пов'язувати геопросторовий контекст з даними.

Entra Web-сервіси підтримують розробку та розгортання веб-додатків. Вони також пропонують функції для пошуку, доставки контенту, управління API, сповіщення та звітування.

Хмарне сховище. Ця категорія послуг надає масштабоване хмарне сховище для структурованих і неструктурованих даних. Вони також підтримують проекти з великими даними, постійне зберігання та архівне зберігання.

Сервіси аналітики забезпечують розподілену аналітику та зберігання даних, а також функції для аналізу в режимі реального часу, аналізу великих дани, машинного навчання, бізнес-аналітики, потоків даних Інтернету речей (IoT) та зберігання даних.

Мережеві послуги. Ця група включає віртуальні мережі, виділені з'єднання і шлюзи, а також послуги з управління трафіком і діагностики, балансування навантаження, хостинг DNS і захист мережі від розподілених атак типу "відмова в обслуговуванні" (DDoS).

Мережа доставки медіа та контенту (CDN). Послуги CDN включають потокове мовлення на вимогу, захист цифрових прав, кодування, відтворення та

індексування медіа.

Інтеграція. Це сервіси для резервного копіювання серверів, відновлення сайтів та підключення приватних і публічних хмар.

Сервіси ідентифікації забезпечують доступ до служб Entra лише авторизованим користувачам і допомагають захистити ключі шифрування та іншу конфіденційну інформацію в хмарі. Послуги включають підтримку Microsoft Entra і багатофакторної автентифікації.

Інтернет речей. Ці сервіси допомагають користувачам збирати, відстежувати та аналізувати дані Інтернету речей з датчиків та інших пристроїв. Сервіси включають сповіщення, аналітику, моніторинг та підтримку кодування і виконання.

DevOps. Ця група надає інструменти для проектів і співпраці, такі як Microsoft Entra DevOps (раніше Visual Studio Team Services), які полегшують процеси розробки програмного забезпечення. Вона також пропонує функції для діагностики додатків, інтеграції інструментів DevOps і тестові лабораторії для тестування збірки та експериментів.

Розробка. Цей сервіс є аналогом GitHub, який допомагає розробникам додатків ділитися кодом, тестувати програми та відстежувати потенційні проблеми. Entra підтримує низку мов прикладного програмування, зокрема JavaScript, Python, .NET і Node.js. Інструменти цієї категорії також включають підтримку Entra DevOps, комплектів для розробки програмного забезпечення (SDK) і блокчейну.

Безпека. Ці продукти надають можливості для виявлення та реагування на загрози безпеці хмарних сервісів, а також для керування ключами шифрування та іншими важливими активами.

Штучний інтелект і машинне навчання надає широкий спектр сервісів, за допомогою яких розробник може впроваджувати можливості штучного інтелекту, машинного навчання та когнітивних обчислень у додатки та набори даних.

Контейнери. Ці служби допомагають підприємствам створювати, реєструвати, організовувати та керувати величезними обсягами контейнерів у хмарі Entra, використовуючи поширені контейнерні платформи, такі як Docker, та платформи

оркестрування, зокрема Kubernetes.

Бази даних. Ця категорія включає пропозиції бази даних як послуги (DBaaS) для SQL і NoSQL, а також інші екземпляри баз даних, такі як Entra Cosmos DB і Entra Database для PostgreSQL. Вона також включає підтримку сховища даних Entra SQL Data Warehouse, кешування та функції інтеграції й міграції гібридних баз даних.

Entra SQL – це флагманська служба баз даних платформи. Це реляційна база даних, яка забезпечує функціональність SQL без необхідності розгортання SQL-сервера.

Міграція – набір інструментів, який допомагає організації оцінити витрати на міграцію робочих навантажень і виконати фактичну міграцію робочих навантажень з локальних центрів обробки даних до хмари Entra.

Управління та адміністрування. Ці служби надають ряд інструментів для резервного копіювання, відновлення, забезпечення відповідності, автоматизації, планування та моніторингу, які допоможуть адміністратору хмари керувати розгортанням Entra.

Змішана реальність. Ці сервіси покликані допомогти розробникам створювати контент для середовища змішаної реальності Windows.

Служба Entra Blockchain дає змогу приєднатися до консорціуму блокчейнів або створити власний.

Microsoft Intune можна використовувати для реєстрації користувацьких пристроїв, що дає змогу поширювати політики безпеки та мобільні додатки на ці пристрої. Мобільні додатки можна розгортати як для груп користувачів, так і для колекції пристроїв. Intune також надає інструменти для відстеження того, які програми використовуються. Функція віддаленого стирання дозволяє безпечно видаляти дані організації з пристроїв, не видаляючи при цьому мобільні додатки користувачів.

Деякі організації використовують Entra для резервного копіювання даних і аварійного відновлення. Організації також можуть використовувати Entra як альтернативу власному сховищу в центрі обробки даних. Публічні хмари

виявилися надійним рішенням для виконання великих обсягів короткочасних завдань, таких як аналіз даних. Організації можуть використовувати майже необмежений об’єм хмарного сховища для зберігання величезних наборів даних, виконання аналітичних завдань, а потім видаляти дані, коли вони старіють або стають непридатними – і все це без придбання або розгортання апаратного забезпечення в локальному центрі обробки даних. Цей тип утилітарних обчислень був основною рушійною силою впровадження публічних хмар з моменту їх появи.

Замість того, щоб інвестувати в локальні сервери та сховища, все більше організацій вирішують запускати деякі або всі свої бізнес-додатки в Entra. Щоб забезпечити доступність, корпорація Microsoft має центри обробки даних Entra, розташовані по всьому світу. Станом на вересень 2023 року служби Microsoft Entra доступні в 55 регіонах у 140 країнах світу. На жаль, не всі служби доступні в усіх регіонах, тому користувачі Entra повинні переконатися, що робоче навантаження та місця зберігання даних відповідають усім чинним вимогам щодо відповідності або іншим законодавчим нормам.

Занепокоєння щодо безпеки даних та дотримання нормативних вимог роблять конфіденційність головною проблемою для абонентів хмарних сервісів. Щоб вирішити ці проблеми, Microsoft створила онлайн Центр довіри, який надає детальну інформацію про ініціативи компанії щодо безпеки, конфіденційності та дотримання нормативних вимог. Згідно з повідомленням Центру довіри, Microsoft використовуватиме дані клієнтів лише в тому випадку, якщо це необхідно для надання узгоджених послуг, і ніколи не розкриватиме дані клієнтів державним органам, якщо цього не вимагає закон.

Водночас Entra надає численні послуги, такі як управління ідентифікацією та доступом, брандмауер та інші служби безпеки, щоб допомогти користувачам Entra створити безпечну інфраструктуру та своєчасно відстежувати вторгнення. Служби безпеки мають вирішальне значення для впровадження публічної хмари, оскільки допомагають користувачам забезпечити конфіденційність даних і важливих робочих навантажень.

1.4 Microsoft Windows Azure Active Directory

Microsoft Windows Azure Active Directory (далі Microsoft Entra ID) – це хмарний сервіс, який надає адміністраторам можливість керувати ідентичностями кінцевих користувачів і правами доступу, але на відміну від Active Directory, керування проходить в хмарному орендарі (далі тенант) Entra. Основні послуги, які включає Entra ID: основний каталог, управління доступом і захист ідентичностей. Entra ID є частиною загальнодоступної платформи хмарних обчислень Microsoft Entra.

Сервіс дає адміністраторам свободу вибору: яка інформація залишатиметься в хмарі, хто може керувати або використовувати інформацію, які служби або додатки можуть отримати доступ до інформації, а також які кінцеві користувачі можуть мати доступ до неї. Entra ID може забезпечити розгортання системи єдиного входу (SSO), щоб кінцевим користувачам не потрібно було вводити паролі кілька разів для доступу до хмарних додатків.

Entra ID використовується IT-адміністраторами, розробниками додатків і орендарями хмарних сервісів Microsoft. Адміністратори використовують Entra ID для керування дозволами ролей і контролю доступу до певних програм і ресурсів для окремих користувачів. Розробники програм можуть використовувати Entra ID для додавання єдиного входу в програми, які працюють з уже наявними обліковими даними користувачів. Entra ID також надає розробникам програм прикладні програмні інтерфейси (API), які використовують наявні ресурси організації. Орендарі хмарних служб Microsoft, таких як Microsoft 365, Dynamics CRM Online або Azure, за замовчуванням є орендарями Entra ID.

Entra ID доступний у чотирьох різних рівнях послуг і цін. Базові функції з певними обмеженнями доступні безкоштовно. Орендарі програм Microsoft 365 отримують більше функціональних можливостей, ніж базові. Entra ID Преміум вимагає додаткової щомісячної передплати та має рівні: P1 і P2, де останній надає повний доступ до всіх функцій Entra ID.

Entra ID керує доступом через облікові записи користувачів, які містять ім'я

користувача та пароль. Користувачів можна об'єднувати в різні групи, яким можна надавати різні привілеї доступу до окремих програм. Облікові записи також можна створювати для хмарних додатків, які можуть бути від Microsoft або стороннього програмного забезпечення як послуги (SaaS), щоб надавати доступ користувачам.

Entra ID використовує SSO для підключення користувачів до програм SaaS. Це дає змогу кожному користувачеві отримати доступ до повного набору програм, на які він має дозвіл, без необхідності щоразу повторно входити в систему. Entra ID створює токени доступу, які зберігаються локально на пристроях співробітників, вони можуть бути створені з обмеженим терміном дії. Для важливих бізнес-ресурсів може вимагатися багатофакторна автентифікація (MFA).

Entra ID містить низку функцій для захисту даних організації. Функції безпеки Entra ID включають MFA, SSO для хмарних SaaS-додатків, адаптивні політики на основі контексту, управління ідентичностями, проксі-додаток для захисту віддаленого доступу та захисне машинне навчання (для захисту від викрадення облікових даних і підозрілих спроб входу).

Наприкінці 2022 року в Entra ID з'явилася функція під назвою "Безпека за замовчуванням", яка блокує застарілі протоколи автентифікації, вимагає MFA для адміністраторів і користувачів, а також вимагає MFA для цінних організаційних ресурсів. Метою стандартних параметрів безпеки є кращий захист цифрових активів, оскільки базові політики доступу в Entra ID розроблені для організацій зі старими клієнтами та додатковими функціями безпеки від сторонніх розробників. Стандартні параметри безпеки призначені для захисту від поширених типів атак, таких як фішинг, розпилення паролів і відтворення сеансів. Якщо їх не вимкнути, зловмисники можуть використовувати застарілі протоколи для автентифікації, обходячи багатофакторну автентифікацію.

1.5 Ліцензування Entra ID

Entra ID доступний у чотирьох різних рівнях ліцензування: безкоштовний (найнижчий), Microsoft 365, Преміум P1 і Преміум P2 (найвищий).

Безкоштовний рівень ліцензування має ліміт на 50 000 об'єктів в одному каталозі. Він містить усі функції керування ідентичностями та доступом для бізнесу. Він не включає управління ідентифікацією та доступом для Microsoft 365, преміум-функції, гібридні ідентичності, умовний доступ, захист ідентичностей, управління ідентичностями та розширене управління груповим доступом.

За даними корпорації Microsoft, до безкоштовного рівня входять такі функції:

- необмежений єдиний вхід;
- федеративна автентифікація (служби федерації Active Directory або сторонній постачальник ідентифікаційних даних);
- керування користувачами та групами;
- реєстрація пристрою;
- синхронізація Entra ID Connect, яка синхронізує локальні каталоги організації до Entra ID;
- Self-service password change (самостійна зміна пароля);
- багатофакторна автентифікація;
- базова звітність системи безпеки та використання;
- функції Entra ID для гостьових користувачів.

Другий найнижчий рівень служб Entra ID доступний для орендарів ліцензій Microsoft 365. Він доступний для орендарів рівнів E1, E3, E5, F1 і F3. Цей рівень не має обмежень на об'єкти каталогів. Він включає всі функції, пропоновані на безкоштовному рівні, а також керування ідентичностями й доступом до програм Microsoft 365, такі як:

- індивідуальне брендування панелей доступу та сторінок входу/виходу з системи;
- самостійне скидання пароля для користувачів хмарних сервісів;

– двостороння синхронізація об'єктів пристроїв між Azure AD і локальними каталогами.

Рівень Преміум P1 надає другий за величиною рівень доступу до Entra ID. Преміум P1 коштує $6 на місяць за користувача. Він включає повну функціональність Entra ID, за винятком захисту ідентичностей і керування ними. Специфічні функції рівня Premium P1 включають усе, що пропонується на рівні Microsoft 365, і навіть більше. А саме:

– самообслуговування скидання пароля з можливістю зворотного запису на місці;

– розширене керування груповим доступом;

– Entra ID Join з автоматичною реєстрацією для керування мобільними пристроями (MDM), налаштуванням локальної політики адміністрування, самостійним відновленням BitLocker;

– розширені звіти про безпеку та використання;

– гібридні ідентичності;

– умовний доступ.

Преміум-рівень P2 коштує $9 на місяць за користувача і включає повний набір функцій Entra ID. Він включає все, що пропонується в P1, а також функції захисту ідентичностей і керування ними.

1.6 Безпека Entra ID

Microsoft Entra ID працює як центральний вузол, ефективно керуючи та забезпечуючи безпеку співробітників, клієнтів і партнерів під час їхньої взаємодії з ресурсами та даними як в екосистемі Entra, так і за її межами. Нижче будуть описані основні переваги використання системи безпеки Entra ID.

Важлива особливість Microsoft Entra ID – це можливість єдиного входу (SSO). Увімкнення єдиного входу (SSO) за допомогою Microsoft Entra ID дозволяє користувачам увійти в систему лише один раз, щоб отримати доступ до своїх

програм Microsoft, а також інших хмарних і локальних ресурсів, використовуючи один і той самий набір облікових даних. Цей підхід спрощує користувацький досвід, зберігаючи при цьому надійні заходи безпеки.

Багатофакторна аутентифікація (MFA) забезпечує додатковий рівень безпеки, зобов'язуючи користувачів підтверджувати свою особу за допомогою декількох методів автентифікації, таких як текстові повідомлення, телефонні дзвінки або мобільні додатки. Під час співпраці із зовнішніми гостьовими користувачами в бізнес-середовищі (B2B) є доцільним захистити свої додатки за допомогою політик багатофакторної автентифікації. У Microsoft Entra ID цієї мети можна досягти за допомогою політик умовного доступу, які вимагають MFA для доступу. Політики MFA можна застосовувати на рівні тенанта, програми або окремого гостьового користувача, так само, як вони застосовуються для членів вашої організації.

Умовний доступ дозволяє адміністраторам встановлювати політики доступу до додатків на основі конкретних умов і атрибутів користувача. У сучасному ландшафті безпеки сфера застосування розширилася за межі мережі організації і охоплює ідентифікацію користувачів та пристроїв. Тепер організації покладаються на індикатори, що базуються на ідентичності, як на найважливіший компонент своїх стратегій контролю доступу. Microsoft Entra Conditional Access об'єднує ці сигнали, полегшуючи прийняття обґрунтованих рішень і забезпечення дотримання організаційних політик. Наприклад, ми можемо встановити політику, яка вимагає багатофакторної автентифікації (MFA), якщо користувач намагається отримати доступ до критично важливої веб-програми з незнайомого місця.

Захист ідентифікаційних даних користувачів за допомогою пильного моніторингу їхнього використання та шаблонів входу в систему є важливим для підтримки безпечного хмарного рішення. Функція захисту ідентифікаційних даних Microsoft Entra ID використовує можливості машинного навчання та сигналів безпеки для виявлення та зменшення ризиків, пов'язаних з ідентифікацією. Вона вміє автоматично блокувати або вимагати додаткової перевірки у відповідь на підозрілі дії під час входу, посилюючи загальний рівень безпеки.

Управління привілейованими ідентичностями Microsoft Entra дає змогу

обмежити безперервний адміністративний доступ до привілейованих ролей, визначити, хто має привілеї доступу та проводити ретельні перевірки привілейованого доступу. Ця функція допомагає підтримувати безпечне та контрольоване середовище для адміністративних операцій.

1.7 Аутентифікація Entra ID

Вибір правильного методу автентифікації є першою проблемою для організацій, які хочуть перенести свої програми в хмару. Не варто ставитися до цього рішення легковажно з наступних причин:

- хмарне середовище, у будь-якому випадку є менш захищеним, ніж локальне;
- метод автентифікації контролює доступ до всіх хмарних даних і ресурсів;
- це основа всіх інших розширених функцій безпеки та взаємодії з користувачем у Microsoft Entra ID.

Ідентичність – це нова площина контролю IT-безпеки, тому автентифікація – це захист доступу організації до нового хмарного простору. Вона посилює їхню безпеку та захищає хмарні додатки від зловмисників.

Організації, які не мають локального каталогу, створюють ідентичності лише в хмарі, що не потребує гібридних рішень. Хмарні ідентичності існують виключно в хмарі й не пов'язані з відповідними локальними ідентичностями.

Коли рішення для гібридних ідентичностей Microsoft Entra є новою площиною контролю для організації, автентифікація є основою доступу до хмарних сервісів. Вибір правильного методу автентифікації – це перше важливе рішення при налаштуванні гібридної ідентичності Microsoft Entra. Обраний метод автентифікації налаштовується за допомогою Azure AD Connect, який також надає користувачам доступ до хмари.

Щоб вибрати метод автентифікації, необхідно врахувати час, наявну інфраструктуру, складність і вартість реалізації вибору. Ці фактори є різними для кожної організації і можуть змінюватися з часом.

Хмарна автентифікація. При виборі цього методу автентифікації, Microsoft

Entra ID буде керувати процесом входу користувачів. У поєднанні з єдиним входом (SSO) користувачі можуть входити в хмарні програми без необхідності повторно вводити свої облікові дані. Для хмарної автентифікації є можливість обрати один із двох варіантів: синхронізація хешу пароля та наскрізна автентифікація.

Синхронізація хешу пароля є найпростішим способом увімкнути автентифікацію для локальних об'єктів каталогів у Microsoft Entra ID. Користувачі можуть використовувати ті самі імена користувачів та паролі, що й у локальній системі, без необхідності розгортати додаткову інфраструктуру. Деякі преміум-функції Microsoft Entra ID, як Захист ідентичностей і Служби доменів Microsoft Entra, вимагають синхронізації хешу пароля, незалежно від того, який метод автентифікації ви вибрали.

Наскрізна автентифікація Microsoft Entra забезпечує просту перевірку паролів для служб автентифікації за допомогою програмного агента, який працює на одному або декількох локальних серверах. Сервери перевіряють користувачів безпосередньо у вашому локальному каталозі Active Directory, а не в хмарі.

Цей метод автентифікації можуть використовувати компанії з вимогами безпеки щодо негайного застосування локальних станів облікових записів користувачів, політик паролів і часу входу в систему.

Федеративна автентифікація. При виборі цього методу автентифікації, Microsoft Entra ID передає процес автентифікації окремій довіреній системі автентифікації, наприклад, локальній службі Active Directory Federation Services (AD FS), для перевірки пароля користувача.

Система автентифікації може забезпечувати інші розширені вимоги до автентифікації, наприклад, багатофакторну автентифікацію третьої сторони.

Деталі що допоможуть у прийнятті рішень:

– Microsoft Entra ID може обробляти вхід для користувачів, не покладаючись на локальні компоненти для перевірки паролів.

– Microsoft Entra ID може передавати вхід користувача до довіреного постачальника автентифікації, такого як AD FS від Microsoft.

Якщо організації потрібно застосувати політики безпеки Active Directory на

рівні користувача, такі як закінчення терміну дії облікового запису, відключення облікового запису, закінчення терміну дії пароля, блокування облікового запису та години входу для кожного входу користувача, Microsoft Entra ID потребує деяких локальних компонентів.

Microsoft Entra ID Protection вимагає синхронізації хешування паролів незалежно від обраного вами методу входу, щоб надавати користувачам звіти про витік облікових даних. Організації можуть перейти на синхронізацію хешу паролів, якщо їхній основний метод входу вийшов з ладу, і він був налаштований до події збою.

Синхронізація хешів паролів вимагає найменших зусиль щодо розгортання, обслуговування та інфраструктури. Цей рівень зусиль зазвичай застосовується в організаціях, де користувачам потрібно лише входити в Microsoft 365, програми SaaS та інші ресурси на основі Microsoft Entra ID. Якщо цю функцію увімкнено, синхронізація хеш-паролів є частиною процесу Azure AD Connect і виконується кожні 30 хвилин.

За бажанням організації можна використовувати аналітику з ідентичностей за допомогою звітів Microsoft Entra ID Protection. Прикладом є звіт про витік облікових даних.

Служби Microsoft Entra Domain Services вимагають синхронізації хешу пароля, щоб надати користувачам їхні корпоративні облікові дані в керованому домені.

Організації, яким потрібна багатофакторна автентифікація з синхронізацією хешу пароля, повинні використовувати багатофакторну автентифікацію Microsoft Entra або користувацькі елементи керування Conditional Access. Ці організації не можуть використовувати сторонні або локальні методи багатофакторної автентифікації, які покладаються на федерацію.

Синхронізація хеш-пам'яті паролів із хмарною автентифікацією є високодоступною хмарною службою, яку можна масштабувати на всі центри обробки даних Microsoft. Щоб переконатися, що синхронізація хешів паролів не припиняється на тривалий час, можна розгорнути другий сервер Microsoft Entra

Connect у режимі очікування в резервній конфігурації.

Наразі синхронізація хешу пароля не призводить до негайного застосування змін у станах локальних облікових записів. У цій ситуації користувач має доступ до хмарних програм, доки стан його облікового запису не буде синхронізовано з Microsoft Entra ID. Організації можуть подолати це обмеження, запустивши новий цикл синхронізації після того, як адміністратори виконають масові оновлення станів локальних облікових записів користувачів. Прикладом може бути вимкнення облікових записів.

Параметри простроченого пароля та заблокованого облікового запису наразі не синхронізуються з Microsoft Entra ID технологією Azure AD Connect. Коли пароль користувача змінюється і встановлюється прапорець "Користувач повинен змінити пароль при наступному вході", хеш пароля не буде синхронізовано з Microsoft Entra ID технологією Azure AD Connect, доки користувач не змінить свій пароль.

Наскрізна автентифікація. Для наскрізної автентифікації знадобиться один або декілька (рекомендовано три) легких агенти, встановлених на існуючих серверах. Ці агенти повинні мати доступ до локальних доменних служб Active Directory, зокрема до локальних контролерів доменів AD. Їм потрібен вихідний доступ до Інтернету та доступ до ваших контролерів доменів. З цієї причини розгортання агентів у периметральній мережі не підтримується.

Наскрізна автентифікація вимагає необмеженого мережевого доступу до контролерів домену. Весь мережевий трафік шифрується і обмежується запитами на автентифікацію.

Наскрізна автентифікація застосовує політику локального облікового запису під час входу. Наприклад, доступ заборонено, якщо стан локального облікового запису користувача вимкнено, заблоковано, закінчився термін дії пароля або спроба входу припадає на неробочий час, коли користувачеві дозволено входити в систему.

Організації, яким потрібна багатофакторна автентифікація з наскрізною автентифікацією, повинні використовувати багатофакторну автентифікацію

Microsoft Entra або користувацькі елементи керування Conditional Access. Ці організації не можуть використовувати сторонні або локальні методи багатофакторної автентифікації, які покладаються на федерацію. Розширені функції вимагають розгортання синхронізації хешів паролів, незалежно від того, чи ви вибрали наскрізну автентифікацію, чи ні. Прикладом може слугувати звіт про витік облікових даних з Identity Protection.

Компанія Microsoft рекомендує розгорнути два додаткові агенти наскрізної автентифікації. Ці додаткові агенти є доповненням до першого агента на сервері Microsoft Entra Connect. Додаткове розгортання забезпечує високу доступність запитів на автентифікацію.

Синхронізація хешів паролів у поєднанні з наскрізною автентифікацією має ще одну перевагу – вона діє як резервний метод автентифікації, коли основний метод автентифікації більше не доступний. Організація може використовувати синхронізацію хешу пароля як резервний метод автентифікації для наскрізної автентифікації, коли агенти не можуть підтвердити облікові дані користувача через значний локальний збій. Перехід на синхронізацію хешів паролів не відбувається автоматично, і адміністратор повинен використати Azure AD Connect для ручного перемикання методу входу.

Федеративна система автентифікації покладається на зовнішню довірену систему для автентифікації користувачів. Деякі компанії хочуть повторно використовувати свої інвестиції в існуючу федеративну систему з гібридним рішенням для ідентичності Microsoft Entra. Обслуговування та управління об'єднаною системою виходить за межі контролю Microsoft Entra ID. Організація, яка використовує об'єднану систему, повинна переконатися, що вона безпечно розгорнута і може впоратися з навантаженням автентифікації.

Взаємодія користувача з федеративною автентифікацією залежить від реалізації функцій, топології та конфігурації ферми федерації. Деяким організаціям потрібна така гнучкість, щоб адаптувати і налаштувати доступ до ферми федерації відповідно до своїх вимог безпеки. Наприклад, можна налаштувати внутрішньо підключених користувачів і пристрої так, щоб вони

входили в систему автоматично, без запиту облікових даних. Ця конфігурація працює, оскільки вони вже ввійшли на своїх пристроях. За необхідності, деякі розширені функції безпеки ускладнюють процес входу користувачів.

Об'єднані системи зазвичай вимагають збалансованого за навантаженням масиву серверів, відомого як ферма. Ця ферма конфігурується у топології внутрішньої мережі та периметральної мережі, щоб забезпечити високу доступність для запитів на автентифікацію. Також такі системи потребують значних інвестицій в локальну інфраструктуру. Більшість організацій обирають цей варіант, якщо у них вже є інвестиції в локальну федерацію або якщо використання постачальника послуг з єдиною ідентифікацією є нагальною потребою бізнесу. Федерація складніша в експлуатації та усуненні несправностей у порівнянні з хмарними рішеннями для автентифікації.

РОЗДІЛ 2 ТЕХНОЛОГІЯ СИНХРОНІЗАЦІЇ КАТАЛОГІВ AZURE AD CONNECT

2.1 Azure AD Connect

Azure AD Connect – це технологія Microsoft, розроблена для допомоги організаціям з гібридними IT-середовищами. Вона входить до складу безкоштовної підписки на Entra. Azure AD Connect пропонує велику кількість функцій, включаючи інтеграцію з федерацією та моніторинг стану. Однак найвідомішою функцією Azure AD Connect є синхронізація каталогів.

Простіше кажучи, організації використовують Azure AD Connect для автоматичної синхронізації ідентифікаційних даних між локальним середовищем Active Directory та Entra ID. Таким чином, користувачі можуть використовувати одні й ті ж облікові дані для доступу до локальних програм і хмарних служб, таких як Microsoft 365.

Для інтеграції цю технологію реалізують на приєднаному до домену сервері в локальному центрі обробки даних. За замовчуванням інсталяція відбувається в режимі експрес-налаштуваннь, який використовується для найпоширенішого сценарію: синхронізації даних між одним локальним лісом, який має один або кілька доменів, і одним клієнтом Entra ID. Якщо компанія має кілька лісів або кілька клієнтів Entra ID, варто розглянути інші варіанти топологій.

За замовчуванням синхронізація виконується в один бік: з локального AD до Entra ID. Однак є можливість налаштувати функцію зворотного запису, щоб синхронізувати зміни з Entra ID назад до локальної AD. Таким чином, якщо користувач змінить свій пароль за допомогою функції самообслуговування керування паролями в Entra ID, пароль буде оновлено в локальному AD.

Окрім паролів, Azure AD Connect може синхронізувати облікові записи користувачів, групи та хеші облікових даних у локальному AD. Більшість атрибутів облікових записів користувачів, як основне ім'я користувача (UPN) та ідентифікатор безпеки (SID), синхронізуються за замовчуванням.

Однак наступні об'єкти та атрибути НЕ синхронізуються:

- будь-які об'єкти та атрибути, які виключено при налаштуванні синхронізації;
- атрибути SidHistory для користувачів і груп;
- об'єкти групової політики (GPO);
- вміст папки Sysvol;
- об'єкти комп'ютерів, приєднаних до локального середовища AD;
- структури організаційних одиниць (OU).

Також важливо розуміти й дотримуватися найкращих практик використання будь-якої програми, що стосується Active Directory та Entra ID. Ключові з них, будуть наведені нижче.

Необхідно захистити сервер, на якому працює Azure AD Connect, так, ніби він є контролером домену. Зокрема, обмежити права локального адміністрування на сервері та встановити контроль над фізичним доступом до сервера. Крім того, варто переконатися, що службовий обліковий запис для інструменту має лише необхідні права і суворо відповідає умовам щодо складності та терміну дії паролів.

За замовчуванням, єдині особи, які можуть використовувати і керувати механізмом синхронізації – це користувач, який його встановив, і локальні адміністратори на комп'ютері, де він запущений. Щоб надати іншим користувачам доступ до інструменту, додайте їх до групи ADSyncAdmins на локальному сервері.

За замовчуванням усі об'єкти користувачів і груп (за винятком описаних вище) буде синхронізовано з локального AD в Entra ID. Але не всі локальні групи слугуватимуть корисним цілям у хмарі. Тому варто переглянути всі локальні групи, пам’ятаючи про те, що існує два основних типи груп AD: групи безпеки, які виконують функції довіреної особи для захисту таких об'єктів, як файловий ресурс або список SharePoint, і групи розповсюдження, які спрощують адресацію повідомлень (в першу чергу електронної пошти). Після перегляду груп необхідно скористатися функцією фільтрації механізму синхронізації, щоб виключити групи, які не стосуються хмарного середовища.

Перш ніж вносити зміни до фільтрації, потрібно тимчасово вимкнути завдання синхронізації за розкладом, щоб ваші зміни не були застосовані до того,

як буде можливість переконатися, що вони правильні.

Зокрема, не варто синхронізувати локальні групи адміністраторів з Entra ID. Метою локальних груп адміністраторів, таких як адміністратори доменів, є керування локальним каталогом. Синхронізація цих груп з Entra ID не дає жодних переваг. Однак це створює зайвий ризик, оскільки ці групи будуть доступні для сторонніх очей, наприклад користувачів Entra ID, які можуть побачити склад (непотрібної) групи адміністраторів і точно знати, які локальні облікові записи можна атакувати фішингом або іншими атаками. Тому дуже важливо використовувати функцію фільтрації, щоб виключити всі групи адміністраторів із синхронізації.

Для керування Entra ID необхідно створити відповідних адміністраторів тільки для тенанту, використовуючи заздалегідь визначені ролі, такі як глобальний адміністратор, адміністратор додатків, адміністратор відповідності та адміністратор SharePoint. Зазначимо, що глобальний адміністратор може змінювати будь-який адміністративний параметр в організації Entra ID, тому корпорація Microsoft рекомендує призначати цю роль не більше ніж п'ятьом особам в організації. Крім того, варто застосувати функції, які пропонує корпорація Microsoft для додаткового захисту облікових записів, яким призначено роль адміністратора, зокрема багатофакторною автентифікацією (MFA) і привілейованим керуванням ідентичностями (PIM).

Entra ID також передбачає створення груп лише в хмарі, включно з групами безпеки та групами розповсюдження, а також групами Microsoft 365. Група Microsoft 365 може захищати об'єкти, як і група безпеки; вона може функціонувати як список розсилки, як і група розсилки; вона також може виконувати роль сховища даних, підтримуваного SharePoint і спільними поштовими скриньками. Групи Microsoft 365 також використовуються в кожній команді в Microsoft Teams.

За замовчуванням синхронізація виконується кожні 30 хвилин. Адміністратор має можливість змінити цикл синхронізації, але корпорація Microsoft рекомендує виконувати синхронізацію щонайменше раз на 7 днів, як зазначено нижче:

– дельта-синхронізація має відбуватися не менше ніж за 7 днів після останньої дельта-синхронізації;

– дельта-синхронізація (після повної синхронізації) повинна відбуватися не менше ніж за 7 днів з моменту завершення останньої повної синхронізації.

Недотримання цих рекомендацій може призвести до проблем, які можна вирішити лише за допомогою повної синхронізації, що в свою чергу може зайняти багато часу.

Багато організацій докладають чимало зусиль для керування й захисту локальної Active Directory. Але не варто думати, що синхронізація локальго AD з Entra ID автоматично означає, що хмарне IT-середовище належним чином керується та резервується. Однією з ключових причин є те, що об'єкти Entra ID, які синхронізуються з локальною AD, часто мають додаткові атрибути, які існують лише в хмарі, як ліцензії користувача Microsoft 365, ролі та політики умовного доступу. Якщо об'єкт користувача з одним або кількома хмарними атрибутами видалено, можна відновити локальний об'єкт користувача AD і за допомогою Azure AD Connect синхронізувати його резервну копію з Entra ID, але хмарні атрибути зникнуть, і користувач не зможе отримати доступ до програм Microsoft 365 або виконувати свої обов'язки, пов'язані з ролями. Тому для хмарного середовища важливо мати рішення для резервного копіювання та відновлення на рівні підприємства.

2.2 Передумови інтеграції

Перш ніж встановлювати Azure AD Connect, необхідно запевнитися в наступних речах.

Microsoft Entra ID:

– для інтеграції потрібен тенант Microsoft Entra. Його можливо отримати разом з ознайомлювальною версією Entra. Для керування Microsoft Entra ID можна використовувати один із наведених нижче порталів:

– центр адміністрування Microsoft Entra;

– портал Microsoft 365.

– необіхдно додати та перевірити домен, який організація планує використовувати в Microsoft Entra ID.

– за замовчуванням орендар Microsoft Entra має 50 000 об'єктів. Якщо верифікувати домен, то ліміт збільшується до 300 000 об'єктів. Якщо необхідно ще більше об'єктів у Microsoft Entra ID, необхідно відкрити заявку на підтримку більшої кількості об’єктів. Якщо організації необхідно більше 500 000 об'єктів, в такому випадку потрібна ліцензія Microsoft 365, Microsoft Entra ID P1 або P2 або Enterprise Mobility + Security.

Підготовка локальних даних:

– необхідно підготувати IdFix (інструмент діагностики каталогу AD) щоб виявити такі помилки, як дублікати та проблеми з форматуванням у локальному каталозі перед синхронізацією з Microsoft Entra ID і Microsoft 365;

– необхідно переглянути додаткові функції синхронізації, які можна ввімкнути в Microsoft Entra ID, і визначте, які з них варто ввімкнути.

Локальна Active Directory:

– версія схеми Active Directory і функціональний рівень лісу повинні бути Windows Server 2003 або новішої версії. Контролери домену можуть працювати з будь-якою версією, якщо дотримано вимоги до версії схеми та рівня лісу;

– контролер домену, що використовується Microsoft Entra ID, має бути доступним для запису. Використання контролера домену, доступного лише для читання (RODC), не підтримується, і Microsoft Azure AD Connect не виконує перенаправлення на запис;

– використання локальних лісів або доменів за допомогою "крапкових" (ім'я містить крапку ".") імен NetBIOS не підтримується;

– рекомендується увімкнути кошик Active Directory.

– політика виконання PowerShell Microsoft Entra Connect запускає підписані сценарії PowerShell як частину інсталяції. Необхідно переконатися, що політика виконання PowerShell дозволяє запуск сценаріїв.

Сервер Microsoft Azure AD Connect:

– важливо, щоб адміністративний доступ до цього сервера був належним чином захищений;

– сервер Microsoft Azure AD Connect повинен розглядатися як компонент рівня 0.

Передумови для встановлення:

– Microsoft Azure AD Connect має бути встановлений на приєднаному до домену Windows Server 2016 або новішої версії. Рекомендується використовувати приєднаний до домену Windows Server 2022;

– мінімальна необхідна версія .NET Framework 4.6.2, також підтримуються новіші версії .NET версії 4.8 і вище, що забезпечує найкращу відповідність вимогам доступності;

– Microsoft Azure AD Connect не можна встановити на Small Business Server або Windows Server Essentials до 2019 року (підтримується Windows Server Essentials 2019). На сервері має бути встановлена версія Windows Server Standard або Windows Server Datacenter;

– на сервері Microsoft Azure AD Connect повинен бути встановлений повний графічний інтерфейс. Встановлення Microsoft Azure AD Connect на Windows Server Core не підтримується;

– при використанні майстра Azure AD Connect для керування конфігурацією служб федерації Active Directory (AD FS), на сервері Microsoft Azure AD Connect не повинна бути ввімкнена групова політика транскрипції PowerShell. Увімкнути транскрипцію PowerShell можливо лише при використанні майстра Microsoft Azure AD Connect для керування конфігурацією синхронізації;

– якщо розгортається AD FS:

  – сервери, на яких встановлено AD FS або проксі для веб-додатків, мають бути Windows Server 2012 R2 або новішої версії;

  – необхідно налаштувати сертифікати TLS/SSL;

  – необхідно налаштувати роздільну здатність імен;

– не підтримується розрив і аналіз трафіку між Microsoft Azure AD Connect і Microsoft Entra ID. Це може призвести до порушення роботи служби.

– якщо для адміністраторів гібридних ідентичностей увімкнено MFA, URL-адреса https://secure.aadcdn.microsoftonline-p.com має бути у списку довірених сайтів. Необхідно додати її до списку довірених сайтів за допомогою Internet Explorer, або погодитися на додавання цієї адреси, при першому запиті MFA.

Рекомендується посилити захист сервера Microsoft Azure AD Connect, щоб зменшити кількість атак на цей важливий компонент вашого IT-середовища:

– необхідно обмежити адміністративний доступ до сервера Microsoft Azure AD Connect адміністраторам домену або іншими групам;

– необхідно створити окремий обліковий запис для всього персоналу з привілейованим доступом. Адміністратори не повинні переглядати веб-сторінки, перевіряти електронну пошту та виконувати повсякденні завдання з високопривілейованими акаунтами;

– необхідно заборонити використання автентифікації NTLM з сервером Azure AD Connect;

– варто переконайтеся, що кожна машина має унікальний пароль локального адміністратора. Рішення для паролів локальних адміністраторів (Windows LAPS) дозволяє налаштувати унікальні випадкові паролі на кожній робочій станції і зберігати їх в Active Directory, захищеної списком ACL. Лише відповідні авторизовані користувачі можуть читати або вимагати скидання цих паролів облікових записів локальних адміністраторів;

– варто впровадити спеціальні робочі станції для всього персоналу з привілейованим доступом до інформаційних систем вашої організації;

– необхідно увімкнути багатофакторну автентифікацію (MFA) для всіх користувачів, які мають привілейований доступ в Microsoft Entra ID або в AD. Однією з проблем безпеки при використанні Micrisoft Azure AD Connect є те, що зловмисник може отримати контроль над сервером Microsoft Azure AD Connect і маніпулювати користувачами в Microsoft Entra ID. Зловмисник не зможе обійти

другий фактор MFA, навіть якщо йому вдасться скинути пароль користувача через Azure AD Connect;

– варто вимкнути м'яке узгодження для тенанта. Soft Matching – це функція, яка допомагає перенести джерело повноважень для наявних хмарних об'єктів до Microsoft Azure AD Connect, але вона пов'язана з певними ризиками безпеки;

– варто вимкнути жорстке перехоплення. Жорстке перехоплення дає змогу Microsoft Azure AD Connect перебрати контроль над об'єктом, керованим у хмарі, і змінити джерело повноважень для об'єкта в Active Directory. Після того, як джерело повноважень об'єкта переходить до Microsoft Azure AD Connect, зміни, внесені в об'єкт Active Directory, який пов'язаний з об'єктом Microsoft Azure AD Connect, перезапишуть оригінальні дані Microsoft Entra, включно з хешем пароля. Зловмисник може скористатися цією можливістю, щоб перехопити контроль над хмарними об'єктами.

Підготовка SQL сервера, який використовує Microsoft Azure AD Connect:

– Microsoft Azure AD Connect потребує бази даних SQL Server для зберігання ідентифікаційних даних. За замовчуванням встановлюється SQL Server 2019 Express LocalDB (полегшена версія SQL Server Express). SQL Server Express має обмеження на розмір 10 ГБ, що дозволяє керувати приблизно 100 000 об'єктів. Якщо потрібно керувати більшим обсягом об'єктів каталогів, необхідно вказати майстру інсталяції на інший SQL Server. Тип інсталяції SQL Server може вплинути на продуктивність Microsoft Entra Connect;

– якщо використовується інша інсталяція SQL Server, мають бути дотримані наступні вимоги:

– Microsoft Entra Connect підтримує всі основні підтримувані версії SQL Server до SQL Server 2022, що працюють під управлінням Windows. Azure SQL Database не підтримується як база даних. Це стосується як бази даних Azure SQL, так і керованого екземпляра Azure SQL;

– необхідно використовувати нечутливе до регістру зіставлення SQL. Ці зіставлення позначаються символом _CI_ у назві. Використання чутливого до регістру зіставлення, позначеного символом _CS_ у назві, не підтримується;

– для одного екземпляра SQL можна використовувати лише один механізм синхронізації. Спільний доступ до екземпляра SQL за допомогою FIM/MIM Sync, DirSync або Azure AD Sync не підтримується.

Облікові записи:

– необхідно мати обліковий запис глобального адміністратора Microsoft Entra або обліковий запис адміністратора гібридної ідентичності для орендаря Microsoft Entra, з яким ви хочете інтегруватися. Цей обліковий запис має бути обліковим записом школи або організації і не може бути обліковим записом Microsoft;

– при використанні експрес-налаштування або оновлення з DirSync, необхідно мати обліковий запис адміністратора підприємства для локальної Active Directory.

Мережеві підключення:

– серверу Microsoft Azure AD Connect потрібен DNS-дозвіл як для інтрамережі, так і для Інтернету. DNS-сервер повинен вміти розпізнавати імена як для локальної Active Directory, так і для кінцевих точок Microsoft Entra;

– Microsoft Azure AD Connect вимагає мережевого підключення до всіх налаштованих доменів;

– Microsoft Azure AD Connect вимагає мережевого підключення до кореневого домену всього налаштованого лісу;

– якщо проксі-сервер або брандмауер обмежують доступ до URL-адрес, необхідно відкрити URL-адреси, задокументовані в діапазонах URL-адрес і IP-адрес Office 365;

– Microsoft Azure AD Connect за замовчуванням використовує TLS 1.2 для шифрування зв'язку між механізмом синхронізації та Microsoft Entra ID. Якщо TLS 1.2 недоступний у базовій операційній системі, Microsoft Entra Connect поступово повертається до старіших протоколів (TLS 1.1 і TLS 1.0);

– при використанні вихідного проксі для підключення до Інтернету, необхідно додати параметр, що показаний на рисунку 2.1, у файл C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config, щоб майстер встановлення та Microsoft Azure AD Connect могли підключитися до

Інтернету та Microsoft Entra ID. Цей текст потрібно ввести в кінці файлу. В цьому коді <PROXYADDRESS> представляє фактичну IP-адресу проксі-сервера або ім'я хоста;

```
<system.net>
    <defaultProxy>
        <proxy
        usesystemdefault="true"
        proxyaddress="http://<PROXYADDRESS>:<PROXYPORT>"
        bypassonlocal="true"
        />
    </defaultProxy>
</system.net>
```

Рисунок 2.1 – параметр, що дозволить підключення до Інтернету, при використанні вихідного проксі-сервера

– якщо проксі-сервер вимагає автентифікації, то необхідно внести зміни до файлу machine.config. Після внесення цих змін до файлу, майстер встановлення та механізм синхронізації відповідатимуть на запити автентифікації від проксі-сервера. Розділ machine.config має виглядати як показано на рисунку 2.2;

```
<system.net>
    <defaultProxy enabled="true" useDefaultCredentials="true">
        <proxy
        usesystemdefault="true"
        proxyaddress="http://<PROXYADDRESS>:<PROXYPORT>"
        bypassonlocal="true"
        />
    </defaultProxy>
</system.net>
```

Рисунок 2.2 – кінцевий результат файлу machine.config

– якщо конфігурація проксі виконується в існуючому налаштуванні, службу Microsoft Azure AD Connect Sync потрібно перезапустити один раз, щоб Microsoft Azure AD Connect зміг прочитати конфігурацію проксі і оновити поведінку;

– коли Microsoft Azure AD Connect надсилає веб-запит до Microsoft Entra ID в рамках синхронізації каталогів, відповідь Microsoft Entra ID може зайняти до 5 хвилин. Зазвичай проксі-сервери мають налаштування тайм-ауту очікування з'єднання. Необхідно переконатися, що в налаштуваннях встановлено принаймні 6

хвилин тайм-ауту або більше.

Компонентні передумови PowerShell та .NET Framework:

– на сервері Azure AD Connect має бути встановлений Microsoft PowerShell 5.0 або пізніша версія;

– на сервері Azure AD Connect має бути встановлений .NET Framework 4.5.1 або пізніша версія.

Передумови DCOM на сервері синхронізації:

– під час встановлення служби синхронізації Microsoft Azure AD Connect перевіряє наявність наступного ключа реєстру HKEY_LOCAL_MACHINE\Software\Microsoft\Ole, тому в цьому розділі реєстру необхідно перевірити, чи наявні та не пошкоджені наступні значення:

– MachineAccessRestriction;

– MachineLaunchRestriction;

– DefaultLaunchPermission;

Передумови для встановлення та налаштування синхронізації на рівні федерації:

– якщо цільовий сервер приєднано до домену, необхідно переконатися, що Windows Remote Managed увімкнено, скориставшись командою Enable-PSRemoting -force у командному вікні PowerShell з прівелійованими правами;

– якщо цільовий сервер є WAP-машиною, що не приєднана до домену, є кілька додаткових вимог, необхідно переконатися, що служба Windows Remote Management/WS- Management (WinRM) запущена за допомогою оснастки Services;

– на комп'ютері, на якому запущено майстер (якщо цільовий комп'ютер не приєднано до домену або він є ненадійним доменом), у командному вікні PowerShell з прівелійованими правами необхідно скористатися командою Set-Item.WSMan:\localhost\Client\TrustedHosts -Value "<DMZServerFQDN>" -Force -Concatenate;

– у диспетчері серверів необхідно додати WAP-вузол DMZ до пулу машин.

Вимоги до сертифікатів TLS/SSL для встановлення та налаштування

синхронізації на рівні федерації:

– рекомендується використовувати один і той самий сертифікат TLS/SSL на всіх вузлах ферми AD FS і на всіх проксі-серверах веб-додатків;

– сертифікат повинен бути X509;

– використання самопідписаного сертифікату на серверах федерації можливе тільки в тестовому лабораторному середовищі. Для виробничого середовища рекомендується отримання сертифікату від загальнодоступного центру сертифікації;

– при використанні сертифікату, якому не довіряють публічно, варто переконатися, що сертифікат, встановлений на кожному проксі-сервері веб-додатків, є довіреним як на локальному сервері, так і на всіх серверах федерації;

– ідентифікатор сертифіката повинен відповідати імені служби федерації (наприклад, sts.contoso.com);

– ідентифікатор сертифіката має бути розширенням альтернативного імені суб'єкта (SAN) типу dNSName. Якщо записи SAN відсутні, то ім'я суб'єкта має вказуватися як загальне ім'я;

– в сертифікаті може бути присутнім кілька записів SAN за умови, що один з них збігається з назвою служби федерації;

– при використанніWorkplace Join, потрібен додатковий SAN зі значенням enterpriseregistration. з суфіксом основного імені користувача (UPN) організації, наприклад, enterpriseregistration.вщьфшт.com;

– сертифікати на основі ключів CryptoAPI наступного покоління (CNG) і постачальників послуг зберігання ключів (KSP) не підтримуються. Як наслідок, необхідно використовувати сертифікат на основі постачальника криптографічних послуг (CSP), а не KSP;

– можлива підтримка сертифікатів wildcard.

Розширення імен для серверів федерації:

– необхідно налаштувати DNS-записи для імені AD FS (наприклад, sts.domain.com) як для інтрамережі (внутрішній DNS-сервер), так і для

екстрамережі (публічний DNS через реєстратора доменів). Для записів DNS інтрамережі необхідно переконайтися, що використовуються записи типу A, а не CNAME. Використання записів типу A необхідне для коректної роботи автентифікації Windows на комп'ютері, приєднаному до домену;

– при розгортанні кількох серверів AD FS або проксі-серверів веб-додатків, необхідно переконатися, що компенсатор навантаження налаштований і що записи DNS для імені AD FS (наприклад, sts.domain.com) вказують на компенсатор навантаження;

– щоб інтегрована автентифікація Windows працювала для браузерів, які використовують Internet Explorer в інтрамережі, необхідно переконатися, що ім'я AD FS (наприклад, sts.domain.com) додано до зони інтрамережі в Internet Explorer. Цю вимогу можна контролювати за допомогою групової політики і розгорнути на всіх комп'ютерах, приєднаних до домену.

Допоміжні компоненти Microsoft Azure AD Connect, що встановлюються при розгортанні технології:

– Microsoft Entra Connect Health;
– утиліти командного рядка Microsoft SQL Server 2022;
– Microsoft SQL Server 2022 Express LocalDB;
– нативний клієнт Microsoft SQL Server 2022;
– Microsoft Visual C++ 14 Перерозподіл дистрибутива Microsoft Visual C++ 14.

Вимоги до апаратного забезпечення Microsoft Azure AD Connect наведені в таблиці 2.1. Дані вимоги необхідні для забезпечення стабільного функціонування, відповідно до кількості об’єктів в локальному каталозі Active Directory.

Таблиця 2.1 – Вимоги до апаратного забезпечення Microsoft Azure AD Connect

Кількість об'єктів в Active Directory	Частота процесора	Об’єм оперативної пам’яті	Розмір жорсткого диска
Менше 10 000	1,6 ГГц	6 ГБ	70 ГБ
10,000-50,000	1,6 ГГц	6 ГБ	70 ГБ

Кількість об'єктів в Active Directory	Частота процесора	Об’єм оперативної пам’яті	Розмір жорсткого диска
100,000-300,000	1,6 ГГц	32 ГБ	300 ГБ
300,000-600,000	1,6 ГГц	32 ГБ	450 ГБ
Понад 600,000	1,6 ГГц	32 ГБ	500 ГБ

Мінімальні вимоги до комп'ютерів, на яких працюють AD FS або проксі-сервери веб-додатків, наступні:

- процесор: двоядерний з частотою 1,6 ГГц або вище;
- об’єм оперативної пам'яті: 2 ГБ або більше;
- віртуальна машина Azure: Конфігурація A2 або вище.

РОЗДІЛ 3 ІНТЕГРАЦІЯ AZURE AD CONNECT ТА НАЛАШТУВАННЯ НЕОБХІДНИХ ФУНЦІЙ

3.1 Розгортання Entra ID Connect з функцією синхронізації хешу паролів

У ролі тестового середовища синхронізації буде виступати віртуальна машина з наступними ресурсами:

- 4 віртуальних процесорних ядра;
- 8 ГБ оперативної пам’яті;
- 40 ГБ дискового простору;
- Підключення до локальної мережі з доступом до мережі Інтернет.

Попередньо на віртуальну машину було встановлено операційну систему Windows Server 2022 Datacenter з можливостями графічного інтерфейса та наступними ролями:

- Active Directory Domain Services;
- File and Storage Servisec (встановлюється за замовчуванням після інсталяції операційної системи);
- Remote Desktop Services.

Після інсталяції ролі Active Directory Domain Services був створений домен hdoua.local, в Active Directory Users and Computers створений OU hdoua_users з користувачами Sync User 1, Sync user 2 та Sync User 3 (рисунок 3.1), які будуть в подальшому синхронізуватися з тенантом Entra ID.

Також був зареєстрований тенант Entra ID hdoua.onmicrosoft.com (рисунок 3.2). При створенні нового тенанта для користувача без орендованого доменного імені, компанія Microsoft до назви домену додає .onmicrosoft.com. Разом з тенантом було орендовано ліцензію Microsoft Entra ID Premium P2 для доступу до всього функціоналу Entra ID.

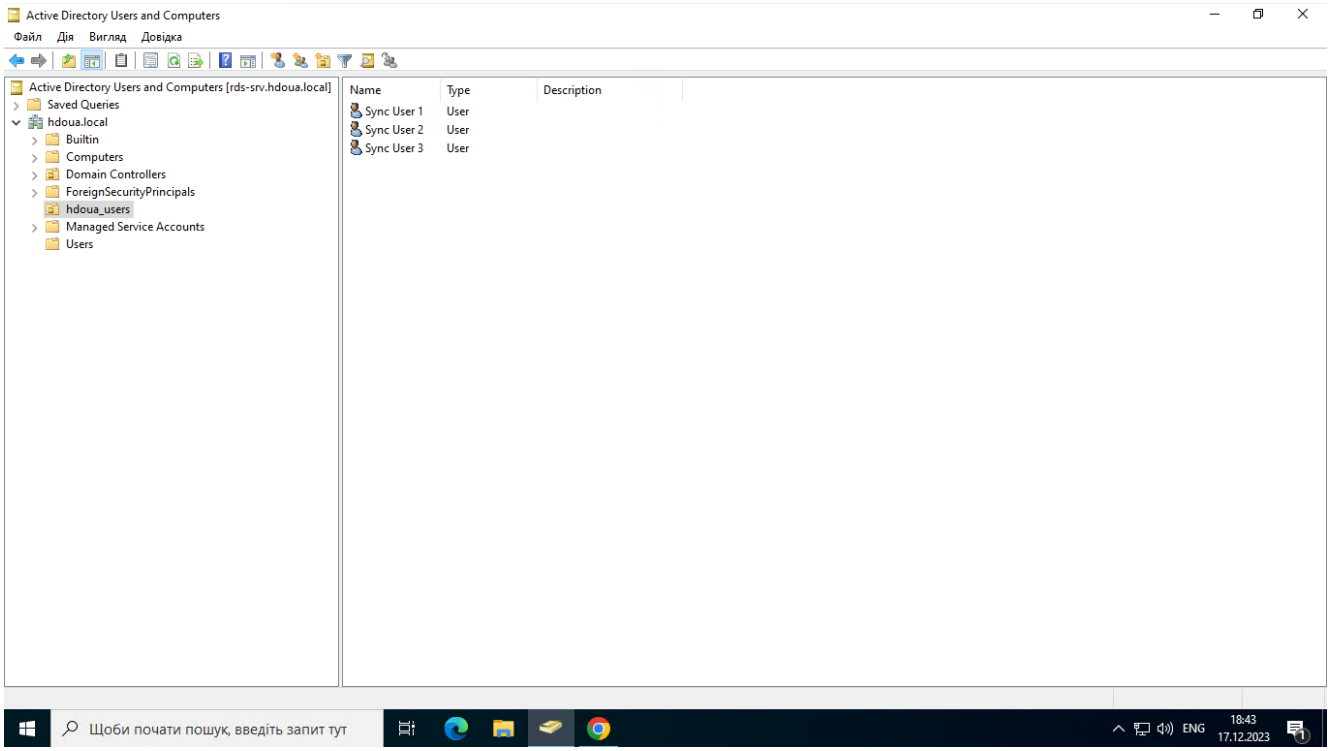


Рисунок 3.1 – AD з користувачами Sync User

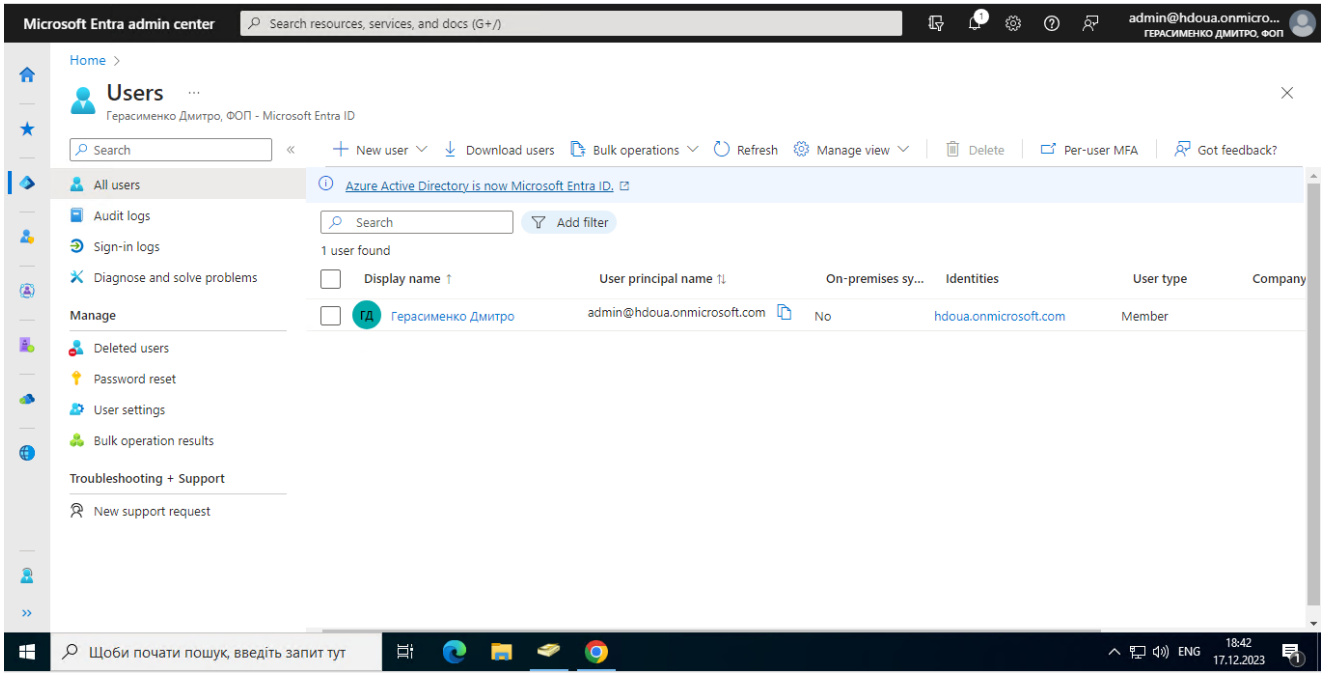


Рисунок 3.2 – тенант hdoua.onmicrosoft.com

При використанні однолісової топології і синхронізації хешу пароля для автентифікації, експрес-налаштування – це варіант з мінімальними затратами часу для встановлення Microsoft Azure AD Connect. Експрес-налаштування – це опція за

замовчуванням для встановлення Microsoft Azure AD Connect, яка використовується для найпоширеніших сценаріїв розгортання.

Перш ніж розпочати інсталяцію Microsoft Azure AD Connect, необіхдно завантажити програму Azure AD Connect з офіційного порталу компанії Microsoft.

Для інтеграції даної технології на сервері, необхідно виконати наступні кроки:

– Увійти на сервер під обліковим записом з правами адміністратора, на буде встановлено Microsoft Azure AD Connect. Після інтеграції технології, цей сервер стане сервером синхронізації Azure AD Connect.

– Необхідно перейти до попередньо завантаженого файлу AzureADConnect.msi і запустити його.

– У розділі Welcome необхідно встановити прапорець погодження з умовами ліцензування й натиснути кнопку Continue.

– У розділі Express Settings потрібно вибрати Use express settings (рисунок 3.3).

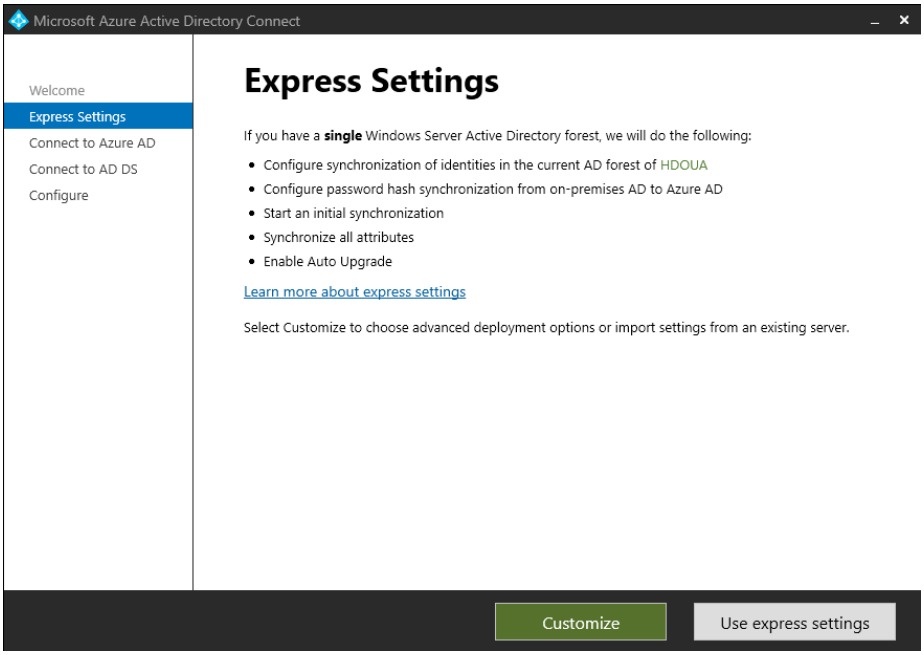


Рисунок 3.3 – вибір Express Settings

– У полі Connect to Microsoft Azure AD ввести ім'я користувача та пароль облікового запису адміністратора Hybrid Identity Administrator і натиснути Next (рисунок 3.4). На прикладі, адміністратором Hybrid Identity Administrator є обліковий запис admin@hdoua.onmicrosoft.com.

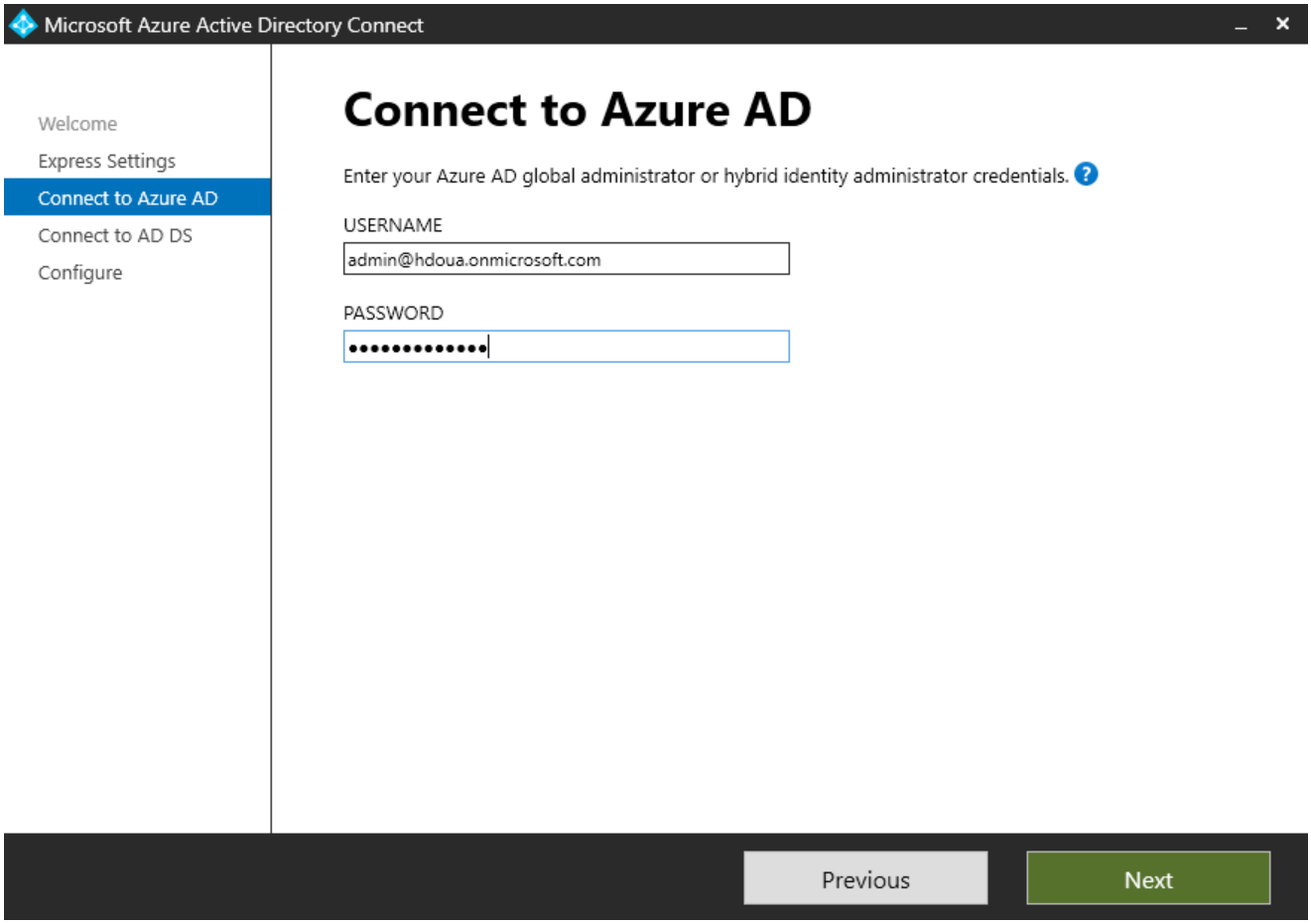


Рисунок 3.4 – Вхід до облікового запису Entra ID

– У полі Connect to AD DS введіть ім'я користувача та пароль для облікового запису Enterprise Admin (рисунок 3.5). Є можливість введення частини домену у форматі NetBIOS або FQDN (DOMAIN\Administrator або domain.com\Administrator). На прикладі, обліковим записом Enterprise Admin є HDOUA\admin.

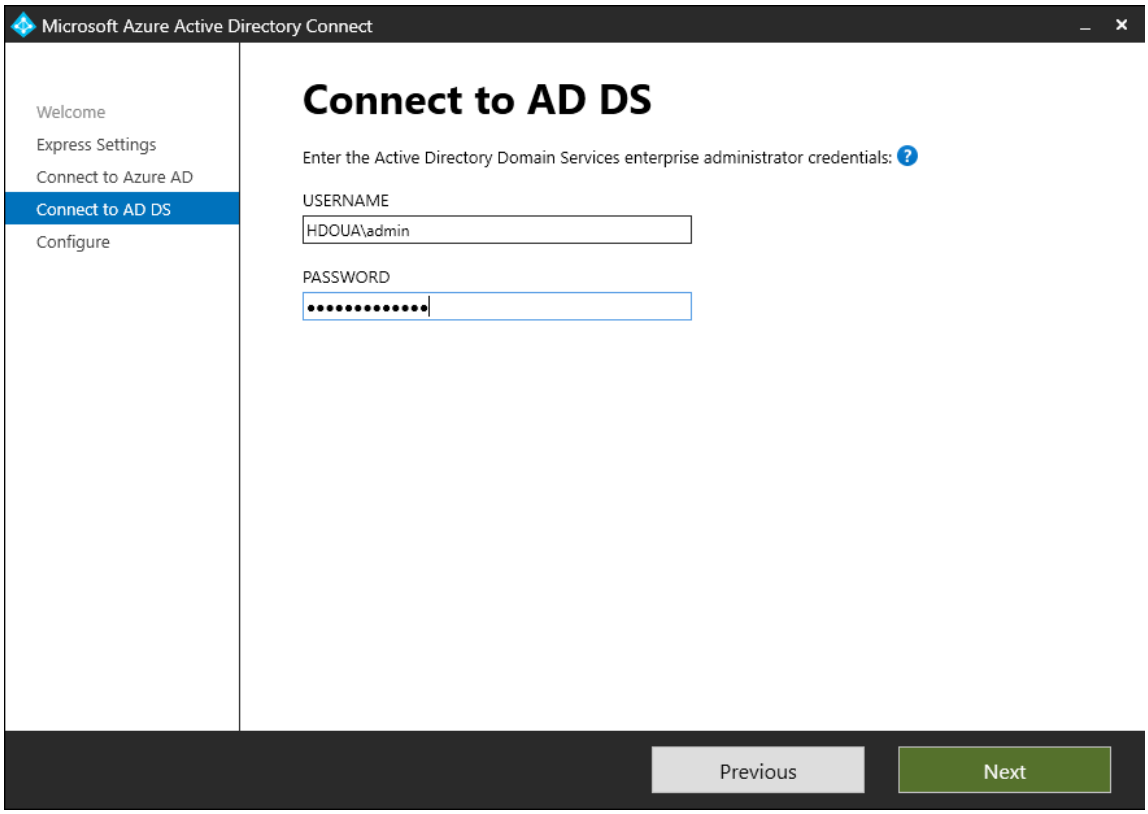


Рисунок 3.5 – Вхід до облікового запису Enterprise Admin

– На етапі Ready to configure, необіхдно вибрати Install (рисунок 3.6).

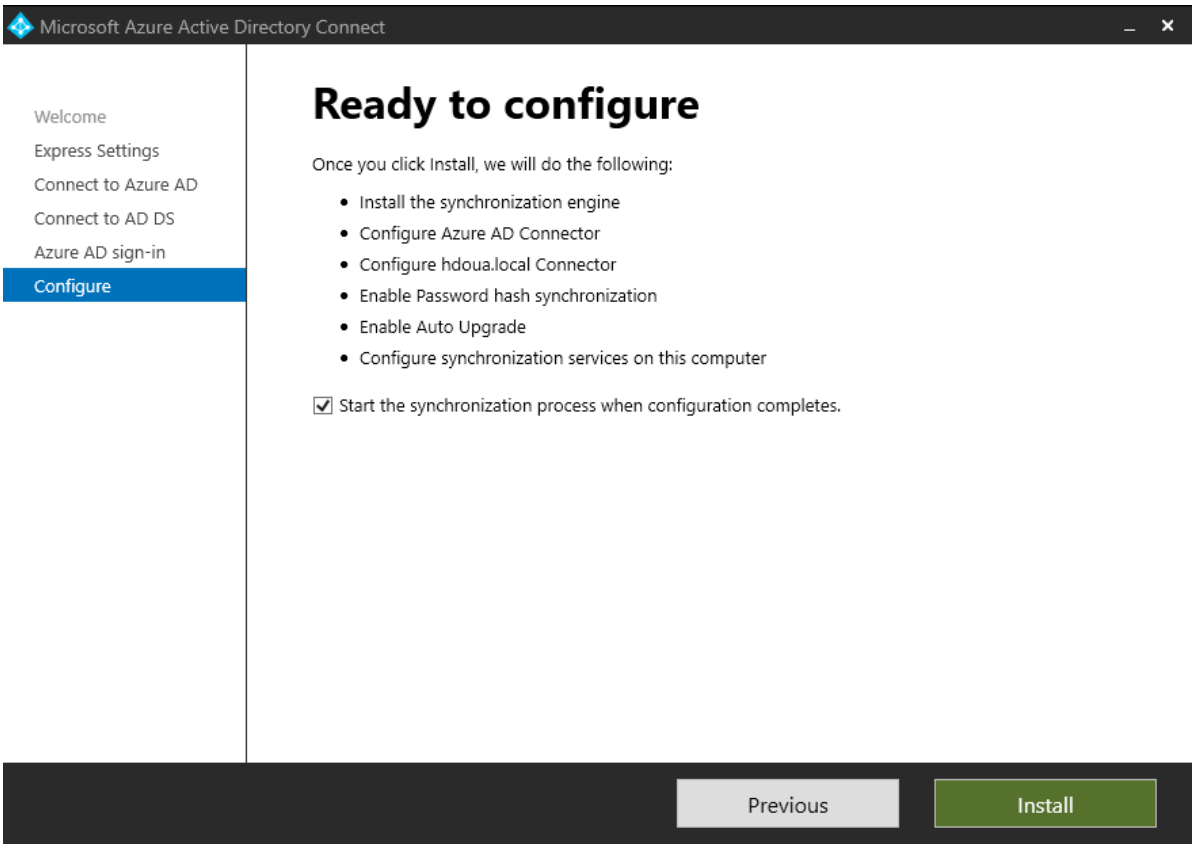


Рисунок 3.6 – етап Ready to configure

Необхідно зняти прапорець Start the synchronithation process when cconfiguration completes якщо є потреба у виконанні додаткових налаштувань, таких як фільтрація організаційних одиниць або груп безпеки, що синрхронізуються.

Якщо прапорець знятий, тио майстер налаштує синхронізацію, але залишить планувальник синхронізації вимкненим. Він не працюватиме, доки його не увімкнуть вручну, повторно запустивши майстер встановлення Azure AD Connect.

Якщо не знімати прапорець з пункту Start the synchronithation process when cconfiguration completes, повна синхронізація усіх користувачів, груп і контактів з Microsoft Entra ID розпочнеться одразу після успішної інсталяції Azure AD Connect.

Якщо в екземплярі Windows Server Active Directory встановлено Exchange, Azure AD Connect розпізнає це і адміністратор матиме можливість увімкнути параметр Exchange Hybrid Deployment, що в свою чергу забезпечить зберігання поштових скриньок Exchange як у хмарі, так і локально одночасно.

- Після завершення інсталяції, необхідно натиснути Exit.
- Перед використанням диспетчера служб синхронізації або редактора правил синхронізації необхідно зробити вихід із сервера або перезапустити його.

Після виконання попередніх кроків і успішної синхронізації Active Directory за допомогою Azure AD Connect, в тенанті Entra ID з’являться локальні користувачі, які вже мають змогу отримувати доступ до хмарних сервісів Microsoft, пройшовши автентифікацію зі своїм паролем локального облікового запису (рисунок 3.7).

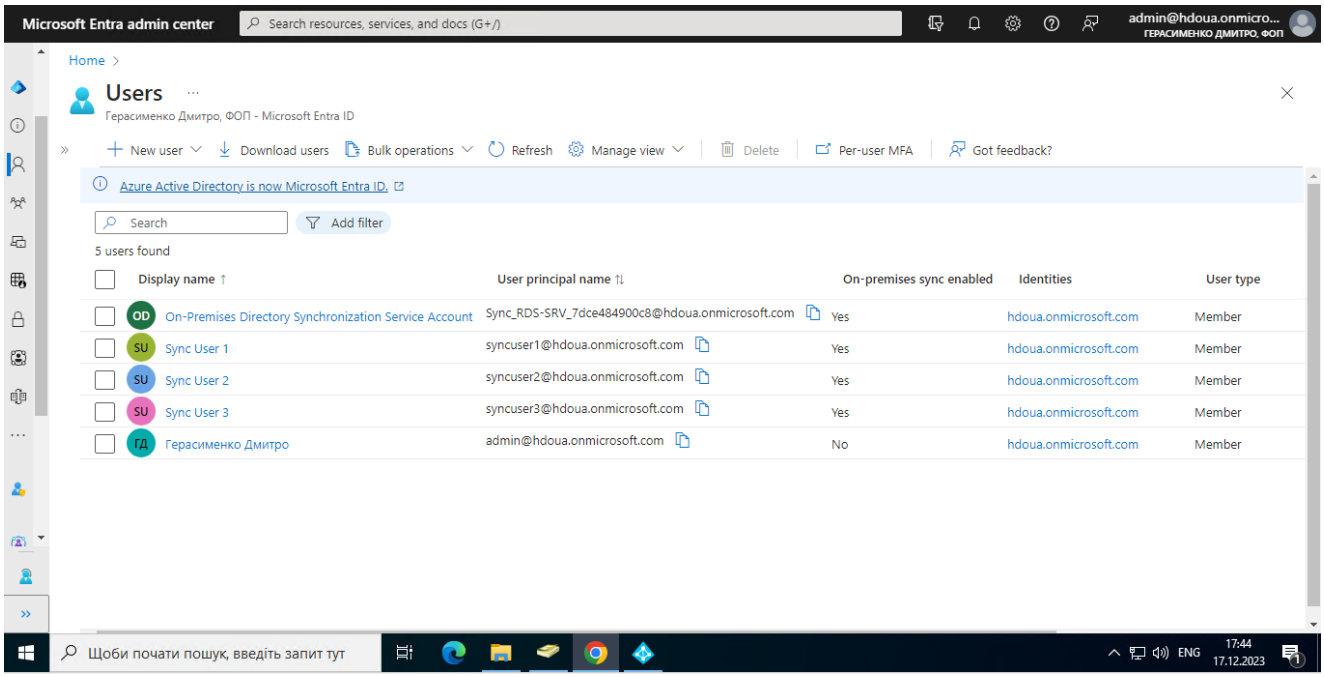


Рисунок 3.7 – синхронізовані користувачі в Entra ID

Серед користувачів Sync User є ще два користувачі:

– On-Premises Directory Synchronization Service Account – це обліковий запис, який отримує інформацію з локального домена і переносить її в тенант, а саме створює користувачів, змінює паролі, назначає групові політики або правила керування ідентичностями.

– admin@hdoua.onmicrosoft.com – глобальний адміністратор тенанта, який створюється автоматично при реєстрації тенанта, де Display name користувача це прізвище та ім’я особи, на яку зареєстрований тенант.

В колонці On-Premises sync enabled можемо спостерігати статус користувачів, де позначка Yes означає синхронізацію облікового запису. За замовчуванням, облікові записи доменного адміністратора та глобального адміністратора тенанта не синхронізуються.

Також в тенанті Entra ID, перейшовши до вкладки Hybrid management – Microsoft Entra Connect – Connect Sync, в пункті Provision Active Directory, параметри Sync status та Password Hash Sync відмічені як Enabled (рисунок 3.8), що свідчить про успішну інтеграцію Microsoft Entra Connect в локальне середовище Active Directory.

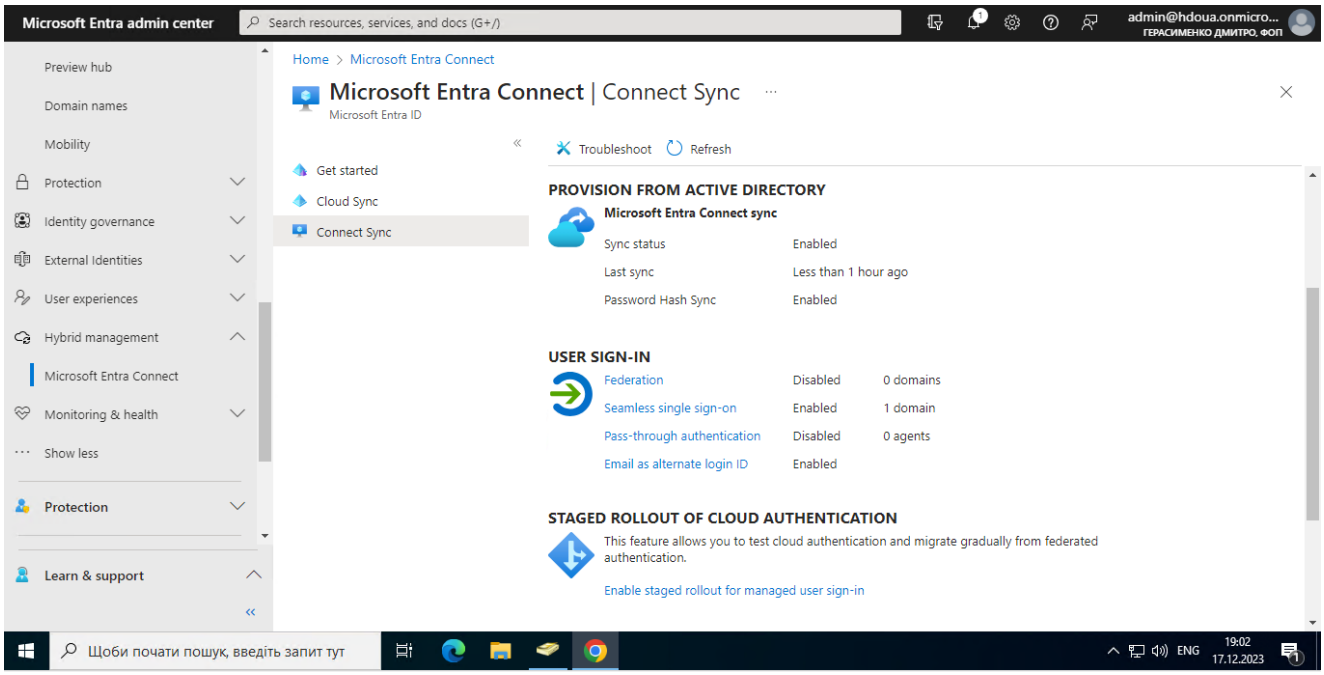


Рисунок 3.8 – статус синхронізації Microsoft Entra Connect

3.2 Принцип роботи синхронізації хеша паролів

Служба домену Active Directory зберігає паролі у вигляді хеш-значення фактичного пароля користувача. Хеш-значення є результатом односторонньої математичної функції (алгоритму хешування). Не існує способу повернути результат односторонньої функції до звичайної текстової версії пароля.

Щоб синхронізувати паролі, Microsoft Entra Connect Sync витягує хеш паролів з локального екземпляра Active Directory. Перед синхронізацією хешу паролів зі службою автентифікації Microsoft Entra, до нього застосовується додаткова обробка безпеки. Паролі синхронізуються для кожного користувача в хронологічному порядку.

Фактичний потік даних процесу синхронізації хешу пароля схожий на синхронізацію даних користувача. Однак паролі синхронізуються частіше, ніж у стандартному проміжку синхронізації каталогів для інших атрибутів. Процес синхронізації хешу паролів виконується кожні 2 хвилини. Є можливість змінити частоту цього процесу. При синхронізації пароля, він перезаписується як існуючий хмарний пароль.

При першому виконанні функції синхронізації хеш-паролів, Azure AD Connect виконує початкову синхронізацію паролів усіх користувачів, що входять до сфери дії програми. Поетапне розгортання дає змогу вибірково протестувати групи користувачів із можливостями хмарної автентифікації, як багатофакторна автентифікація Microsoft Entra, умовний доступ, захист ідентифікаційних даних від витоку, керування ідентифікаційними даними та інші, перш ніж переходити на синхронізацію робочого домена.

Коли ви змінюєте локальний пароль, оновлений пароль синхронізується протягом 2 хвилин. Функція синхронізації хешу пароля автоматично повторює невдалі спроби синхронізації. Якщо під час спроби синхронізації пароля виникає помилка, вона буде зареєстрована у засобі перегляду подій.

Синхронізація пароля не впливає на користувача, який зараз авторизований у системі. Синхронізована зміна пароля, яка відбувається під час вашого входу до хмарного сервісу, одразу не впливає на ваш поточний сеанс у хмарному сервісі. Однак, коли хмарна служба вимагатиме від вас повторної автентифікації, вам потрібно буде вказати новий пароль. Користувач повинен ввести свої корпоративні облікові дані вдруге для автентифікації в Microsoft Entra ID, незалежно від того, чи ввійшов він у свою корпоративну мережу. Однак цю схему можна мінімізувати, якщо користувач встановить прапорець "Тримати мене в системі" (KMSI) під час входу. Цей вибір встановлює сеансовий файл cookie, який обходить автентифікацію протягом 180 днів. Поведінку KMSI можна увімкнути або вимкнути за допомогою адміністративного середовища Microsoft Entra. Крім того, є можливість зменшити кількість запитів на введення пароля, налаштувавши Microsoft Entra join або Microsoft Entra hybrid join, які автоматично реєструють користувачів, коли вони перебувають на своїх корпоративних пристроях, підключених до вашої корпоративної мережі.

Основні етапи, які виконуються при синхронізації хеша паролів:

– Кожні дві хвилини агент синхронізації хешів паролів на сервері AD Connect запитує збережені хеші паролів (атрибут unicodePwd) з домен контролера. Цей запит виконується за допомогою стандартного протоколу реплікації MS-DRSR,

який використовується для синхронізації даних між контролерами доступу. Обліковий запис служби повинен мати права на реплікацію змін у каталогах і реплікацію змін у всіх каталогах AD (надаються за замовчуванням під час інсталяції), щоб отримати хеші паролів.

– Перед відправкою домен контролер шифрує хеш пароля MD4 за допомогою ключа, який є хешем MD5 ключа сеансу RPC і солі (унікальний рядок даних, який передається хеш-функції разом з паролем). Потім він надсилає результат агенту синхронізації хешу пароля через RPC. Домен контролер також передає сіль агенту синхронізації за допомогою протоколу реплікації, щоб агент зміг розшифрувати пакет даних.

– Після того, як агент синхронізації хешу пароля отримав зашифрований пакет, він використовує MD5CryptoServiceProvider і сіль для генерації ключа, щоб розшифрувати отримані дані назад в оригінальний формат MD4. Агент синхронізації хешу пароля ніколи не має доступу до відкритого тексту пароля. Агент синхронізації хешу пароля використовує MD5 виключно для сумісності протоколу реплікації з домен контролером і він використовується лише локально між домен контролером та агентом синхронізації хешу пароля.

– Агент синхронізації хешу пароля розширює 16-байтовий двійковий хеш пароля до 64 байт, спочатку перетворюючи хеш у 32-байтовий шістнадцятковий рядок, а потім перетворюючи цей рядок назад у двійковий з кодуванням UTF-16.

– Агент синхронізації хешу пароля додає до 64-байтового бінарного файлу сіль для кожного користувача, що складається з 10-байтової солі, для додаткового захисту оригінального хешу.

– Агент синхронізації хешу пароля комбінує хеш MD4 з сіллю для кожного користувача і вводить його у функцію PBKDF2. Використовується 1000 ітерацій алгоритму хешування з ключем HMAC-SHA256.

– Агент синхронізації хешу пароля приймає отриманий 32-байтовий хеш, додає до нього сіль для кожного користувача та кількість ітерацій SHA256 (для використання Microsoft Entra ID), після чого передає рядок з Microsoft Entra Connect до Microsoft Entra ID через TLS.

– Коли користувач намагається увійти в Microsoft Entra ID і вводить свій пароль, пароль пропускається через той самий процес MD4+salt+PBKDF2+HMAC-SHA256. Якщо отриманий хеш збігається з хешем, що зберігається в Microsoft Entra ID, це означає, що користувач ввів правильний пароль і пройшов автентифікацію.

3.3 Активація служби самостійного скидання пароля SSPR

Функція самостійного скидання пароля Microsoft Entra (SSPR) дає користувачам можливість змінити або скинути свій пароль без участі адміністратора або служби підтримки. Якщо Microsoft Entra ID заблокує обліковий запис користувача або він забуде свій пароль, він може слідувати підказкам по відновленню пароля, щоб розблокувати себе і повернути доступ до ресурсів. Ця функція зменшує кількість звернень до служби підтримки орієнтовно на 20-30% та мінімізує втрату продуктивності IT-відділу організації.

Microsoft Entra ID дозволяє увімкнути SSPR для всіх, вибраних або окремих користувачів. Ця можливість дозволяє вибрати підгрупу користувачів для тестування процесу реєстрації та робочого процесу SSPR. Коли результат роботи процесу SSPR буде задовільним, адміністратор зможе вибрати групу користувачів, для яких варто увімкнути дану функцію.

У наступних кроках описано процес налаштування SSPR для набору користувачів усієї організації. Для забезпечення максимально комфортної роботи із системою усіх користувачів.

– Необхідно увійти до центру адміністрування Microsoft Entra як адміністратор політики автентифікації або вищими правами.

– Перейти до пункту Protection – Password reset в меню ліворуч.

– На сторінці Properties у розділі Self service password reset виберіть Selected.

– Якщо необхідна група не відображається, необхідно вибрати пункт No selected groups, потім знайти і вибрати групу Microsoft Entra, яка в даному випадку є All Company.

– Щоб увімкнути SSPR для вибраних користувачів, натисніть Save.

Рисунок 3.9 показує, що самостійне скидання паролю увімкнене для групи All Company, до якої автоматично додаються усі створені або синхронізовані з Active Directory облікові записи.

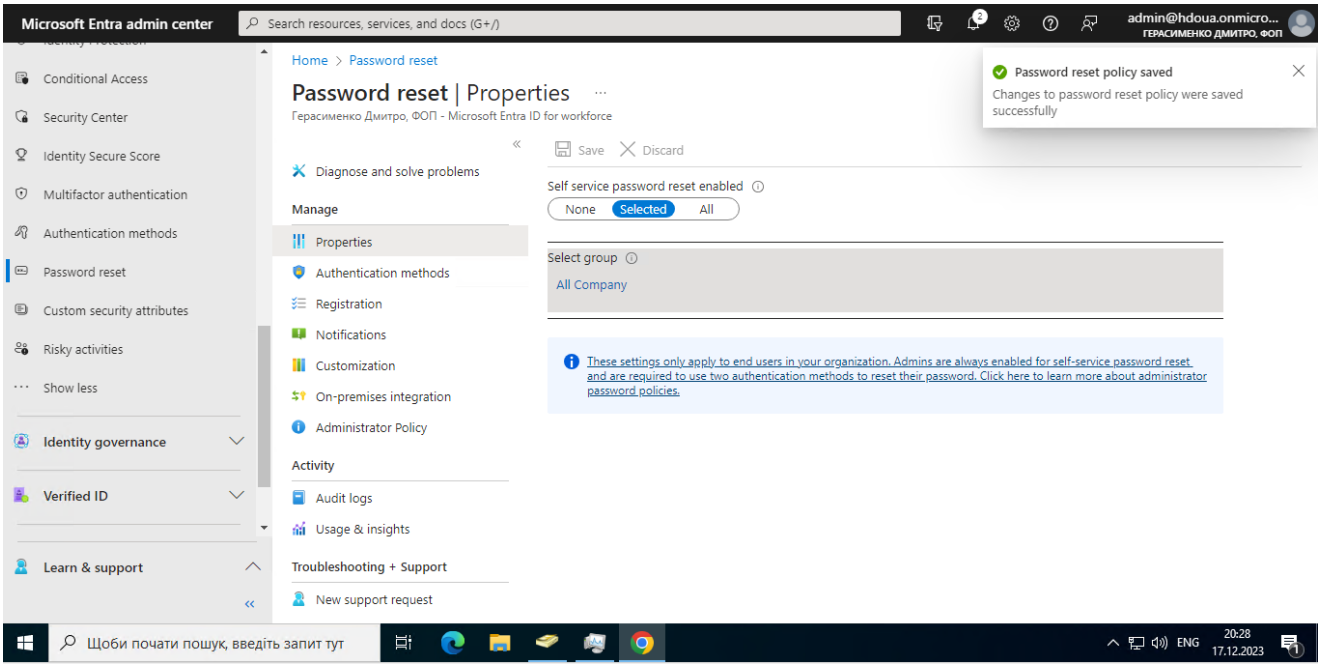


Рисунок 3.9 – SSPR увімкнено для групи All Company

Коли користувачам потрібно розблокувати свій обліковий запис або скинути пароль, їм буде запропоновано підтвердження особистості через MFA. Цей додатковий фактор автентифікації гарантує, що Microsoft Entra ID завершить лише схвалені події SSPR. Адміністратор Entra ID має можливість вибрати, які методи автентифікації дозволити, на основі реєстраційної інформації, наданої користувачем.

– У меню зліва на сторінці Authentication methods необхідно встановити Number of methods required to reset, на 2.

– Вибрати Methods available to users, які будуть дозволені в організації. На цьому етапі необхідно встановити прапорці, щоб увімкнути наступні методи:

– сповіщення в мобільному додатку;

– код мобільного додатку;

– електронна пошта;

– мобільний телефон.

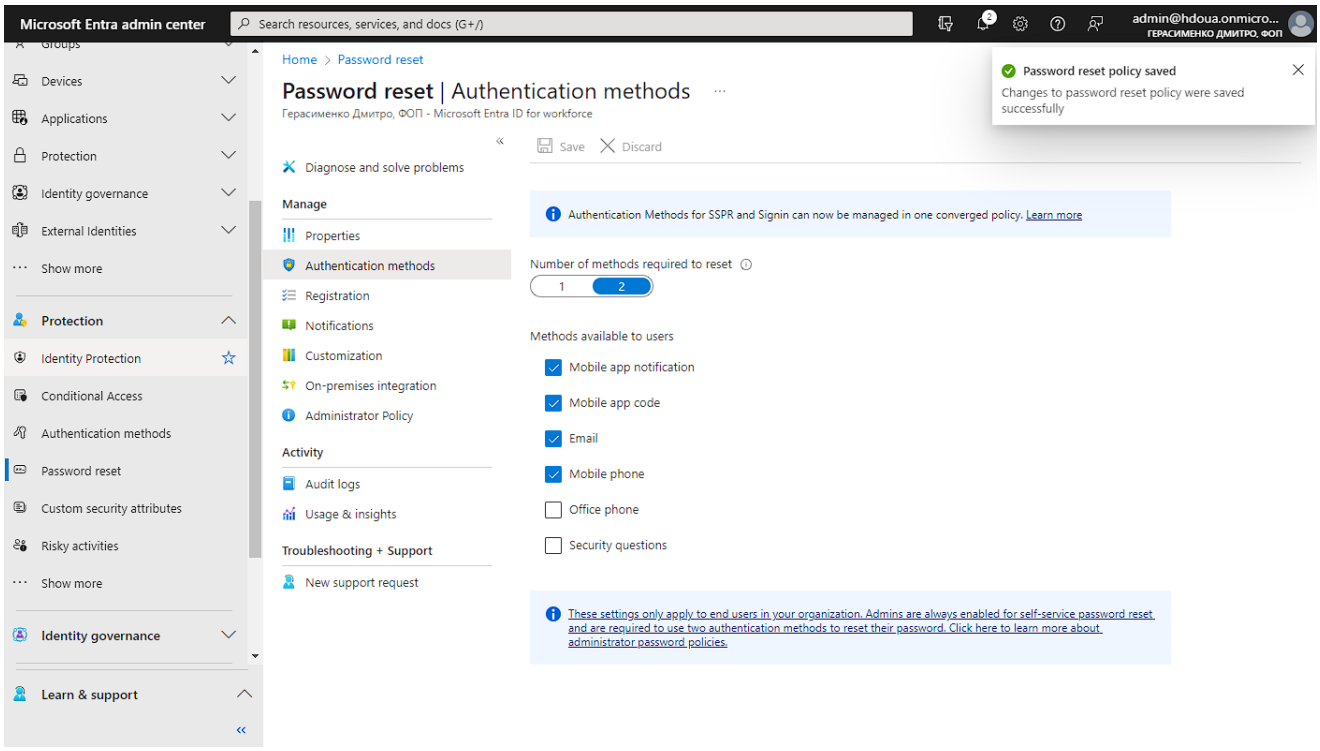


Рисунок 3.10 – вибір методів MFA для SSPR

Адміністратор може ввімкнути інші методи автентифікації, такі як офісний телефон або секретні питання, якщо цього вимагають політики безпеки організації.

– Щоб застосувати методи автентифікації, потрібно натиснути Save.

Перш ніж користувачі зможуть розблокувати свій обліковий запис або скинути пароль, вони повинні зареєструвати свої контактні дані (мобільний телефон або електронну пошту). Microsoft Entra ID використовує цю контактну інформацію для різних методів автентифікації, налаштованих на попередніх кроках.

Адміністратор може вручну ввести цю контактну інформацію, або ж користувачі можуть перейти на реєстраційний портал і надати її самостійно. Наступними кроками буде налаштування Microsoft Entra ID так, щоб він запитував користувачів про реєстрацію під час наступного входу.

– У меню Passwords reset зліва виберіть Registration і встановіть параметр Yes для опції Require users to register when singing in.

– Далі встановлюємо Number of days before users are asked to re-confirm their authentication information, рівною 180. В такому випадку користувачам буде приходити запит на підтвердження їх контактних даних раз на пів року.

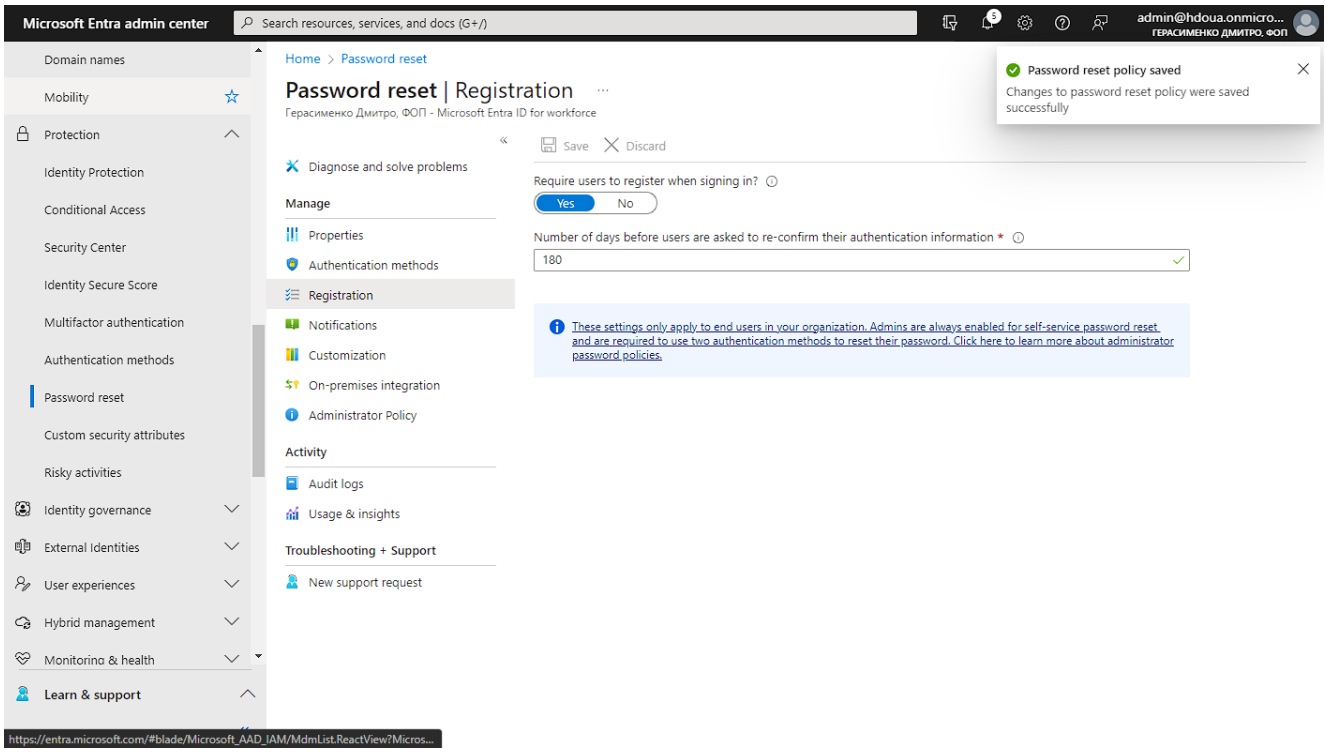


Рисунок 3.11 – налаштування запитів на отримання контактої інформації користувачів

Контакту інформацію важливо зберігати актуальною. Якщо на момент початку події SSPR контактна інформація буде застарілою, користувач не зможе розблокувати свій обліковий запис або скинути пароль.

– Щоб застосувати налаштування реєстрації, натисніть Зберегти (рисунок 3.10).

Для інформування користувачів про активність облікових записів, Адміністратор можете налаштувати Microsoft Entra ID на надсилання сповіщень електронною поштою, коли відбувається подія SSPR. Ці сповіщення можуть стосуватися як звичайних облікових записів користувачів, так і облікових записів адміністраторів. Для облікових записів адміністраторів ці сповіщення надають додатковий рівень обізнаності, коли пароль привілейованого облікового запису адміністратора скинуто за допомогою SSPR. Microsoft Entra ID сповіщатиме всіх

глобальних адміністраторів, коли хтось використовує SSPR в обліковому записі адміністратора.

– У меню зліва на сторінці Сповіщення необхідно налаштувати наступні опції:

– встановити значення Yes для параметра Notify users on password resets;

– встановити значення Yes для параметра Notify all admins when other admins reset their passwords.

– Щоб застосувати налаштування сповіщень, натисніть Зберегти (рисунок 3.12).

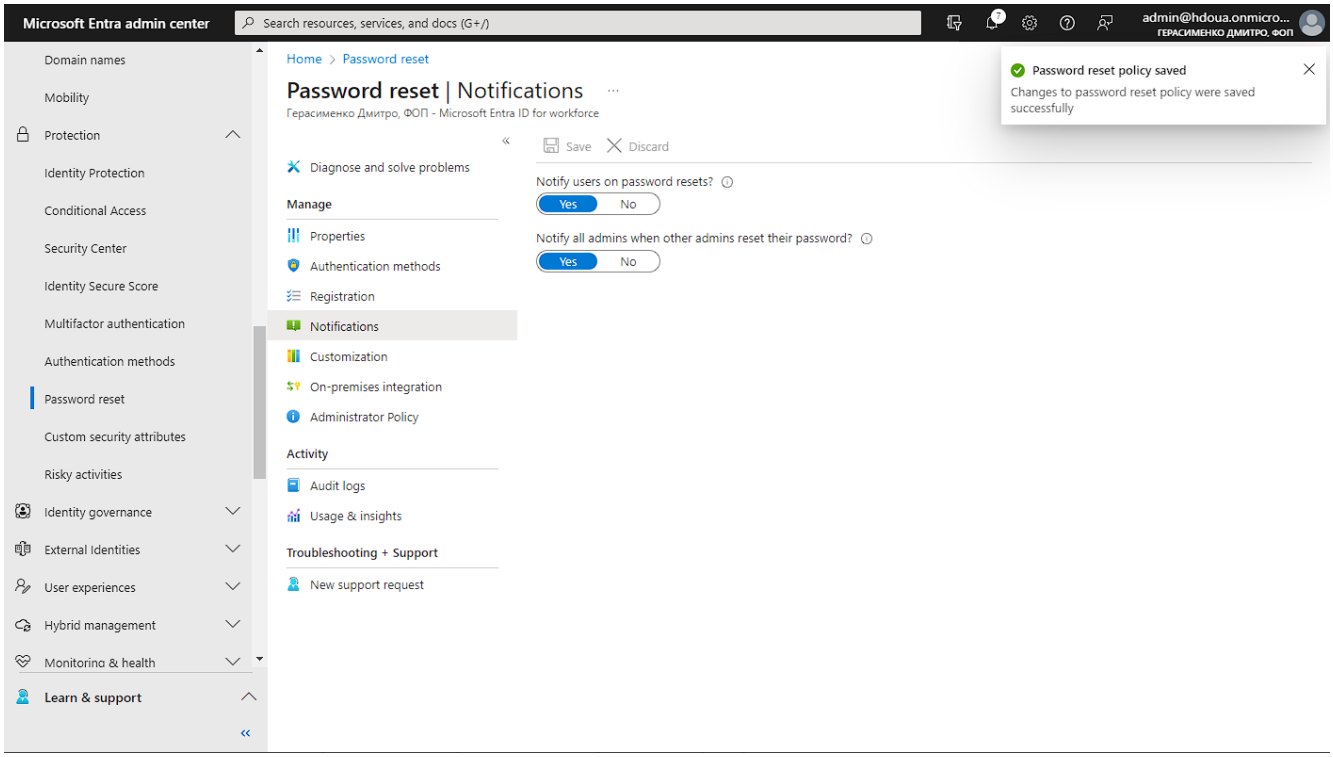


Рисунок 3.12 – застосування налаштувань сповіщення про успішне скидання пароля процедурою SSPR

Якщо користувачі потребують додаткової допомоги в процесі SSPR, є можливість налаштувати посилання "Зв'язатися з адміністратором". Користувач може перейти за посиланням на портал технічної підтримки організації або написати відповідного листа на електронну адресу технічної підтримки чи адміністратора тенанта, який буде вказаний на сторінці скидання пароля SSPR.

– У меню ліворуч в пункті Customization потрібно встановити значення Yes для параметру Customize helpdesk link.

– У полі Custom helpdesk email or URL необхідно ввсети адресу електронної пошти або URL-адресу веб-сторінки, на якій користувачі можуть отримати додаткову допомогу від IT-спеціалістів організації. В даному випадку це буде електронна пошта адміністратора тенанта, на яку користувачі можуть написати лист з запитом на допомогу у скиданні пароля.

– Щоб застосувати кастомне посилання, натисніть Зберегти (рисунок 3.13).

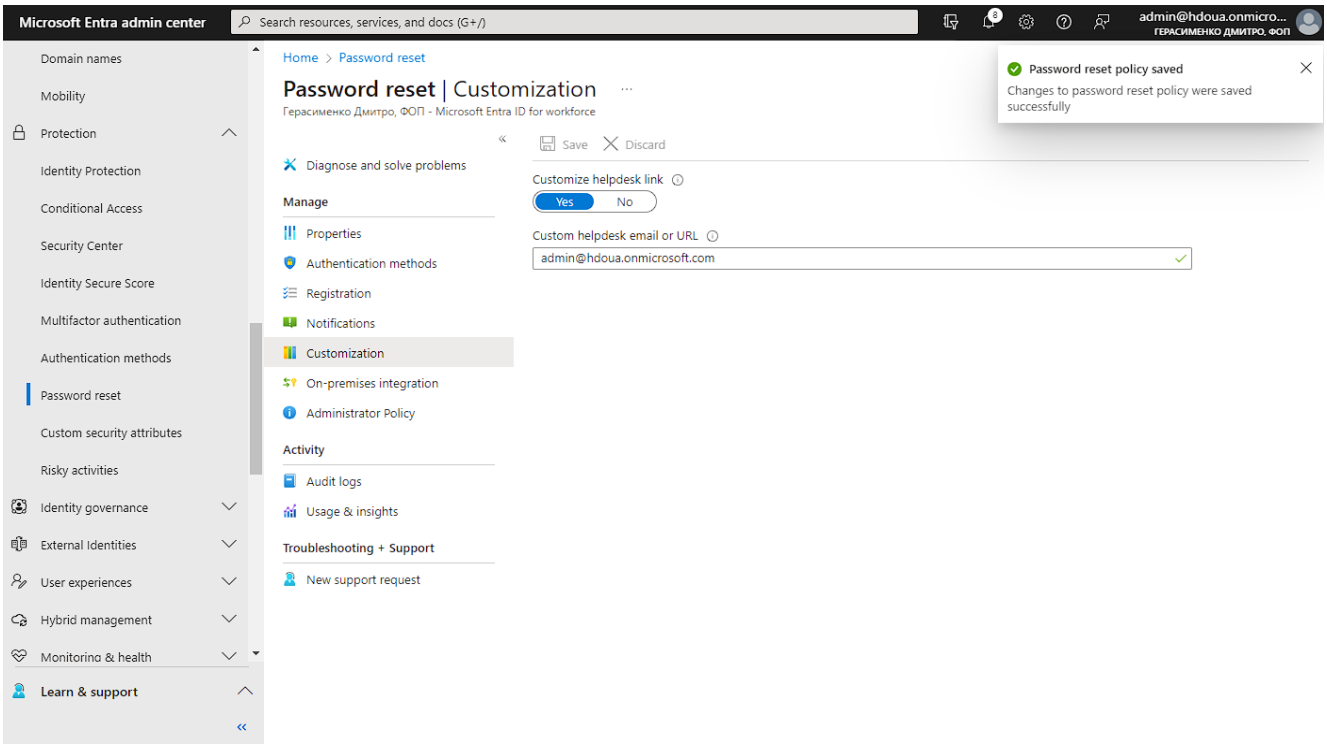


Рисунок 3.13 – застосування налаштувань додаткових можливостей отримання технічної підтримки при скиданні пароля

Увімкнувши і налаштувавши SSPR, варто протестувати процес SSPR з користувачем, який входить до групи All Company. У наступному прикладі використовується обліковий запис користувача syncuser1.

– Щоб побачити процес реєстрації вручну, необхідно відкрити нове вікно браузера в режимі InPrivate або інкогніто і перейти на https://aka.ms/ssprsetup. Microsoft Entra ID спрямовуватиме користувачів на цей реєстраційний портал під час наступного входу.

– Потрібно увійти під тестовим користувачем, який не є адміністратором, наприклад і зареєструйте контактну інформацію про свої методи автентифікації. В даному випадку це буде користувач syncuser1@hdoua.onmicrosoft.com.

– Після завершення натиснути на Looks good, як підтвердження того, що така процедура прийнятна для системи скидання пароля і закрити вікно браузера.

– Потім необхідновідкрити нове вікно браузера в режимі InPrivate або інкогніто і перейти за адресою https://aka.ms/sspr.

– Ввести дані облікового запису тестового користувача, який не є адміністратором (syncuser1@hdoua.onmicrosoft.com), ввести символи з CAPTCHA й натиснути Далі (рисунок 3.14).

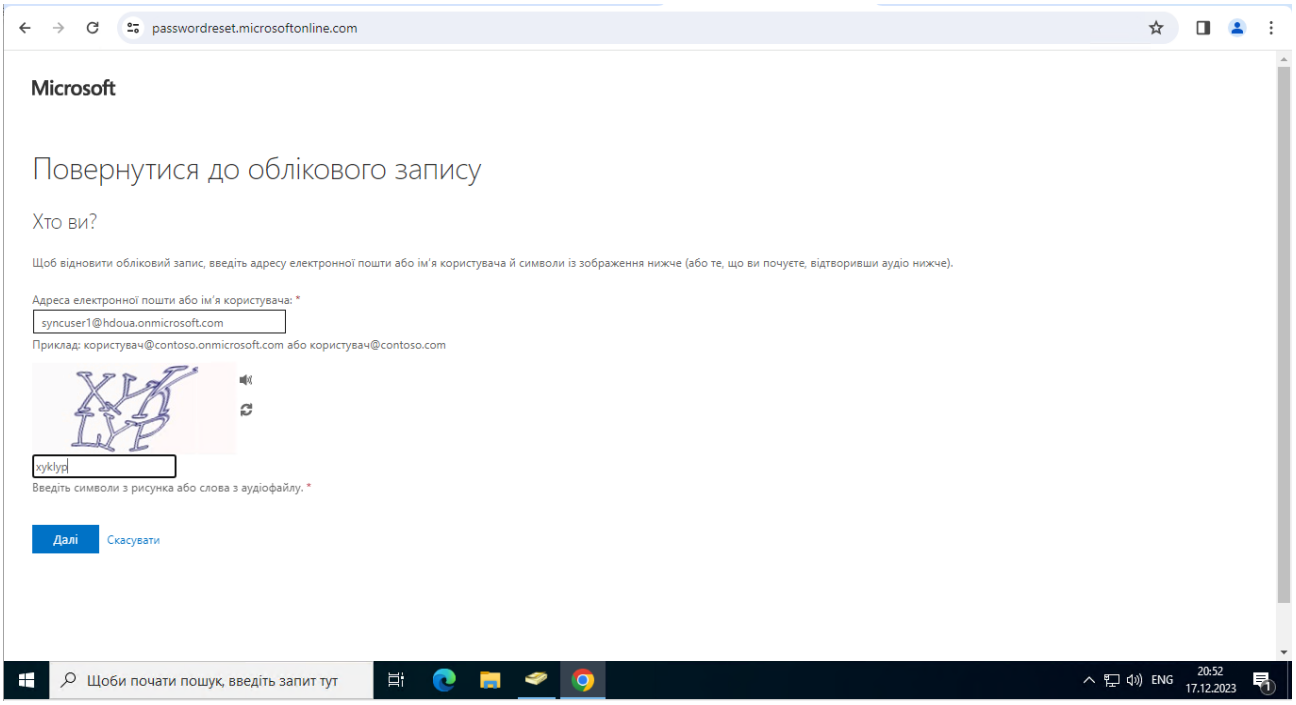


Рисунок 3.14 – сторінка скидання пароля користувача

– Необхідно виконати 2 етапи підтвердження особи за допомогою методів, які були налаштовані як методи автентифікації для скидання пароля (сповіщення в мобільному додатку, код мобільного додатку, сповіщення електронною поштою або сповіщення за номером мобільного телефона) щоб скинути пароль. Після завершення процедури, користувач отримає сповіщення на електронну пошту про те, що його пароль було скинуто.

3.4 Активація єдиного входу SSO в Microsoft ID на основі пароля

Єдиний вхід (Single Sign-On, далі SSO) – це метод автентифікації, який дозволяє користувачам входити за допомогою одного набору облікових даних до кількох незалежних програмних систем. Використання SSO означає, що користувачеві не потрібно входити в кожну програму, якою він користується. Завдяки SSO користувачі можуть отримати доступ до всіх необхідних програм без необхідності автентифікації за допомогою різних облікових даних.

За допомогою SSO на основі паролів користувачі під час першого входу в додаток вводять ім'я користувача та пароль. Після першого входу Microsoft Entra ID надає ім'я користувача та пароль до програми. SSO на основі пароля дозволяє безпечно зберігати та відтворювати пароль до програми за допомогою розширення для веб-браузера або мобільного додатку. Ця опція використовує існуючий процес входу в програму, дозволяє адміністратору керувати паролями і не вимагає від користувача знання пароля. Для налаштування функції SSO потрібно виконати наступні кроки.

– Увійти до центру адміністрування Microsoft Entra з правами адміністратора хмарних додатків або вище.

– Перейти до розділу Identity – Applications – Enterprise applications – All applications. Далі натиснути + New application.

– В поле пошуку ввести назву бажаної програми або веб-сторінки. Для спрощення пошуку, усі програми можна відфільтрувати за фільтром Single Sign-On: Password. Як приклад буде обрано програму Adobe Sign.

– Вибрати необхідну програму і натиснути Create.

– Далі буде запропоновано налаштування з 5 етапів (рисунок 3.15), обов’язковими з яких є перші 3: Assign users and groups, Set up single sing on Provision user accounts.

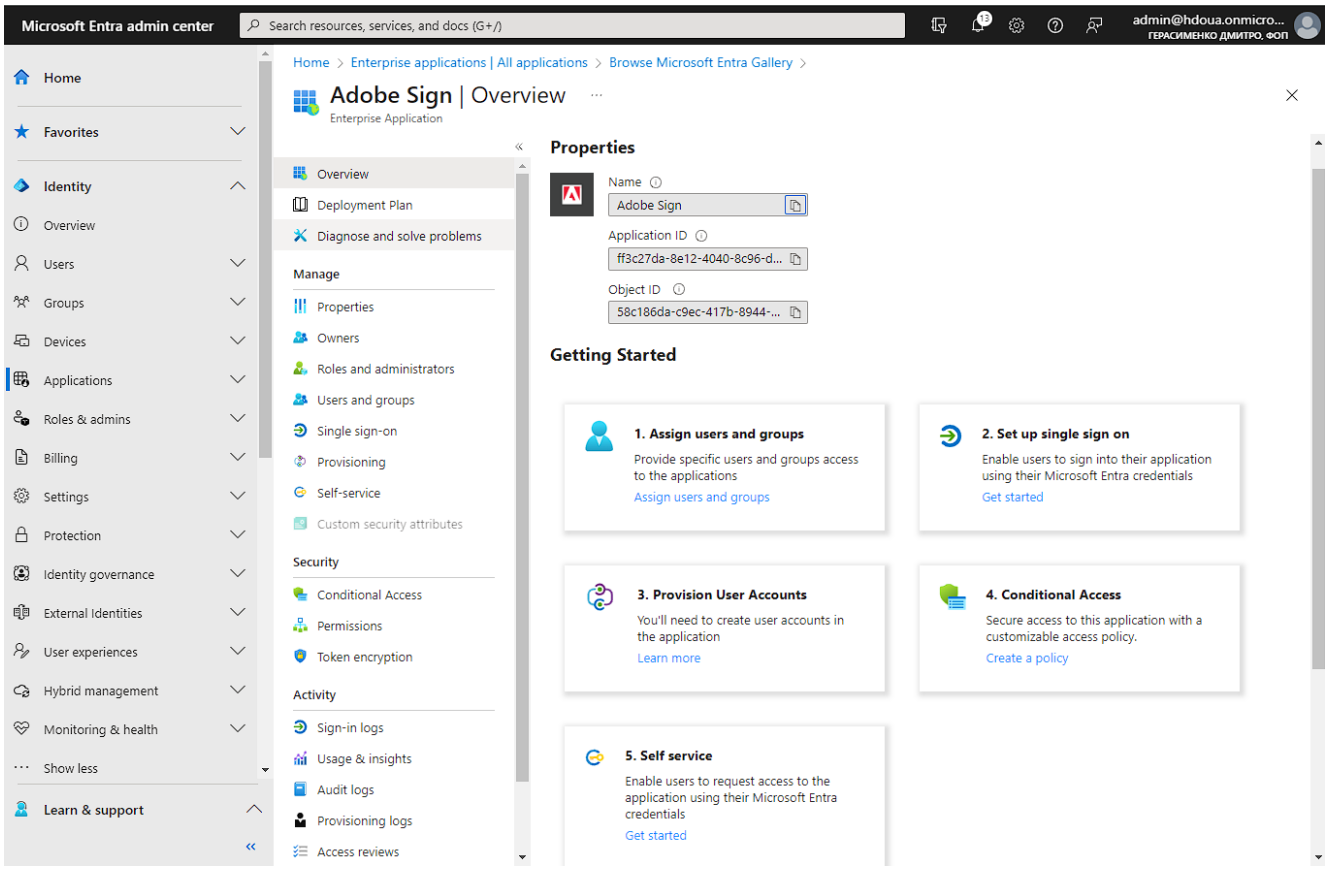


Рисунок 3.15 – початок налаштування SSO для конкретної веб-сторінки

– На етапі Assign users and groups необхідно обрати групи або користувачів, яким буде доступний SSO до цієї програми.

– На етапі Set up single sing on необхідно обрати метод SSO за допомогою пароля і підтвердити попередньо введену URL-адресу сторінки для входу, натиснувши Save.

– Microsoft Entra ID проаналізує HTML-код сторінки входу на наявність полів для введення імені користувача та пароля, в які будуть автоматично вводитися облікові дані.

– На етапі Provision user accounts необхідно ввести ім'я користувача та пароль, які будуть використовуватися для користувача або групи. Якщо цього не зробити, користувачам буде запропоновано ввести облікові дані під час запуску.

Після усіх налаштувань, програма буде відображатися в списку доступних для SSO (рисунок 3.16). З цього моменту, коли вибрані для SSO користувачі будуть

входити до програмних ресурсів Adobe, вхід буде автоматичний, без введення логіна і пароля користувача Adobe.

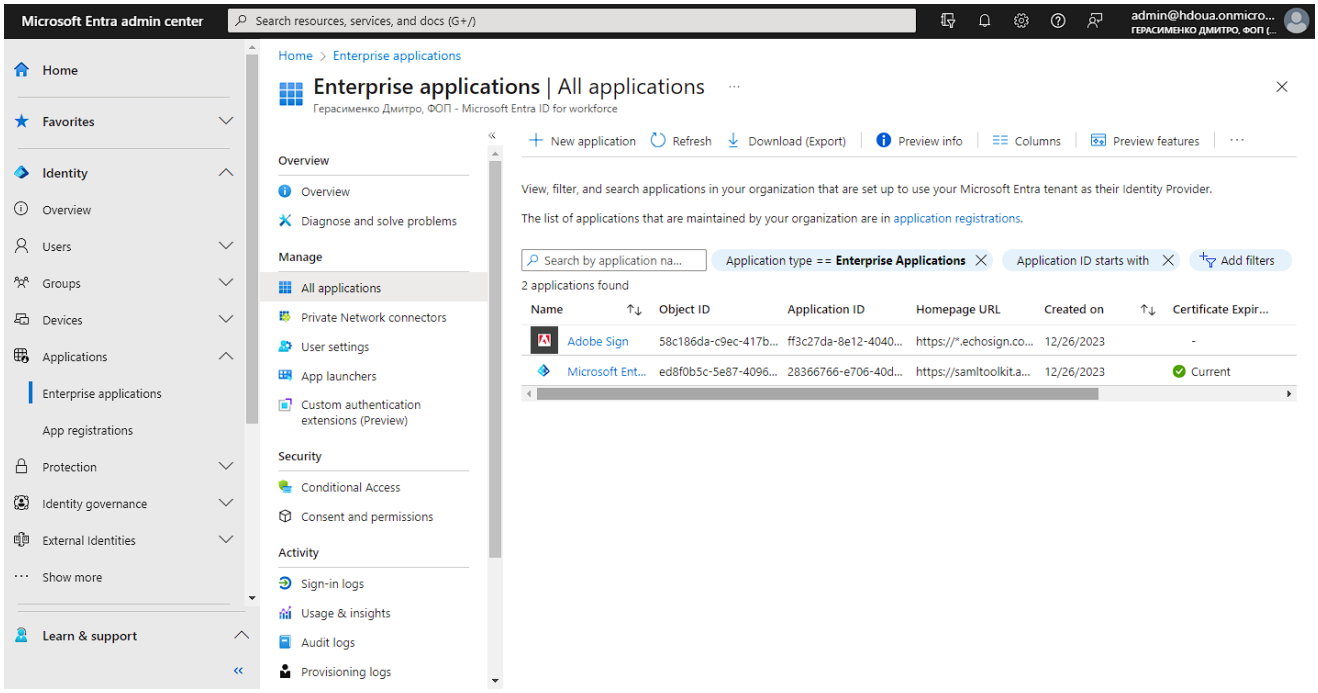


Рисунок 3.16 – відображення програми Adobe Sing в списку програм з налаштованим SSO

3.5 Активація функції зворотного запису пароля

Функція зворотного запису пароля може використовуватися для синхронізації змін паролів у Microsoft Entra з локальним середовищем AD DS. Microsoft Azure AD Connect надає безпечний механізм для надсилання цих змін паролів назад до існуючого локального каталогу з Microsoft Entra ID.

Для коректної роботи зі зворотним записом SSPR обліковий запис, вказаний у Microsoft Azure AD Connect, повинен мати відповідні дозволи та встановлені опції. А саме дозволи:

- скидання пароля;
- зміни пароля;
- запису lockoutTime;
- запису pwdLastSet;

– розширені права на Unexpire Password для кореневого об'єкта кожного домену у цьому лісі, якщо ц еще не встановлено.

Якщо ці дозволи непризначені, зворотний запис може здаватися налаштованим правильно, але користувачі будуть стикатись з помилками, при керуванні локальними паролями з хмари.

Щоб налаштувати відповідні дозволи для запису пароля, необхідно виконати наступні кроки:

– У локальному середовищі AD DS відкрийте Active Directory Users and Computers з обліковим записом, який має відповідні права адміністратора домену.

– У меню Вигляд необхідно переконатися, що ввімкнено параметр Додаткові функції.

– На лівій панелі правою кнопкою миші виберіть об'єкт, який представляє корінь домену, потім виберіть Властивості – Безпека – Додатково.

– На вкладці Дозволи виберіть Додати.

– У полі Основний необхідно вибрати обліковий запис, до якого слід застосувати дозволи (обліковий запис, який використовується Microsoft Azure AD Connect.

– У розкривному списку Застосовується до виберіть об'єкти Нащадків користувачів.

– У розділі Дозволи встановити прапорець для опції Reset password (рисунок 3.17).

– У розділі Властивості потрібно встановити прапорці для наступних опцій:

  – write lockoutTime;

  – write pwdLastSet.

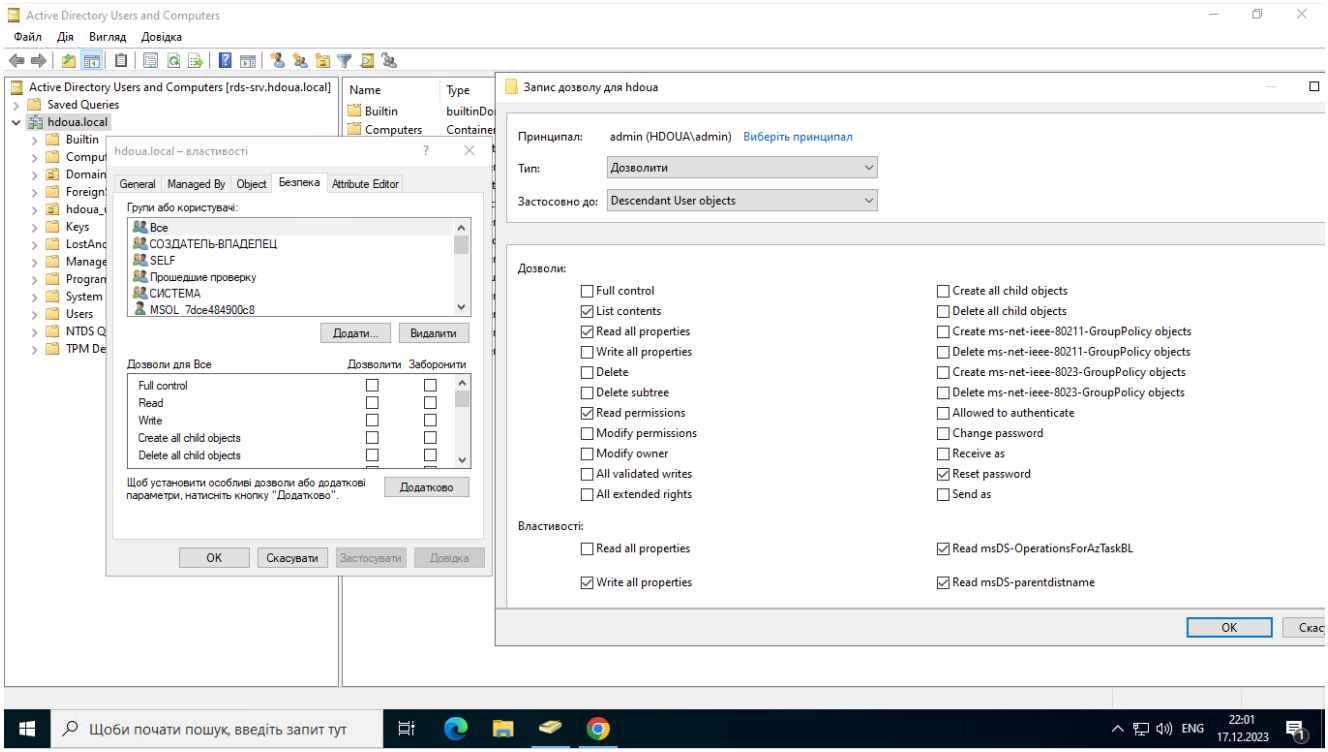


Рисунок 3.17 – Активація дозволу Reset password облікового запису синхронізації

– По закінченню натуснути Застосувати/OK.

– На вкладці Дозволи виберіть Додати.

– У полі Основний необхідно вибрати обліковий запис, до якого слід застосувати дозволи (обліковий запис, який використовується Microsoft Azure AD connect).

– У розкривному списку Застосовується до вибрати обліковий запис, що використовується Microsoft Azure AD connect і всі об'єкти-нащадки.

– У розділі Дозволи встановити прапорець для опції Невичерпний термін дії пароля.

– По закінчнню налаштувань натиснути Застосувати/OK і вийти з усіх відкритих діалогових вікон.

При оновленні дозволів, може знадобитися до години часу, щоб ці дозволи були репліковані до всіх об'єктів у локальному каталозі.

Політики паролів у локальному середовищі AD DS можуть перешкоджати коректній обробці скидання паролів. Щоб відновлення пароля працювало

найефективніше, групову політику для параметра Мінімальний вік пароля слід встановити на 0. Цей параметр можна знайти в застосунку gpedit.msc у розділі Конфігурація комп'ютера – Політики – Параметри Windows – Параметри безпеки – Політики облікових записів – Політики паролів (рисунок 3.18).

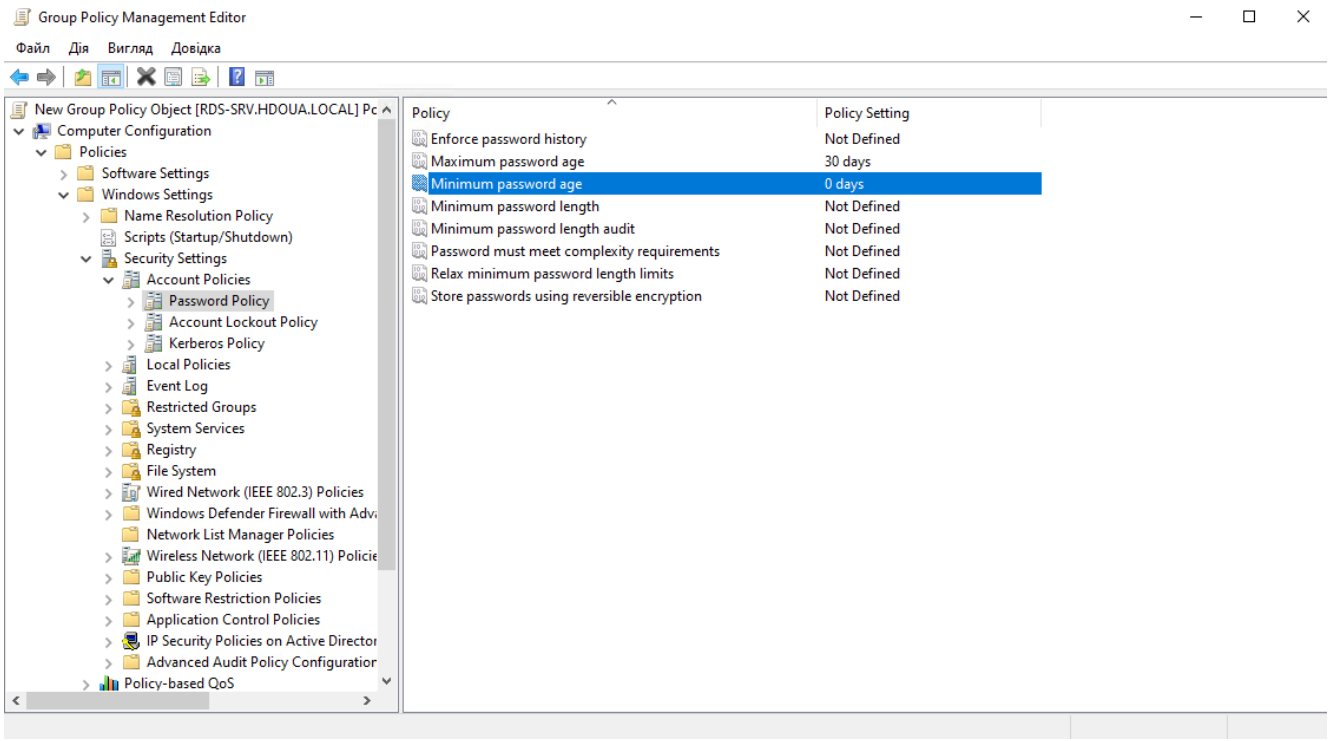


Рисунок 3.18 – політика Мінімальний віку пароля

При оновленні групової політики, необіхдно дочекатися реплікації оновленої політики або скористайтеся командою gpupdate /force. У крайньому випадку, перезавантаження сервера також призводить до негайного оновлення групових політик.

Якщо потрібно дозволити користувачам змінювати або скидати паролі більше одного разу на день, мінімальний вік пароля має бути встановлений на 0.

Відновлення пароля запрацює після успішного оцінювання локальних політик паролів.

Також цю функцію необхідно активувати безпосередньо в програмі Microsoft Entra Connect.

– Необхідно увійти на сервер Microsoft Azure AD Connect і запустити майстер конфігурації Microsoft Azure AD Connect.

– На сторінці Welcome вибрати Configure.

– На сторінці Additional Tasks вибратиCustomize synchronization options і натиснути Next.

– На сторінці Connect to Azure AD ввести обліковий запис глобального адміністратора для тенанта Entra і натиснути Next.

– На сторінках Connect Directories і Domain/OU Filtering натиснути Next.

– На сторінці Optional features встановити прапорець навпроти Password writeback і натисніть Next (рисунок 3.19).

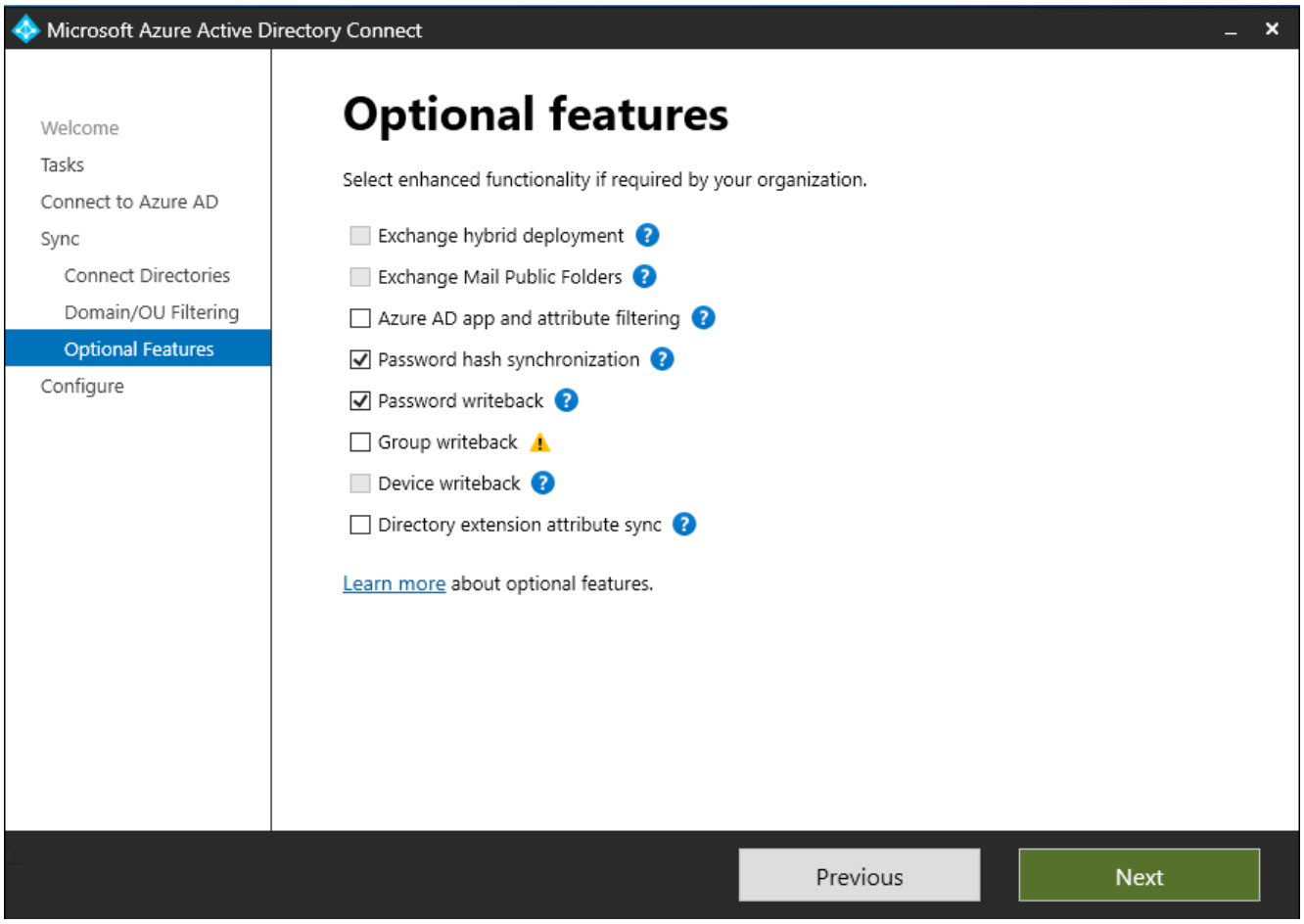


Рисунок 3.19 – Вибір функції Password writeback

– На сторінці Ready to Configure натиснути Configure і дочекатися завершення процесу.

– Коли налаштування буде завершено, натиснути Exit.

Увімкнувши функцію Password writeback у Microsoft Azure AD Connect, необхідно налаштувати цю ж функцію в Microsoft Entra SSPR. SSPR можна

налаштувати на запис за допомогою агентів синхронізації Microsoft Azure AD Connect Sync та агентів забезпечення Microsoft Azure AD Connect. При увімкненні SSPR для використання зворотного запису пароля, користувачі, які змінюють або скидають свій пароль, також синхронізують цей пароль з локальним середовищем AD DS.

Щоб увімкнути запис пароля в SSPR, необхідно виконати наступні кроки.

– Увійти до центру адміністрування Microsoft Entra як глобальний адміністратор.

– Перейти до розділу Protection – Password reset і вибрати On-premises integration.

– Встановити прапорець навпроти пункту Write back passwords with Microsoft Entra Connect cloud sync.

– Встановити прапорець Allow users to unlock accounts without resetting their password (рисунок 3.20).

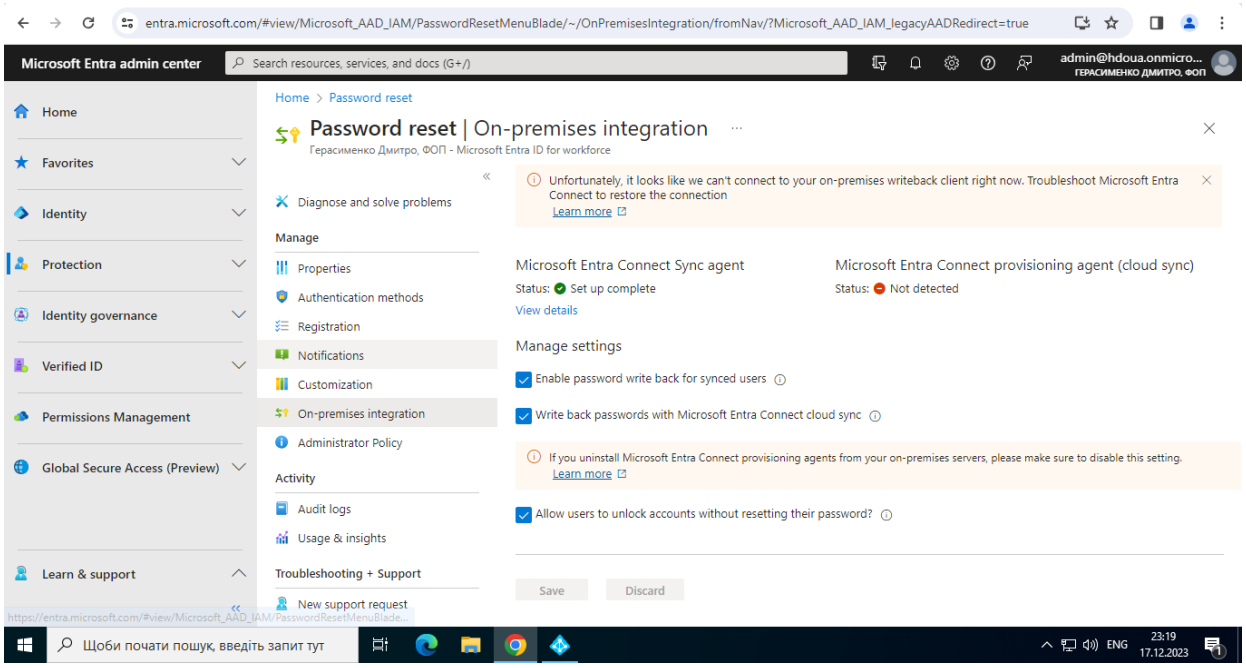


Рисунок 3.20 – вибір функції writeback password в Entra ID SSPR

– По закінченню налаштувань, необхідно вибрати Save.

Після проведення усіх налаштувань, користувачі матимуть можливість змінювати паролі до локальних ресурсів AD DS за допомогою процедури SSPR в хмарному середовищі Microsoft Entra ID.

ВИСНОВКИ

В процесі реалізації методики інтеграції сервісів Microsoft 365 та Azure Active Directory для забезпечення єдиної системи аутентифікації були здійснені налаштування сервера, оренда тенанта Microsoft Azure та впровадження синхронізації даних між локальним каталогом Active Directory та хмарним каталогом Azure Active Directory за допомогою технології Azure AD Connect. Додатково були налаштовані функції самостійного скидання пароля (SSPR), функція єдиного входу (SSO) на основі пароля та функція зворотного запису пароля (passwords writeback).

Впровадження синхронізації даних між локальним Active Directory та Azure Active Directory, з використанням Azure AD Connect, сприяло створенню єдиної точки входу для користувачів у середовищі Microsoft. Це забезпечує консистентність даних та ефективність управління обліковими записами.

Додавання функціоналу SSPR, SSO та passwords writeback покращило безпеку та зручність управління обліковими записами, забезпечуючи користувачам та адміністраторам додаткові інструменти для автоматизації та підвищення продуктивності.

Інтеграція забезпечує однаковий рівень доступу до ресурсів як на локальних, так і на хмарних платформах, забезпечуючи єдність робочого процесу. При цьому велика увага приділена безпеці, забезпечуючи високий ступінь захисту облікових записів та конфіденційної інформації.

Щодо майбутніх напрямків розвитку, важливо розглядати можливості розширення інтеграції з іншими хмарними сервісами, підвищення безпеки та розширення підтримки пристроїв для забезпечення більшої гнучкості та відповідності сучасним вимогам робочого середовища.

Також одним з перспективних напрямків розвитку є можливість створення повноцінної гібридної системи каталогів, вже за допомогою технології Entra Cloud Sync, яка поєднає в собі локальний та хмарний підходи до управління

директоріями. Це створить унікальну можливість використовувати переваги обох середовищ, забезпечуючи гнучкість доступу до ресурсів для користувачів.

Створення гібридної системи каталогів дозволить зберігати чутливі дані локально, забезпечуючи швидкий та надійний доступ, а водночас забезпечить можливість використання переваг хмарних технологій для масштабування та глобального управління.

Підтримка гібридних каталогів також відкриватиме нові можливості для ефективного управління розподіленими командами та ресурсами, надаючи можливість централізованого контролю над інфраструктурою в хмарному середовищі.

Цей напрямок розвитку дозволить налагоджувати баланс між локальною і хмарною інфраструктурою, враховуючи специфіку бізнес-потреб та забезпечуючи оптимальний рівень продуктивності та безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Active Directory Domain Services Overview [Електронний ресурс] – https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

2. Directory System Agent [Електронний ресурс] - https://learn.microsoft.com/uk-ua/windows/win32/ad/directory-system-agent?redirectedfrom=MSDN

3. Active Directory: Designing a Multisite AD DS Administrative Model [Електронний ресурс] - https://archive.org/details/isbn_9780735619173/page/840/mode/2up

4. What is Azure Active Directory (Azure AD) and how does its usage help businesses enhance IT security? [Електронний ресурс] – https://cloud.smart-it.com/news-post/what-is-azure-active-directory-azure-ad/

5. Technet Magazine - Integrating Azure AD with on-premises AD [Електронний ресурс] – https://web.archive.org/web/20200430162954/https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc160894(v=msdn.10)?redirectedfrom=MSDN

6. Introducing Windows Server 2003 Functional Levels [Електронний ресурс] – https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780036(v=ws.10)?redirectedfrom=MSDN#w2k3tr_ad_over_qbjd

7. Installing Active Directory on Windows Server 2012 [Електронний ресурс] – https://docs.rackspace.com/docs/installing-active-directory-on-windows-server-2012

8. The History of Microsoft Azure [Електронний ресурс] – https://techcommunity.microsoft.com/t5/educator-developer-blog/the-history-of-microsoft-azure/ba-p/3574204

9. Microsoft Entra Identity and Access Management [Електронний ресурс] – https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id

10. Microsoft Azure [Електронний ресурс] – https://habr.com/ru/hubs/azure/articles/

11. Microsoft Azure від DataGroup [Електронний ресурс] – https://www.datagroup.ua/b2b/dlya-viddalenoyi-roboty/microsoft-azure

12. Private Cloud Solution з використанням Azure [Електронний ресурс] – http://integritysys.com.ua/solutions/privatecloud-solution-azure/

13. Windows Azure Active Directory [Електронний ресурс] – https://learn.microsoft.com/en-us/shows/windows-azure-active-directory/cartoon

14. Microsoft Entra Pricing [Електронний ресурс] – https://www.microsoft.com/uk-ua/security/business/microsoft-entra-pricing

15. Fundamentals of Microsoft Entra [Електронний ресурс] – https://learn.microsoft.com/en-us/entra/fundamentals/whatis

16. Hybrid Identity - What is Password Hash Synchronization (PHS) [Електронний ресурс] – https://learn.microsoft.com/ru-ru/entra/identity/hybrid/connect/whatis-phs

17. Hybrid Identity - Choosing AD AuthN [Електронний ресурс] – https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn

18. Authentication, Authorization, and Identification Articles [Електронний ресурс] – https://training.qatestlab.com/blog/technical-articles/authentication-authorization-and-identification/

19. Azure AD Connect: How It Works and Best Practices for Synchronizing Your Data [Електронний ресурс] – https://blog.quest.com/azure-ad-connect-how-it-works-and-best-practices-for-synchronizing-your-data/

20. Azure AD Connect Install and Setup Guide [Електронний ресурс] – https://activedirectorypro.com/azure-ad-connect-install-setup-guide/

21. Azure AD Connect - How to Connect Install Prerequisites [Електронний ресурс] – https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-install-prerequisites

22. SSPR: A Tool for Password Management [Електронний ресурс] – https://cloud.smart-it.com/news-post/sspr-a-tool-for-password-management/

23. Azure SSPR User Guide [Електронний ресурс] – https://www.staffs.ac.uk/students/docs/pdf/digital-services/azure-sspr-user-guide.pdf

24. What is AWS SSO (Single Sign-On) [Електронний ресурс] – https://aws.amazon.com/ru/what-is/sso/

25. How works single sign-on [Електронний ресурс] – https://habr.com/ru/companies/nixys/articles/563244/

26. Tutorial: Enable SSPR Writeback in Microsoft Entra [Електронний ресурс] – https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr-writeback

27. Concept: SSPR Writeback in Microsoft Entra [Електронний ресурс] – https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-writeback

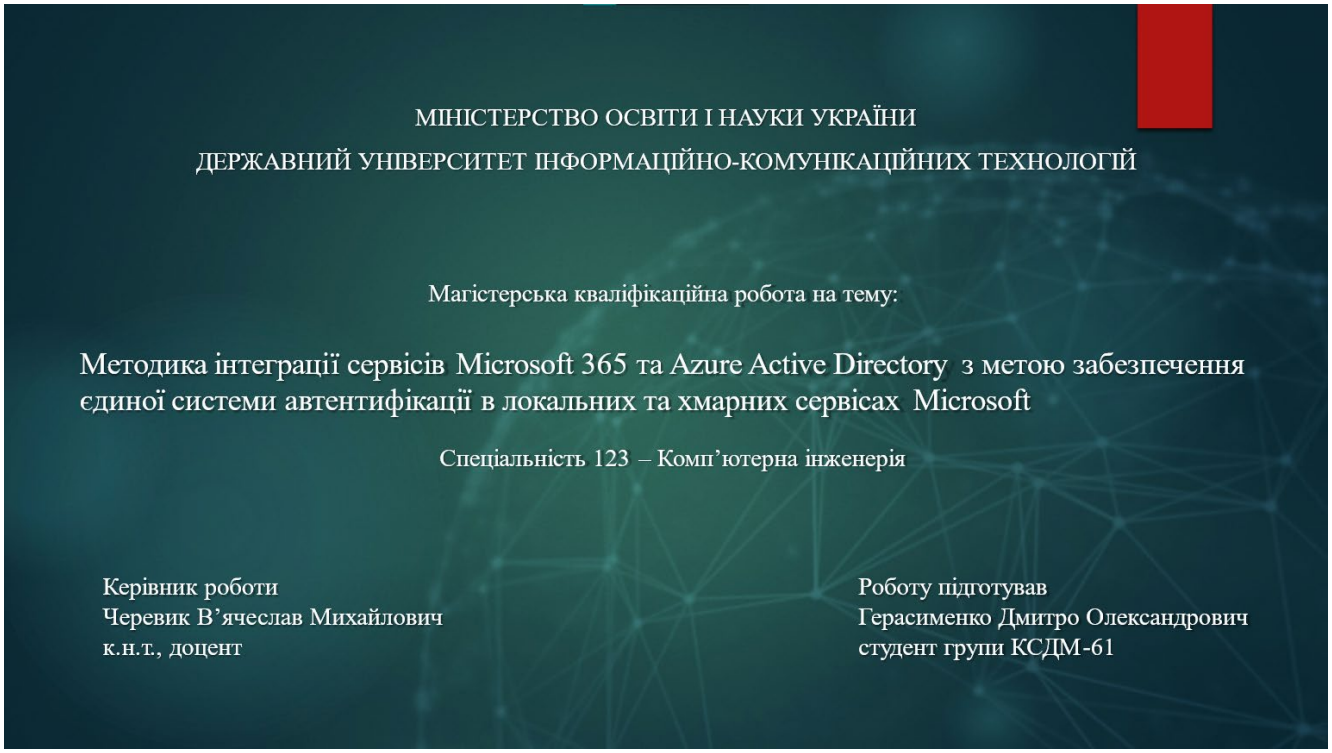
28. How to Enable Password Writeback in Azure AD [Електронний ресурс] – https://www.manageengine.com/products/self-service-password/kb/how-to-enable-password-writeback-in-azure-ad.html

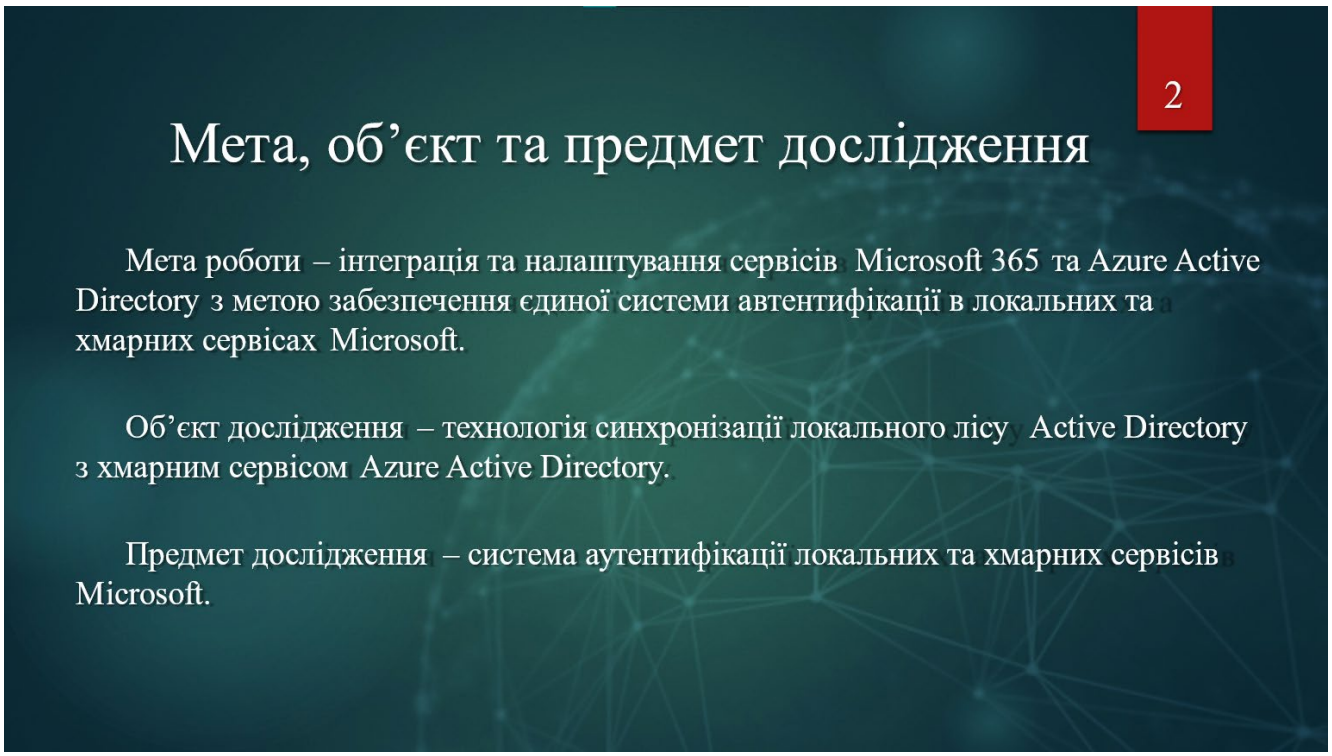
29. What is Azure Password Writeback? [Електронний ресурс] – https://www.xavor.com/blog/what-is-azure-password-writeback/

30. How does the SSPR service relieve your IT department of 20-30% of routine work [Електронний ресурс] – https://cloud.smart-it.com/news-post/sspr-a-tool-for-password-management/

31. Microsoft Entra seamless single sign-on for your Microsoft 365 test environment [Електронний ресурс] – https://learn.microsoft.com/en-us/microsoft-365/enterprise/single-sign-on-m365-ent-test-environment?view=o365-worldwide

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

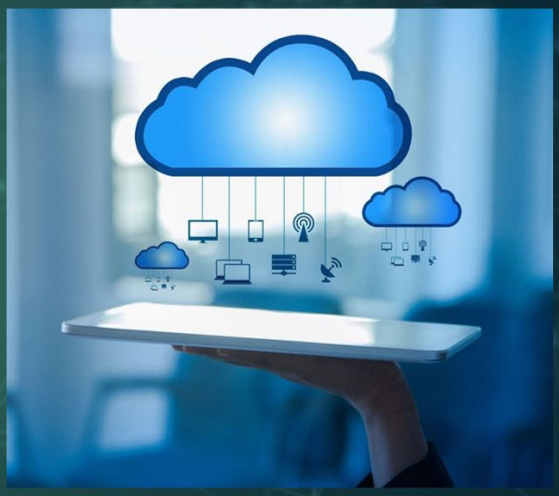




Актуальність дослідження

3

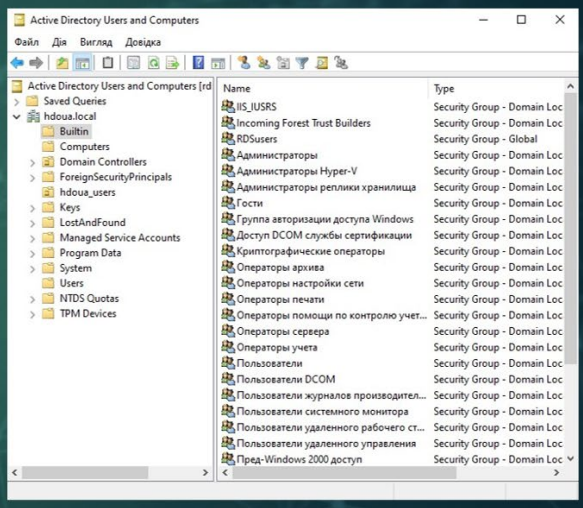
На сьогоднішній день використання хмарних ресурсів стає все більш стратегічно важливим для компаній у зв'язку з швидкою цифровою трансформацією та ростом потреб у гнучкості та мобільності. Azure AD Connect в цьому контексті грає ключову роль, дозволяючи організаціям інтегрувати свої локальні ідентифікаційні системи з хмарним сервісом Azure Active Directory.



Active Directory

4

Active Directory (AD) – це сервіс директорії, розроблений компанією Microsoft, який забезпечує централізоване управління ідентифікацією та доступом користувачів до ресурсів в мережі комп'ютерів у схемі Windows. AD використовується для зберігання інформації про користувачів, групи, комп'ютери та інші ресурси, а також для автентифікації та авторизації в комп'ютерних мережах.

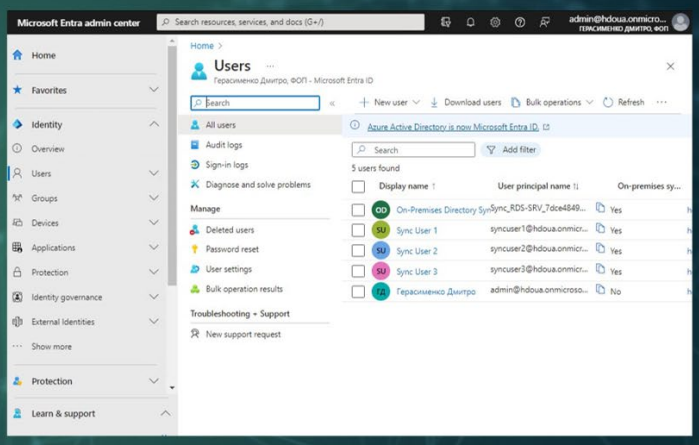


Azure Active Directory

5

Azure Active Directory (Entra ID) – це хмарний сервіс ідентифікації від Microsoft, який забезпечує централізоване управління ідентифікацією та доступом до хмарових та локальних ресурсів. Він включає в себе функції автентифікації, авторизації та синхронізації з локальним Active Directory.

Основна різниця між Azure AD і традиційним Active Directory полягає в тому, щоAzure AD спрямований на хмарні технології та використовується для управління ідентифікацією у хмарових сервісах та за межами традиційної локальної мережі, в той час якActive Directory використовується для управління ідентифікацією на локальних комп'ютерах у схемі Windows.



Тенант Azure AD

6

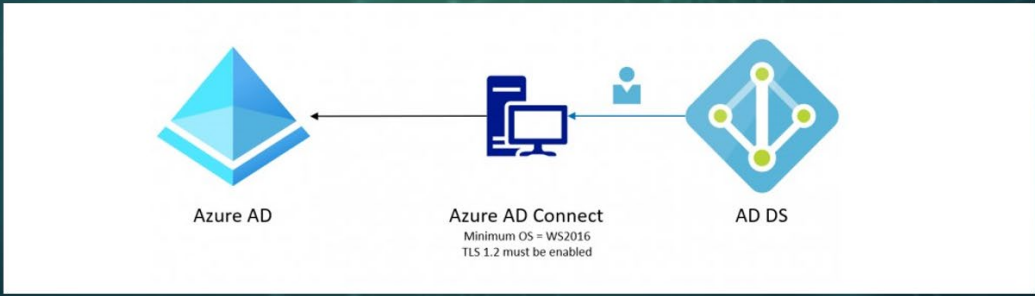
Тенант – це термін, який часто використовується в хмарних обчисленнях, зокрема в сервісах, які надаються хмарними платформами. Тенант вказує на окремий екземпляр сервісу чи програмного забезпечення, який призначений для використання однією конкретною організацією чи користувачем.

У контексті Azure та Azure Active Directory термін "тенант" означає окремий екземпляр Azure AD, який використовується та налаштовується конкретною організацією для управління ідентифікацією та доступом. Кожна організація, яка використовує хмарні сервіси Microsoft, створює свій власний тенант Azure AD, і усі об'єкти (користувачі, групи, застосунки тощо) управляються в межах цього тенанту.

7

Azure AD Connect

Azure AD Connect – це інструмент від Microsoft, який дозволяє забезпечити синхронізацію даних ідентифікації користувачів між локальним Active Directory та Azure Active Directory (Entra ID). Це допомагає створити єдиний ідентифікатор для користувачів у гібридних або хмарових середовищах, полегшуючи управління доступом та ідентифікацією.



8

Передумови інтеграції

Апаратні вимоги

- Процесор з частотою не менше 1.6 ГГц
- Оперативна пам'ять з об'ємом не менше 6 ГБ
- Дискового простору з об'ємом не менше 70 ГБ
- Підключення до мережі Інтернет

Програмні вимоги

- Операційна система Windows Server 2016 або вище з можливостями графічного інтерфейсу
- Підтримка сертифікатів TLS 1.2
- Обліковий запис з правами Адміністратора підприємства
- Тенант Azure AD
- Обліковий запис з правами адміністратора грібридних ідентичностей або вище
- Компоненти PowerShell 5.0 і .NET Framework 4.5.1 або вище

9

Тестове середовище

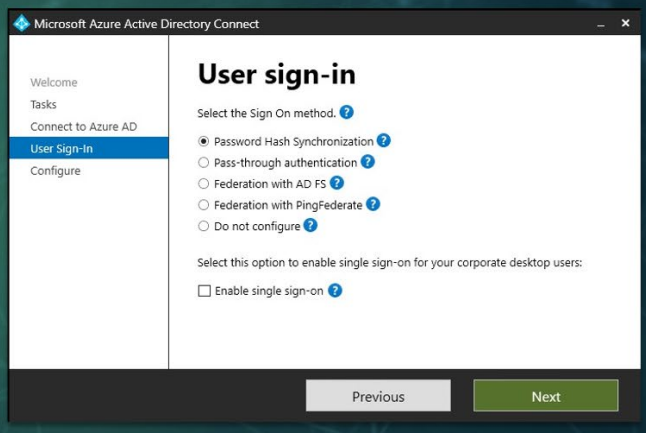
- Віртуальна машина з 4 віртуальними процесорами з частотою 3.8 ГГц кожен, 8 ГБ оперативної пам'яті, 70 ГБ дискового простору, 100 Мбіт/с підключення до Інтернету
- Операційна система Windows Server 2022 з ролями FS, AD DS та RDS
- Домен AD DS hdoua.local
- Тенант hdoua.onmicrosoft.com
- Ліцензії Microsoft 365 Бізнес Стандарт та Entra ID Premium P2.

10

Налаштування синхронізації хешів паролів

Під час синхронізації хешів паролів за допомогою Azure AD Connect, паролі користувачів шифруються та перетворюються в хеші перед відправленням до Azure Active Directory (Azure AD). Застосовується одностороннє шифрування, що означає, що хеш паролю відправляється, але неможливо відновити вихідний пароль з хеша.

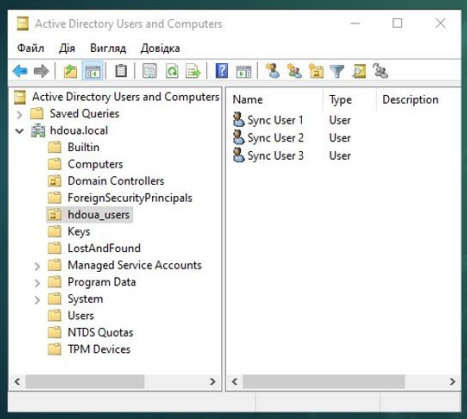
Використовуючи алгоритм шифрування SHA-256, Azure AD Connect створює унікальний хеш для кожного паролю та відправляє його до Azure AD. Це забезпечує безпечний та ефективний механізм синхронізації паролів між локальним Active Directory та Azure AD, забезпечуючи єдиний ідентифікатор для користувачів у гібридних або хмарових середовищах.

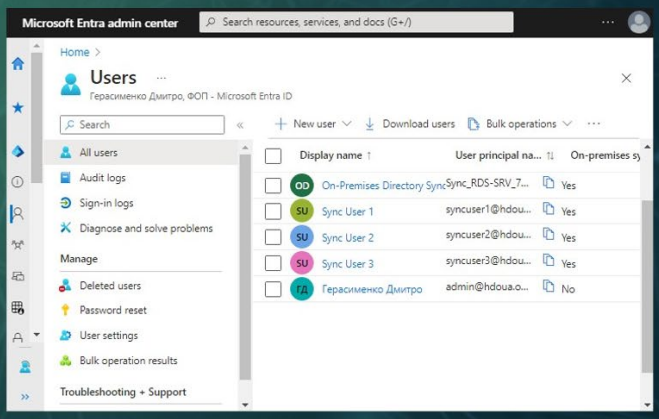


Синхронізація даних між AD та Azure AD

11

Одразу після закінчення налаштування Azure AD Connect, система запускає процес повної синхронізації вибраних груп, користувачів та їх паролів. Після закінчення синхронізації, користувачі зможуть отримувати доступ до хмарних ресурсів Azure та локальних ресурсів AD DS за допомогою одного ідентифікатора.

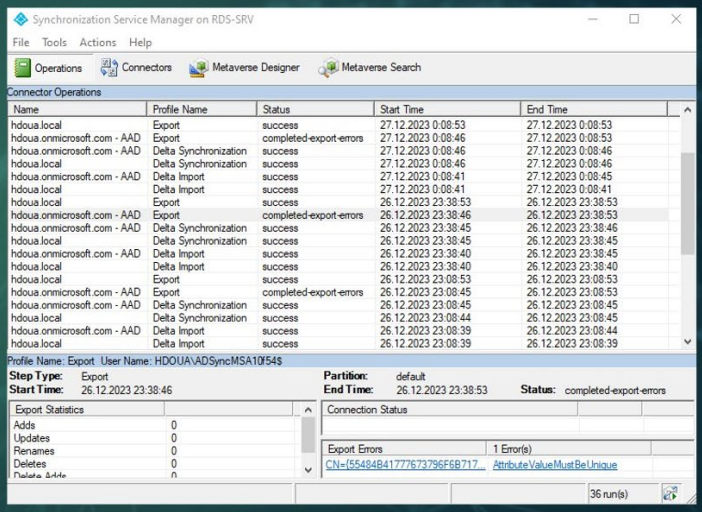




Azure AD Connect Synchronization Service Manager

12

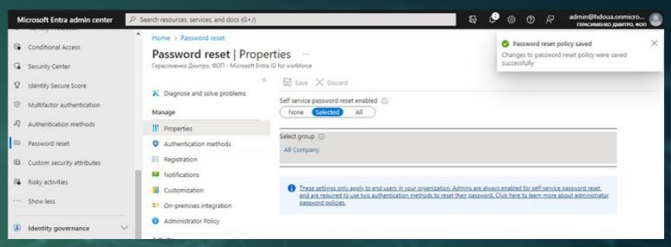
Azure AD Connect Synchronization Service Manager – це інструмент від Microsoft, який входить до складу Azure AD Connect. Він використовується для керування та моніторингу процесу синхронізації між локальним Active Directory та Azure Active Directory (Azure AD). Основні функції Synchronization Service Manager включають моніторинг, керування об'єктами, діагностика помилок та планування синхронізації



Self Service Password Reset

13

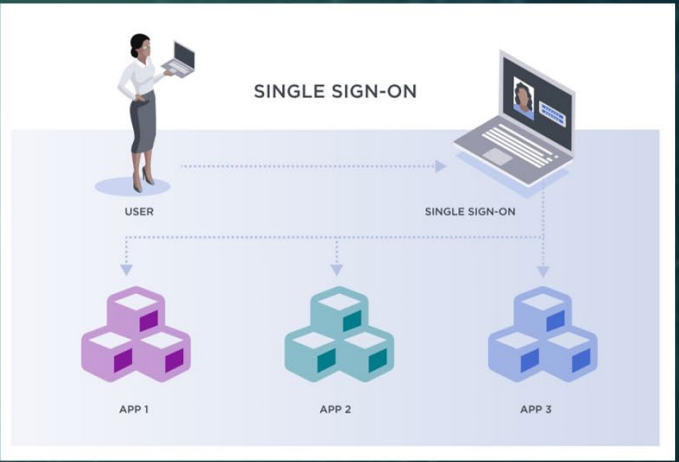
Self-Service Password Reset (SSPR) є інноваційною функцією в області безпеки та ідентифікації, яка дозволяє користувачам самостійно відновлювати чи скидати свої паролі без необхідності звертатися до служби підтримки. Цей функціонал розроблений з урахуванням зручності для кінцевих користувачів та полегшує процес управління паролями в сучасних організаціях. Користувачі отримують доступ до спеціального порталу самообслуговування, де можуть використовувати різні методи аутентифікації, такі як електронна пошта, SMS-повідомлення або питання безпеки, для безпечного та ефективного відновлення доступу до своїх облікових записів. SSPR допомагає зменшити навантаження на IT-підтримку та підвищує безпеку паролів завдяки персоналізованим методам відновлення, забезпечуючи ефективний та зручний процес для користувачів.



Single Sign-On на основі пароля

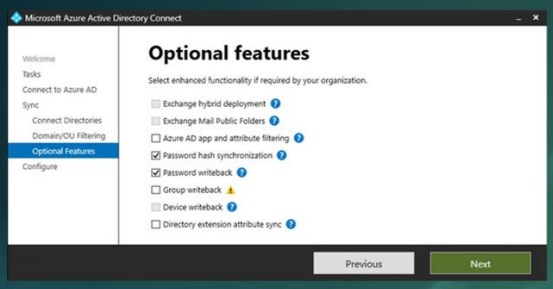
14

Single Sign-On (SSO) на основі пароля - це технологічний підхід, який дозволяє користувачам отримати доступ до різних систем та послуг, використовуючи лише один ідентифікаційний засіб, а саме пароль. У звичайному сценарії, коли користувач вводить свій пароль для автентифікації на одному ресурсі чи сервісі, інформація про автентифікацію зберігається, і користувач автоматично отримує доступ до інших систем, якщо вони підтримують ту саму систему ідентифікації.

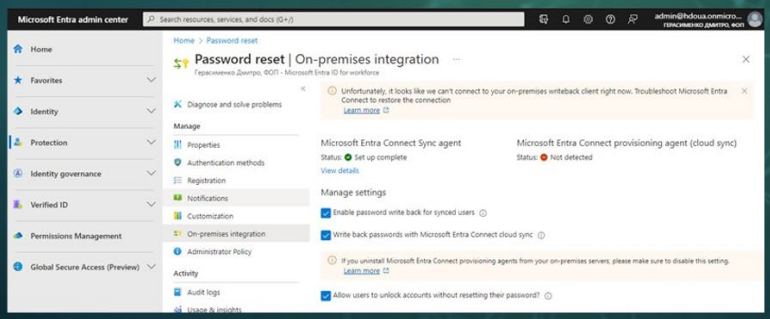


Password writeback

15



Password Writeback в Azure AD Connect - це функціонал, який дозволяє синхронізувати зміни паролів в Azure Active Directory (Azure AD) назад до локального Active Directory. Це особливо корисно в гібридних інфраструктурах, де користувачі можуть змінювати свої паролі через Azure AD, і ці зміни автоматично відображаються у локальному Active Directory. При цьому забезпечується єдина точка управління паролями для користувачів незалежно від того, де вони здійснюють зміни.



За допомогою Password Writeback, організації можуть полегшити управління паролями для користувачів, які працюють як у хмарових, так і у локальних середовищах, сприяючи безпеці та зручності в одному централізованому інтерфейсі.

Переваги використання налаштованої системи

16

Синхронізація хешу паролів

Забезпечує безпеку та консистевність паролів між локальним та хмаровим середовищами, покращуючи управління ідентифікацією.

Self Service Password Reset

Підвищує зручність для користувачів, дозволяючи їм самостійно скидати чи відновлювати паролі, зменшуючи навантаження на службу підтримки.

Password Writeback

Дозволяє синхронізувати зміни паролів з Azure AD назад до локального Active Directory, забезпечуючи єдиний підхід до управління паролями.

Single Sign-On на основі пароля

Забезпечує зручність для користувачів, дозволяючи одноразово увійти до різних систем за допомогою єдиного пароля.

Майбутні напрямки розвитку

17

Щодо майбутніх напрямків розвитку, важливо розглядати можливості розширення інтеграції з іншими хмарними сервісами, підвищення безпеки та розширення підтримки пристроїв для забезпечення більшої гнучкості та відповідності сучасним вимогам робочого середовища.

Також одним з перспективних напрямків розвитку є можливість створення повноцінної гібридної системи каталогів, вже за допомогою технології Entra Cloud Sync, яка поєднає в собі локальний та хмарний підходи до управління директоріями. Це створить унікальну можливість використовувати переваги обох середовищ, забезпечуючи гнучкість доступу до ресурсів для користувачів.

Створення гібридної системи каталогів дозволить зберігати чутливі дані локально, забезпечуючи швидкий та надійний доступ, а водночас забезпечить можливість використання переваг хмарних технологій для масштабування та глобального управління.

Підтримка гібридних каталогів також відкриватиме нові можливості для ефективного управління розподіленими командами та ресурсами, надаючи можливість централізованого контролю над інфраструктурою в хмарному середовищі.

Цей напрямок розвитку дозволить налагоджувати баланс між локальною і хмарною інфраструктурою, враховуючи специфіку бізнес-потреб та забезпечуючи оптимальний рівень продуктивності та безпеки.

Висновки

18

В процесі реалізації методики інтеграції сервісів Microsoft 365 та Azure Active Directory для забезпечення єдиної системи автентифікації були здійснені налаштування сервера, оренда тенанта Microsoft Azure та впровадження синхронізації даних між локальним каталогом Active Directory та хмарним каталогом Azure Active Directory за допомогою технології Azure AD Connect. Додатково були налаштовані функції самостійного скидання пароля (SSPR), функція єдиного входу (SSO) на основі пароля та функція зворотного запису пароля (passwords writeback).

Впровадження синхронізації даних між локальним Active Directory та Azure Active Directory, з використанням Azure AD Connect, сприяло створенню єдиної точки входу для користувачів у середовищі Microsoft. Це забезпечує консистентність даних та ефективність управління обліковими записами.

Додавання функціоналу SSPR, SSO та Passwords writeback покращило безпеку та зручність управління обліковими записами, забезпечуючи користувачам та адміністраторам додаткові інструменти для автоматизації та підвищення продуктивності.