ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ
АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ IAM СИСТЕМ НА ПІДПРИЄМСТВІ НА ПРИКЛАДІ ВПРОВАДЖЕННЯ SOFFID IAM»**

на здобуття освітнього ступеня магістра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

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

_____ Максим БАКЛИКОВ
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ІСДМ-61
Максим БАКЛИКОВ
Ім'я, ПРІЗВИЩЕ

Керівник: Аліна ТУШИЧ
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Доктор філософії (PhD), доцент

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

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем
Ступінь вищої освіти Магістр
Спеціальність підготовки 126 Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою Інженерії програмного забезпечення автоматизованих систем
Каміла СТОРЧАК
«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бакликову Максиму Івановичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Дослідження ефективності застосування IAM систем на підприємстві на прикладі впровадження Soffid IAM
керівник кваліфікаційної роботи Аліна Тушич, доктор філософії (PhD), доцент
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «____» _____ 2023 р. № _____

2. Строк подання кваліфікаційної роботи «_____» _____ 2023 р.

3. Вихідні дані до кваліфікаційної роботи
Системи керування ідентичністю та доступом (IAM)
Технологія віртуалізації Proxmox VE
Науково-технічна література з питань, пов'язаних з обліком ідентифікаційних даних

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Здійснити аналіз процесу обліку ідентифікаційних даних
2. Провести аналіз наявних на ринку IAM рішень
3. Дослідити технології, що застосовуються у сучасних системах IAM
4. Обрати систему IAM та обґрунтувати цей вибір
5. Розробити модель IT інфраструктури для розгортання системи IAM
6. Розробити кроки щодо впровадження системи IAM в існуючу інфраструктуру
7. Провести аналіз отриманих результатів

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання «____» _____ 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз систем керування ідентичністю та доступом, вибір IAM системи для впровадження	25.10.2023-10.11.2023	виконав
2	Вивчення системи віртуалізації Proxmox VE та розробка інфраструктурної моделі	11.11.2023-20.11.2023	виконав
3	Встановлення серверної частини Soffid на віртуальну машину	20.11.2023-01.11.2023	виконав
4	Підключення до Soffid керованих систем – контролера домену та поштового сервера Zimbra	2.11.2023-15.11.2023	виконав
5	Імпорт користувачів з контролера домену в Soffid та аналіз отриманих результатів	16.12.2023-20.12.2023	виконав
6	Розробка демонстраційних матеріалів (презентації)	20.12.2023-25.12.2023	виконав

Здобувач вищої освіти _____ Максим БАКЛИКОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Аліна ТУШИЧ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 126 стор., 90 рис., 6 табл., 20 джерел.

Мета роботи – автоматизувати процес обліку ідентифікаційних даних та керування доступом співробітників до ресурсів компанії за рахунок впровадження в існуючу IT інфраструктуру системи IAM.

Об'єкт дослідження – процес обліку ідентифікаційних даних.

Предмет дослідження – система керування ідентичністю та доступом.

Методи дослідження – технологія віртуалізації Proxmox VE, за допомогою якої була розроблена модель IT інфраструктури підприємства.

Короткий зміст роботи:

У ході роботи над завданням було проаналізовано низку систем керування ідентичністю та доступом, у результаті чого для подальших досліджень була обрана система з відкритим початковим кодом Soffid IAM.

Щоб дослідити ефективність застосування IAM системи на підприємстві була розроблена модель віртуального середовища, що імітує фізичну інфраструктуру підприємства. На віртуальні машини цієї моделі були встановлені компоненти Soffid IAM – консоль та головний сервер синхронізації а також додаткові сервери синхронізації на кожну з керованих систем-сателітів. Також за допомогою цієї моделі були розроблені кроки з перенесення користувачів з контролера домену до системи Soffid.

Зроблено висновки щодо ефективності застосування системи Soffid IAM.

Сфера застосування – адміністрування та кібербезпека

КЛЮЧОВІ СЛОВА: IAM, ІДЕНТИЧНІСТЬ, ДОСТУП, БЕЗПЕКА, АВТОМАТИЗАЦІЯ, ОБЛІК, ІДЕНТИФІКАЦІЯ, АУТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, РЕПОЗИТОРІЙ.

ABSTRACT

Text part of the master's qualification work: 126 pages, 90 pictures, 6 tables, 20 sources.

The aim of this work is to bring all the benefits which Identity and Access Management systems can provide by implementing an IAM system into the existing IT infrastructure

The object of research is the Identity management process.

The subject of research is an Identity and Access Management system.

The research method is the Proxmox VE virtualization technology, which have been used to develop a model of virtual environment.

Summary of the work:

A bunch of Identity and Access Management systems were analyzed, and as a result Soffid IAM system – an open-source, comprehensive, flexible, multiplatform product – was chosen for further research.

In order to investigate the efficiency of IAM system implementation in business, a model of a virtual environment with simulating the enterprise infrastructure was developed.

Soffid IAM components were installed on the virtual machines of this model – Soffid console and the main synchronization server, as well as next synchronization servers for each of the managed satellite systems. Also, the steps to migrate users from the domain controller to the Soffid system were developed using this model.

Conclusions were made regarding the efficiency of Soffid IAM.

Scope of application: administration and cybersecurity

KEYWORDS: IAM, IDENTITY, ACCESS, SECURITY, MANAGEMENT, ACCOUNTING, IDENTIFICATION, AUTHENTICATION, AUTHORIZATION, REPOSITORY.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

2FA	Two-Factor Authentication	Двофакторна аутентифікація
AD	Active Directory	Служба каталогів Microsoft
API	Application Programming Interface	Прикладний програмний інтерфейс
CA	Certification Authority	Центр сертифікації
DNS	Domain Name System	Система доменних імен
ESSO	Enterprise Single Sign-On	Технологія корпоративного єдиного входу
FQDN	Fully Qualified Domain Name	Повноцінне доменне ім'я
GPL	General Public License	Загальна публічна ліцензія
IAM	Identity and Access Management	Керування ідентифікацією та доступом
IDaaS	Identity as a Service	Ідентичність як послуга
IdM	Identity Management	Керування ідентифікацією
IdP	Identity Provider	Постачальник ідентифікаційних даних
IGA	Identity Governance Administration	Адміністративне керування ідентичністю
IRC	Identity Risk and Compliance	Управління ризиками та дотриманням вимог
IT	Information technology	Інформаційні технології
JDK	Java Development Kit	Комплект розробника Java
LDAP	Lightweight Directory Access Protocol	Полегшений протокол доступу до каталогів
MFA	Multi-Factor Authentication	Багатофакторна аутентифікація
PAM	Privileged Account Management	Управління привілейованими акаунтами
SaaS	Software as a service	Програма як послуга
SIEM	Security Information and Event Management	Системи управління
SSL	Secure Sockets Layer	Рівень захищених сокетів
SSO	Single Sign-On	Технологія єдиного входу
TLS	Transport Layer Security	Захист на транспортному рівні
XACML	eXtensible Access Control Markup Language	Розширювана мова розмітки контроля доступу

ВСТУП

На підприємствах з великою кількістю працівників та багатьма сервісами та ресурсами, до яких співробітникам надається персональний доступ (за логіном та паролем) стає актуальним питання обліку ідентифікаційних даних, а також керування рівнями доступу, які отримують співробітники залежно від своїх посад. Основна проблема, з якою постійно стикаються адміністратори великих підприємств, – зробити так, щоб користувачі отримували доступ до необхідних ресурсів, але в жодному разі не мали доступу до конфіденційної інформації, яка їм не потрібна. Ці задачі вирішуються впровадженням на підприємстві системи IAM – Identity and Access Management – системи керування ідентичністю та доступом.

Переваги систем IAM активно досліджують компанії, які власне і розробляють рішення IAM, такі світові гіганти як Microsoft [1] та Oracle [2], а також і невеликі локальні українські як GlobalLogic [3]. Але у відкритих даних цих компаній немає практичних кроків і конкретних рекомендацій щодо процесу впровадження системи IAM.

Крім того, у статтях цих компаній пропонується використовувати системи керування ідентичністю та доступом їх власної розробки, але ці системи, як правило, коштують дуже дорого. Однією з цілей даної роботи було знайти доступну альтернативу дорогим комерційним продуктам з керування ідентичністю та доступом. Питання вартості таких систем особливо актуальне для України, де багато підприємств зазнають фінансових труднощів. Тому акцент був зроблений на користь систем з відкритим початковим кодом, які розповсюджуються за ліцензією GPL – ліцензії на вільне програмне забезпечення.

Основною метою роботи є розробити практичні кроки щодо впровадження системи IAM на працюючому підприємстві. Для досягнення цієї мети було поставлено та вирішено такі завдання:

- здійснити аналіз процесу обліку ідентифікаційних даних;
- провести аналіз наявних на ринку IAM рішень;
- дослідити технології, що застосовуються у сучасних системах IAM;
- обрати систему IAM та обґрунтувати цей вибір;
- встановити та налаштувати серверну частину Soffid IAM;
- підключити до сервера Soffid керовані системи-сателіти на прикладі контролера домену Active Directory та поштового сервера Zimbra;
- проимпортировать користувачів контролера домену до Soffid IAM.

Об'єктом дослідження цієї роботи є процес обліку ідентифікаційних даних. Цей процес дуже важливий, оскільки безпосередньо пов'язаний із кібербезпекою. Це дослідження є актуальним оскільки з обліком ідентичності так чи інакше стикаються і малі і великі підприємства України.

Предметом дослідження є система керування ідентичністю та доступом. Ця система автоматизує процес обліку ідентифікаційних даних. Завдяки впровадженню такої системи підприємство отримує суттєві переваги – такі як автоматичне створення та видалення облікових записів по всіх керованих системах, централізоване управління користувачами, підвищення кібербезпеки та ефективності адміністрування завдяки контролю доступу на основі ролей.

У роботі було використано такий метод дослідження, як створення віртуального оточення з кількох віртуальних машин, що імітують фізичні сервери підприємства. Дане оточення використовувалося для розгортання системи Soffid IAM з подальшим дослідженням результатів роботи даної системи керування ідентичністю та доступом. Цей метод дозволив фіксувати кожен успішний результат дослідження шляхом створення знімка віртуальної машини. І навпаки, у разі невдалого експерименту робилося повернення до попереднього стану віртуальної машини.

Всі кроки в ході роботи над поставленим завданням були записані та описані в даній роботі, оскільки на сьогоднішній день не існує жодного більш-менш чіткого та докладного посібника з встановлення, налаштування та впровадження системи

Soffid IAM в інфраструктуру працюючого підприємства. Єдиним джерелом інформації при встановленні та налаштуванні системи Soffid IAM був сайт розробників [4]. Але на практиці дуже часто виявлялося, що посібники, наведені на їхньому сайті, не завжди актуальні, тому встановлена за інструкцією програма відмовлялася працювати. Доводилося самостійно шукати причини цих помилок і вирішувати проблеми, що виникають. У зв'язку з цим отримані та описані в даній роботі результати є повністю унікальними і претендують на високий ступінь новизни.

У практичному плані ці результати можуть бути застосовані на будь-якому підприємстві України, де є потреба в автоматизації обліку ідентифікаційних даних. Особливо корисною дана робота буде тим закладам, де на даний момент користувачі зберігаються у контролері домену Windows, оскільки в цій роботі докладно описано процедуру імпорту поточних користувачів підприємства із контролера домену до Soffid IAM.

Попередні результати цієї роботи були апробовані на Всеукраїнської науково-технічної конференції «Сучасний стан та перспективи розвитку IOT» яка проходила 7 квітня 2023 року в Києві. Тези на тему «Ефективність застосування IAM системи на підприємстві» було опубліковано у збірнику, присвяченому цій конференції.

1 АНАЛІЗ ПРОЦЕСУ ОБЛІКУ ІДЕНТИФІКАЦІЙНИХ ДАНИХ

1.1 Історія появи систем управління обліковими даними

Уявімо процес організації доступу до IT-ресурсів у компанії без автоматизації. При прийомі на роботу відділ кадрів вносить нового співробітника у облікову систему. Потім інформація про нього потрапляє до IT-відділу. IT-відділ створює обліковий запис у службі каталогів Active Directory, створює для співробітника поштову скриньку. Далі, звернувшись до системного адміністратора, новий працівник отримує доступ до спільних папок, бази даних, інших додатків. Найчастіше системний адміністратор повинен узгоджувати надання того чи іншого доступу з керівництвом.

Якщо в невеликій компанії організація доступу вирішується шляхом прямих комунікацій та новачок протягом дня зможе отримати доступ до всього, що потрібно для роботи, то в географічно розподіленій компанії зі штатом понад 500 осіб на це можуть піти дні.

За кілька років роботи в компанії співробітник буквально "обростає" доступами в різні системи, при цьому він ніколи не просить "відібрати доступ". Якщо у компанії присутні працівники за контрактом або сезонні робітники, то при розторгненні контракту доступ до ресурсів має бути припинено.

У співробітника може змінюватися посада, телефон, прізвище, і ці зміни повинні відображатись відразу у всіх інформаційних системах. За відсутності автоматизації ці зміни доведеться вносити до кожної системи вручну. При зміні посади слід пам'ятати, які ресурси потрібно відібрати, а які надати.

Якщо в компанії декілька інформаційних систем, наприклад, система документообігу, бухгалтерська програма, корпоративна пошта, з'являється

завдання управління паролями. Пароль у кожній системі створюється окремо, і вони можуть не співпадати. Користувачеві важко запам'ятати кілька паролів, і це призводить до того, що вони зберігаються на папері і тим самим компрометуються. Якщо користувач забув пароль або його обліковий запис було заблоковано через неправильно введені дані, йому доведеться звертатися до системного адміністратора і чекати на його допомогу, а доступ йому потрібен негайно.

При звільненні працівника необхідно заблокувати йому доступ до всіх систем компанії і іноді це важливо зробити дуже швидко. Такий процес у масштабах великої організації забирає у IT-відділу багато часу, неминуче призводить до помилок та, як наслідок, фінансових втрат.

1.2 Поняття Identity Management

На сьогоднішній день існує безліч систем, що вирішують подібні завдання. Найчастіше ми зустрічаємо термін Identity Management (IdM), що означає керування обліковими записами або електронними уявленнями користувачів. Але як правило, від IdM-системи вимагається керувати не лише обліковими записами, але й доступом до систем. Тому зазвичай говорячи про IdM, мають на увазі Identity and Access Management (IAM).

Вибір рішень IAM на ринку досить різноманітний. Є рішення, які можна встановлювати на серверах компанії, та рішення, які можна орендувати у форматі хмарного сервісу (Identity as a Service). Можна також розробити свою IAM систему на основі open-source рішень або пропрієтарного програмного забезпечення власної розробки [1].

В інтернеті можна знайти багато статей на тему, що таке IAM і чому так важливо його використовувати. Але в цих статтях справа не доходить до практичних кроків і конкретних рекомендацій, яку саме IAM-систему варто обрати.

Під Identity and Access Management розуміють набір технологій та програмних продуктів, що відповідають задачам управління життєвим циклом облікових записів та управління доступом до різних систем у компанії [2]. Система ідентифікації та управління доступом – це рішення, яке виконує роль ядра, що об'єднує всі дані про співробітника в організації: не тільки ПІБ і унікальний ідентифікатор, але й коли він влаштувався, яку посаду займає, які права має, і, відповідно, до яких систем повинен мати доступ [3].

1.3 Переваги використання IAM

Тепер розглянемо, як виглядає процес створення користувачів на підприємстві з системою IAM.

З появою нового співробітника інформація про нього вноситься лише до однієї облікової системи, а саме – до списку користувачів IAM. Немає необхідності вносити ці дані повторно до інших систем та баз даних. Інформація про цього користувача буде автоматично розповсюджена по всіх керованих системах, що під’єднані.

Далі на основі атрибутів користувача (посада, відділ) IAM системою буде надано доступ даному співробітнику тільки до тих систем та в тому обсязі, які йому необхідно мати згідно із посадою (тобто потрібні для виконання своїх функціональних обов'язків). IAM система може перевіряти значення атрибутів на відповідність правилам та забороняти створення некоректних записів, наприклад,

із незаповненою посадою. Це виключить появу співробітників із неконтрольованим доступом.

Тепер за будь-яких змін достатньо внести їх в одному місці – і вони автоматично будуть відображені у всіх під’єднаних системах. Так, наприклад, користувач, змінюючи свій пароль, автоматично отримує такий самий пароль у всіх системах. При переведенні чи звільненні співробітника система відбирає у нього доступ до всіх керованих систем майже миттєво.

Впровадження системи IAM дає безліч переваг – від посилення кібербезпеки до зниження накладних витрат на супровід.

1.3.1 Захист від порушень безпеки даних

Коли користувачам доводиться входити в кілька програм і багаторазово вводити паролі для доступу до різної інформації, вони зазвичай створюють паролі, які легше вводити і запам'ятовувати. Завдяки таким інструментам автентифікації, як SSO та MFA, користувачам більше не потрібно багато разів вводити один і той же пароль або запам'ятовувати кілька паролів. Ці інструменти знімають з користувача тягар вигадування «складних» паролів для запобігання зламам та інцидентам інформаційної безпеки. Замість цього для входу в систему буде потрібна інформація, яка легко доступна користувачеві, наприклад його відбиток пальця або відповідь на секретне питання, яке відноситься до відомостей, відомих тільки йому. Більшість інструментів SSO та MFA в обов'язковому порядку шифрують дані та використовують хешування для зберігання паролів.

1.3.2 Належний рівень доступу авторизованим користувачам

IAM спрощує відстеження ролей користувачів та їх прав доступу, а також зміну цих ролей по мірі підвищення чи звільнення співробітників. З її допомогою легше зробити так, щоб користувачі отримували доступ до необхідних ресурсів, але в жодному разі не отримували доступ до конфіденційної інформації, яка їм не потрібна.

Системи IAM повинні забезпечувати зручне керування доступами до цифрових ресурсів та при цьому максимально автоматизувати дії, які виконують адміністратори для підтримки системи в актуальному стані. Один із основних способів досягнути такої гнучкості та автоматизації без втрати можливості контролювати доступ – це пов'язати ролі з посадами та ієрархією всередині компанії. Як додаткові параметри також можна використовувати бізнес-підрозділи, регіони, в яких вони розташовані, та інші елементи, щоб підтримувати актуальність доступу до певної інформації.

1.3.3 Збільшення продуктивності

Організація та автоматизація загальних процесів керування ідентичністю та контролем доступу на підприємстві покращить управління життєвим циклом облікових записів та наданого доступу. Автоматизоване надання доступу користувачам при прийомі на роботу, у період адаптації або в процесі внутрішнього переміщення та зміни ролей скоротить витрачений час та зменшить кількість помилок, що безумовно підвищить продуктивність. В цілому, ефективні

можливості IAM покращать взаємодію з користувачем, управління доступом до корпоративних ресурсів та безпеку систем практично без втручання IT персоналу.

1.3.4 Оптимізація ініціалізації та деактивації користувачів

Коли співробітника звільняють або користувач залишає свій обліковий запис бездіяльним протягом тривалого часу, його облікові дані для входу стають потенційним ризиком для безпеки організації. Надійна система IAM дозволить швидко та легко деактивувати користувача та його облікові записи у всіх системах, особливо у разі звільнення співробітника з компанії. Коли користувач має доступ до багатьох різних програм, між останнім днем роботи співробітника та деактивацією його облікового запису може пройти деякий час. IAM дозволяє виконати деактивацію лише одним натисканням, знижуючи ризик порушення безпеки.

1.3.5 Задоволеність користувачів

Процеси IAM спростять процедури щодо кроків, необхідних для запиту, надання та управління доступом до ресурсів, що підвищить задоволеність користувачів.

Використання ефективної системи управління ідентифікацією та доступом має знизити складність процесів для кінцевих користувачів, власників додатків та

системних адміністраторів. Система IAM повинна максимально виключити паперові та ручні процеси. Автоматизація дозволить кінцевим користувачам переглядати свої облікові записи та самостійно керувати ними, наприклад, виконувати скидання пароля. Служби IAM дозволять користувачам вибирати унікальний пароль на свій вибір і спростять запам'ятовування облікових даних. З впровадженням системи єдиного входу на підприємстві, яка синхронізує паролі в кількох системах, користувачеві буде достатньо запам'ятати тільки один пароль. При належній реалізації користування системою керування ідентичністю та доступом має бути простим та інтуїтивно зрозумілим для кінцевого користувача.

1.3.6 Зменшення фінансових витрат

По суті, будь-який бізнес, який інвестує в керування ідентичністю та доступом, інвестує у себе. Незважаючи на те, що багато хто побоюється початкових витрат, вони дуже швидко окупаються. Ці вкладення варто сприймати як унікальну страховку від ризиків. З впровадженням IAM підприємство отримує систему, через яку здійснюється керування доступом до всіх її ресурсів. Оскільки все керування здійснюється безпосередньо з консолі IAM, витрати на підтримку інших систем зменшуються. Це вже є величезна перевага.

По-друге, завдяки безпеці IAM підприємство уникне проблем, з якими воно може зіткнутися, якщо облікові дані співробітника будуть скомпрометовані. За наявності додаткових рівнів безпеки у вигляді другого фактора та неможливості увійти в систему якимось іншим способом, це не призведе до якихось серйозних наслідків. У разі порушення інформаційної безпеки компанії, вона може постраждати фінансово, а також втратити репутацію та своїх постійних клієнтів.

1.4 Компоненти IAM систем

Identity and Access Management – це сукупність політик, процесів та технологій, які дозволяють організаціям керувати цифровими посвідченнями та контролювати доступ користувачів до важливої корпоративної інформації. Основна мета систем IAM – це визначення цифрової ідентичності для кожної людини чи ресурсу. Після того як ця цифрова ідентичність встановлена, її необхідно підтримувати, змінювати і контролювати протягом усього життєвого циклу користувальницького доступу до ресурсу.

Цей процес керування ідентичністю та доступом включає у собі три основні концепції: ідентифікація, аутентифікація та авторизація. Вони тісно пов'язані, але не тотожні. Давайте детальніше розглянемо кожну з ключових концепцій для кращого розуміння.

Ідентифікація – це можливість однозначно ідентифікувати користувача системи або додаток, що виконується в системі. Це можна зробити за допомогою імені користувача, ідентифікатора процесу або чогось іншого, що може однозначно ідентифікувати суб'єкт. Системи безпеки використовують цей ідентифікатор при визначенні того, чи може суб'єкт отримати доступ до об'єкта.

Аутентифікація – це можливість довести, що користувач або програма дійсно є тими, за кого вони себе видають.

Наприклад, розглянемо користувача, який входить до системи, вводячи ім'я користувача та пароль. Система використовує ім'я користувача для ідентифікації користувача. Система аутентифікує користувача під час входу до системи, перевіряючи правильність наданого пароля.

Існує 3 основні методи аутентифікації:

1) фактор знання – те, що ви знаєте – наприклад, пароль або відповідь на секретне запитання;
2) фактор володіння – те, що у вас є – наприклад, посвідчення особи, смарт-карта або токен безпеки;
3) фактор невід'ємності – те, чим ви є – використання біометрії, наприклад, відбиток пальця.

Інструменти аутентифікації IAM можуть включати двофакторну 2-factor authentication (2FA) або багатофакторну multi-factor authentication (MFA) аутентифікацію, які використовують комбінацію вищезгаданих категорій для посилення безпеки – наприклад, ваш пароль та ваш смартфон. Інструменти IAM також можуть включати служби єдиного входу single sign-on (SSO), які дозволяють користувачеві отримувати доступ до всіх програм через один централізований вхід.

Авторизація – це надання чи делегування дозволів певній особі чи групі користувачів. Авторизація виконує решту процесів управління ідентичністю та доступом до ресурсів організації після аутентифікації користувача. Системні адміністратори керують правами доступу користувачів, а система IAM гарантує, що користувачі отримують доступ тільки до тих даних, які абсолютно необхідні для виконання посадових обов'язків. У надійній системі IAM доступ до даних визначається виданою співробітнику роллю, яка налаштована таким чином, що задовольняє всі його робочі потреби.

Резюмуючи, можна констатувати таке: аутентифікація – це те, ким ви є, а авторизація – це те, що вам доступне.

1.5 Технології IAM

В IAM виділяють два різні технологічні підходи:

– технологія корпоративного єдиного входу – Enterprise Single Sign-On (ESSO або просто SSO);
– технологія постачальника ідентифікації – Web SSO, Identity Provider (IdP).

У першому випадку при впровадженні технології на кожен персональний пристрій встановлюють програму-агент ESSO. Коли пристрій включають, ESSO просить користувача пройти ідентифікацію та аутентифікацію з використанням комбінації методів – перевірки пароля, смарт-картки, біометрії.

Після цього користувач може запустити потрібну йому програму. У свою чергу, програма нічого не знає про використання ESSO і під час запуску спробує показати користувачеві екран запиту логіну та паролю. Але агент ESSO перехоплює екран входу і сам підставляє замість користувача його логін і пароль.

Таким чином, користувач отримає надійну ідентифікацію/аутентифікацію при вході в пристрій, а також зручний автоматичний вхід до всіх інформаційних систем компанії. Але такий підхід зумовлений так званим обманом додатків. Вхід в них за допомогою логіну/паролю в обхід запущеного агента ESSO як і раніше можливий, отже, зберігається багато загроз, що властиві парольної аутентифікації, і це, безумовно, недолік.

Є ще один важливий момент у використанні ESSO – обмеженість пристроїв, на яких можливе встановлення агента. Можуть виникнути проблеми з підтримкою Linux, MacOS, iOS чи Android.

Другий технологічний підхід – впровадження IdP. Цей підхід позбавлений недоліків ESSO. Користувач може використовувати будь-які пристрої, а для роботи достатньо веб-браузера. В якості пристроїв можуть застосовуватися не тільки ПК та смартфони, а й голосові станції, ігрові приставки і навіть Smart TV.

Розплатою за таку гнучкість стає необхідність підтримки з боку програм можливості підключення до IdP. Іншими словами, додаток має підтримувати будь-який стандарт взаємодії з IdP. Але більшість популярних додатків та хмарних сервісів вже вміють це робити, тому це не є недоліком.

При використанні IdP користувач звертається до програми, а вона замість відображення свого екрана входу надсилає серверу запит на ідентифікацію. Якщо IdP вже знає користувача, то відбувається перевірка дозволу на вхід до програми та реєстрація факту відвідування. Після цього дані про користувача, що отримані з каталогу облікових записів компанії, повертаються до додатка. Якщо ж IdP не знає користувача, то попросить його спочатку пройти ідентифікацію та аутентифікацію. Замість простої перевірки логіну/паролю IdP може використовувати додаткові методи аутентифікації, в залежності від контексту входу та політики доступу. Наприклад, при вході до програми з робочої мережі користувач може бути автоматично ідентифікований за результатами перевірки в домені (технологія Kerberos SSO). Якщо ж користувач хоче зайти в якусь дуже важливу програму або, наприклад, здійснює вхід з мережі інтернет з незнайомого пристрою, то IdP може запросити додаткового підтвердження – запропонувати ввести разовий пароль, надісланий по SMS, або згенерований мобільним додатком разових паролів.

2 АНАЛІЗ ТА ВИБІР СИСТЕМИ КЕРУВАННЯ ІДЕНТИЧНІСТЮ

2.1 Вибір системи IAM

Згідно з підсумковим звітом саміту Gartner з керування ідентичністю та доступом, до 2025 року 75% постачальників послуг кіберстрахування вимагатимуть використання принципів своєчасного управління привілейованим доступом. Також за даними Fortune Business Insights прогнозується значне зростання ринку IAM, починаючи з 12,26 млрд. доларів США в 2020 році до приблизно 34,52 млрд. доларів США у 2028 року. Це демонструє, наскільки серйозно організації ставляться до IAM і що кібербезпека вступає в епоху, коли ідентифікація стоїть на першому місці.

Сьогодні на ринку є досить багато систем IAM – як від маловідомих розробників, так і від таких гігантів цифрової індустрії, як Microsoft[5] і Oracle[6]. Більшість із них мають хмарну структуру, коли база даних і вся система управління ідентифікаційними даними знаходяться на хмарних сервісах – тобто на серверах компанії-розробника, що пропонує свій програмний продукт. Плюсом таких хмарних рішень є те, що вам не потрібно мати свій власний сервер і займатися його обслуговуванням, проте суттєвий мінус полягає в тому, що такий сервіс не буває безкоштовним і за його використання доведеться платити щомісячну абонплату. Вартість такої системи відрізняється і розраховується, як правило, виходячи з кількості унікальних користувачів (співробітників компанії).

Іншим варіантом систем IAM, який можна знайти на ринку, є рішення, що встановлюються безпосередньо на сервер підприємства. Мінусом таких рішень є те, що як мінімум необхідно мати сервер для встановлення програмного забезпечення. Крім того, налаштування та впровадження IAM системи також

швидше за все доведеться здійснювати власними силами, звертаючись за допомогою до розробників, якщо виникають труднощі. Плюсом таких рішень є те, що більшість таких продуктів поширюється за ліцензією GPL, що робить їх по суті безкоштовними.

Наведемо приклади як одних, так і інших варіантів рішень.

2.1.1 Хмарні рішення IAM

JumpCloud – це хмарне рішення на платформі Open Directory, яке підключає співробітників організації практично до будь-якого ресурсу, а також налаштовує та захищає їх віддалені пристрої, де б вони не працювали.

За допомогою JumpCloud адміністратори можуть забезпечити автоматичну реєстрацію для надання користувачам та пристроям у будь-якій точці світу автоматизованих робочих процесів із єдиної веб-консолі. Вони можуть реалізувати адаптивний безпечний віддалений доступ, щоб вимагати MFA при вході в систему до цінних та конфіденційних ресурсів, та послабити MFA для звичайних робочих процесів користувачів, коли вони отримують доступ до повсякденних ресурсів з довірених пристроїв та мереж. JumpCloud дозволяє адміністраторам реалізувати можливості безпеки Zero Trust, які гарантують, що користувачі зможуть отримувати доступ тільки до тих ресурсів, що їм потрібні, і лише з довірених пристроїв та мереж.

Thales – світовий лідер у галузі високих технологій – надає рішення, продукти та послуги, які дозволяють клієнтам зміцнити свій захист, ставлячи людей у центр процесу прийняття рішень. Компанія Thales вивела на ринок своє інноваційне рішення для управління доступом SafeNet Trusted Access, яке є

хмарним рішенням з інтегрованою платформою, яка плавно поєднує єдиний вхід, політики, засновані на ризиках, та універсальні методи аутентифікації, не порушуючи при цьому гнучкості та зручності використання для користувачів.

Рішення забезпечує спрощену аутентифікацію та керування доступом, максимально спрощує доступ користувачів до хмарних сервісів та звільняє від необхідності використовувати паролі. Важливі функції цього рішення включають багатофакторну сучасну аутентифікацію, простий доступ до хмари за допомогою Smart Single Sign-On, гнучку політику доступу на основі сценаріїв, детальні політики доступу для оптимальної безпеки та безпечний доступ для підрядників і партнерів. Thales пропонує єдину панель перегляду подій доступу до всіх ресурсів, забезпечуючи чітке уявлення та гарантуючи, що потрібним людям буде надано доступ до потрібних програм у потрібний час. Дотримання вимог спрощується, оскільки рішення забезпечує прозорість всіх подій доступу і, будучи хмарною службою, також може швидко розгортатися та легко масштабуватись по мірі розвитку потреб організації.

Okta – провідний постачальник послуг керування ідентичністю та доступом. Компанія пропонує службу IAM корпоративного рівня, розроблену для хмари, але сумісну з низкою локальних програм. Понад 10 000 організацій по всьому світу мають досвід використання Okta для управління особистими даними своїх співробітників та клієнтів. Okta Workforce Identity забезпечує захист цифрових облікових записів для глобальних команд, підтримуючи як безпечні хмарні додатки, так і гібридні середовища. Okta також підтримує спеціально створені додатки та надає користувачам єдиний доступ до всіх корпоративних облікових записів без пароля, що призводить до покращення огляду та контролю.

Функції Okta Workforce Identity включають безпечний інтелектуальний доступ для співробітників та клієнтів за допомогою єдиного входу та багатофакторної аутентифікації, а також розширений доступ до сервера та універсального каталогу, в якому розміщуються всі користувачі, групи та пристрої. Okta надає адміністраторам комплексну панель управління, де вони можуть

керувати внутрішніми та зовнішніми користувачами та переглядати докладні звіти. Okta також забезпечує управління життєвим циклом, що дозволяє вам легко керувати доступом за допомогою автоматизації, шлюз доступу, який розширює можливості локальних додатків, але захищає хмару та керування доступом за допомогою API.

Oracle – американська багатонаціональна компанія комп'ютерних технологій, одна з найбільших у світі компаній-розробників програмного забезпечення за доходами та ринковою капіталізацією. Компанія найбільш відома як постачальник програмного забезпечення та технологій баз даних, хмарних систем та корпоративних програмних продуктів у сферах людського капіталу, взаємовідносин та безпеки. Oracle Cloud (OC IAM) – це хмарне рішення IDaaS, яке забезпечує всебічне охоплення варіантів використання ідентичності та доступу для співробітників, партнерів та споживачів.

Oracle Cloud Identity and Access Management — це рішення, яке пропонує високоадаптивні політики та можливості доступу, які підтримують численні IT-програми та сервіси, а також дозволяють швидко підключати користувачів та сервіси. Ключові особливості цього рішення IAM включають гнучкий вхід в систему з різними варіантами аутентифікації, просте адміністрування користувачів і доступ за допомогою зручних для розробників API і прикладів коду, вбудовані функції звітності та аудиту активності та ризиків, а також широке та гнучке охоплення додатків. Це рішення дозволяє створювати групи користувачів та керувати ними з консолі адміністратора, призначати доступ до програм, а також надає панель моніторингу для швидкого доступу до додатків. Oracle IAM надає користувачам можливість керувати доступом і правами в різних хмарних та локальних програмах. Платформа працює відповідно до стратегії нульової довіри, яка висуває на перший план ідентифікацію як ключовий механізм контролю безпеки для сьогоденних IT-середовищ.

Azure Active Directory (Azure AD) — це хмарна служба керування ідентичністю та доступом від Microsoft, яка допомагає співробітникам входити до

своїх облікових записів та отримувати доступ до ресурсів, необхідних для Office 365 та підключених додатків. Цей продукт управляє ідентифікаційними даними загальною кількістю більш ніж 1,2 мільярда по всьому світу і щодня обробляє понад 8 мільярдів аутентифікації.

Microsoft Azure AD дозволяє користувачам O365 реалізувати єдиний вхід, який спрощує доступ до підключених додатків та автоматизує робочі процеси життєвого циклу користувача. Це рішення забезпечує підвищену безпеку облікового запису за допомогою багатофакторної аутентифікації, яку можна реалізувати через мобільний додаток Microsoft Authenticator. Адміністратори можуть легко інтегрувати своїх користувачів у сторонні програми та служби за допомогою Azure та зручних інструментів розробки на основі API. Завдяки використанню Microsoft Azure AD організації можуть ефективніше захищати облікові дані користувачів за рахунок застосування суворої політики аутентифікації та умовного доступу, а також безпечно керувати ідентичністю, гарантуючи, що ключові дозволи надаються лише відповідним користувачам. Azure AD інтегрується з тисячами програм SaaS, і адміністратори можуть легко застосовувати політики умовного доступу зі своєї панелі моніторингу O365 для консолідації та захисту доступу до облікових записів.

2.1.2 On-premise рішення

WSO2 Identity Server – це сервер ідентифікації з відкритим початковим кодом, який пропонує повне рішення для керування ідентичністю та доступом для забезпечення належного рівня безпеки в мережі підприємства. Цей менеджер ідентичності обслуговує систему єдиного входу з багатофакторною

аутентифікацією, яка дозволяє користувачам отримувати доступ до внутрішніх ресурсів із різних додатків та пристроїв, ввівши облікові дані лише один раз.

WSO2 також надає інтерфейс користувача для входу, який працює окремо як веб-додаток і може бути змінений за потреби. Це рішення керування ідентифікаційним доступом пропонує консоль управління, де адміністратор може створювати користувачів з унікальними ролями. Крім того, ця об'єднана система управління ідентичністю є абсолютно безкоштовною, з відкритим початковим кодом, яка працює з багатьма службами, додатками та включає підтримку API. Система має комплексну документацію, що стосується робочого процесу, розробки та розгортання. WSO2 написаний в основному на Java з використанням інших мов, таких як JavaScript та HTML.

Keycloak – це продукт з відкритим початковим кодом для реалізації єдиної точки аутентифікації та авторизації. Keycloak підтримує SSO Single-Sign-On, кілька протоколів – OpenID Connect, OAuth 2.0, SAML 2.0, вхід із соціальних мереж, а також підтримує LDAP і Active Directory. Він також підтримує спеціальні політики паролів.

Keycloak має клієнт-серверну інфраструктуру. Його можна розширювати, щоб додавати нові корисні функції за допомогою власних кваліфікованих розробників. Keycloak містить добре написану документацію та спільноту, яка зростає з кожним днем.

2.2 Обґрунтування вибору Soffid IAM

Серед усього різноманіття доступних на ринку систем IAM важливо зробити правильний вибір. У процесі роботи над цим проектом були розглянуті різні системи, як платні, так і безкоштовні, проте перевага надавалася вільно

розповсюджуваному програмному забезпеченню. В результаті був обраний продукт іспанської компанії-розробника – Soffid IAM.

Soffid є цілою платформою ідентифікації, яка об'єднує управління доступом (AM), керування ідентичністю (IGA), управління ризиками та дотриманням вимог ідентифікації (IRC) та управління привілеями (PAM) на одній комплексній платформі та з єдиною інформаційною панеллю. Основна ідея компанії – це забезпечення безпеки та продуктивності на одній платформі.

Розглянемо кожен із основних напрямків платформи трохи докладніше.

2.2.1 Управління доступом (Access Management)

У сучасному корпоративному середовищі непросто знайти баланс між безпекою та зручністю в управлінні доступом користувачів до спільних ресурсів.

Access Management є основою, яка усуває потребу у кількох паролях, профілях користувачів та додаткових труднощах, які дратують користувачів та уповільнюють роботу з додатками. Доступ до корпоративних програм повинен бути безпечним, але при цьому простим, швидким та точним. Це саме те, що забезпечує Access Management від Soffid.

Основні компоненти Access Management:

- Корпоративний єдиний вхід (ESSO). Повністю кероване корпоративне рішення для єдиного входу, яке підвищує безпеку технологічних ресурсів і водночас знижує експлуатаційні витрати, спричинені втратою паролів, затримками аутентифікації або зміною адреси.
- Єдиний вхід для Web додатків (WSSO). Це універсальний веб-модуль єдиного входу, який автоматизує процес веб-аутентифікації та забезпечує центральну точку для розгортання корпоративних веб-додатків. Модуль

XACML забезпечує дуже детальний контроль доступу навіть для застарілих програм.

– Портал самообслуговування. Це унікальний та універсальний веб-інтерфейс, за допомогою якого кінцевий користувач може переглядати або змінювати свої облікові дані, керувати бізнес-процесами, керувати своїм профілем або запускати програми. Усі дії виконуються з однієї точки входу. Це істотна перевага, завдяки якій забезпечується зручність та простота використання і, як наслідок, максимальна продуктивність.
– Єдиний каталог. Ця функція гарантує, що всі сховища паролів (джерела авторизації) завжди синхронізуються між собою. Вона забезпечується механізмом синхронізації Soffid та повністю прозора для кінцевого користувача.

2.2.2 Identity Governance Administration (Керування ідентичністю)

Дуже важливо швидко надати співробітникам компанії необхідні інструменти та додатки, де б вони не знаходилися. За допомогою Soffid надання доступу користувачам стає простим та безпечним. Це допомагає уникнути надлишкових дозволів, автоматично регулюючи чи видаляючи доступ користувачів по мірі зміни їхнього статусу, допомагаючи знизити ризики та водночас підвищити відповідність вимогам та продуктивність. Управління користувачами здійснюється через конектори, чи агенти. Ці агенти діють як міст між Soffid та іншими системами, де є репозиторії користувачів.

Soffid має набір стандартних конекторів, які забезпечують дуже просту інтеграцію з найбільш популярними репозиторіями, включаючи каталоги LDAP,

MS Active Directory, реляційні бази даних, а також найбільш поширені операційні системи.

До системи керування ідентичністю входять:

– Автоматичне створення користувачів (User Provisioning). Автоматичне створення користувачів здійснюється через конектори або агенти, які з'єднують Soffid із керованими системами. Ці агенти можуть діяти будь-яким способом: або створюючи чи змінюючи облікові записи користувачів в керованій системі, або реєструючи існуючі облікові записи користувачів в репозиторії Soffid.
– Управління ролями. Хоча з технічної точки зору ролі належать до репозиторію, з організаційної точки зору вони належать до додатків або до інформаційних систем. Для кожної інформаційної системи визначено відповідні ролі, а для кожного додатка – список відповідальних осіб.
– Двигун бізнес-процесів. Soffid має, розширює та покращує двигун JBPM jBoss. Завдяки цьому унікальному механізму Soffid дозволяє керувати потоками прийняття рішень.
– Атестація. Атестація передбачає наявність інструментів для перевірки та підтвердження поточного статусу та наданих прав доступу. Для цього існує перевірка ролі (власник додатку перевіряє дозволи, надані кожній ролі додатка) та призначення ролей (керівник відділу перевіряє набір дозволів, які мають бути надані кожному користувачу в його відділі, а відповідальний за додаток перевіряє набір дозволів, наданих користувачам зазначеного додатку).
– Звітність. Soffid підтримує створення звітів з кількох точок консолі, пов'язаних як з ідентичністю, так і з авторизацією, подіями, аудитом та іншим. Будь-який звіт можна експортувати у вигляді електронної таблиці одним натисканням миші.

2.2.3 Identity Risk & Compliance (Ризики та дотриманість вимогам)

Деякі спеціальні облікові записи, облікові дані та секрети дозволяють будь-кому, хто ними заволодіє, контролювати ресурси організації, відключати системи безпеки та отримувати доступ до величезних обсягів конфіденційних даних. Такі повноваження можуть забезпечити необмежений доступ, тому не дивно, що внутрішні аудитори та нормативні акти встановлюють особливі вимоги до контролю та звітності щодо використання цих облікових даних. Взаємопов'язані IT-системи оптимізують бізнес-процеси, але можуть неправильно трактувати ризики, які необхідно виявляти, аналізувати та відстежувати відповідно до концепції корпоративного управління ризиками та дотриманістю вимогам (англ. Governance, Risk, and Compliance – GRC). Soffid оснащений всім необхідним для цього функціоналом – керування привілейованими обліковими записами, створення записів з низьким рівнем доступу, розподіл функцій, а також процеси повторної сертифікації.

Інтелектуальна аналітика Soffid постійно відстежує та виявляє нові ризики доступу, забезпечуючи комунікацію між інформаційними системами із застосуванням концепції GRC, допомагаючи менеджерам з ризиків створювати цілісні стратегії управління ризиками підприємства.

В цьому беруть участь наступні підсистеми:

– Аудит. Всі дії, що виконуються, зберігаються в базі даних Soffid. Цю інформацію можна отримати за допомогою самого Soffid або будь-якого зовнішнього програмного забезпечення. Система аудиту може бути підключена до зовнішньої системи, наприклад, до системи управління подіями безпеки (Security Information and Event Management – SIEM) для здійснення більш складного аналізу чи під’єднання системи сповіщення.
– Обмежені облікові записи. Soffid дозволяє певним користувачам створювати та змінювати інші облікові записи, користувачів, групи,

додатки, ролі тощо в залежності від їх ролі в організаційному підрозділі або наданих їм ролей. При цьому схема дозволів обмежує коло користувачів, облікових записів, груп або ролей, до яких можуть звертатися інші користувачі. Додатково може бути підключений модуль XACML (eXtensible Access Control Markup Language – Розширювана мова розмітки контроля доступу) для визначення політики управління на основі атрибутів.

- Role Mining (Інтелектуальний аналіз ролей). Модуль інтелектуального аналізу ролей Soffid застосовує методи інтелектуального аналізу даних для створення бізнес-профілів на основі наданих на даний момент дозволів. У цьому контексті інструмент дозволяє адміністратору вибрати стратегію, яка найкраще відповідає його потребам: профілі з високим ступенем модифікації, загальні або збалансовані профілі. Інтелектуальний аналіз ролей мінімізує витрати на адміністрування та керування обліковими записами, і пропонує, які ролі вам слід використовувати, а від яких варто відмовитися.
- Федерація. Федерація дозволяє інтегрувати Soffid із найбільш популярними хмарними службами без необхідності передавати паролі зовнішнім постачальникам. Він сумісний з федерацією SAML, а також з OpenID.
- Переатестація. Soffid керує всім процесом створення нових сертифікатів для обраних додатків чи користувачів та ідеально інтегрується в систему робочого процесу Soffid. Це дозволяє спростити складний процес та підвищити продуктивність компанії без шкоди для її безпеки.

2.2.4 Privileged Account Management (Управління привілеями)

Потреба у привілейованих облікових записах є загальною для більшості інформаційних систем. Ці облікові записи необхідні для виконання запланованих завдань по налаштуванню та обслуговуванню, а також раптових завдань, таких як відновлення апаратного або програмного збою або відновлення резервної копії. Саме у зв'язку з необхідністю використання цих облікових записів позапланово, керування ними має поєднувати в собі безпеку, визначеність та гнучкість.

Для ефективного управління цими обліковими записами продукт Soffid має необхідну логіку для ідентифікації акаунтів, їх класифікації за рівнем ризику та схемою використання, розподілу та наданням відповідальним користувачам, автоматичного чи планового процесу зміни паролів, процесу доставки паролів авторизованим користувачам та автоматичному впровадженню паролів, коли таке застосування має сенс.

Привілейовані облікові записи можуть використовуватися більш ніж однією людиною, однак PAM гарантує, що тільки одна людина може використовувати такий обліковий запис у будь-який момент часу. Це дозволяє завжди ідентифікувати, хто зробив ті чи інші зміни у системі, а також хто і коли володів цими правами.

За високих вимог до безпеки агенти Soffid повинні встановлюватися на кожній керованій системі, підвищуючи безпеку системи в цілому. З точки зору безпеки та аутентифікації зв'язок між основним сервером та сервером синхронізації керованого хоста використовує взаємну аутентифікацію та шифрування TLS.

Soffid підключатиметься до цільової системи кожного разу, коли потрібна інформація про існуючі облікові записи, треба створити новий акаунт чи відключити старий. Але це можна зробити двома різними способами: з локальним агентом або без нього.

2.3 Етапи впровадження IAM системи

Найчастіше завдання можуть здаватися складними, якщо зосередитися на загальній картині, і впровадження IAM у цьому сенсі нічим не відрізняється. Успішні проекти IAM використовують поступовий методичний підхід до реалізації та розбиваються на п'ять основних етапів: аналіз, архітектура, реалізація, тестування та перехід до підтримки (рис. 2.1).

Поетапний підхід до проектів управління ідентичністю дозволяє компанії поділити реалізацію на керовані частини. На кожному етапі умови, витрати, графік та результати чітко визначені, і всі сторони приходять до згоди перед переходом до наступного етапу.

Типовий приклад поетапного підходу до проектів комплексного керування ідентичністю включає розгортання рівня служби каталогів, за яким йде рівень управління доступом та наступний рівень надання привілеїв.

Впровадження поетапного підходу до рішення з управління ідентичністю та доступом дозволяє організаціям отримати негайну віддачу від своїх інвестицій, зберігаючи при цьому гнучкість для зміни курсу у разі потреби.

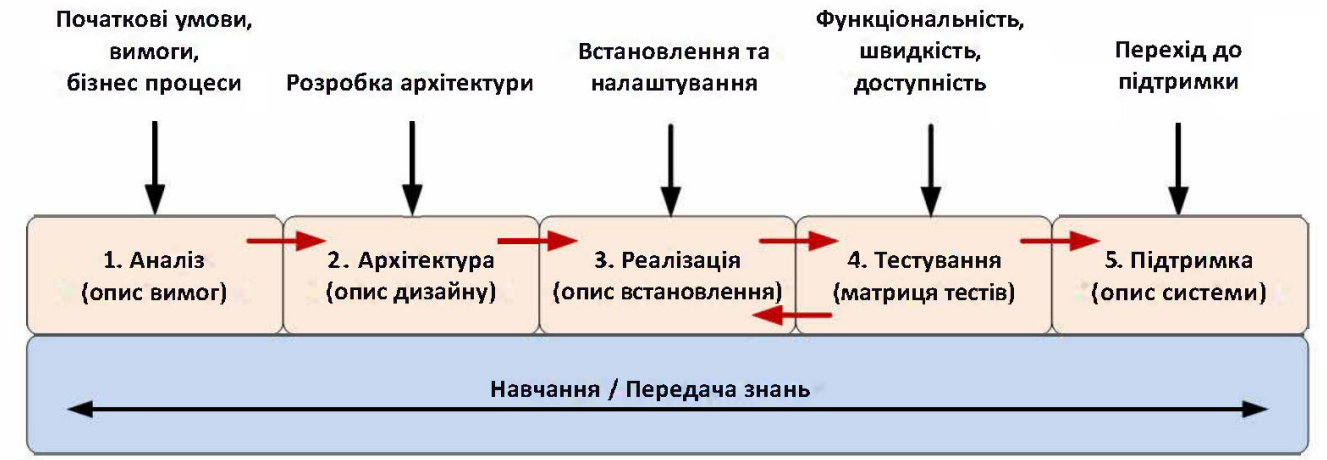


Рисунок 2.1 Етапи впровадження IAM системи

Більшість рішень з управління ідентичністю та доступом наслідують загальний п'ятиетапний підхід (аналіз, розробка архітектури, реалізація, тестування та підтримка), який можна побачити на наступній діаграмі.

2.3.1 Аналіз та визначення

Етап Аналіз та визначення дозволяє визначити обсяг робіт та розділити його між членами команди проекту. На цьому етапі ви отримаєте найкраще уявлення про те, як розділити проект на кілька невеликих фрагментів, а потім зможете визначити, скільки часу займе кожен фрагмент. Це дозволяє ефективно планувати час та гроші для проекту.

На етапі аналізу та виявлення потрібно зустрітися як з бізнес-, так і з технічно зацікавленими сторонами, щоб визначити існуючі умови, зрозуміти бізнес- та технічні фактори, а також визначити процеси та процедури, які можуть так чи інакше вплинути на ваше рішення.

Наприкінці цього етапу ви повинні мати можливість чітко сформулювати як існуюче, так і майбутнє середовище, а також розуміти причини, з яких проект реалізується.

2.3.2 Розробка архітектури

Мета етапу Архітектура – взяти інформацію з попереднього етапу та розробити дизайн, який відповідає цілям проекту в рамках обмежень організації. Крім того, може обговорюватися або погоджуватися дорожня карта або кроки, необхідні для переходу від поточного стану до кінцевого. Це може включати прийняття рішення про апаратне забезпечення, програмне забезпечення, вимоги до даних або внесення змін, необхідних для досягнення кінцевого стану.

Наприкінці цього етапу у вас має бути чітке уявлення про те, як виглядатиме кінцевий стан. Це включає такі елементи як параметри сервера та системи обробки бази даних, перелік додатків та порядок роботи з ними, адміністрування, а також питання конфіденційності та безпеки.

Як тільки ви зрозумієте, як виглядатиме остаточний стан, у вас буде краще уявлення про те, що потрібно для переходу з поточного стану. Це дозволить визначити план проекту та повідомити приблизні терміни зацікавленим сторонам бізнесу.

2.3.3 Реалізація

Етап реалізації включає всі завдання, необхідні для розробки кінцевого стану. Це включає побудову центру обробки даних, налаштування операційної системи, встановлення програмного забезпечення, конфігурування і тонке налаштування, завантаження даних, створення адміністративних інтерфейсів і практично будь-які інші завдання, які необхідні для досягнення кінцевого стану.

На цьому етапі проводиться початкове функціональне та користувальницьке тестування, щоб переконатися, що ви робите продукт, що відповідає як вимогам, так і потребам кінцевих користувачів. Одночасно з цим пишеться документація, яка буде використовуватись ще довгий час після завершення проекту. Сюди входять інструкції з експлуатації та підтримки, посібники зі встановлення та будь-яка інша документація, яка допомагає в моніторингу та обслуговуванні продуктів, пов'язаних з керуванням ідентичністю. Саме на цьому етапі починається початкове навчання допоміжного персоналу та інтеграція продукту з рішеннями моніторингу та підтримки.

Етапи впровадження та тестування тісно пов'язані між собою, оскільки можливо виявити, що дефекти, виявлені під час тестування, призводять до змін у реалізації. Необхідно запланувати кілька ітерацій між цими двома етапами перед тим, як переходити до запуску рішення у виробництво.

2.3.4 Тестування

Етап Тестування необхідний для визначення відповідності кінцевого продукту вимогам, встановленим на етапі Аналізу. Сюди входять функціональні вимоги (засновані на певних варіантах використання), вимоги до продуктивності (засновані на потребах користувачів або інших додатків) та вимоги високої доступності (для забезпечення безперервності бізнесу у випадку збою).

Щойно буде встановлено, що реалізація відповідає кожному з певних вимог (з яких «мета використання» є однією з найважливіших), настає час перейти до реалізації командою підтримки. Офіційна передача в службу підтримки повинна включати всі посібники з експлуатації та усунення неполадок, а також докладну

інформацію про те, як звертатися до служби підтримки і до будь-яких постачальників, пов'язаних з рішенням.

2.3.5 Підтримка

Етап впровадження завершено, і тепер продукт відображає прогнозований кінцевий стан. Рішення було протестоване, щоб переконатися, що воно відповідає вимогам бізнесу, технічним вимогам та вимогам кінцевих користувачів, і тепер рішення готове до переходу до експлуатації, коли його можна буде супроводжувати власною командою підтримки або сторонньою організацією.

Бувають випадки, коли для вирішення більш складних проблем може бути залучена команда розробки та реалізації проекту, але зазвичай група підтримки має бути в змозі впоратися з більшістю проблем, які можуть виникнути. Це означає, що група підтримки пройшла адекватну підготовку і володіє необхідними попередніми знаннями про операційну систему, мережі та процеси, реалізовані в загальному рішенні.

Після того, як реалізація була передана команді підтримки, впровадження системи IAM у підприємство можна вважати завершеним.

3 ІНТЕГРАЦІЯ SOFFID IAM В ІСНУЮЧУ IT ІНФРАСТРУКТУРУ

Для демонстрації процесу інтеграції Soffid IAM в існуючу IT інфраструктуру підприємства створимо віртуальне оточення, що складається з контролера домену на базі Windows Server 2022 та поштового сервера Zimbra.

Для сервера віртуалізації було обрано платформу Proxmox Virtual Environment версії 7.4.

3.1 Встановлення серверної частини Soffid

Для розгортання сервера створимо віртуальну машину (lxc контейнер) з наступними параметрами (рис. 3.1).

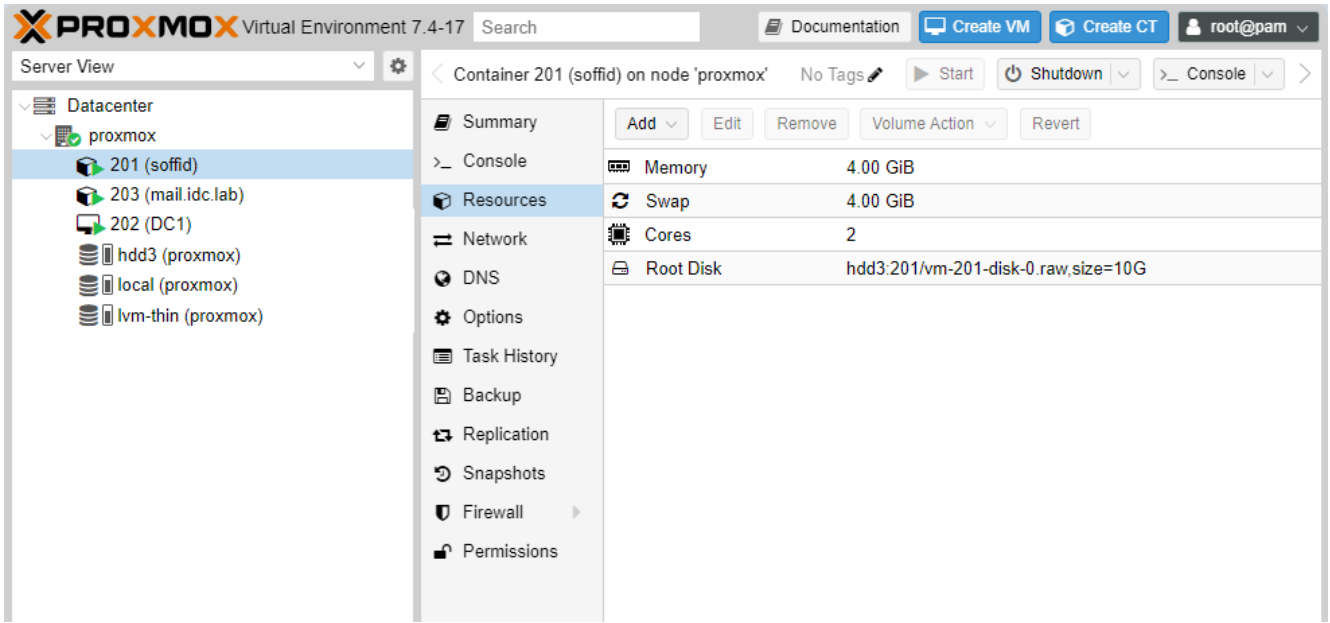


Рисунок 3.1 Параметри контейнера soffid

Контейнер було розгорнуто з використанням шаблону debian-12-standard.

Серверна частина Soffid Identity and Access Management (Soffid IAM) складається із двох компонентів:

1) Soffid IAM Console;
2) Soffid Sync Server.

3.1.1 Встановлення та підготовка бази даних

Насамперед, необхідно встановити та підготувати базу даних, необхідну для роботи Soffid IAM.

На даний момент Soffid підтримує такі бази даних:

– MySQL;
– MariaDB;
– PostgreSQL;
– Oracle;
– Microsoft SQLServer.

Для цього прикладу була обрана база даних MariaDB.

Встановимо СУБД MariaDB із стандартного репозиторію Debian.

```
# apt update
# apt install mariadb-server
```

Після завершення встановлення потрібно запустити сценарій безпеки, який видалить ненадійні параметри та захистить БД від несанкціонованого доступу.

```
# mysql_secure_installation
```

Цей сценарій поставить низку питань, за допомогою яких він внесе поправки до параметрів безпеки БД. Спочатку він попросить запровадити поточний root-

пароль. Оскільки ми встановили MariaDB щойно та ще не внесли жодних змін до конфігурації, цього пароля в нас поки що немає, тому просто натискаємо Enter.

У наступних двох питаннях скрипт запропонує настроїти пароль root для бази даних. Слід відповісти на них ні, натиснувши на N і клавішу Enter. У Debian обліковий запис root MariaDB тісно пов'язаний з автоматизованим обслуговуванням системи, тому не можна змінювати стандартні методи аутентифікації цього облікового запису. Інакше при оновленні пакета mariadb база даних може пошкодитися, а доступ до облікового запису root може бути втрачено. Тому у випадках, коли потрібно використовувати аутентифікацію за паролем, рекомендується налаштовувати додатковий обліковий запис адміністратора.

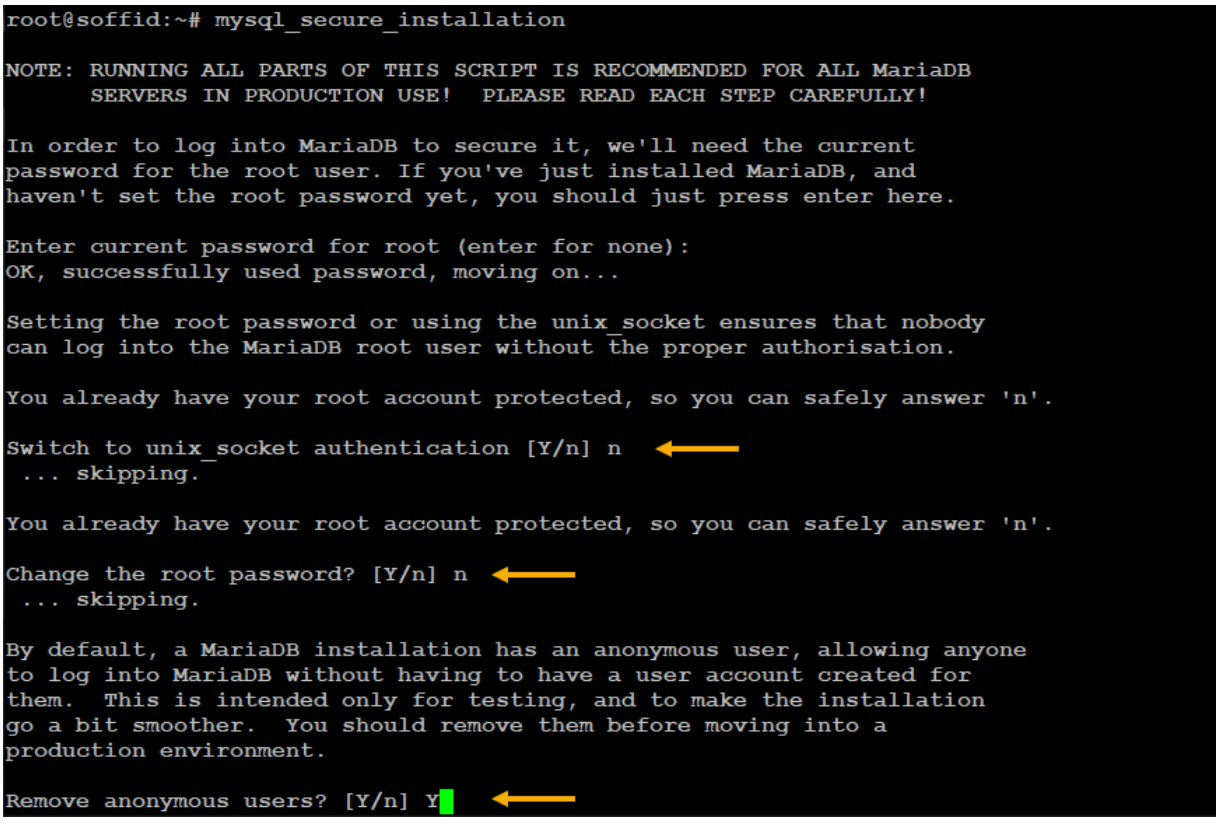


Рисунок 3.2 Запуск скрипту з налаштування безпеки БД

На інші запитання можна відповісти так, натиснувши Y та Enter. Це видалить анонімних користувачів та тестові бази даних, відключить віддалений root логін та оновить поточні налаштування MariaDB (рис. 3.2).

У Debian-дистрибутивах MariaDB користувач root за замовчуванням підтримує аутентифікацію за допомогою плагіна unix_socket, а не через пароль. Це в багатьох випадках дозволяє підвищити безпеку та зручність використання, але також може ускладнити роботу, якщо вам необхідно дозволити доступ до зовнішньої програми (у нашому випадку це Soffid).

Оскільки сервер використовує root-користувача для таких завдань, як ротація логів, запуск та зупинка сервера, аутентифікацію облікового запису root краще не змінювати. Зміна облікових даних у файлі /etc/mysql/debian.cnf може спрацювати на початковому етапі, але подальші оновлення пакетів перезапишуть усі зміни. Натомість розробники рекомендують створити окремий обліковий запис адміністратора з парольною автентифікацією.

Отже, створимо обліковий запис під назвою admin з тими ж правами, що й у root, але з підтримкою парольної автентифікації. Для цього відкриємо командну консоль MariaDB. Потім створимо користувача з максимальними привілеями та підтримкою парольної аутентифікації. У команді вкажемо ім'я та пароль нового користувача.

```
  # mysql
  MariaDB [(none)]> GRANT ALL ON *.* TO 'admin'@'localhost' IDENTIFIED BY
'password' WITH GRANT OPTION;
```

Перед встановленням Soffid необхідно заздалегідь створити базу даних. Для цього, не виходячи з консолі MariaDB, виконаємо команду create database soffid. Потім перевіримо отриманий результат командами show databases та select User from mysql.user. Після закінчення вийдемо з консолі MariaDB користуючись командою quit (рис. 3.3).

```
  MariaDB [(none)]> create database soffid;
  MariaDB [(none)]> show databases;
  MariaDB [(none)]> select User from mysql.user;
  MariaDB [(none)]> quit
```

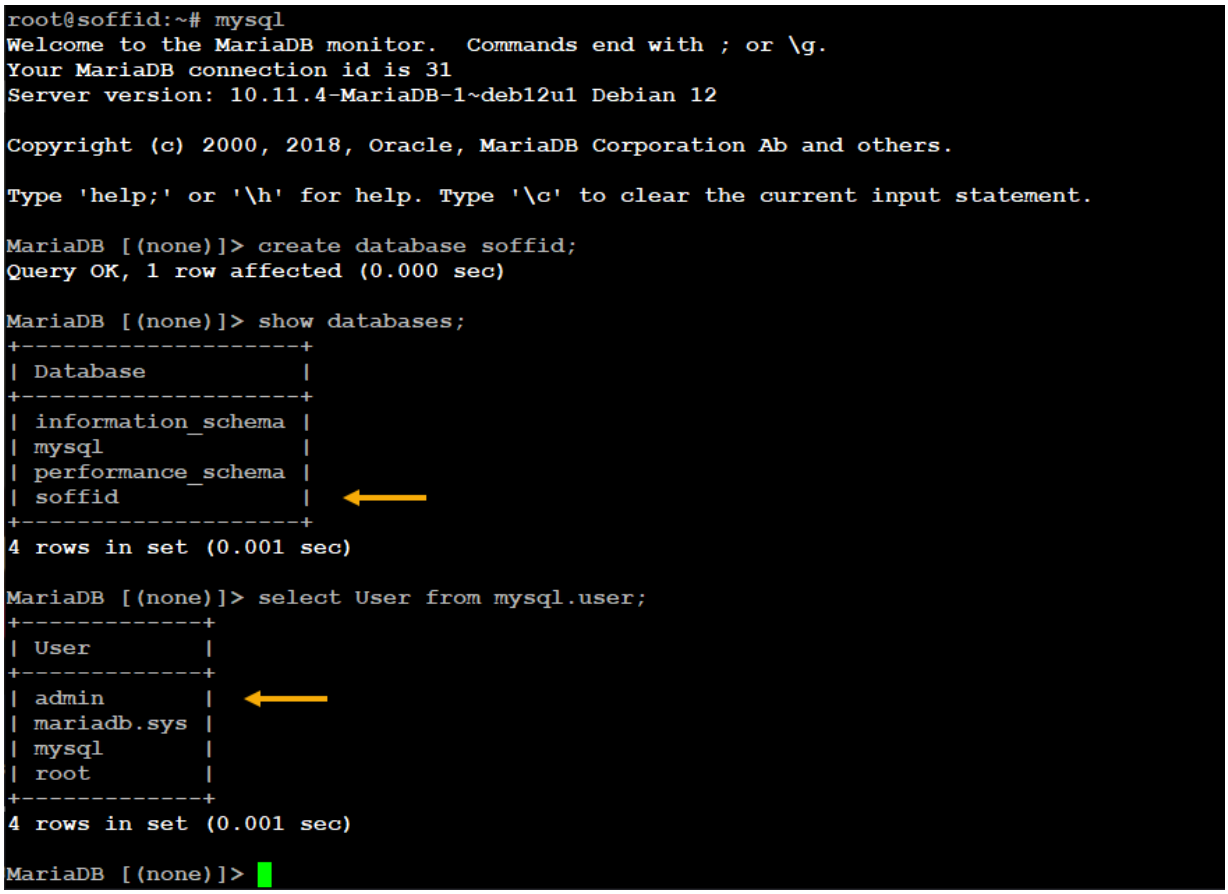


Рисунок 3.3 Створення бази даних soffid

Далі необхідно внести до конфігураційного файлу mariadb невеликі зміни. Цей файл знаходиться за адресою /etc/mysql/mariadb.conf.d/50-server.cnf

```
# mcedit /etc/mysql/mariadb.conf.d/50-server.cnf
```

Знайдемо рядок max_allowed_packet у розділі * Fine Tuning, розкоментуємо його та поміняємо значення на 512M

```
max_allowed_packet    = 512M
```

Далі знайдемо розділ * InnoDB (за замовчуванням у ньому немає опцій) та додамо наступний рядок

```
innodb_log_file_size  = 256M
```

Ці опції усувають проблеми, які можуть виникнути під час роботи з файлами великих розмірів. Вони необхідні, щоб, зокрема, завантажувати файли розширень на сервер. Збережемо зміни та перезапустимо mysql

```
# systemctl restart mysql
```

3.1.2 Встановлення Java JDK

Перш, ніж приступати до встановлення Soffid IAM, нам потрібно переконатися, що в системі встановлена відповідна версія Java JDK. Дізнатися версію java можна за допомогою команди:

```
# java -version
```

Для коректної роботи Soffid 3 розробники рекомендують використовувати Java JDK 11. До складу Debian 12 за замовчуванням включено пакет openjdk-17-jre – 17-а версія Java Runtime Environment, проте спроба використовувати цю версію в комплекті з Soffid виявилася невдалою – сервер синхронізації Soffid Sync server при запуску видавав помилку. Тому було ухвалено рішення встановити пакет openjdk-11-jre, доступний у Sid репозиторії. Це нестабільний репозиторій, що містить останні пакети, що надійшли до Debian, проте не пройшли належної перевірки. Тому важливо зробити так, щоб не вся система Debian оновлювалася з unstable репозиторію, а тільки один пакет, що цікавить нас. Це досягається створенням спеціального файлу налаштувань менеджера пакетів. У цьому файлі ми пропишемо, який саме пакет скачуватиметься з нестабільного репозиторію, а також виставимо пріоритети репозиторіям, завдяки чому система не буде використовувати нестабільний репозиторій під час перевірки оновлень.

Отже, спочатку потрібно підключити репозиторій Debian Sid. Для цього відкриємо в текстовому редакторі файл /etc/apt/sources.list і додамо до кінця два рядки. Ці дії потрібно робити під правами root.

```
# mcedit /etc/apt/sources.list
```

Додамо в кінець два рядки:

```
deb http://deb.debian.org/debian unstable main contrib non-free
deb-src http://deb.debian.org/debian unstable main contrib non-free
```

Збережемо зміни та вийдемо. Важливо в цей момент не намагатися оновити систему, оскільки якщо зараз запустити оновлення, абсолютно всі пакети Debian оновляться до нестабільних версій. Щоб цього не сталося, перейдемо до наступного кроку – закріплення пакетів.

Закріплення дозволяє визначити, який саме пакет завантажуватиметься з нестабільного репозиторію замість того, щоб звідти завантажувалися всі пакети. Для цього створимо файл у каталозі /etc/apt/ з ім'ям preferences. І відкриємо його у текстовому редакторі.

```
# touch /etc/apt/preferences
# mcedit /etc/apt/preferences
```

Додамо такий код у цей файл:

```
Package: *
Pin: release a=bookworm
Pin-Priority: 500

Package: openjdk-11-jre
Pin: release a=unstable
Pin-Priority: 1000

Package: *
Pin: release a=unstable
Pin-Priority: 100
```

Після збереження цього файлу можна виконати оновлення репозиторію та запустити інсталяцію Java 11

```
# apt update
# apt install openjdk-11-jre
```

Після закінчення встановлення знову запустимо команду java -version, щоб перевірити результат (рис. 3.4).

```
root@soffid:~# java -version
openjdk version "11.0.21" 2023-10-17
OpenJDK Runtime Environment (build 11.0.21+9-post-Debian-1)
OpenJDK 64-Bit Server VM (build 11.0.21+9-post-Debian-1, mixed mode, sharing)
root@soffid:~#
```

Рисунок 3.4 Перевірка версії Java

3.1.3 Встановлення Soffid IAM Console

Для встановлення Soffid IAM необхідно мати:

– Windows або Linux (Ubuntu – найпопулярніший варіант);
– Java JDK 8 або вище. Рекомендується Java JDK 11;
– 8GB RAM - 8 Гб оперативної пам'яті;
– не менше 10 Гб дискового простору;
– підтримувану СУБД.

За адресою http://download.soffid.com/download знаходяться всі доступні для скачування інсталяційні пакети Soffid. Щоб мати можливість завантажувати файли з цього ресурсу, необхідно пройти безкоштовну реєстрацію. Розкриємо рядок SOFFID 3 Console та завантажимо останню версію Debian/Ubuntu installer. На момент написання роботи останньою версією була version 3.5.9.4 (рис. 3.5).

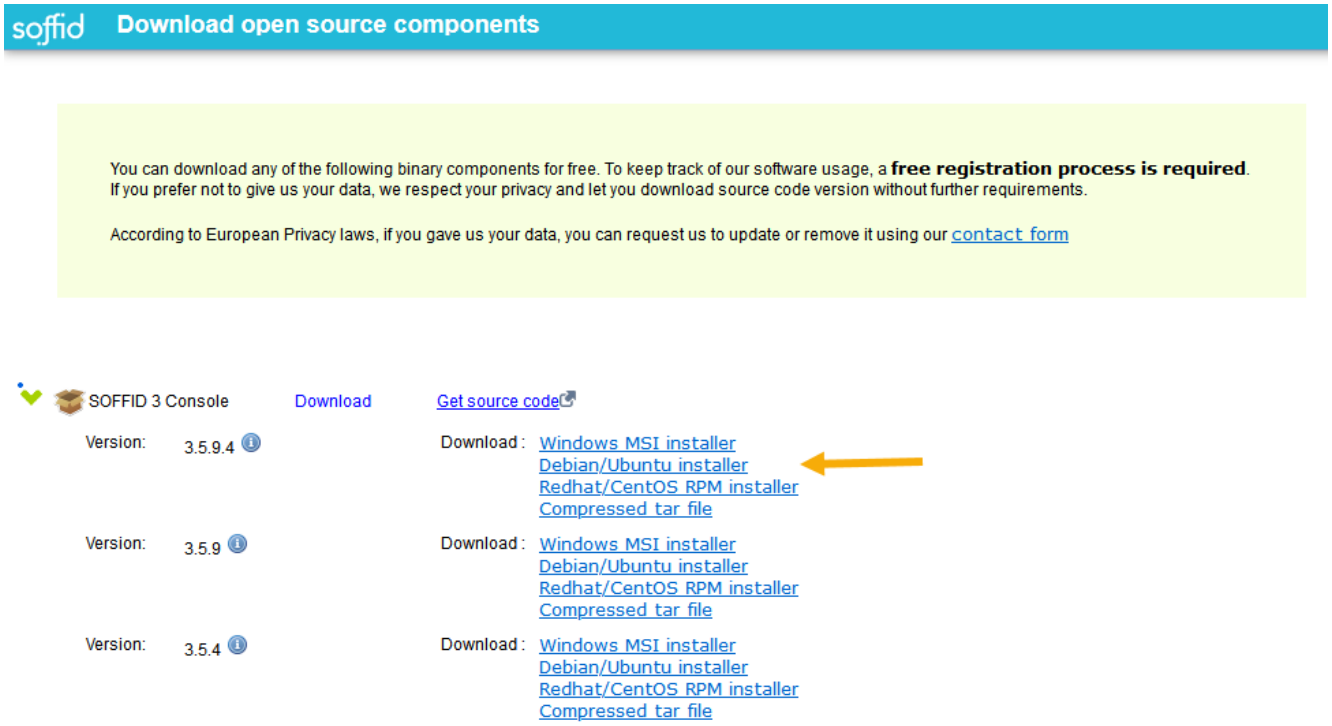


Рисунок 3.5 Завантаження інсталяційного пакету Soffid Console

Рисунок 3.6 Форма авторизації на сервері Soffid Download

При натисканні на посилання завантажиться форма, в якій потрібно ввести User name і Password. Якщо у вас ще немає облікових даних, потрібно натиснути кнопку Register та пройти безкоштовну реєстрацію (рис. 3.6).

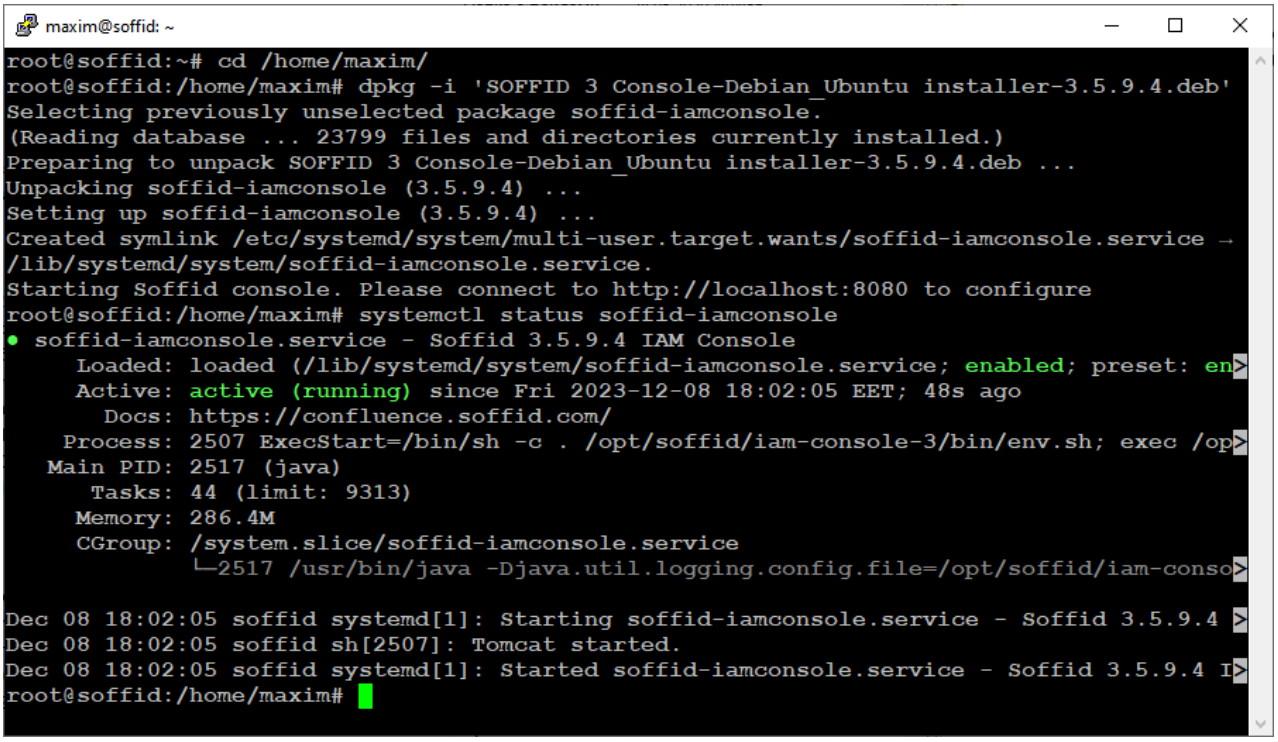


Рисунок 3.7 Встановлення Soffid Console

Після реєстрації та введення облікових даних отримуємо файл SOFFID 3 Console-Debian_Ubuntu installer-3.5.9.4.deb. Завантажуємо скачаний файл на сервер. Для цього найкраще скористатися програмою WinSCP, яка забезпечує захищене копіювання файлів між комп'ютером та сервером.

Переходимо до каталогу зі скачаним файлом та встановлюємо його за допомогою команди dpkg -i. Ці дії також треба виконувати з привілеями root.

```
# dpkg -i 'SOFFID 3 Console-Debian_Ubuntu installer-3.5.9.4.deb'
```

Під час інсталяції створюється та запускається служба IAM Console. Після завершення роботи інсталятора можна перевірити статус служби за допомогою команди:

```
# systemctl status soffid-iamconsole
```

Зелений напис active (running) свідчить про те, що установка пройшла успішно і можна переходити до налаштування Soffid (рис. 3.7).

3.1.4 Первинне налаштування Soffid Console

Для налаштування Soffid Console відкриємо веб-браузер та перейдемо на сторінку http://192.168.2.201:8080, де 192.168.2.201 – ip адреса сервера Soffid (рис. 3.8).

Тиснемо Configure і приступаємо до налаштування. Заповнюємо поля.

Host name: якщо є домен, то вказуємо повне ім'я разом із доменом. В іншому випадку можна залишити значення за замовчуванням – IP-адреса сервера.

User name та Password: Вказуємо логін та пароль користувача БД з привілеями root, якого ми створили на етапі встановлення та підготовки бази даних (п. 3.1.1).

Рисунок 3.8 Сторінка Soffid Console при першому вході

Driver: MariaDB

URL: jdbc:mariadb://localhost/soffid

Далі тиснемо Connect (рис. 3.9). Якщо все було зроблено правильно, то коннект з базою даних пройде без помилок і встановлення продовжиться. На наступному кроці вам буде запропоновано створити обліковий запис адміністратора Soffid. Ім'я можна залишити за замовчуванням – admin, а пароль потрібно вигадати свій і внести його у відповідні два поля.

Після закінчення введення натиснемо Startup (рис. 3.10).

Рисунок 3.9 Налаштування з'єднання Soffid Console з базою даних

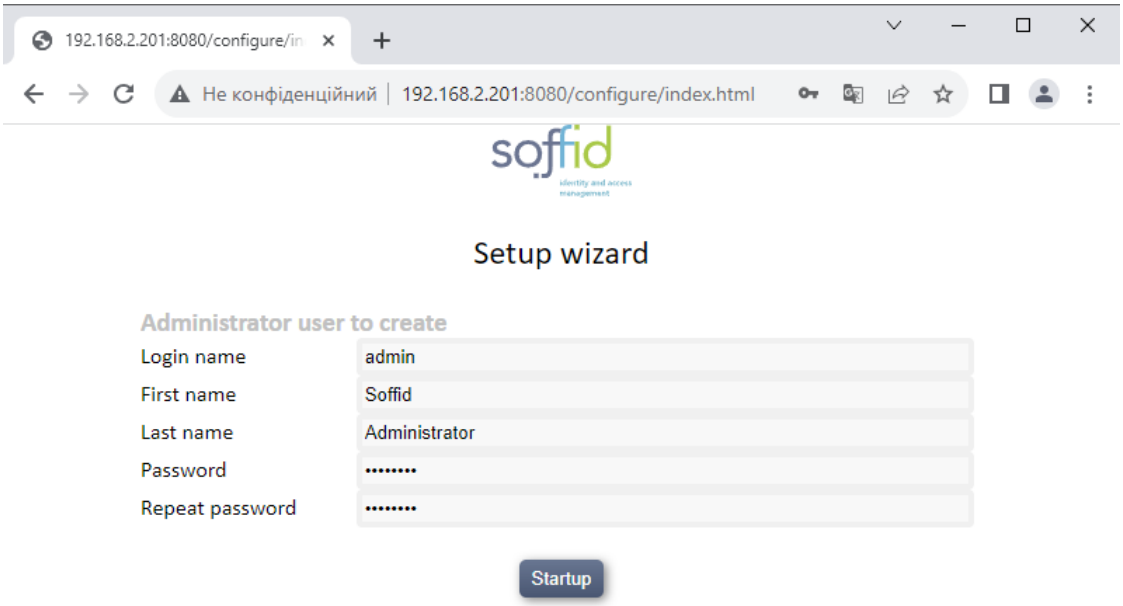


Рисунок 3.10 Налаштування облікового запису admin

Після тривалої паузи, пов'язаної з тим, що під час першого запуску Soffid створює об'єкти бази даних, з'явиться вікно входу в систему (рис. 3.11).

Рисунок 3.11 Вікно входу до системи Soffid

Введемо логін та пароль, створені на попередньому кроці, та натиснемо Login. Запуститься короткий ознайомлювальний тур, який розповість про переваги використання Soffid та основні елементи інтерфейсу. На останньому екрані можна

відключити цю презентацію, пересунувши перемикач Dismiss this introduction в положення Yes. В іншому випадку цей ознайомлювальний тур запускатиметься при кожному вході в систему.

3.1.5 Встановлення Soffid Sync Server

Наступним кроком необхідно встановити та налаштувати Soffid Sync Server. Це основний компонент, завдяки якому інші системи-сателіти підключаються до бази даних Soffid за допомогою агентів.

Заходимо на офіційний сайт http://www.soffid.com/download/ та завантажуємо інсталятор SOFFID 3 Sync server. Для входу на сайт використовуємо ті самі облікові дані, які використовувалися при завантаженні Soffid Console.

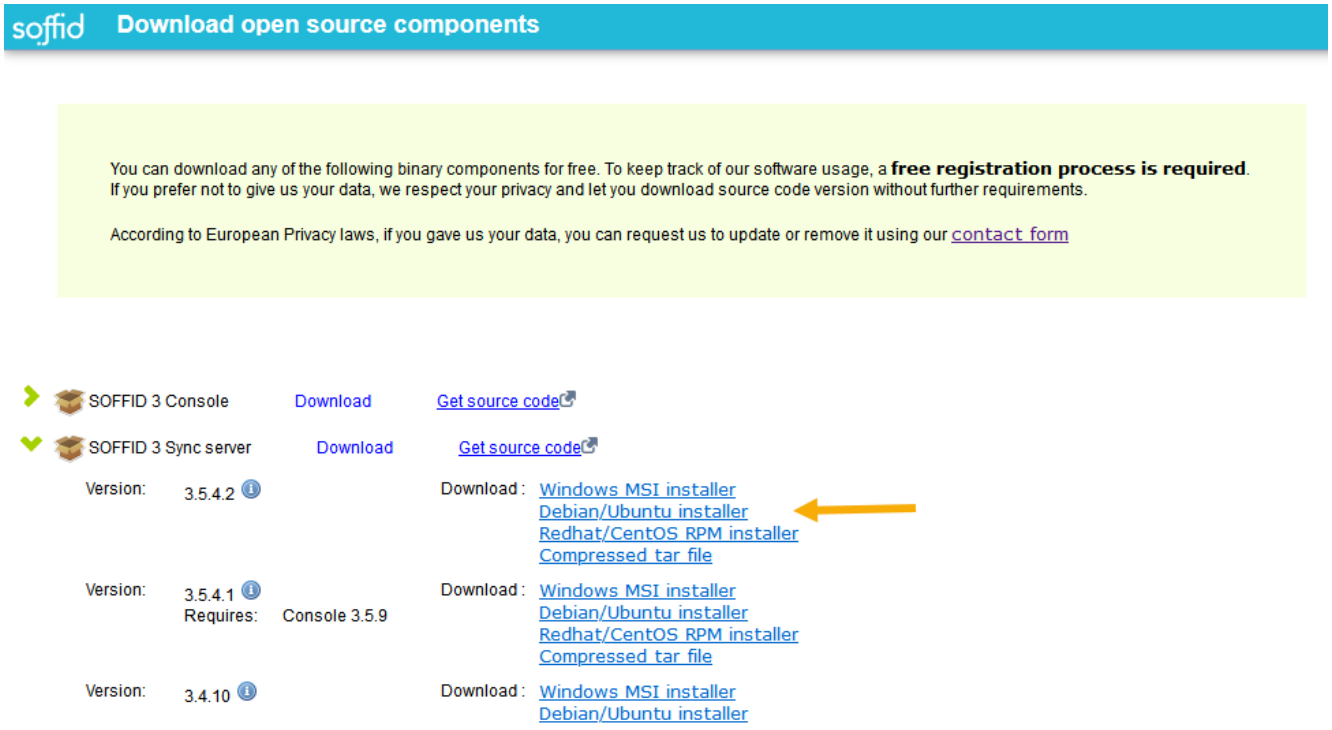


Рисунок 3.12 Завантаження інсталяційного пакету Soffid Sync Server

На момент написання роботи останньою версією Soffid Sync server була Version 3.5.4.2 (рис. 3.12). Натискаємо на посилання Debian/Ubuntu installer. Отримуємо файл SOFFID 3 Sync server-Debian_Ubuntu installer-3.5.4.2.deb. За допомогою програми WinSCP або подібної завантажуємо скачаний файл на сервер.

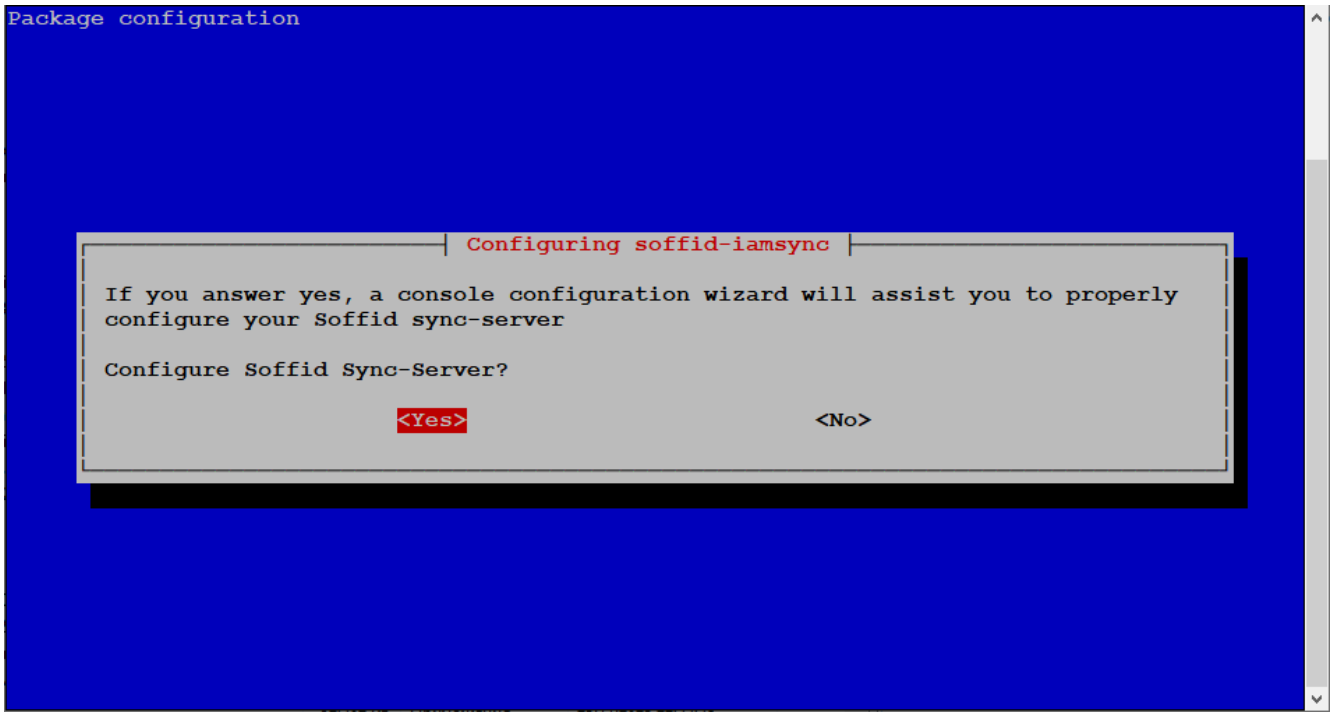


Рисунок 3.13 Встановлення Soffid Sync Server

Далі переходимо в каталог з інсталятором та виконуємо команду установки пакета. Встановлення слід виконувати з консолі під користувачем root.

```
# dpkg -i 'SOFFID 3 Sync server-Debian_Ubuntu installer-3.5.4.2.deb'
```

Під час встановлення консолі з'явиться пропозиція запустити configuration wizard (конфігураційний скрипт). Однак, навіть якщо відповісти на це питання Yes, скрипт з невідомих причин не запуститься (рис. 3.13). Тому скористаємося рекомендаціями розробників щодо запуску конфігураційного скрипту вручну. Насамперед, зупинимо сервіс syncserver командою:

```
# systemctl stop soffid-iamsync.service
```

Потім потрібно видалити попередню конфігурацію в тому випадку, якщо скрипт уже запускався раніше. З'ясувати це можна, перевіривши вміст каталогу /opt/soffid/iam-sync/conf

```
# ls -l /opt/soffid/iam-sync/conf/
```

Якщо він пустий, робити нічого не треба. В іншому випадку виконуємо команду для його очищення

```
# rm /opt/soffid/iam-sync/conf/*
```

Все готово. Можна запускати конфігураційний скрипт. Запускати його потрібно від імені користувача soffid. На сайті розробників цього не написано, але якщо запустити скрипт від імені root, то частина конфігураційних файлів виявиться недоступною для soffid, що призведе до різних помилок та проблем у роботі Soffid Sync server. Тому для запуску скрипта скористаємося командою sudo -u soffid (у системі має бути встановлений пакет sudo – якщо його немає, то слід встановити його командою apt install sudo).

```
# sudo -u soffid /opt/soffid/iam-sync/bin/configure
```

Відповімо на запитання майстра з налаштування (рис. 3.14).

Перше питання конфігураційного скрипту звучить так: «Це ваш перший Sync server у мережі?» - Відповімо у (Так).

Далі нам потрібно буде відповісти ще на 5 питань:

1) Database URL (jdbc:....): введемо ту саму URL, що ми використовували при налаштуванні Soffid Console (jdbc:mariadb://localhost/soffid);
2) Database user: користувач бази даних – вкажемо того ж користувача, що ми використовували під час налаштування Soffid Console для підключення до бази даних;
3) Password: пароль від цього користувача;
4) This server host name: необхідно ввести повне ім'я сервера з доменом (якщо є), або коротке ім'я (без домену). IP адресу тут вказувати не можна.
5) Port to listen to [1760]: номер TCP порту. Sync server прийматиме з'єднання від консолі (Soffid Console) та інших серверів синхронізації (Sync servers) саме на цьому порту. Значення за замовчуванням – 1760. Рекомендується використовувати це значення, тому залишимо його, натиснувши Enter.

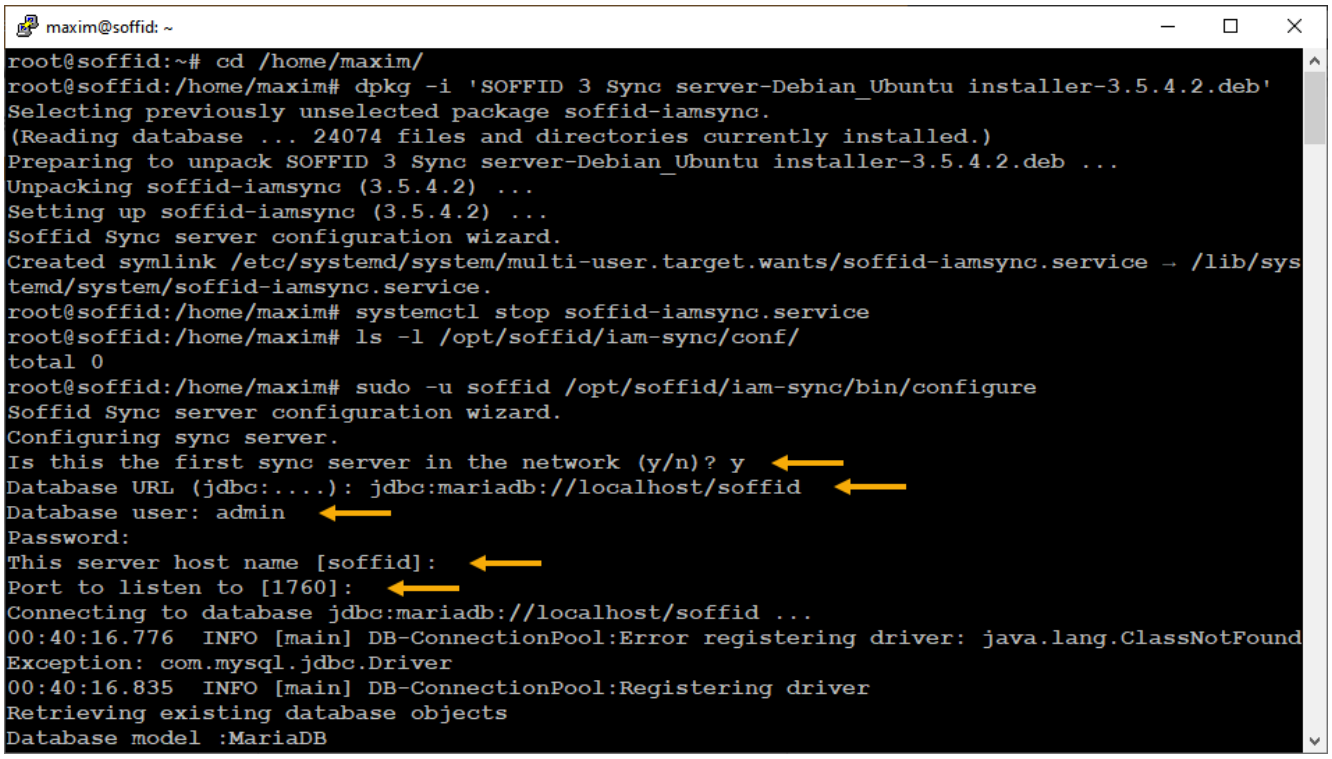


Рисунок 3.14 Налаштування Soffid Sync Server

З виходом Soffid 3 номер порту за замовчуванням змінився з 760 на 1760. Це пов'язано з тим, що у новій версії Soffid системні сервіси почали працювати від імені непривілейованого користувача (що з точки зору безпеки правильніше).

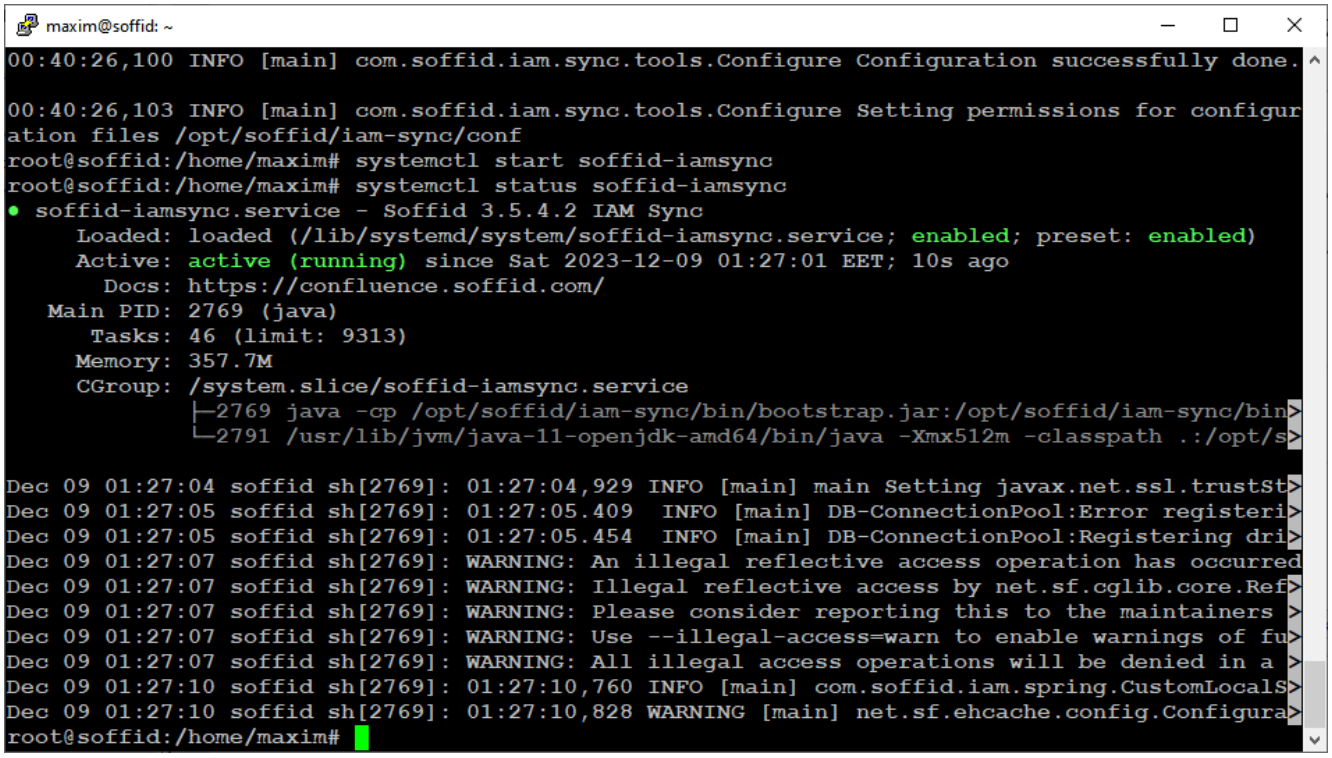


Рисунок 3.15 Перевірка статусу Soffid Sync Server

Саме тому номер порту довелося міняти, оскільки номери портів до 1000 можуть використовуватися лише системним користувачем root. Після налаштування сервіс необхідно запустити та перевірити його статус (рис. 3.15).

```
# systemctl start soffid-iamsync
# systemctl status soffid-iamsync
```

Перевіримо результат у веб-консолі. Перейдемо в Main Menu > Administration > Configuration > Integration engine > Synchronization servers.

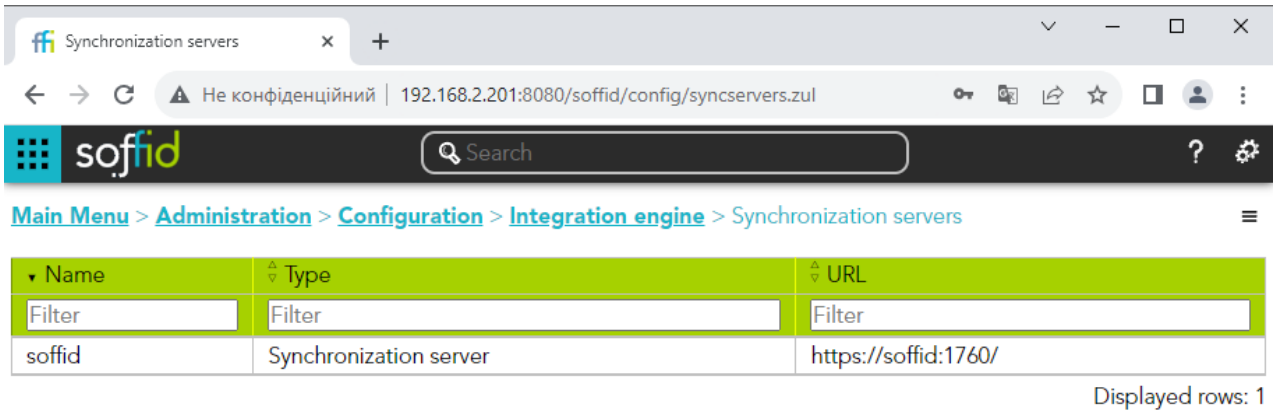


Рисунок 3.16 Сервери синхронізації Soffid

Там ми маємо побачити таку картину (рис. 3.16). Якщо натиснути на рядок з сервером soffid, побачимо його деталі (рис. 3.17).

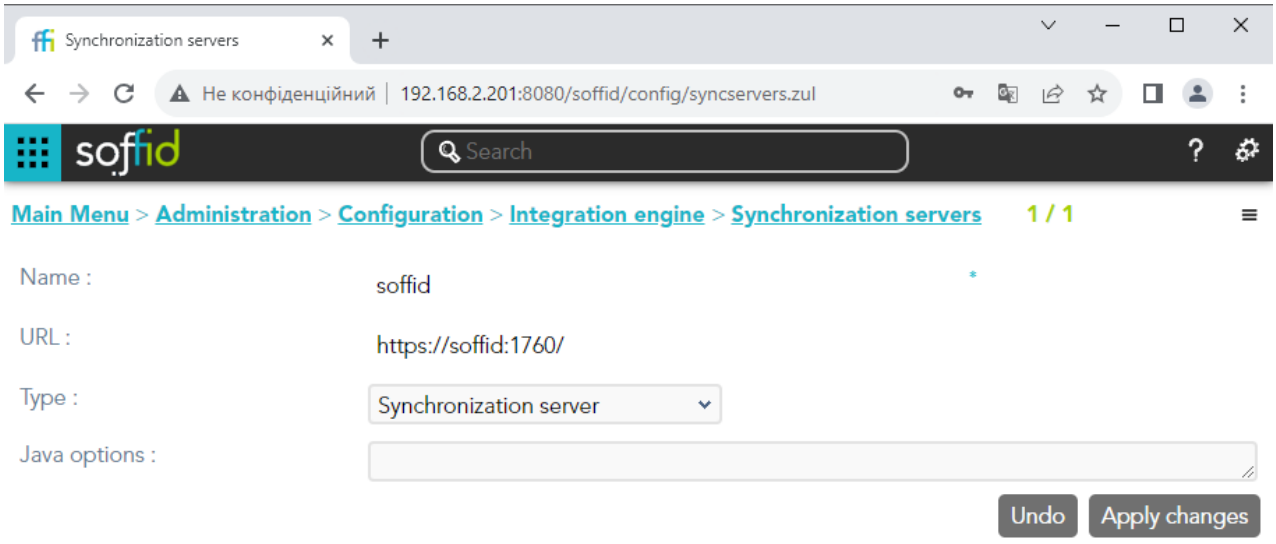


Рисунок 3.17 Подробиці сервера синхронізації Soffid

На цьому встановлення серверної частини Soffid 3 закінчено. На даному етапі можна зробити контрольне перезавантаження та перевірити результат.

3.1.6 Налаштування Password policy

Важливим елементом безпеки є політика паролів, що створюються (Password policy). Усі паролі, які призначаються адміністратором, генеруються випадковим чином або створюються самими користувачами, проходять обов'язкову перевірку на відповідність встановленій політиці. Якщо пароль недостатньо складний – наприклад, занадто короткий або не містить певних груп символів – система не прийматиме такий пароль і запропонує користувачеві його змінити.

У Soffid усі користувачі поділяються за типами. Цей поділ дозволяє:

– сортувати списки з великою кількістю користувачів;
– застосовувати різні політики паролів;
– вводити обмеження при синхронізації з керованими системами;
– робити автоматизацію налаштування за допомогою скриптів.

За замовчуванням у системі Soffid створюється три типи користувачів:

– External user – зовнішні користувачі;
– Internal user – внутрішні користувачі;
– SSO account – облікові записи єдиного входу.

Налаштуємо політику паролів для внутрішніх користувачів, які будуть використовуватись у нашій моделі.

Зайдемо в меню Main Menu > Administration > Configuration > Security settings > Password policies і натиснемо на рядку Default password policy Internal user. У вікні, що з’явиться внесемо такі зміни (рис. 3.18).

Change allowed: Yes – якщо Yes (Так), користувачеві дозволено змінювати автоматично згенеровані паролі;

Query allowed: Yes – якщо Yes (Так), користувачеві дозволено переглядати свій поточний пароль;

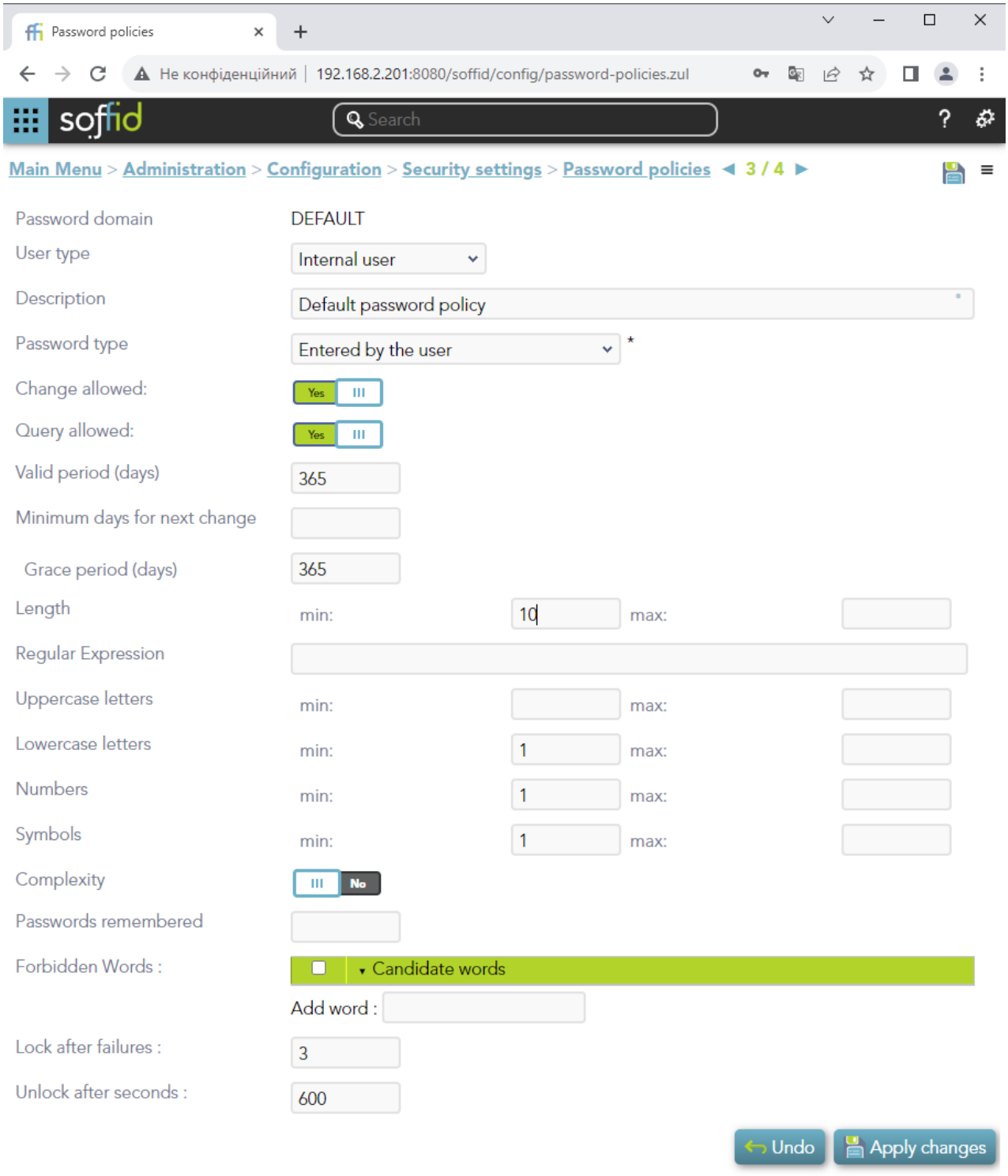


Рисунок 3.18 Налаштування Password policy для Internal user

Length min: 10 – мінімальна довжина пароля;

Lowercase letters min: 1 – мінімальна кількість малих літер у паролі;

Numbers min: 1 – мінімальна кількість цифр у паролі;

Symbols min: 1 – мінімальна кількість спеціальних символів у паролі.

Цими налаштуваннями ми встановлюємо, що пароль повинен бути не менше 10 символів довжиною і повинен як мінімум мати одну малу літеру, одну цифру та один спеціальний символ. Наявність у паролі великих літер не є обов'язковою.

3.2 Підключення контролера домену до Soffid

Розглянемо підключення до сервера Soffid контролера домену, розгорнутого на базі Windows Server 2022. Припустимо, на момент впровадження Soffid IAM, на підприємстві вже є працюючий контролер домену, в якому зберігаються облікові записи всіх користувачів-співробітників підприємства. Стоїть завдання не просто підключити наявний контролер домену до сервера Soffid, а й проімпортувати користувачів, які вже знаходяться на контролері домену, до бази даних або репозиторію Soffid.

3.2.1 Захист протоколу LDAP

За замовчуванням у Active Directory трафік за протоколом LDAP між контролером домену та клієнтами не шифрується, тобто дані по мережі передаються у відкритому вигляді. Потенційно це означає, що зловмисник за допомогою сніфера пакетів може прочитати ці дані. Для стандартного Windows середовища це не є критичним, проте при використанні сторонніх програм, що використовують LDAP, таких як Soffid, це стає актуальним.

Soffid при підключенні до контролера домену регулярно обмінюється з ним даними, включаючи інформацію про паролі. Такі операції повинні обов'язково здійснюватися через безпечний канал, унеможливлюючи витік конфіденційних даних. Захистити дані, що передаються за протоколом LDAP між додатком і контролером домену, можна за допомогою SSL версії протоколу LDAP – LDAPS, який працює на порту 636, на відміну від LDAP, який використовує 389-й порт. Для цього на контролері домену необхідно встановити спеціальний сертифікат SSL. Сертифікат може бути стороннім (виданим третьою стороною), самопідписаним або виданим корпоративним центром сертифікації.

Якщо в інфраструктурі підприємства вже є розгорнутий корпоративний центр сертифікації Certification Authority (CA), то він може бути використаний для видачі такого сертифіката. У нашій моделі такого центру сертифікації поки що немає, тому його потрібно налаштувати. Для цього додамо роль Active Directory Certificate Services. Відкриємо Server Manager і виберемо там Add roles and features. Далі, за майстром установки, на кроці вибору ролей сервера відзначаємо Active Directory Certificate Services (рис. 3.19).

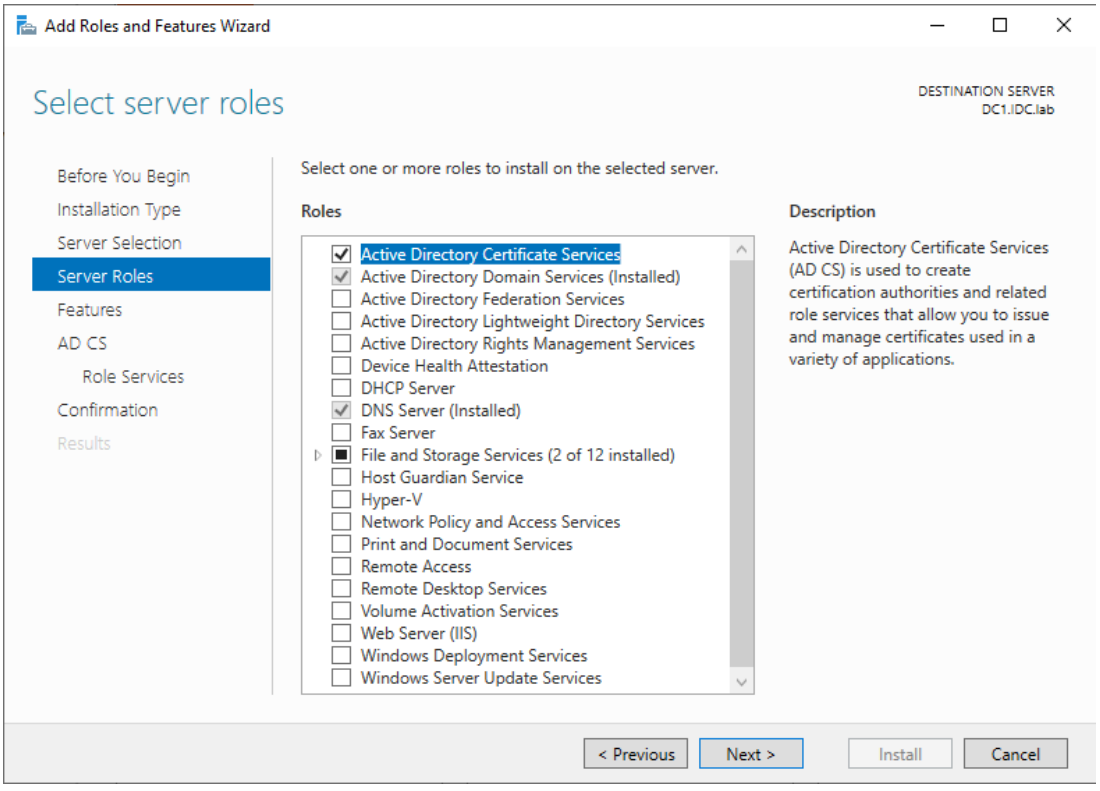


Рисунок 3.19 Крок вибору ролей сервера

На кроці вибору служб ролей відзначаємо Certification Authority (рис. 3.20).

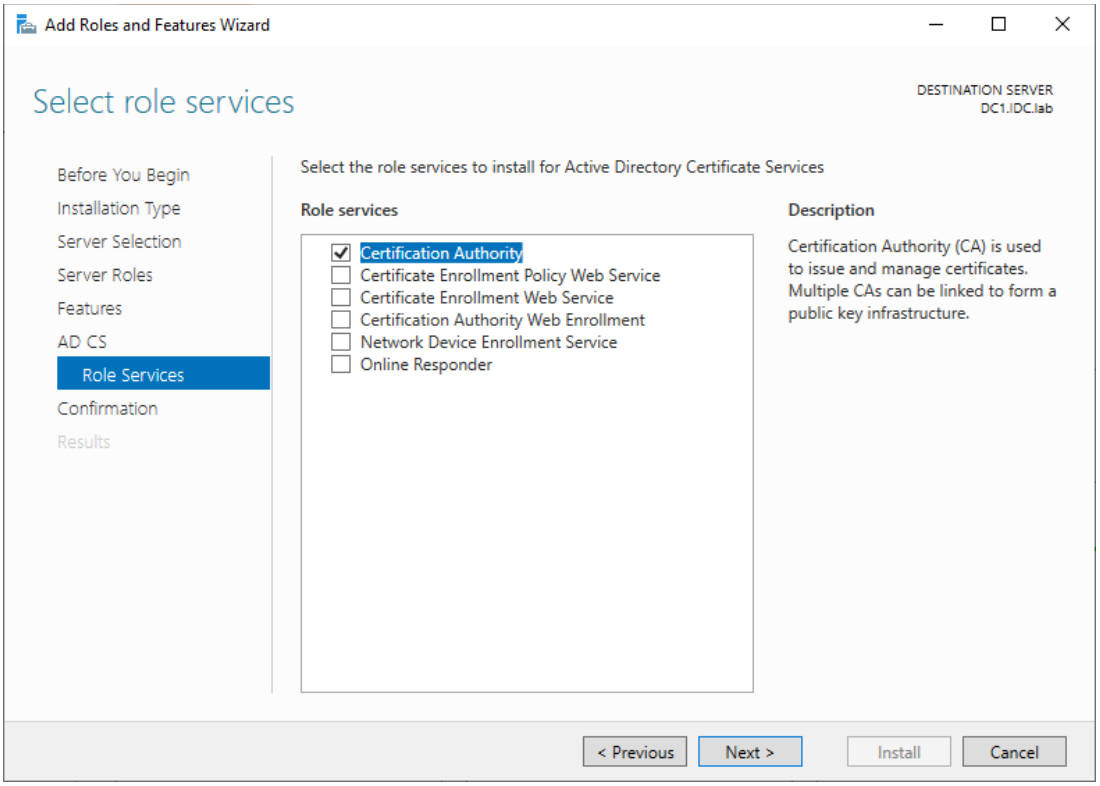


Рисунок 3.20 Крок вибору служб ролей

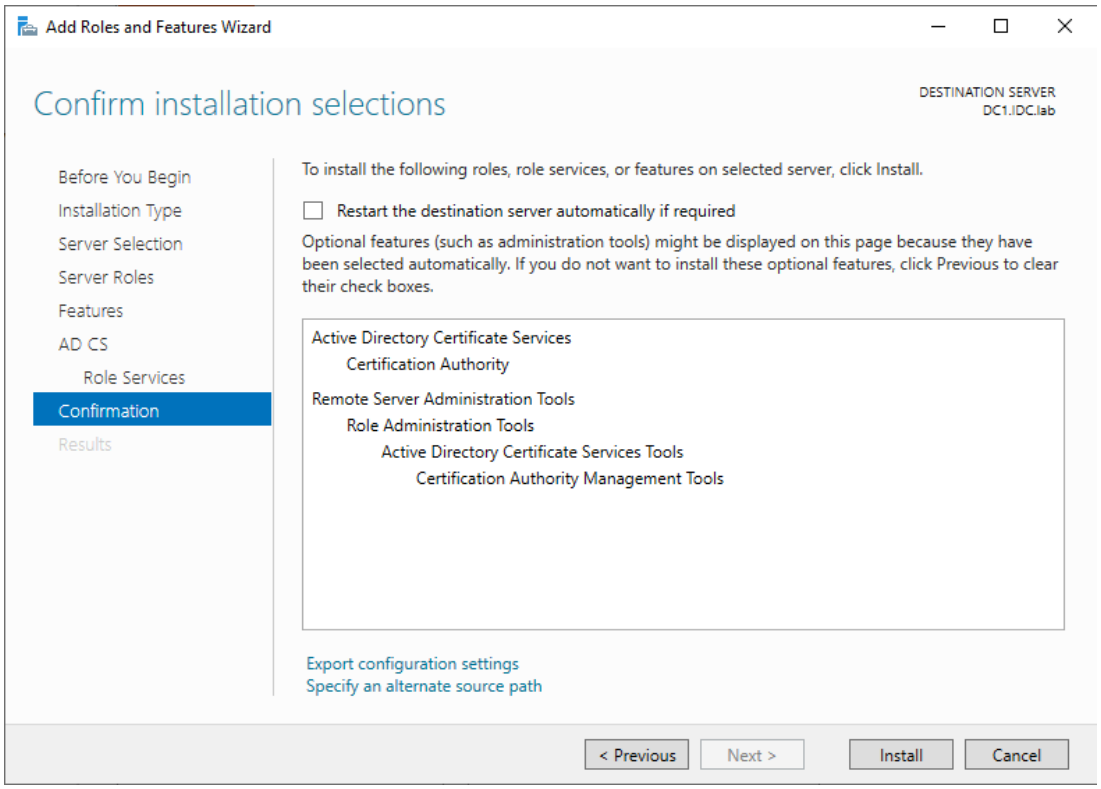


Рисунок 3.21 Запуск процесу встановлення ролі

Перевіряємо обрані компоненти та натискаємо Install (рис. 3.21).

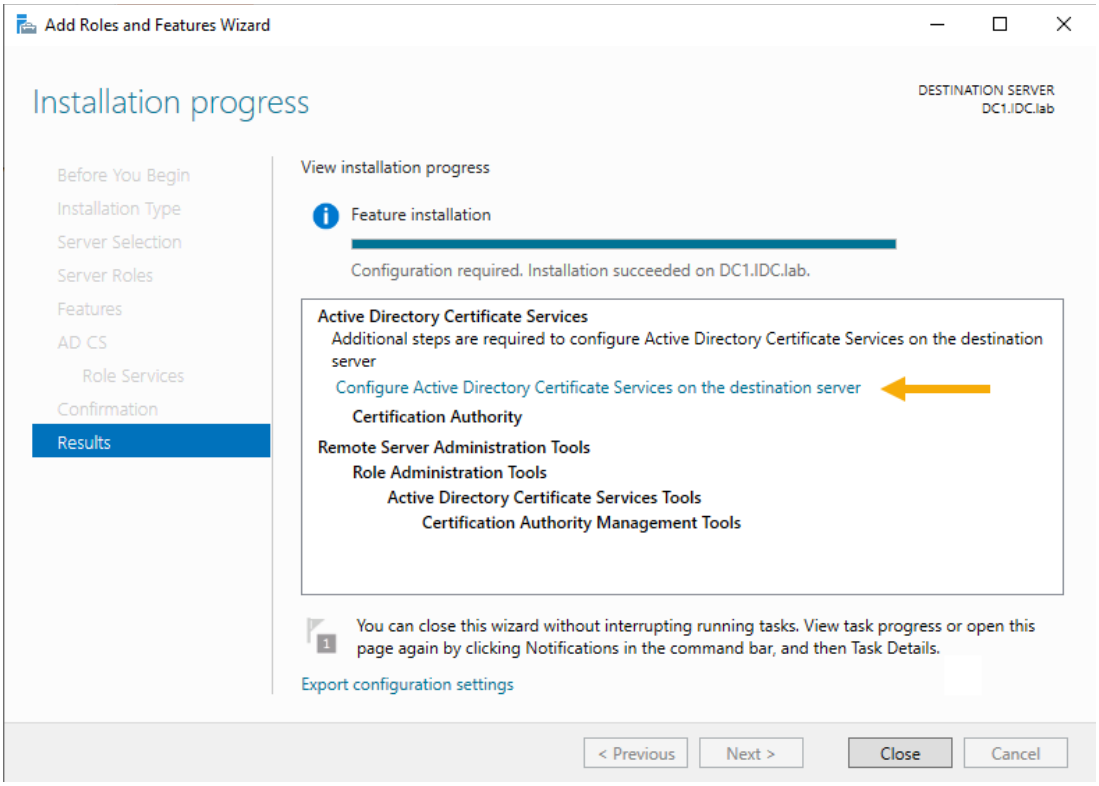


Рисунок 3.22 Завершення встановлення ролі

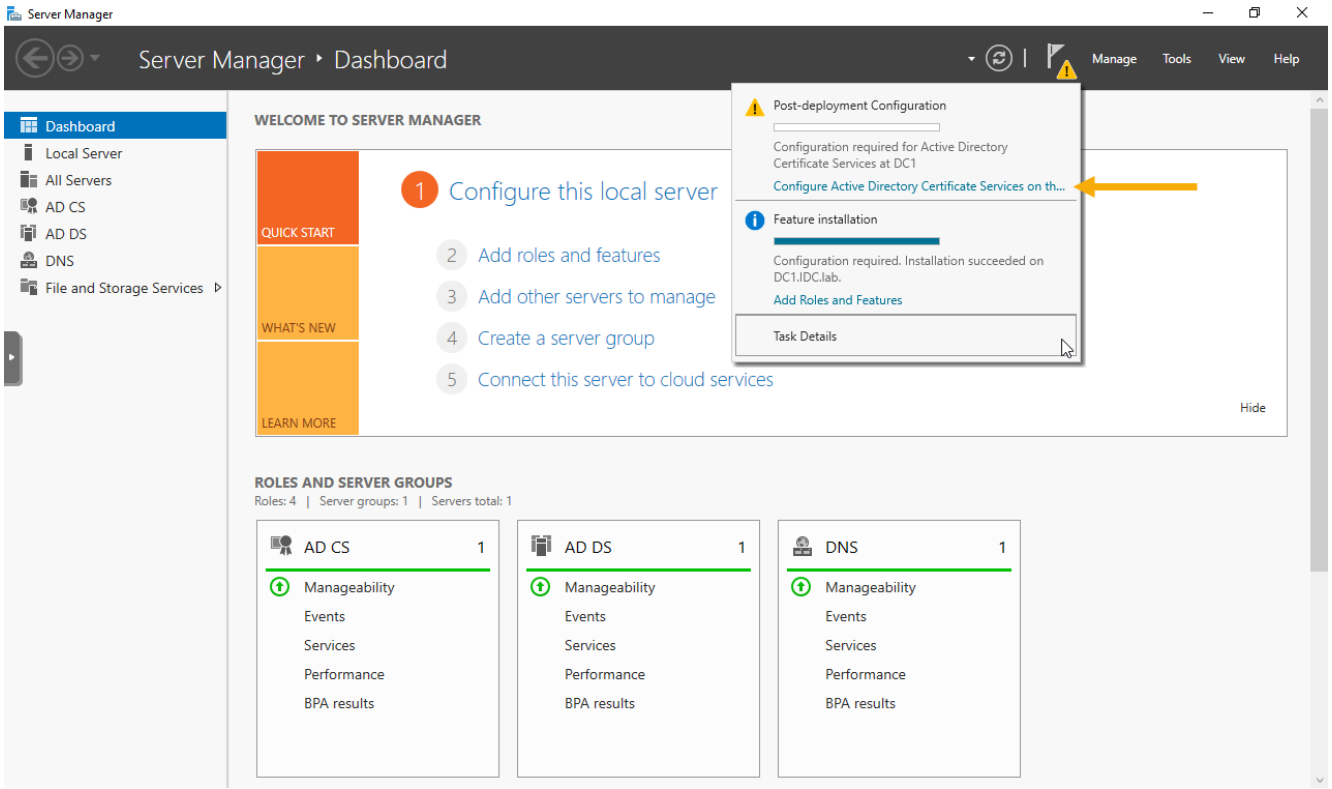


Рисунок 3.23 Запуск конфігуратора у Диспетчері серверів

На останньому кроці майстра натисніть на рядок Configure Active Directory Certificate Services on the destination server для переходу до процесу випуску кореневого сертифіката (рис. 3.22). Якщо це вікно випадково було закрито без запуску конфігуратора, то запустити його можна через Диспетчер серверів. В області повідомлень має з'явитись відповідна опція (рис. 3.23).

Переходимо до налаштування центру сертифікації. Для цього ми можемо використовувати облікові дані поточного користувача – адміністратора домену.

Тут і далі ми залишатимемо в основному значення, які пропонуються системою за умовчанням. Тому для стислості будемо наводити тільки ключові скріншоти, а також ті, де вносилися зміни.

Credentials – залишаємо за замовчуванням і тиснемо Next (рис. 3.24).

Role Services – ставимо галочку в рядку Certification Authority і тиснемо Next.

Setup Type – залишаємо перемикач у значенні Enterprise CA – Next.

CA Type – знову залишаємо значення за замовчуванням – Root CA – Next.

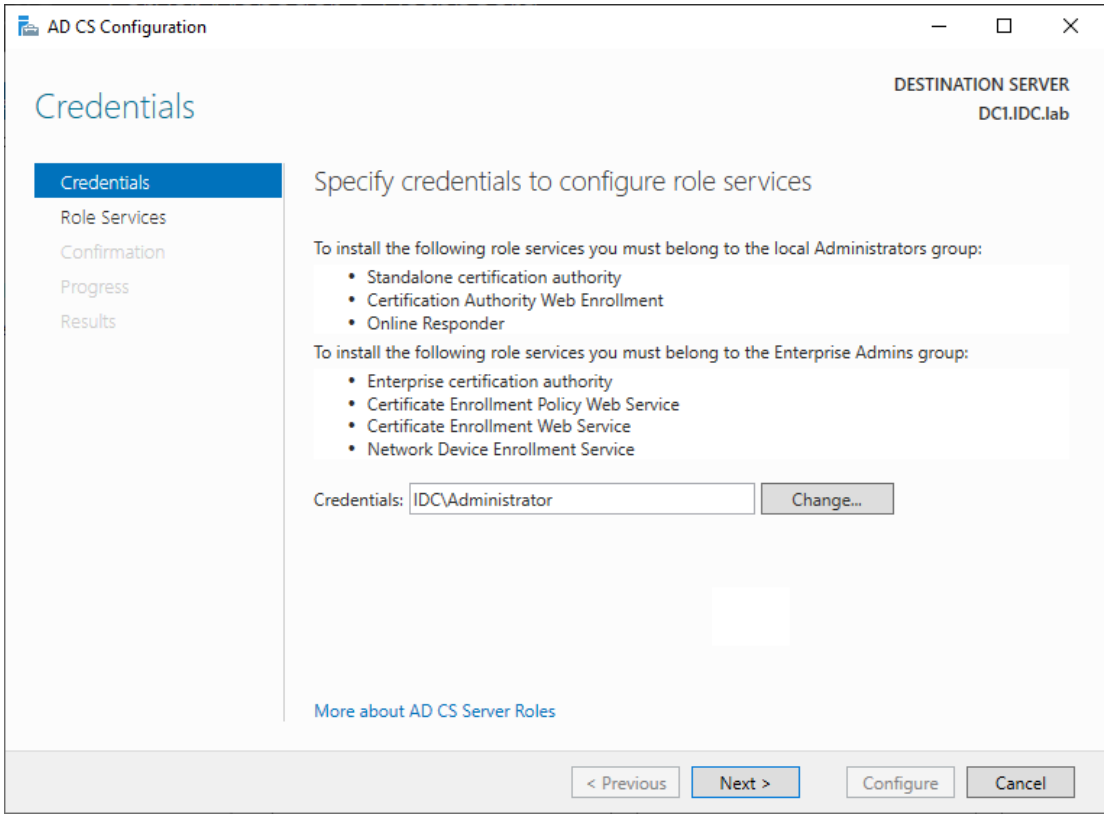


Рисунок 3.24 Налаштування Credentials центру сертифікації

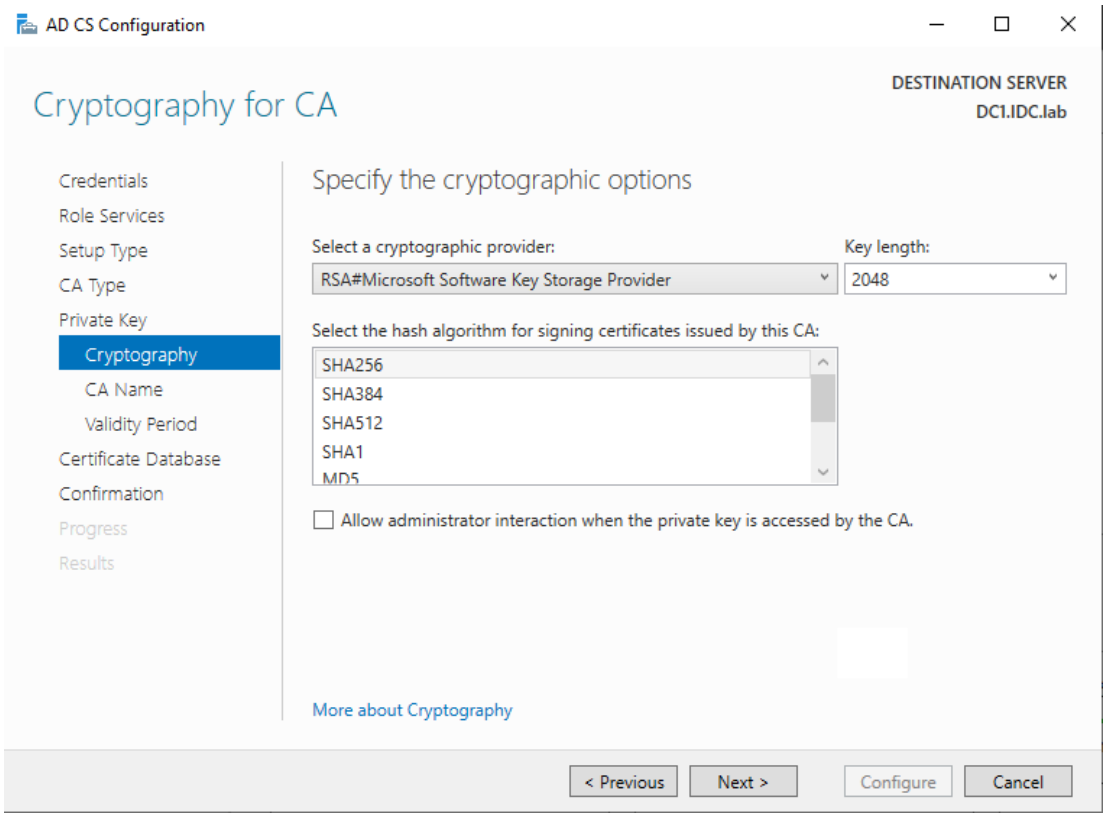


Рисунок 3.25 Налаштування шифрування центру сертифікації

Private Key – Create a new private key – Next

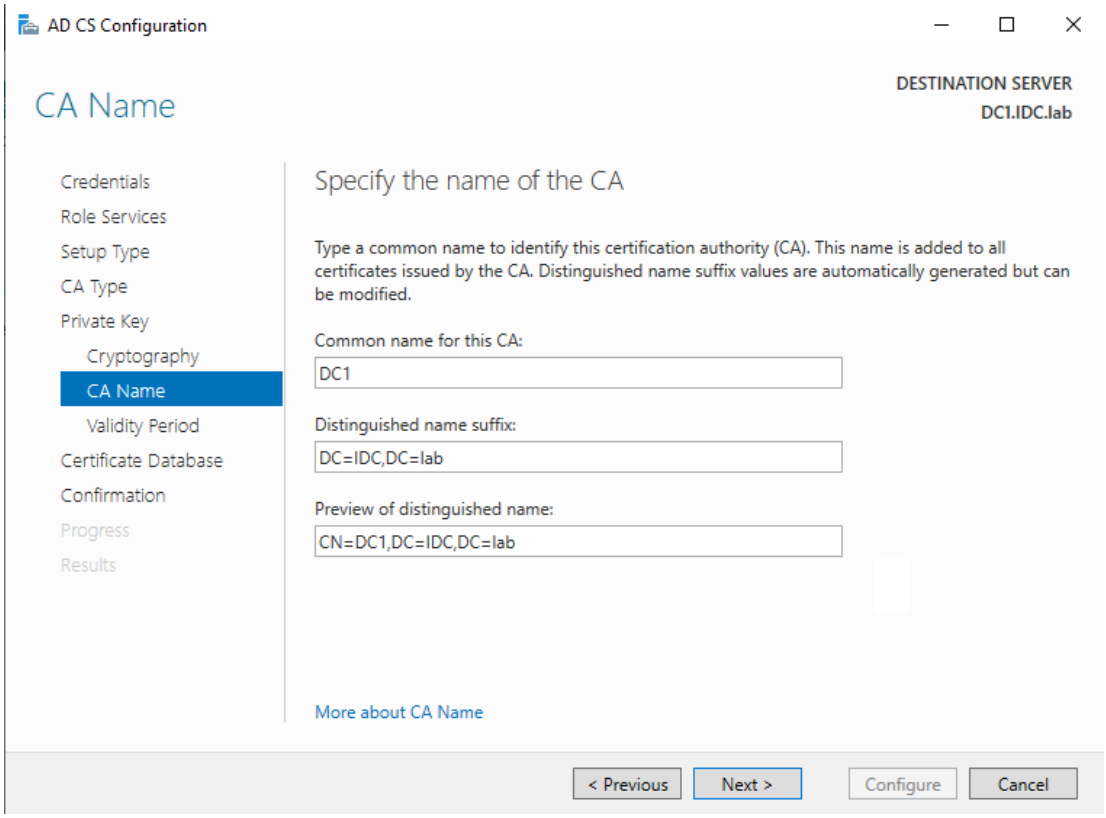


Рисунок 3.26 Налаштування імені центру сертифікації

Cryptography for CA – тут рекомендується вибрати алгоритм SHA256, який система пропонує використовувати за промовчанням (рис. 3.25).

CA Name – Ім'я Центру сертифікації – повинно збігатися з hostname комп'ютера. Це одна з вимог до сертифікату LDAPS. У нашому випадку це DC1 (рис. 3.26).

Наступний крок – Термін дії. Тут варто поставити значення побільше. Якщо залишити значення за замовчуванням – 5 років, то через 5 років агент контролера домену раптово перестане працювати, і на виявлення проблеми та її усунення може піти багато сил та часу.

CA Database – нічого не міняємо, тиснемо Next.

На останньому етапі підтверджуємо наш вибір натисканням кнопки Configure.

Після завершення дивимось на результат (рис. 3.27).

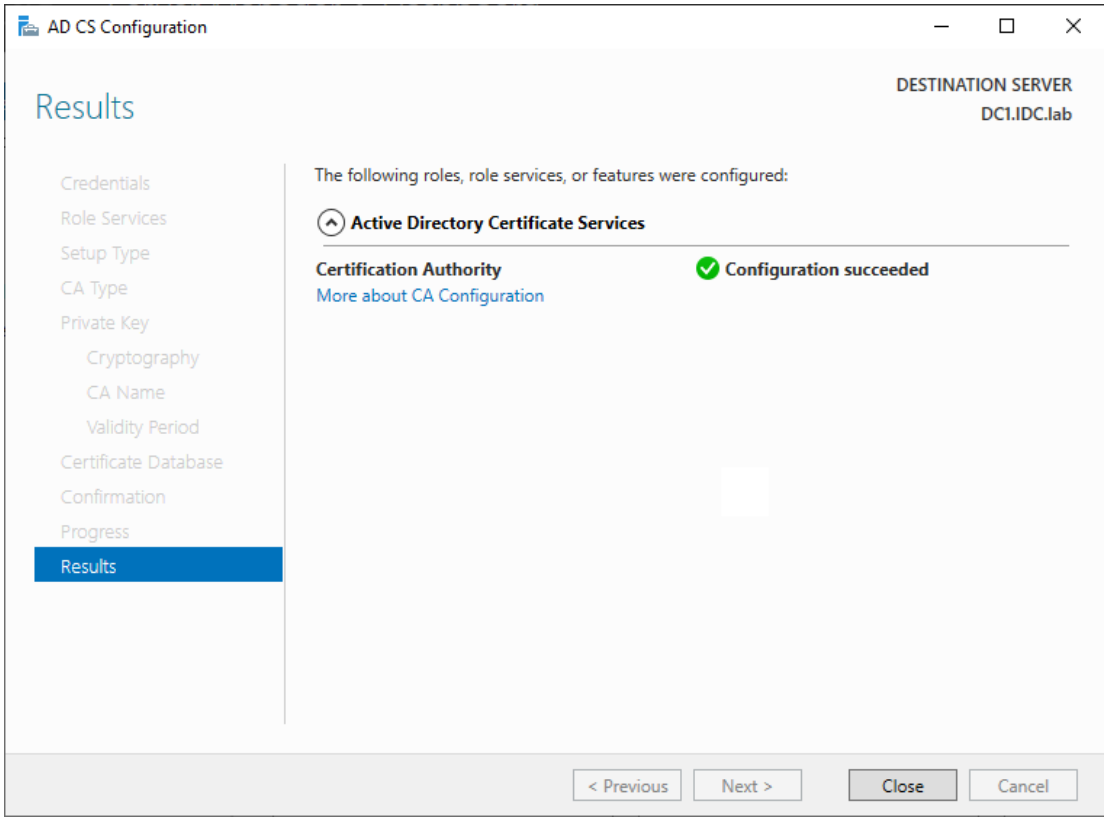


Рисунок 3.27 Результат налаштування центру сертифікації

У результаті кореневий сертифікат Active Directory буде додано до сховища довірених кореневих центрів сертифікації підприємства. Але це сховище оновиться лише при наступному застосуванні групової політики. Щоб це сталося, перезавантажимо сервер.

Після перезавантаження зайдемо в Server Manager і в меню Tools відкриємо Certification Authority.

Розкриємо дерево та в розділі Issued Certificates (Видані сертифікати) побачимо наш сертифікат контролера домену (рис. 3.28).

Наступним етапом нам потрібно зберегти сертифікат у файл, щоб потім мати можливість проімпортувати його до Soffid Sync server.

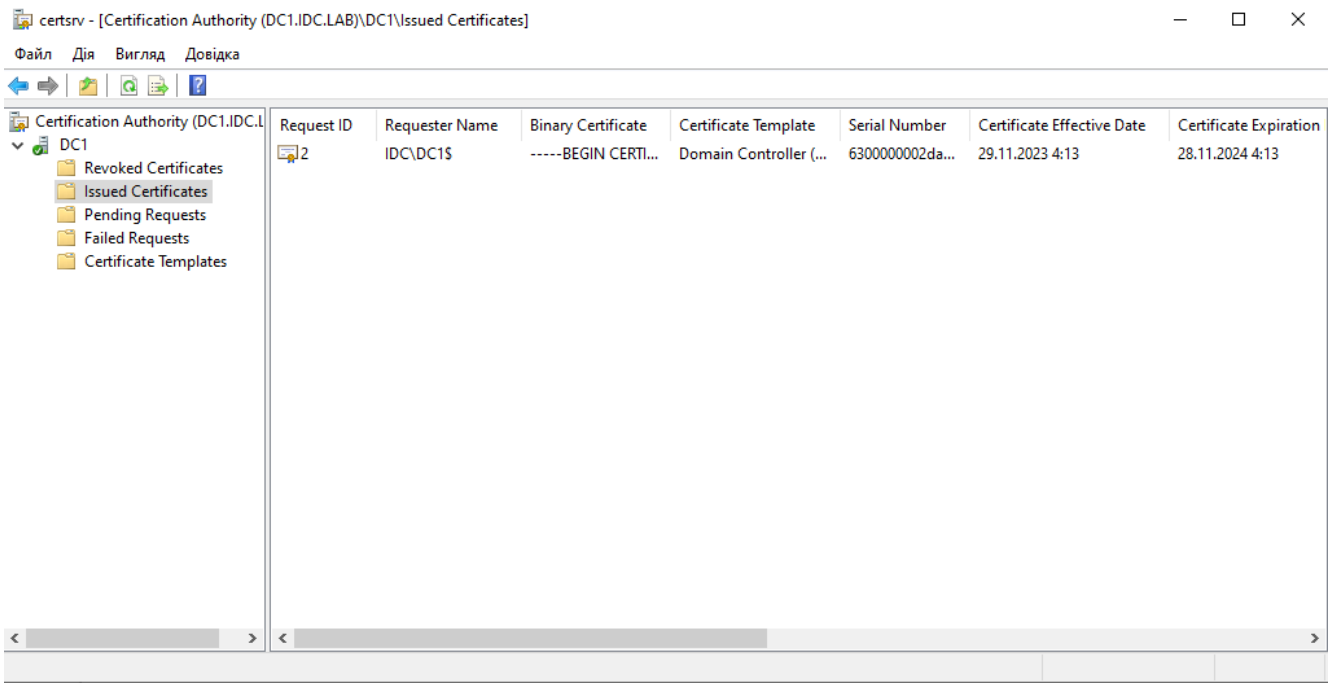


Рисунок 3.28 Сертифікат контролера домену у списку Issued Certificates

Подвійним натисканням миші відкриваємо сертифікат та переходимо на вкладку Шлях сертифікації. Обираємо кореневий сертифікат (DC1) і натискаємо кнопку Переглянути сертифікат (рис. 3.29).

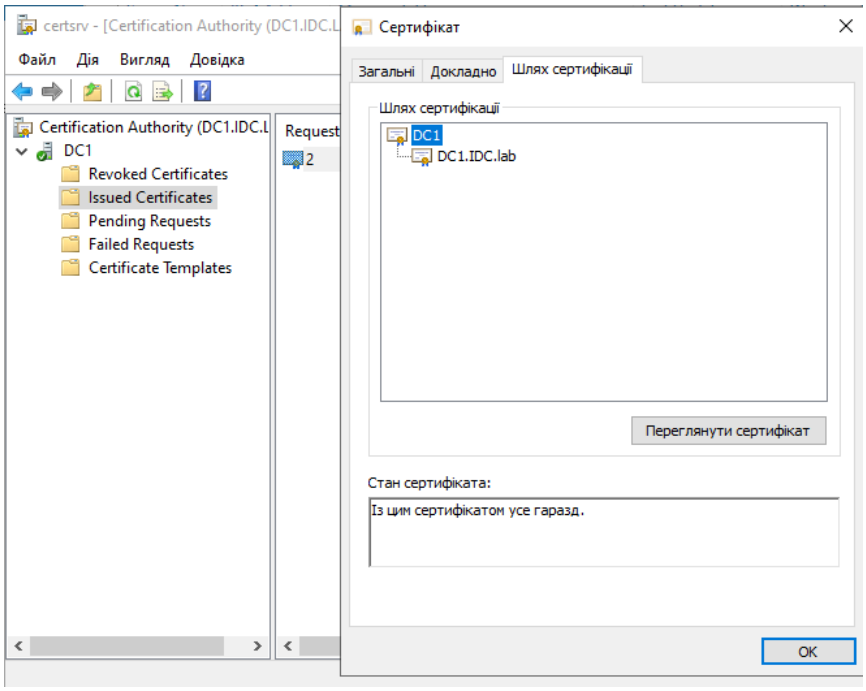


Рисунок 3.29 Перегляд сертифікату контролера домену

У вікні, що відкрилося, переходимо на вкладку Докладно і тиснемо на кнопку Копіювати до файлу… (рис. 3.30).

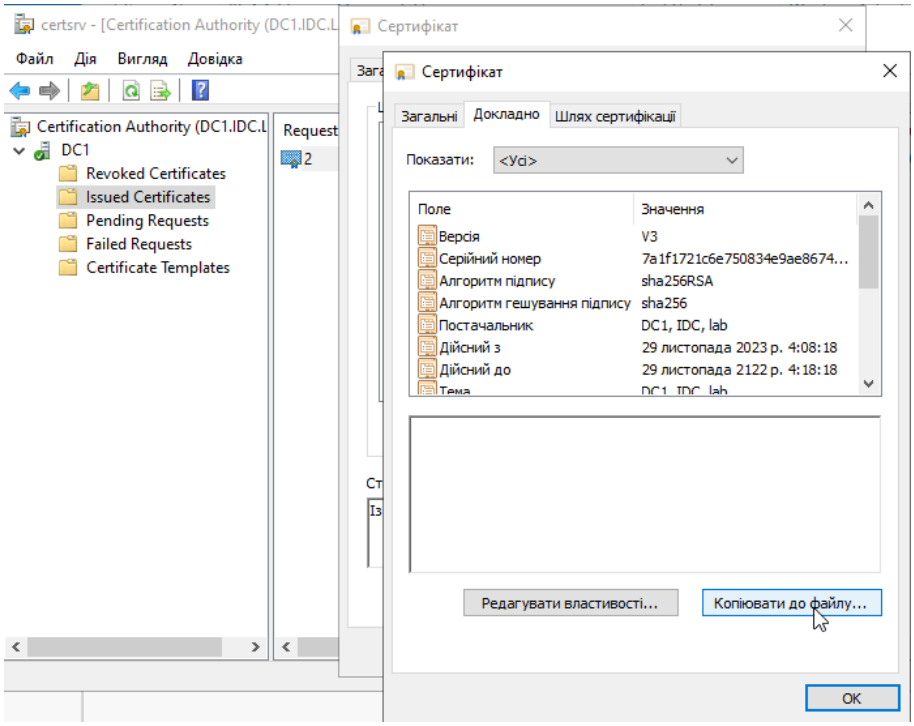


Рисунок 3.30 Перегляд кореневого сертифікату контролера домену

Запуститься Майстер експорту сертифікатів. На першому екрані просто тиснемо Далі.

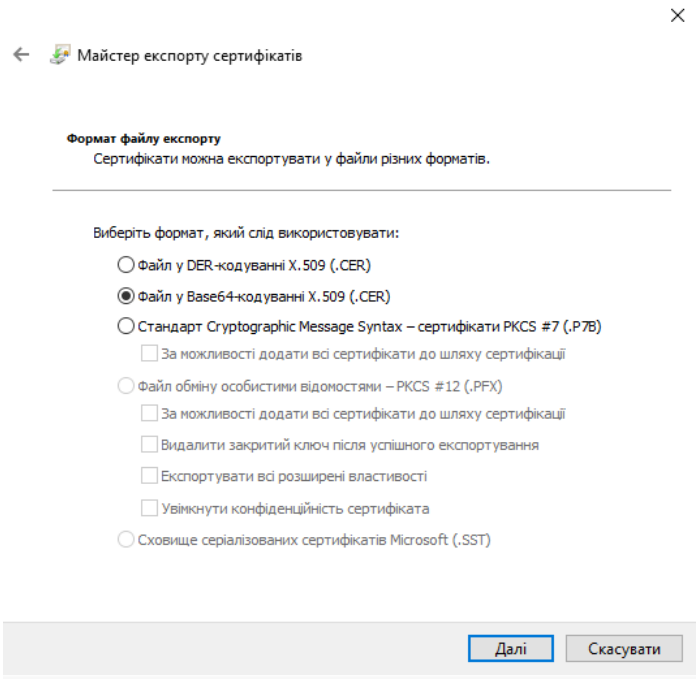


Рисунок 3.31 Майстер експорту сертифікатів

На другому кроці Формат файлу експорту вибираємо другий варіант – Файл у Base64-кодуванні X.509 (.CER) і тиснемо Далі (рис 3.31).

Через кнопку Огляд… вибираємо папку та ім'я файлу та тиснемо Зберегти. Далі натискаємо Далі.

Щоб завершити процес експорту сертифіката, натиснемо Готово.

Запам'ятаймо папку та ім'я файлу, куди ми зберегли сертифікат. Ця інформація нам знадобиться пізніше, коли ми встановимо Soffid Sync server на контролер домену.

3.2.2 Встановлення Java на Windows Server

Перш ніж встановлювати Soffid, встановимо Java, оскільки без неї наш Sync server не працюватиме. Причому в останніх версіях інсталятора немає перевірки

наявності Java в системі по ходу встановлення Soffid Sync server. Тому якщо попередньо не встановити Java, то Soffid Sync server все одно встановиться, але не повністю, оскільки без Java не запуститься конфігуратор (майстер налаштування). При цьому жодних повідомлень про помилки ми не побачимо, а в логах буде порожньо.

Починаючи з версії Soffid Sync server 3.3.2, розробники перейшли на використання Java 11, тому використовувати звичайну Java Runtime Environment з сайту java.com вже не вийде, оскільки вона містить бібліотеки версії Java 8.

Щоб встановити Java 11, нам знадобиться скачати Java SE Development Kit 11, доступний для завантаження на сайті oracle.com. Щоб завантажувати файли з цього ресурсу, необхідно мати обліковий запис. Якщо облікового запису немає, то доведеться пройти реєстрацію – вона не дуже складна та абсолютно безкоштовна.

Отже, переходимо за посиланням https://www.oracle.com/cis/java/technologies/javase/jdk11-archive-downloads.html і знаходимо файл під нашу операційну систему. Для Windows Server це буде Windows x64 Installer. Натискаємо на посилання для скачування, входимо до облікового запису Oracle і отримуємо файл jdk-11.0.20_windows-x64_bin.exe.

Запускаємо інсталятор та встановлюємо Java.

Відразу після цього необхідно вручну налаштувати змінні оточення, оскільки під час встановлення Java Development Kit вони не додаються.

Насамперед копіюємо шлях до каталогу, в який було встановлено Java. За замовчуванням він буде таким: C:\Program Files\Java\jdk-11.

Далі відкриваємо Настройки та натискаємо значок Система. У списку зліва вибираємо пункт Про програму, в підрозділі Пов'язані налаштування знаходимо та відкриваємо Додаткові налаштування системи. На вкладці Додатково натискаємо кнопку Змінні оточення. У розділі Системні змінні натиснемо кнопку Створити… та вкажємо такі дані (рис. 3.32).

Ім'я змінної: JAVA_HOME

Значення змінної: C:\Program Files\Java\jdk-11 – шлях може відрізнятися.

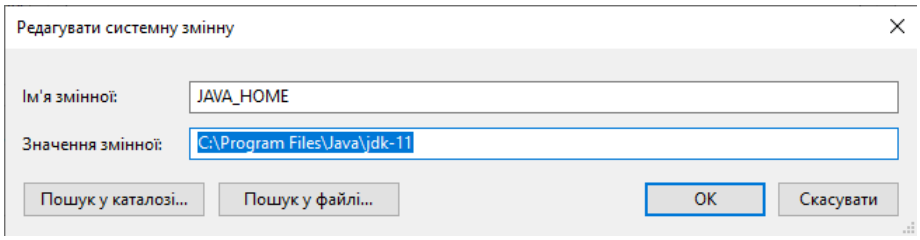


Рисунок 3.32 Додавання змінній оточення

Збережемо зміни, натиснувши ОК. Тепер у списку Системні змінні знайдемо змінну оточення Path, оберемо її та натиснемо Редагувати…. У вікні, що з'явиться, натиснемо кнопку Створити, щоб додати рядок з новим значенням: %JAVA_HOME%\bin. Вносимо значення та натиснемо ОК – як у поточному вікні, так і у двох попередніх – спочатку у вікні Змінні оточення і потім у вікні Властивості системи (рис 3.33).

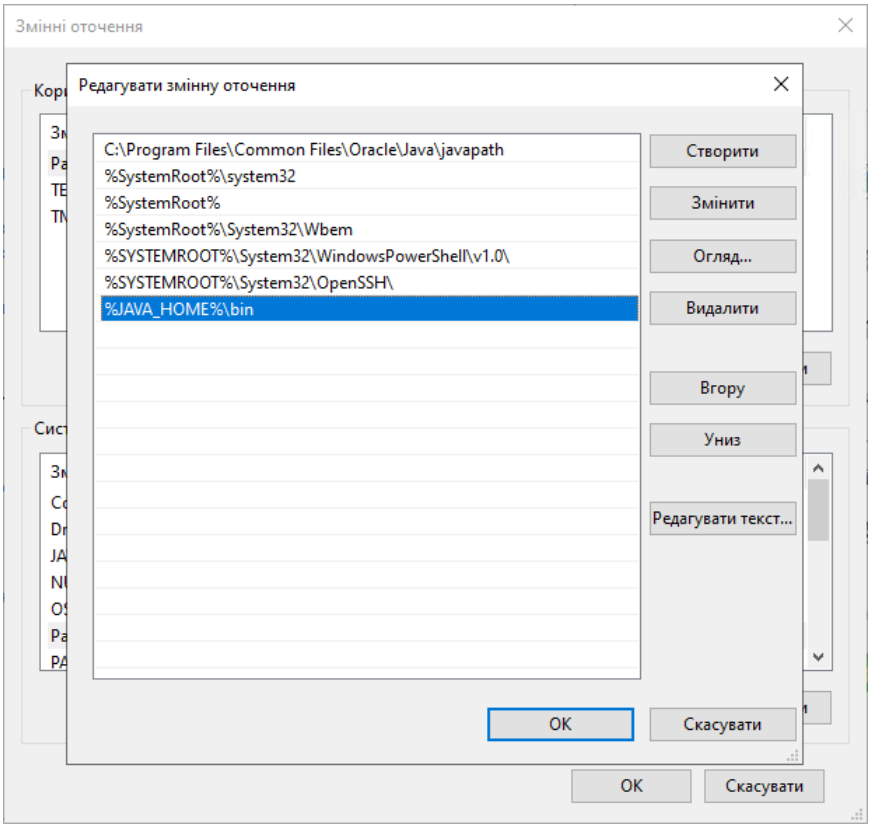


Рисунок 3.33 Редагування змінній оточення

Для перевірки відкриємо консоль (Win+R, cmd) та послідовно вкажемо дві команди:

```
echo %JAVA_HOME%
java --version
```

Якщо JDK встановлено правильно і змінні оточення налаштовані коректно, результат буде приблизно таким (рис. 3.34).

Рисунок 3.34 Перевірка змінних оточення

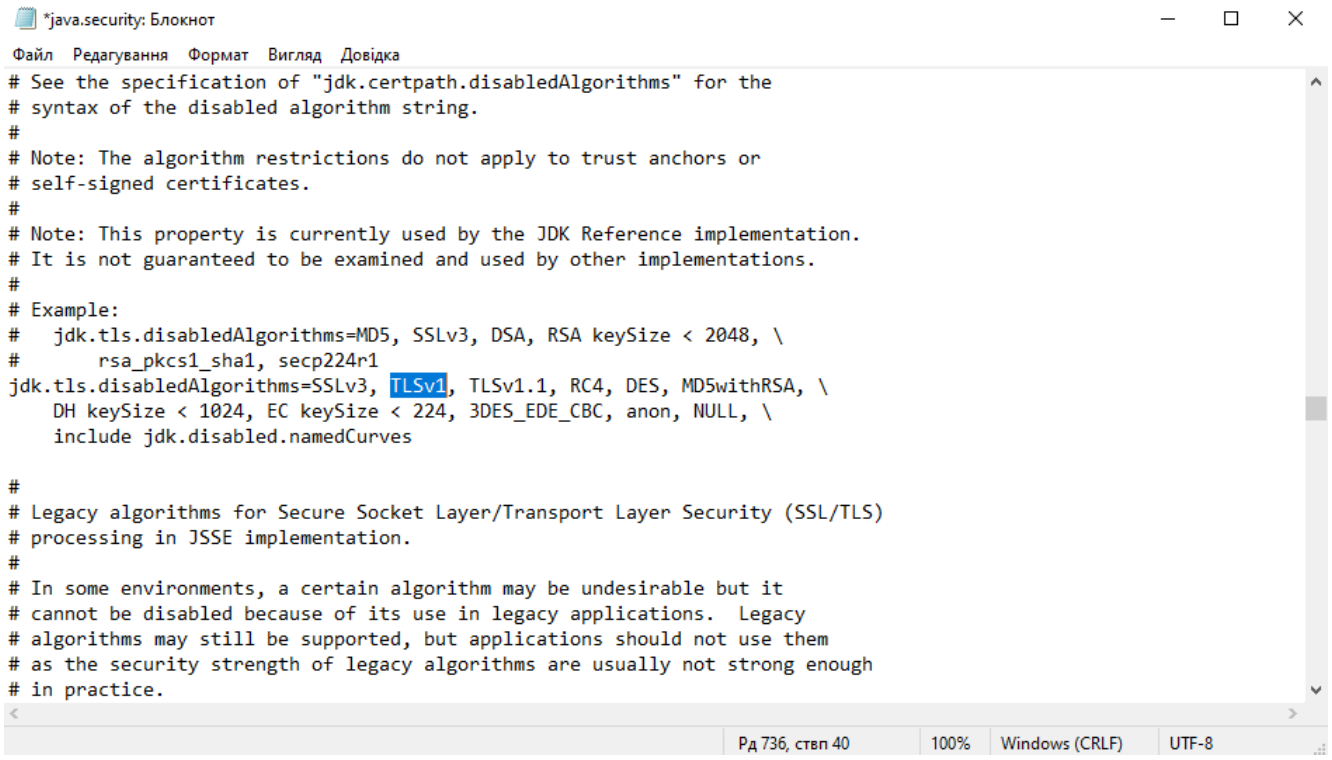


Рисунок 3.35 Налаштування параметрів безпеки Java

Після встановлення Java необхідно виправити параметри безпеки. Якщо цього не зробити, сервер швидше за все не зможе приєднатися до агента і на етапі установки з'єднання з’явиться помилка: The server selected protocol version TLS10 is not accepted by client preferences. Це пов'язано з тим, що сервер Soffid використовує TLS v1, який за замовчуванням вимкнено у Java JDK 11 for Windows.

Заходимо в папку з встановленою Java (у нашому випадку це C:\Program Files\Java\jdk-11) і переходимо там в папку conf, а потім в security. Знаходимо там файл java.security та відкриваємо його у текстовому редакторі (рис 3.35). Шукаємо опцію jdk.tls.disabledAlgorithms та видаляємо параметр TLSv1. Зберігаємо зміни.

На цьому встановлення та налаштування Java завершується.

3.2.3 Встановлення та налаштування Sync Server

На сторінці завантаження Soffid http://download.soffid.com/download/ знаходимо та завантажуємо інсталятор SOFFID 3 Sync server для операційної системи Windows. Якщо потрібно, вказуємо реєстраційні дані.

На момент написання статті останньою доступною версією Soffid Sync server була Version 3.5.4.2 (рис. 3.36). Натискаємо на посилання Windows MSI Installer та отримуємо файл SOFFID 3 Sync server-Windows MSI installer-3.5.4.2.msi.

Копіюємо файл на сервер контролера домену. Найпростіше це зробити, зайшовши на віддалений робочий стіл та скориставшись функцією копіювання-вставки файлів.

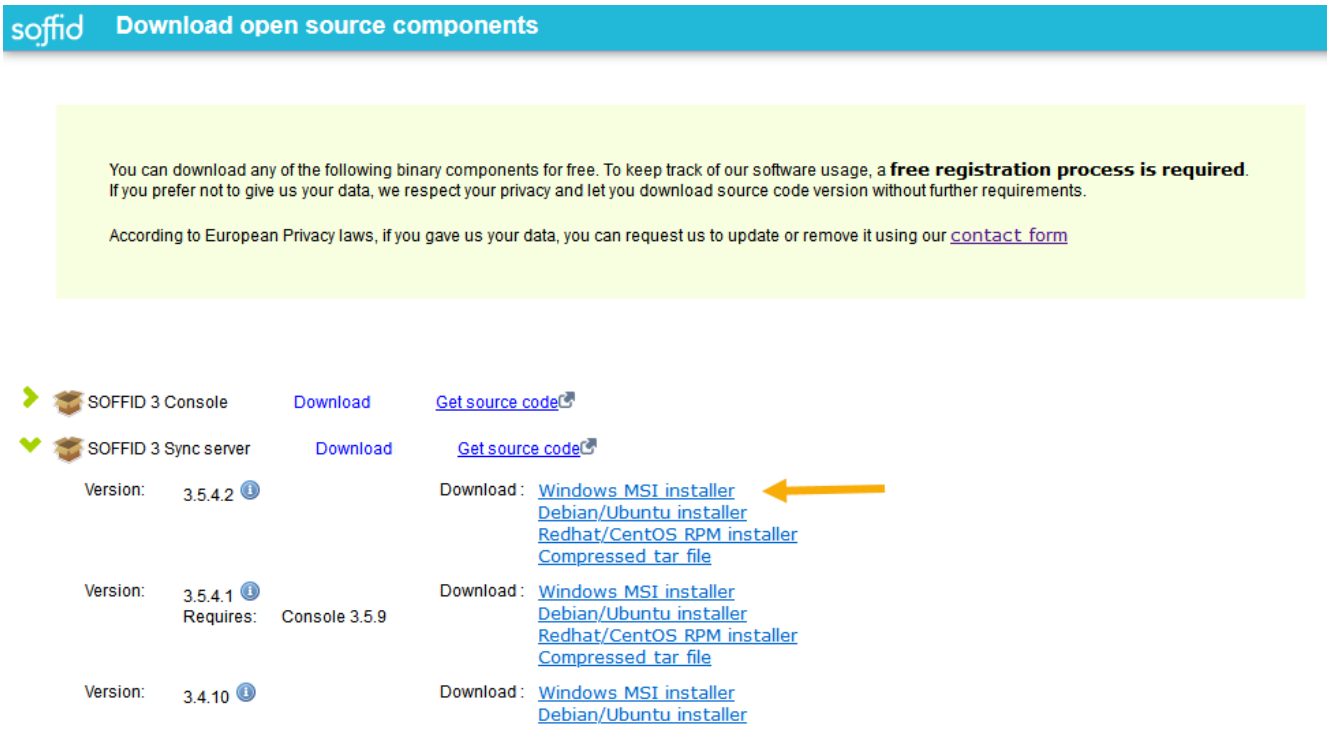


Рисунок 3.36 Завантаження пакету Soffid Sync Server для Windows

Перед тим, як запустити установку Soffid Sync server, нам потрібно переконатися, що Sync server агент, який встановлюється, зможе підключитися до основного Sync server, адресу якого ми вкажемо в процесі конфігурації. Наприклад, якщо в якості рядка підключення буде використовуватися рядок https://soffid:1760, то ми повинні переконатися, що комп'ютер зможе перетворити ім'я сервера на ip адресу. Якщо в якості імені сервера використовується FQDN (від англ. Fully Qualified Domain Name – повноцінне доменне ім'я), то система швидше за все зможе перетворити його за допомогою DNS сервера – у цьому випадку нічого додатково робити не потрібно. Але якщо, як у прикладі, використовується скорочене ім'я, то тоді нам необхідно додати у файл hosts рядок, за допомогою якого Windows перетворить це ім'я сервера на ip адресу.

Файл hosts знаходиться у каталозі C:\Windows\System32\drivers\etc. Відкриємо його за допомогою текстового редактора та додамо в кінець рядок виду (рис. 3.37):

```
192.168.2.201   soffid
```

Збережемо зміни.

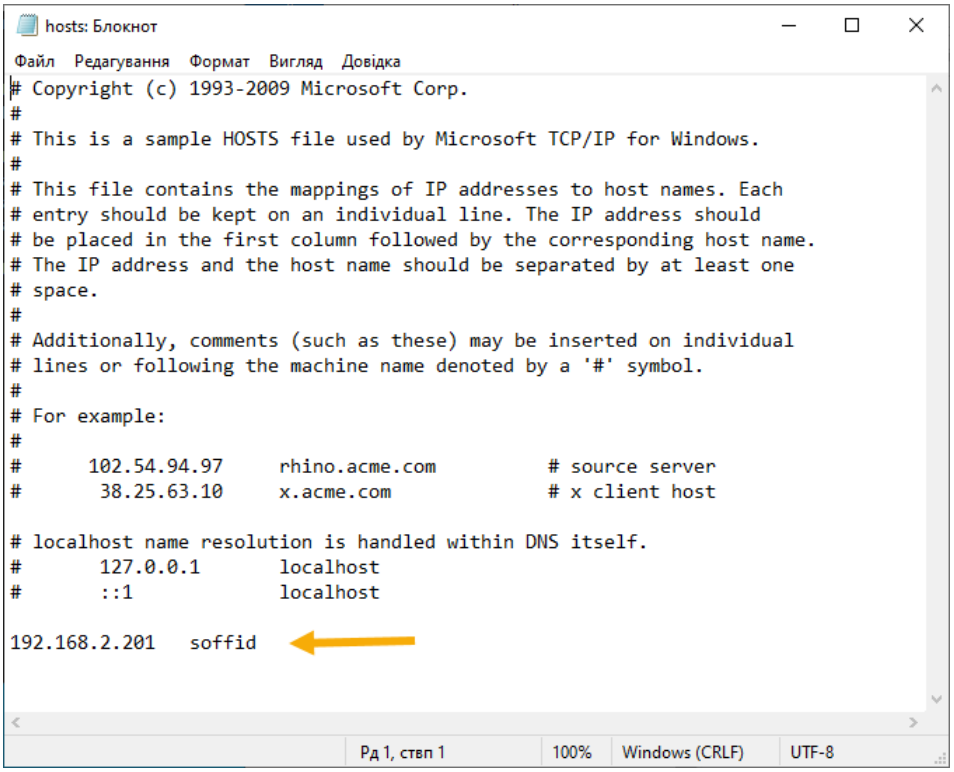


Рисунок 3.37 Редагування файлу hosts на контролері домену

Тепер можна приступати до встановлення Soffid Sync server.

Запускаємо інсталятор. У процесі встановлення запуститься Soffid Sync server configuration wizard (Майстер налаштування Soffid Sync server). Якщо цього не станеться, завжди можна запустити майстер налаштування вручну за допомогою наступної команди:

```
"%ProgramFiles%\soffid\iam-sync\bin\configure.bat"
```

Ця команду запустить скрипт майстра первинного налаштування. Його слід запускати з командного рядка Адміністратора. У тому числі, цей скрипт може стати в нагоді, якщо з якихось причин знадобиться налаштувати Sync server повторно. У цьому випадку достатньо видалити попередню конфігурацію, очистивши вміст папки C:\Program Files\Soffid\IAM-Sync\conf, і запустити вказаний файл C:\Program Files\Soffid\IAM-Sync\bin\configure.bat.

Почнеться процес конфігурації Sync server, під час якого нам потрібно буде відповісти на такі запитання (рис. 3.38):

1) Is this the first sync server in the network? – Це ваш перший Sync server у мережі? Оскільки даний сервер встановлюється на системі, що підключається (контролері домену), то вочевидь, він не є першим сервером в мережі. Перший сервер був встановлений разом із Soffid Console на етапі встановлення серверної частини Soffid. Відповімо n (Hi)
2) Connect to a cloud service? Enter ‘n’ to connect to an on-premise service: n (Нет) – Приєднатись до хмарного сервісу? Введіть 'n', щоб підключитися до сервера підприємства. У нашому випадку ми використовуємо свій сервер Soffid та хочемо підключатися до нього. Тому відповідаємо Hi.
3) Server URL: https://soffid:1760
4) Tenant: [master] Залишимо значення за замовчуванням (натиснемо Enter)

На наступному кроці необхідно ввести облікові дані. У процесі налаштування першого сервера синхронізації на лінукс-сервері, при відповіді на аналогічне запитання ми вказували логін та пароль адміністратора бази даних MariaDB. При налаштуванні другого та всіх наступних серверів вже не потрібно вводити облікові дані бази даних. Натомість потрібно вказати URL-адресу основного сервера синхронізації (при відповіді на третє запитання), а також ім'я користувача та пароль консолі Soffid.

5) User: користувач Soffid. Введемо користувача admin, якого ми використовуємо для входу до web-інтерфейсу Soffid.
6) Password: пароль від цього користувача.
7) This server host name: необхідно ввести повне ім'я сервера з доменом (якщо є), або коротке ім'я (без домену). IP адресу тут вказувати не можна.
8) Port to listen to [1760]: номер TCP порту, на якому працюватиме служба Sync server. Рекомендовано використовувати значення за замовчуванням. Погодимося, натиснувши Enter.

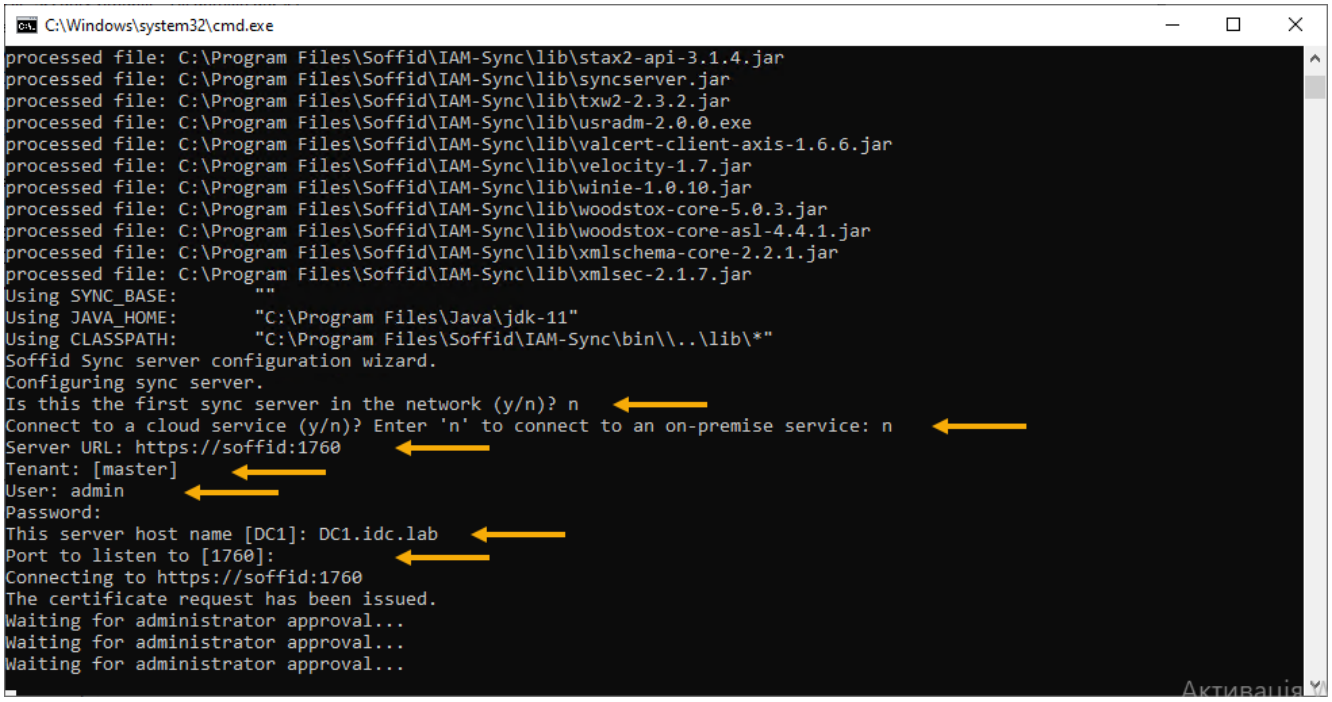


Рисунок 3.38 Встановлення Soffid Sync Server на контролері домену

Після відповіді на останнє запитання майстер налаштування спробує підключитися до основного сервера синхронізації. Якщо з'єднання буде успішним, на екрані з'являться рядки:

```
Waiting for administrator approval…
```

Це означатиме, що у консолі адміністратора Soffid сервера з'явився запит на підключення керованої системи, який потрібно схвалити. Відкриваємо веб консоль Soffid та переходимо в Main Menu > My tasks.

У списку задач користувача admin з'явилася нова задача (Task) з темою New sync server request – Запит від нового сервера синхронізації (рис. 3.39).

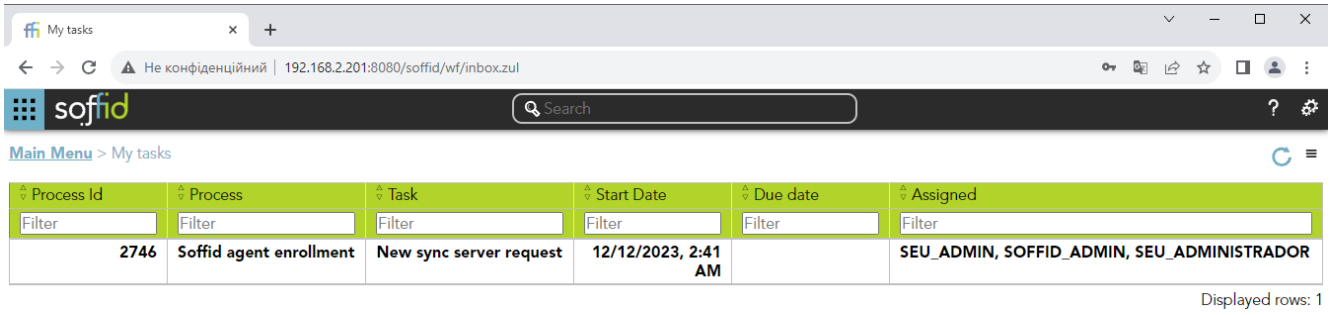


Рисунок 3.39 Запит від нового сервера синхронізації

Натискаємо на цей рядок лівою кнопкою миші, щоб відкрити задачу. З'явиться вікно (рис. 3.40). У цьому вікні потрібно натиснути кнопку Take ownership, щоб схвалити запит на додавання нового сервера.

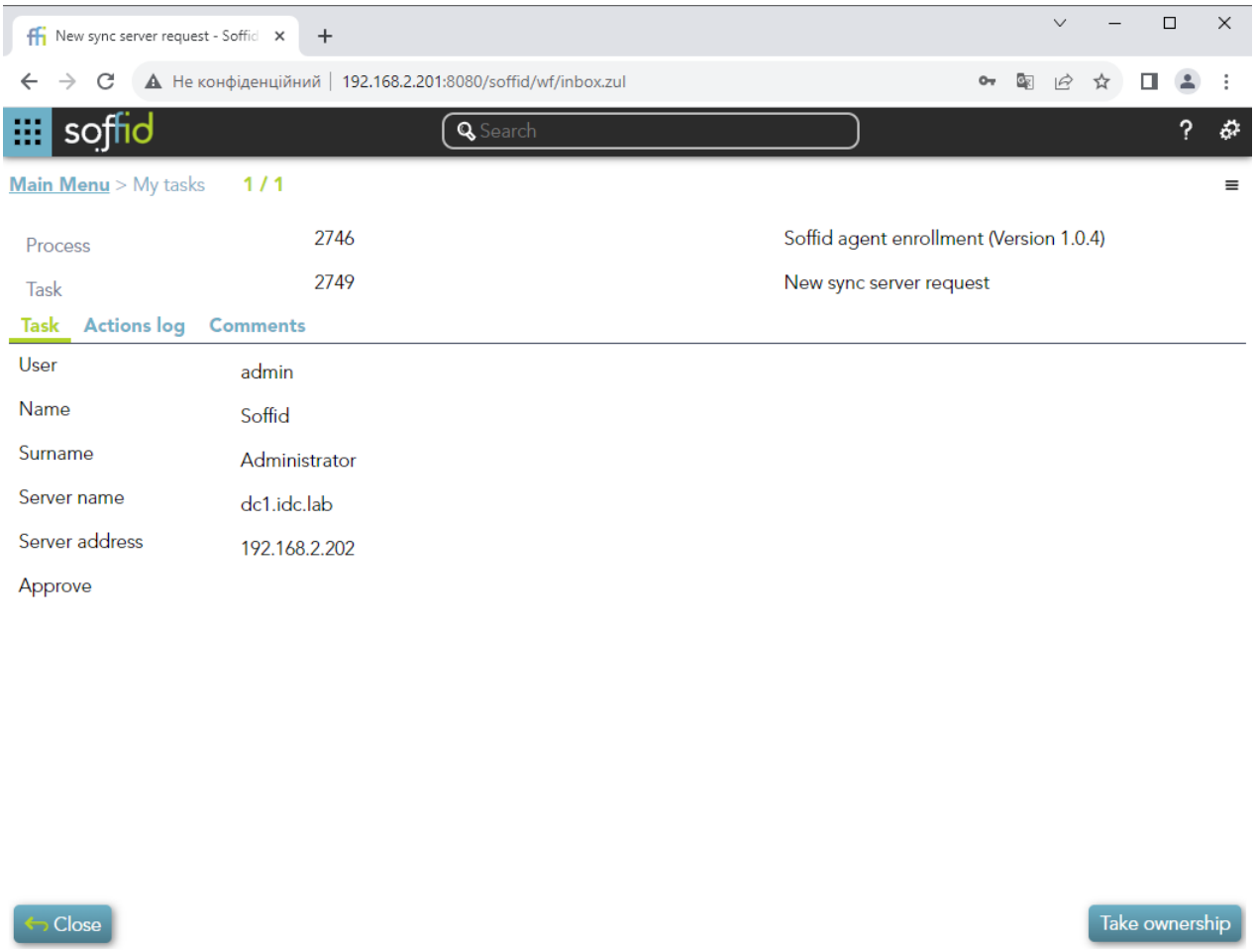


Рисунок 3.40 Подробиці запита від нового сервера синхронізації

Після натискання на кнопку Take ownership навпроти рядка Approve з'явиться список, що випадає. Оберемо в ньому значення Approve та натиснемо End. Запит буде схвалено.

У Soffid можна додавати сервер без підтвердження в консолі. Для цього потрібно додати глобальний параметр, який керує цим процесом. Щоб це зробити, треба перейти в меню Start – Soffid Configuration – Soffid Parameters та створити там новий параметр soffid.server.register зі значенням direct.

Після підтвердження запиту повернемося до контролера домену, де виконується майстер налаштування Sync server. Після декількох секунд паузи там

з'явиться інформація про запуск Soffid Sync server і майстер автоматично завершиться (рис. 3.41).

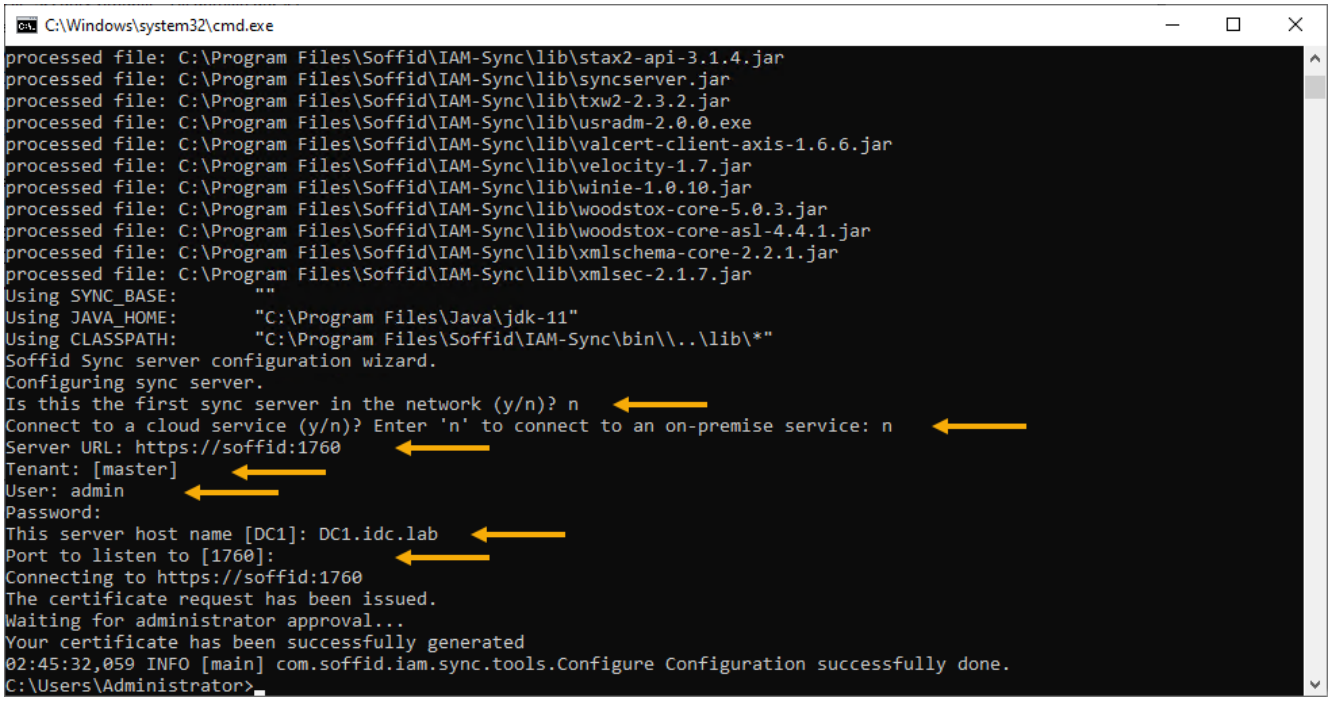


Рисунок 3.41 Успішне завершення налаштування Soffid Sync Server

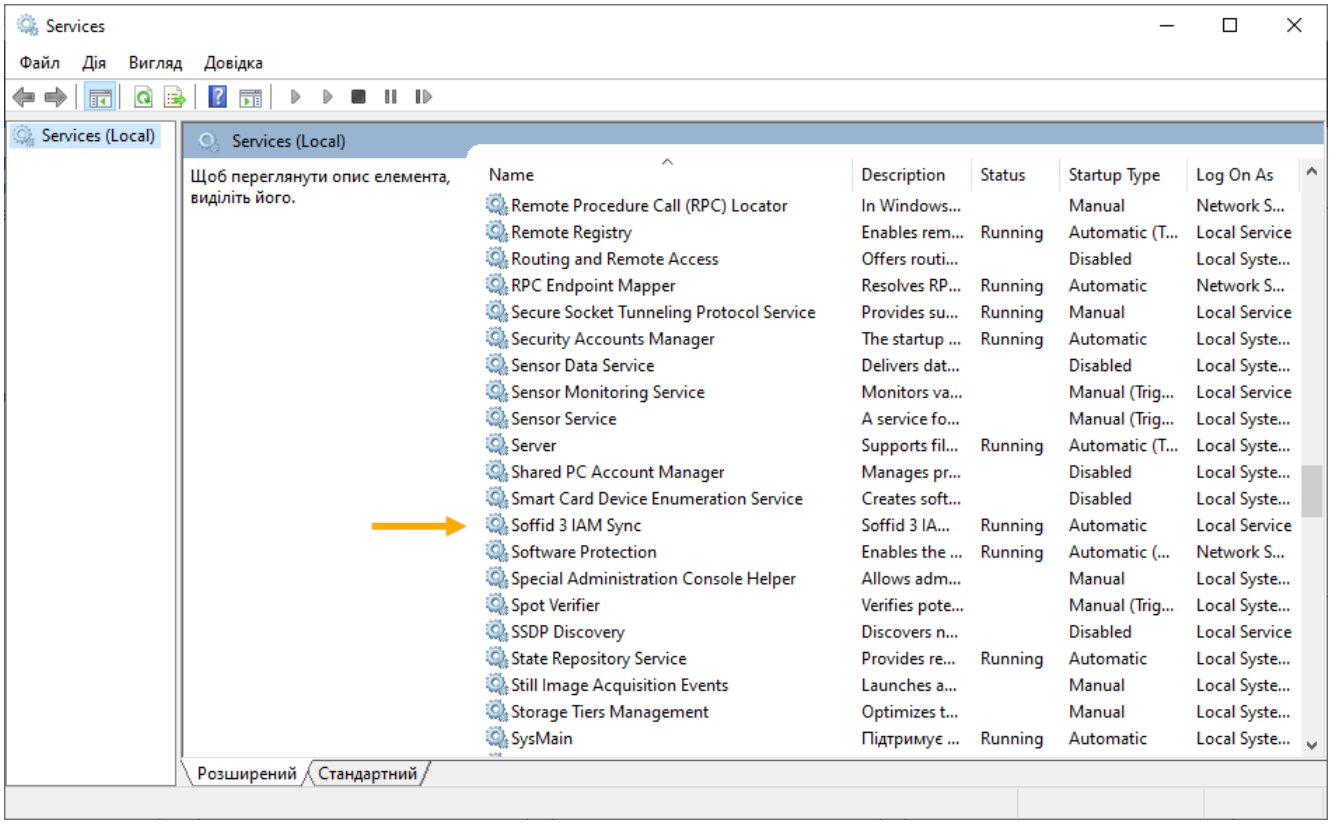


Рисунок 3.42 Служба Soffid 3 IAM Sync

Щоб переконатися, що встановлення та запуск Soffid Sync server пройшли успішно, відкриємо оснащення Services. Для цього зайдемо до Server Manager і в меню Tools оберемо пункт Services (рис. 3.42).

Якщо ви бачите у списку службу Soffid 3 IAM Sync і вона знаходиться в стані Виконується, значить все гаразд.

3.2.4 Імпорт сертифіката домену до сховища Sync Server

Настав час додати до сховища сертифікатів Soffid IAM Sync Server наш сертифікат контролера домену, який ми створили та вивантажили у файл кількома кроками раніше (п. 3.2.1). Ця операція дозволить агенту сервера підключатись до контролера домену по захищеному протоколу LDAPS (LDAP Secure, із шифруванням SSL). Для цього відкриємо на комп'ютері з Active Directory Командний рядок в режимі Адміністратор, перейдемо до каталогу з бінарними файлами Java і виконаємо імпорт сертифіката за допомогою утиліти keytool:

```
  cd c:\Program Files\Java\jdk-11\bin\
  keytool -importcert -v -file "[Шлях до файлу сертифіката]\[Ім’я файлу сертифіката].cer" -keystore "c:\Program Files\Soffid\IAM-Sync\conf\cacerts" -storepass changeit -alias DC1
```

Шлях до папки bin Java може відрізнятися залежно від версії. Також потрібно вказати повний шлях до файлу сертифіката, замінивши на відповідні значення блоки [Шлях до файлу сертифіката] та [Ім'я файлу сертифіката].

Якщо все було зроблено правильно, розпочнеться процес імпорту та на екрані з'явиться питання Trust this certificate? [no], на який треба відповісти yes та натиснути Enter (рис. 3.43).

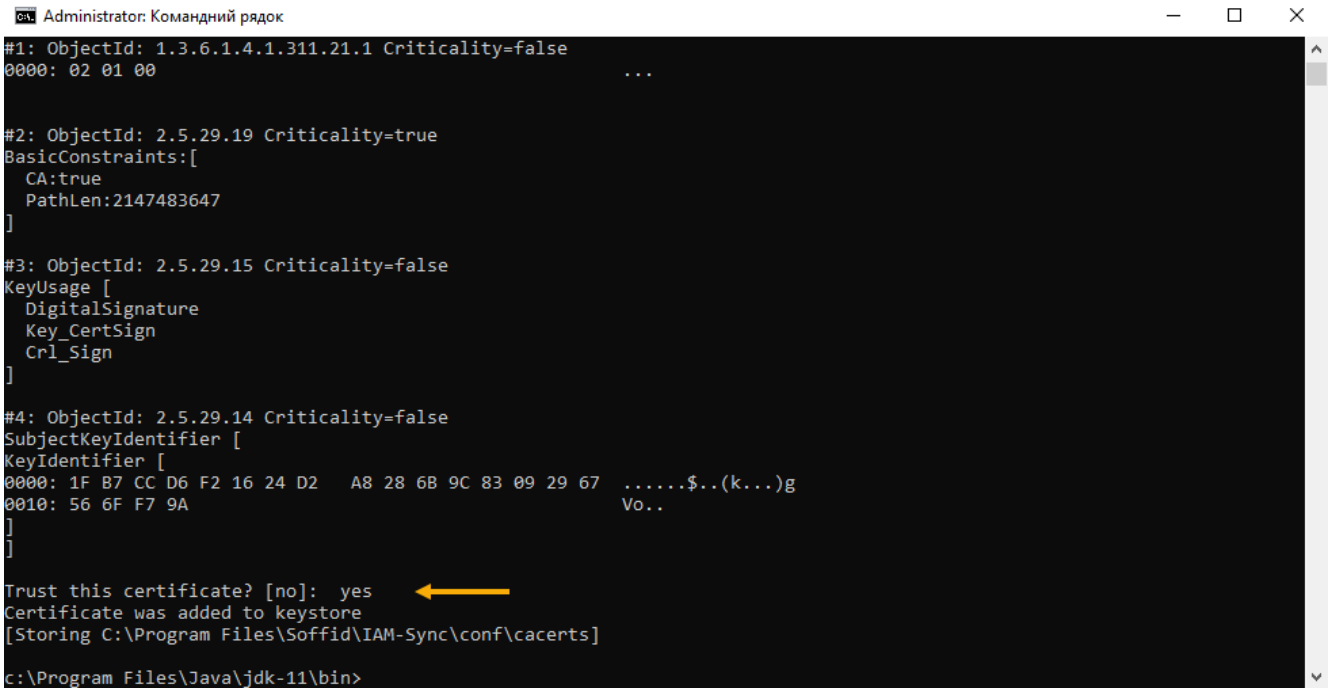


Рисунок 3.43 Імпорт сертифіката домену до сховища Sync Server

Після того, як ви імпортували сертифікат, можна перевірити, чи з'явився він у сховищі за допомогою команди:

```
  keytool -list -v -keystore "c:\Program Files\Soffid\IAM-Sync\conf\cacerts"
-storepass changeit -alias DC1
```

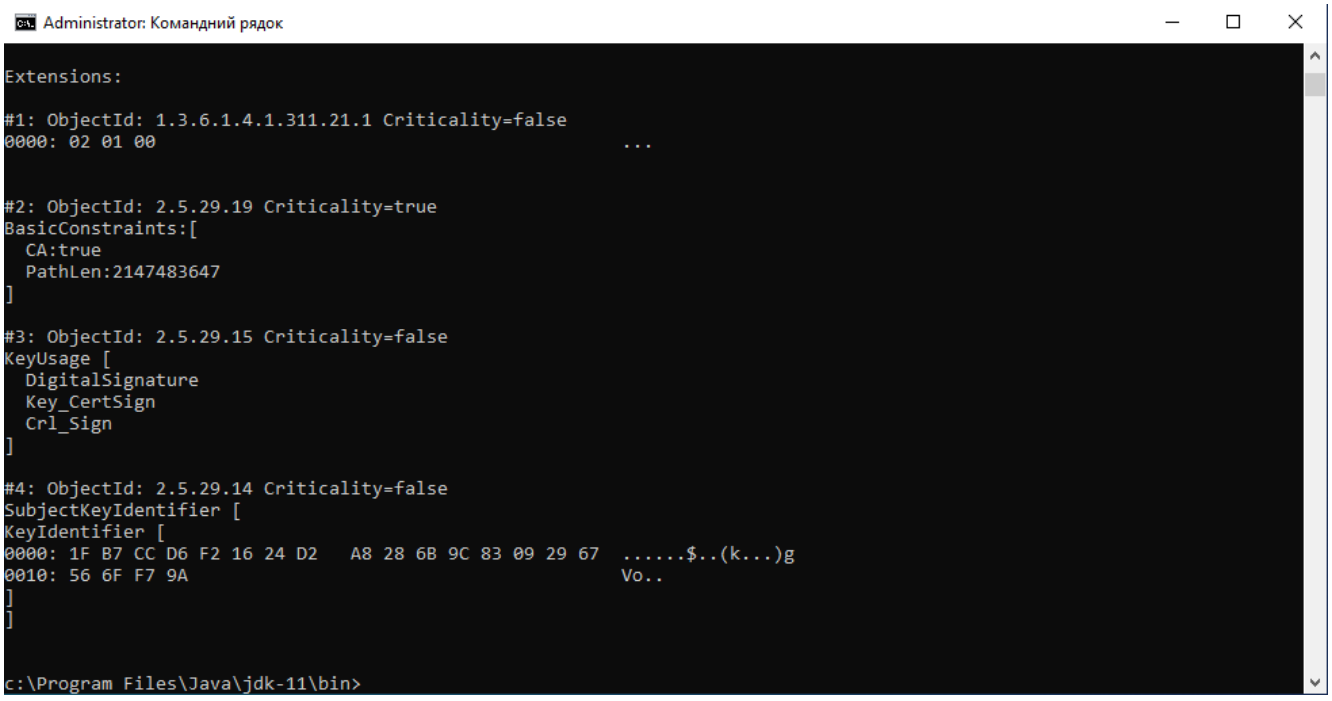


Рисунок 3.44 Перевірка наявності сертифіката домену

Результат роботи цієї команди наведено на рисунку 3.44. На екрані ми маємо побачити, власне, сам сертифікат у текстовому вигляді – це означатиме, що сертифікат успішно імпортований.

Якщо сертифікат не буде знайдено – наприклад, якщо ми ще не встигли його імпортувати, ми побачимо наступне повідомлення про помилку:

```
keytool error: java.lang.Exception: Alias <DC1> does not exist
```

У цьому випадку необхідно все перевірити і, можливо, повторити кроки з експортом та імпортом сертифіката.

3.2.5 Встановлення агента Active Directory на сервері Soffid

В останніх версіях Soffid Sync Server плагін для Active Directory (Windows plugin) вже встановлено. Але якщо виявиться, що його немає, його завжди можна завантажити з сайту розробника та встановити вручну. Щоб це зробити, достатньо зайти на сторінку завантаження Soffid http://download.soffid.com/download/ та у розділі Connectors завантажити останню версію конектора Windows (including Active Directory).

Установка відбувається у веб консолі Soffid. Заходимо в меню Main Menu > Administration > Configuration > Global Settings > Plugins. Натискаємо на плюс і вибираємо завантажений файл. Якщо все пройде успішно, у списку з'явиться новий плагін (рис. 3.45).

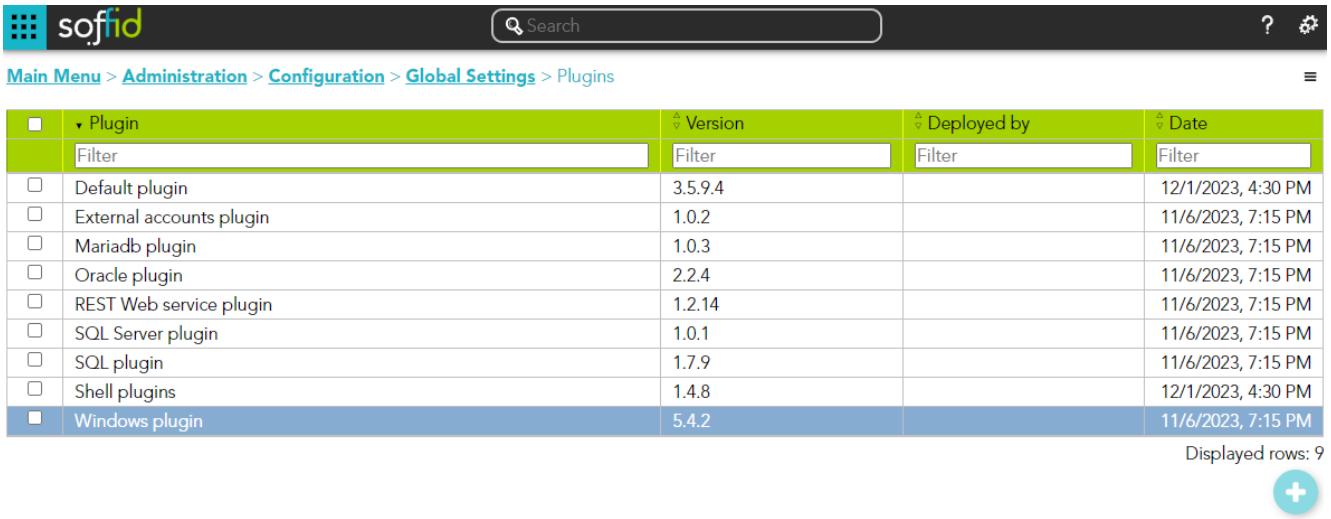


Рисунок 3.45 Windows plugin у списку плагінів Soffid

Перш ніж розпочати налаштування агента перевіримо один важливий момент. Потрібно переконатися, що сервер має доступ до служби Soffid Sync server, що працює на стороні Windows Server (на комп'ютері з контролером домену). Як ми знаємо, вона працює на комп'ютері з ім'ям DC1 на порту 1760. По-перше, потрібно переконатися, що сервер зможе перетворити ім'я комп'ютера на його адресу. Це не завжди можливо. Наприклад, у нашому випадку в імені сервера використовується домен idc.lab, але оскільки такого домена не існує, DNS сервер не зможе перетворити це ім’я на ip адресу. Крім цього, може використовуватися коротке ім'я сервера, взагалі без домену. У таких випадках треба відредагувати файл hosts на сервері, додавши до нього відповідний рядок.

У Debian, як і в багатьох інших Linux-системах, файл hosts знаходиться за адресою /etc/hosts.

```
# mcedit /etc/hosts
```

Додаємо в кінець файлу рядок виду (замініть ip адресу та ім'я на свої)

```
192.168.2.202 dc1.idc.lab DC1
```

Тепер ми можемо бути впевнені, що сервер зможе перетворити ім’я контролера домену на ip адресу (рис. 3.46).

Залишається перевірити доступність порту 1760.

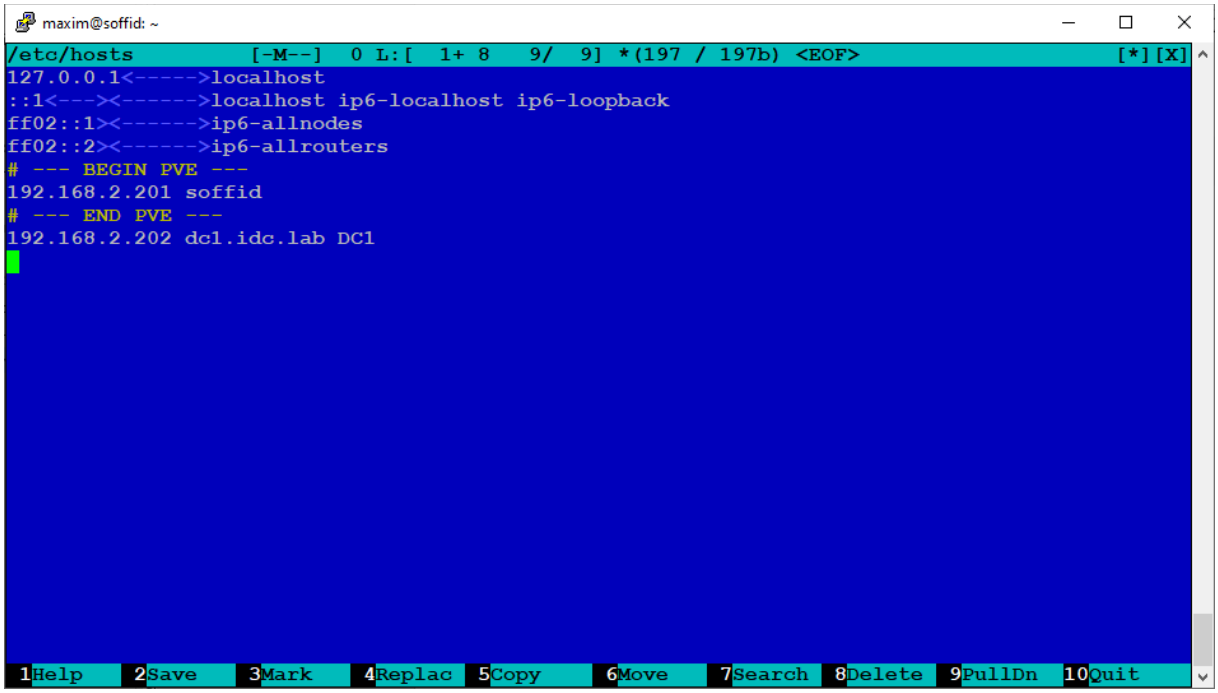


Рисунок 3.46 Редагування файлу hosts на сервері Soffid

За замовчуванням на сервері Windows з контролером домену включений брандмауер, який блокує підключення до порту 1760. Тому потрібно повністю відключити брандмауер (не рекомендується), або відкрити порт 1760 в налаштуваннях брандмауера. Розглянемо другий варіант.

Відкриємо налаштування брандмауера. Для цього зайдемо до Диспетчера серверів і в меню Tools оберемо пункт Windows Defender Firewall with Advanced Security.

Виберемо Правила для вхідних підключень Inbound Rules у дереві зліва, потім меню Дії – New Rule… Запуститься Майстер створення правила для нового підключення.

На першому кроці Rule Type (Тип правила) оберемо Port – Next.

На другому кроці Protocol and Ports виберемо Протокол TCP, Specific local ports та вкажемо порт Soffid Sync server – 1760 – Next.

На наступному кроці Action (Дія) виберемо Allow the connection (Дозволити підключення) – Next.

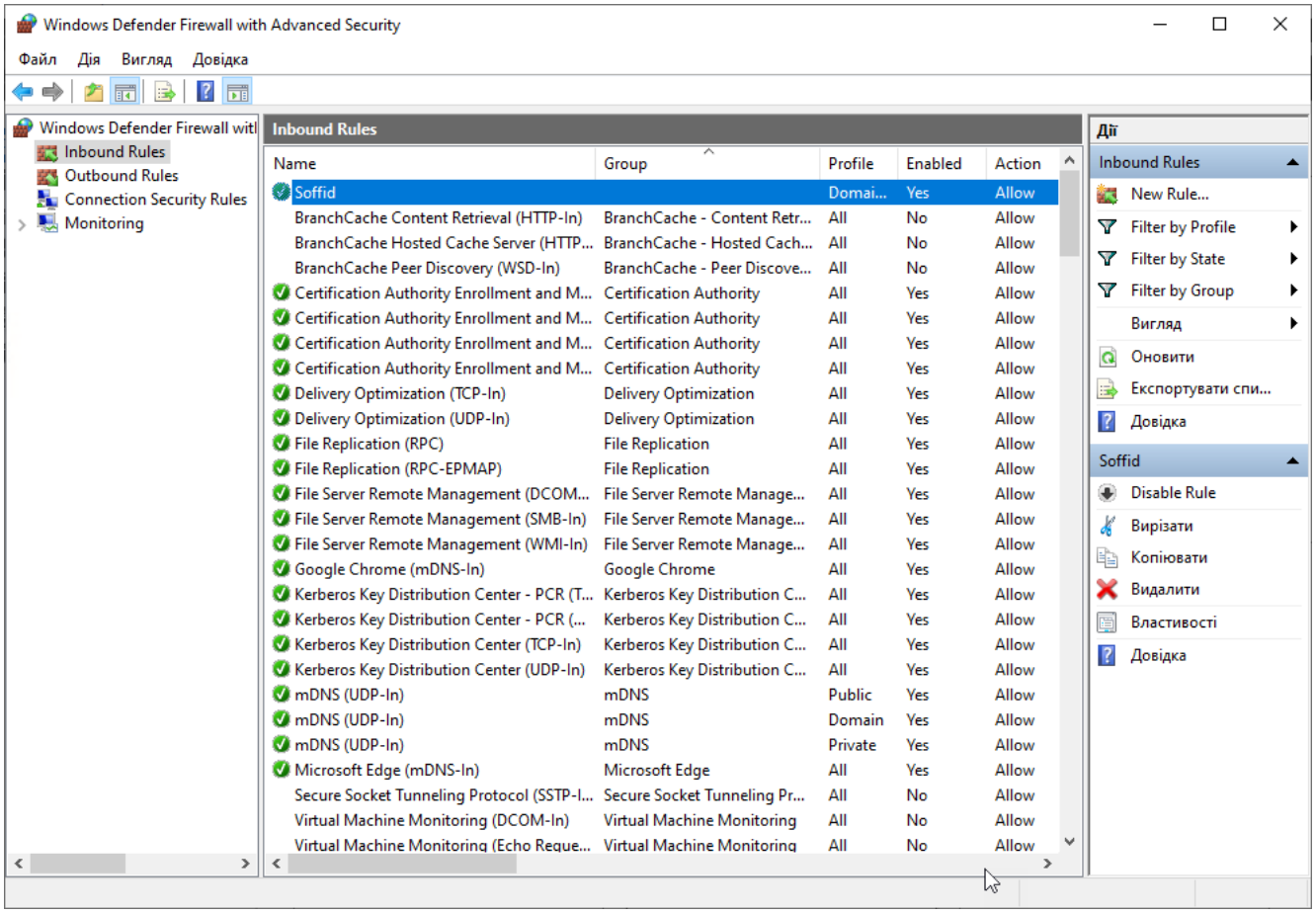


Рисунок 3.47 Налаштування брандмауера Windows

На наступному кроці Profile (Профіль) знімемо галку з опції Public, залишивши тільки Domain та Private – Next.

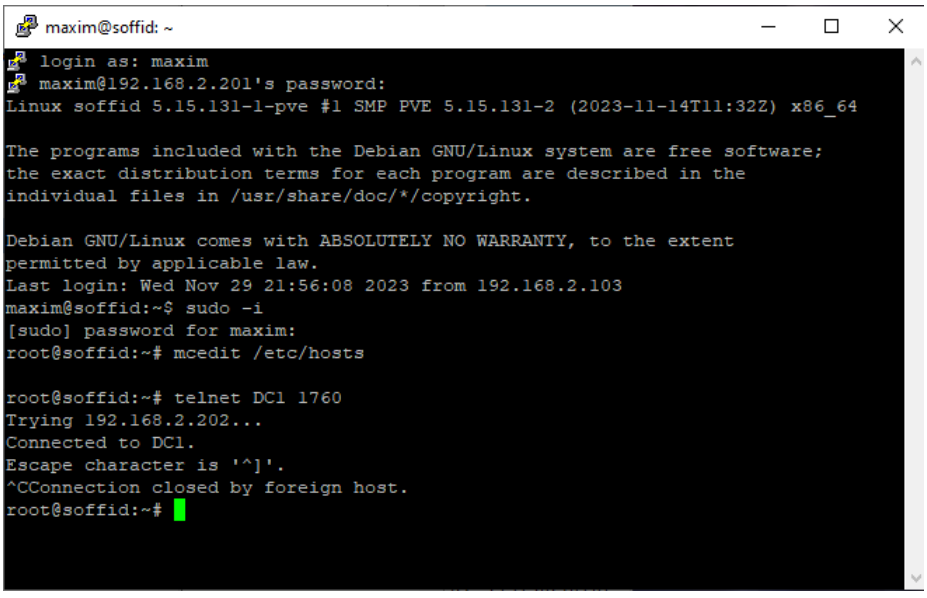


Рисунок 3.48 Перевірка доступності порту за допомогою команди telnet

На останньому етапі Name (Ім'я) дамо нашому правилу відповідну назву, наприклад – Soffid – і натиснемо Finish. В результаті в списку правил брандмауера з'явиться наше новостворене правило для порту 1760 (рис. 3.47).

Щоб перевірити, чи порт дійсно доступний, виконаємо на сервері Soffid команду telnet.

```
# telnet DC1 1760
```

Якщо з'єднання встановлюється (з'являється рядок Connected to DC1), це означає, що порт відкритий і можна приступати до додавання агента (рис. 3.48).

Відкриємо веб-консоль Soffid і перейдемо до розділу, присвяченого агентам – Main Menu > Administration > Configuration > Integration engine > Agents. Спочатку натиснемо іконку у вигляді лупи, щоб відобразилися всі встановлені та активні агенти. Після цього натиснемо іконку з плюсом, щоб додати нового агента. Заповнимо поля.

Name: Active Directory

Description: Windows Server 2022 Datacenter

Type: Active Directory – оберемо зі списку, що випадає

Server: dc1.idc.lab – виберемо сервер, який ми налаштовували раніше (п. 3.2.3)

Trust passwords: Yes – означає, що ми дозволяємо системі змінювати паролі зі свого боку. Soffid довірятиме таким паролям.

Якщо параметр Trust passwords вимкнено, то Soffid бере керування паролями на себе. Наприклад, якщо час дії пароля, згенерованого в консолі Soffid, минув, то Soffid заблокує цей пароль і користувач не зможе підключитися до керованої системи. Soffid зможе видати новий пароль та передати його агенту, але користувач не зможе поміняти його на стороні керованої системи.

Authoritative identity source: Yes (optional)

Необхідно включити цю опцію, якщо ми хочемо використовувати Active Directory як джерело для створення користувачів у Soffid. Зазвичай вона вмикається

для первинного завантаження користувачів у Soffid, а потім вимикається, оскільки надалі цими користувачами вже управляє Soffid.

Read only: No

Якщо увімкнути цю опцію, то жодних змін на стороні керованої системи вноситись не буде. Корисна на етапі тестування в продакшн середовищі. У тестовому оточенні цю опцію рекомендується вимикати.

Manual account creation: No (optional)

Ця опція відповідає за автоматичне створення облікових записів. Якщо ми не хочемо, щоб Soffid автоматично створював облікові записи, опцію треба включити. Але на період, коли Active Directory буде використовуватись як Authoritative identity source, цю опцію потрібно вимкнути.

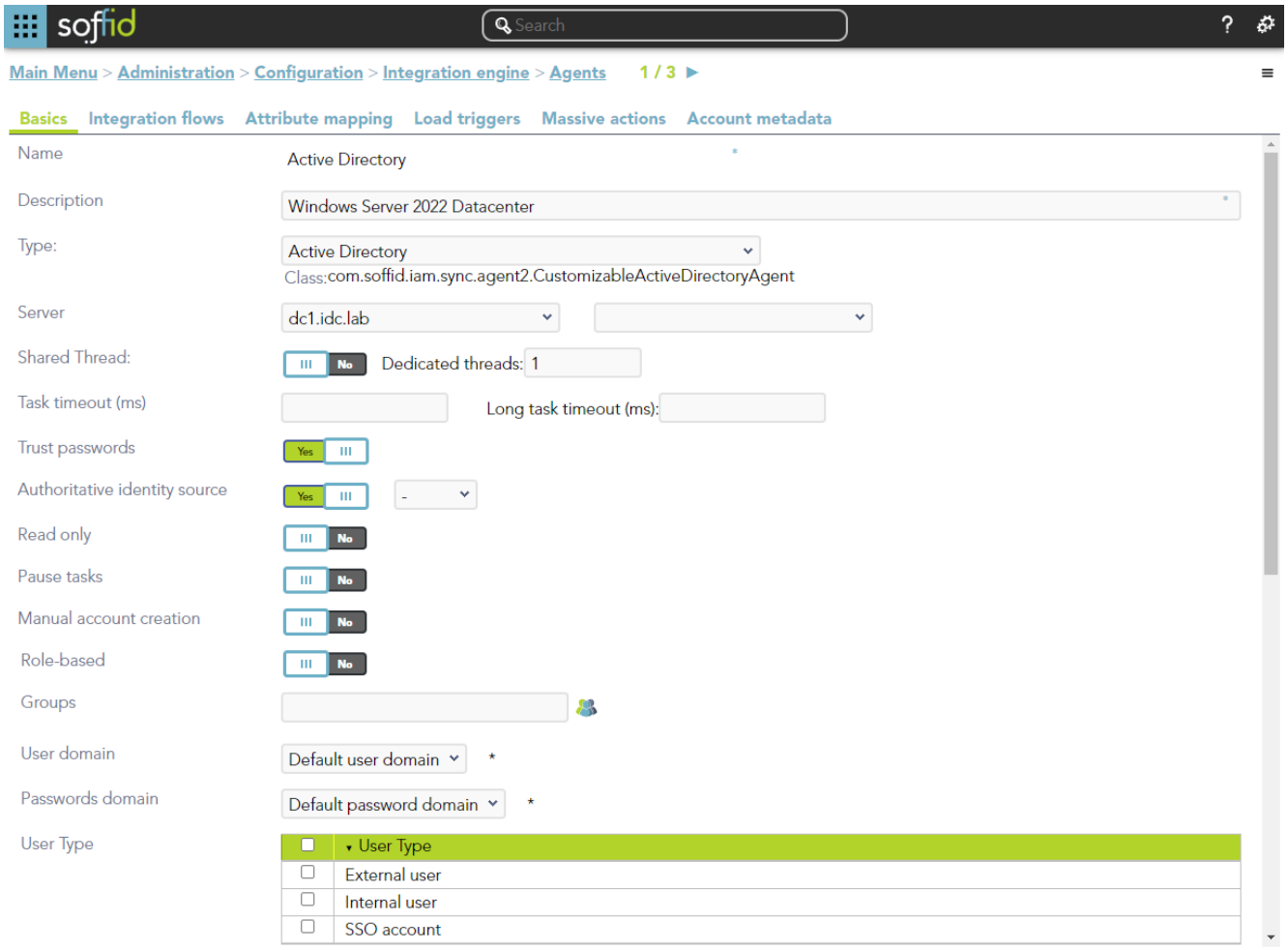


Рисунок 3.49 Основні налаштування агента Active Directory

User domain: Default user domain (вибрати зі списку)

Password domain: Default password domain (вибрати зі списку)

Перша частина сторінки додавання агента виглядатиме так (рис. 3.49). Перейдемо до налаштувань підключення (Connector parameters):

Hostname: DC1

LDAP base DN: dc=idc,dc=lab

Principal name: cn=Administrator,cn=Users,dc=idc,dc=lab

Password: введемо пароль користувача Administrator на контролері домену

Enable debug: Yes (на етапі тестування рекомендується увімкнути)

Accepted certificates: Only trusted certificates (вибрати зі списку)

Інші поля можна залишити у значеннях за замовчуванням.

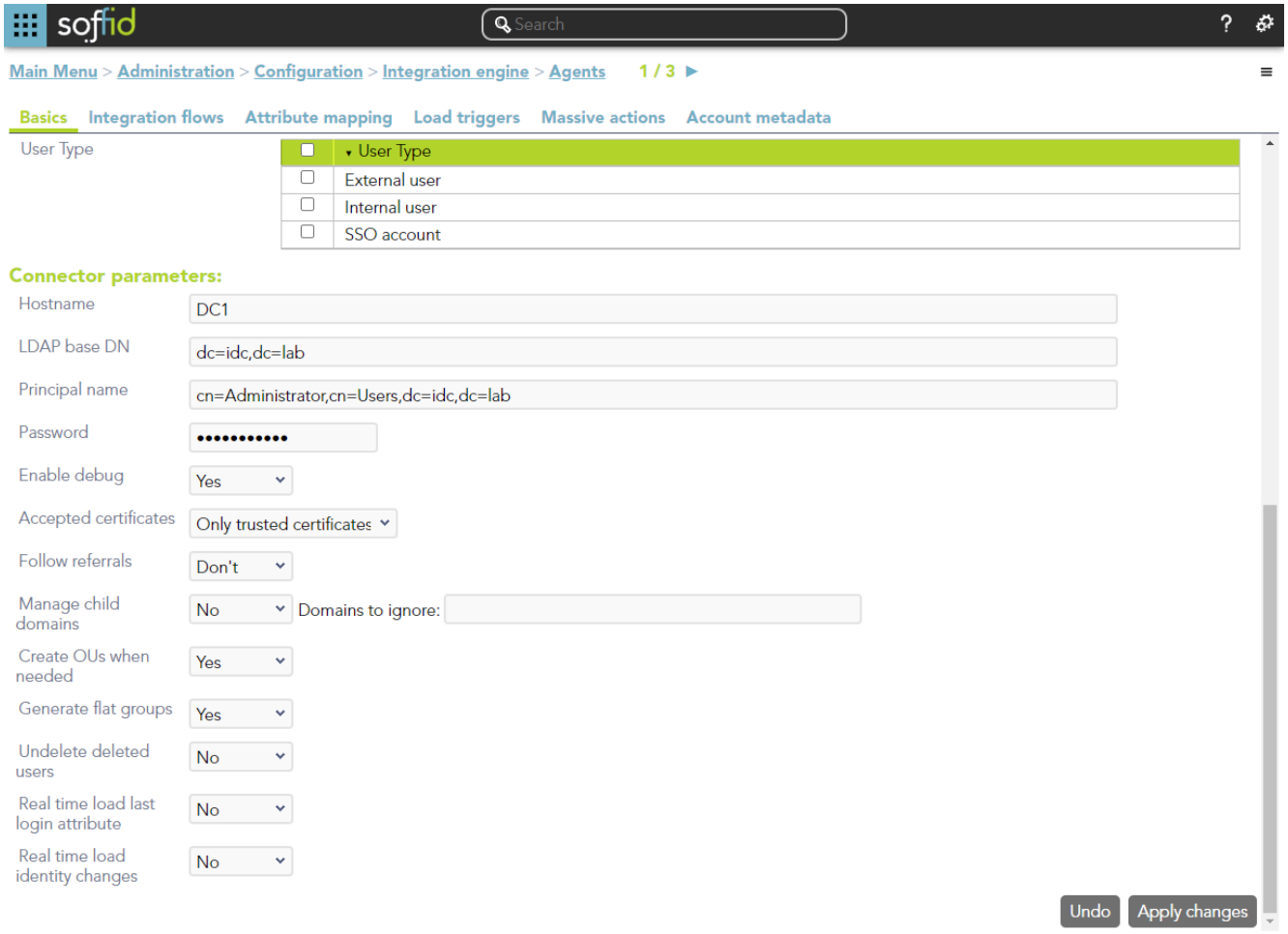


Рисунок 3.50 Налаштування підключення агента Active Directory

Натиснемо кнопку Apply changes внизу праворуч або іконку з дискетою у верхньому правому кутку. Результат представлений на рисунку 3.50.

Тепер слід перевірити, чи наш агент підключився до сервера. Це має статися автоматично. Статус або стан агента можна перевірити у відповідному розділі інтерфейсу. Отже, перейдемо в Main Menu > Administration > Monitoring and reporting > Sync server monitoring та натиснемо там кнопку View Agents. Ми маємо побачити таку картину (рис. 3.51).

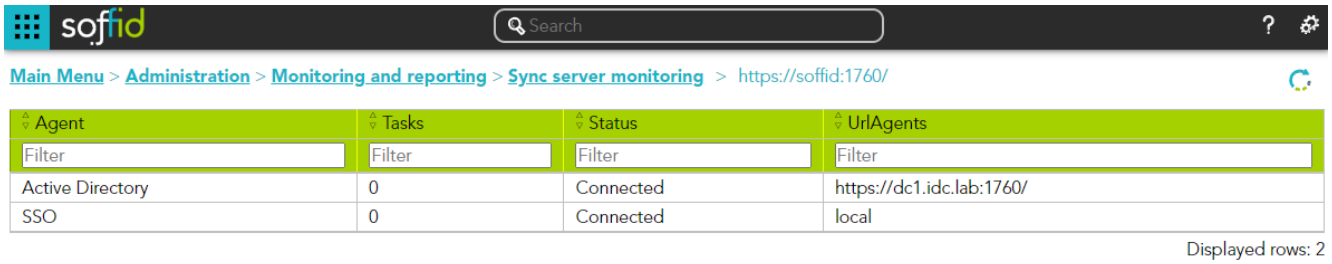


Рисунок 3.51 View agents – Перегляд статусу агентів

Якщо статус агента Connected (Підключено) – все гаразд. Можна приступати до наступного етапу налаштування.

3.2.6 Налаштування Attribute mapping агента Active Directory

Повернемося до налаштування агента. Для цього перейдемо в меню Main Menu > Administration > Configuration > Integration engine > Agents та натиснемо на іконку у вигляді лупи праворуч. У списку знайдемо рядок Active Directory і натиснемо на ньому – відкриються основні налаштування агента. Перейдемо на вкладку Attribute mapping, щоб налаштувати об'єкти та атрибути.

Натисніть плюс у рядку System objects, щоб додати новий об'єкт. Для початку створимо об'єкт account based on account.

Заповнимо його властивості (Properties). Натиснемо на стрілочку зліва від Properties, щоб розкрити дерево (спочатку там буде порожньо). Додамо нову властивість (натиснемо на плюс у рядку Property) та введемо значення відповідно до таблиці 3.1.

Таблиця 3.1 Властивості об'єкта account

Property	Value
rename	false

За замовчуванням агент Active Directory може перейменовувати або переміщувати об'єкти (користувачів) на контролері домену, що може призвести до несподіваних результатів. Тому краще за допомогою цієї властивості таку можливість відключати.

Далі заповнимо системні атрибути. Розкриємо список System attribute, натиснувши на стрілочку зліва. Для додавання атрибуту натиснемо кнопку плюс. Усього необхідно додати п'ять атрибутів. Назви атрибутів та їх значення наведено у таблиці 3.2.

Таблиця 3.2 Атрибути об'єкта account

System attribute	Direction	Soffid attribute
sAMAccountName	↔	accountName
relativeBaseDn	←	"cn=Users"
objectClass	←	"user"
displayName	→	accountDescription
UserAccountControl == 514 ? true : false	→	accountDisabled

Збережемо зміни, натиснувши дискету у верхньому правому кутку. Результат представлено на рис. 3.52.

Протестуємо отримання об'єктів агентом. Для цього натиснемо кнопку Test.

Для поточної моделі ми заздалегідь створили на контролері домену кілька користувачів, оскільки передбачається, що впровадження Soffid IAM здійснюється на підприємстві, де вже присутній контролер домену. Оскільки нам відомо, які користувачі є на цьому домені, ми оберемо одного з них для перевірки роботи агента. Після натискання кнопки Test з'явиться поле Account, де потрібно ввести ім'я цього користувача (рис. 3.53).

Після чого натиснемо кнопку Fetch system raw data.

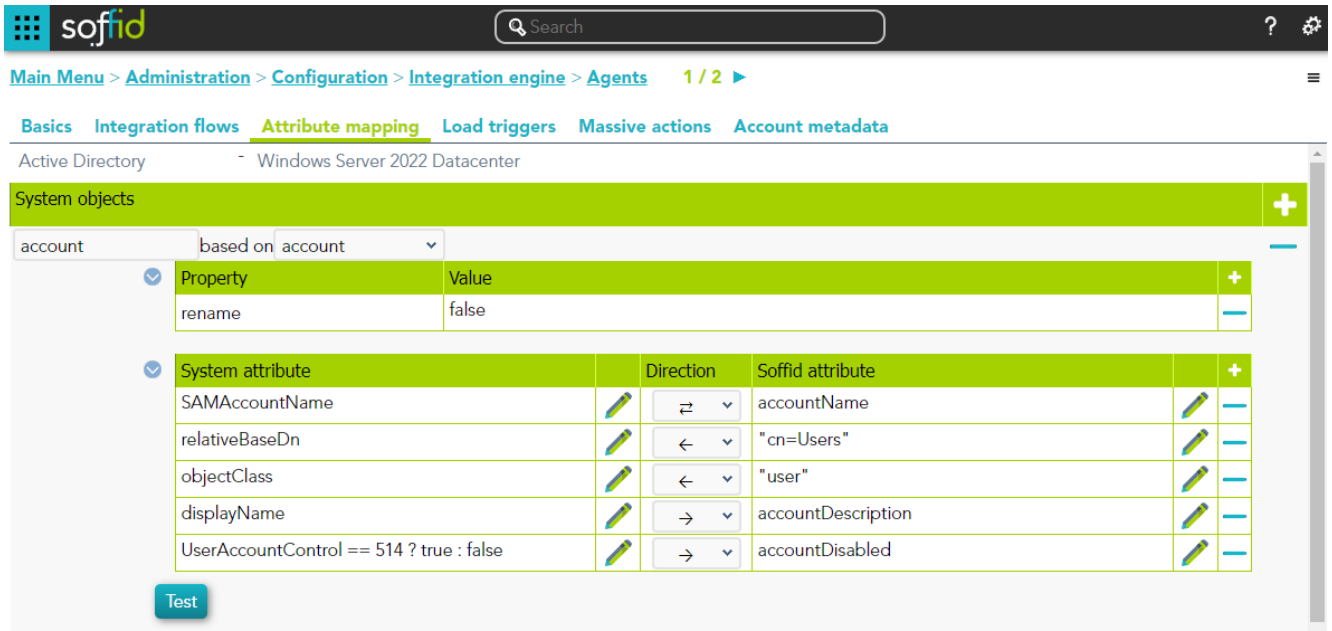


Рисунок 3.52 Налаштування Attribute mapping for account

Якщо агент настроєно правильно, ми побачимо детальну інформацію про обліковий запис користувача. Отриманий результат показаний на рисунку 3.54.

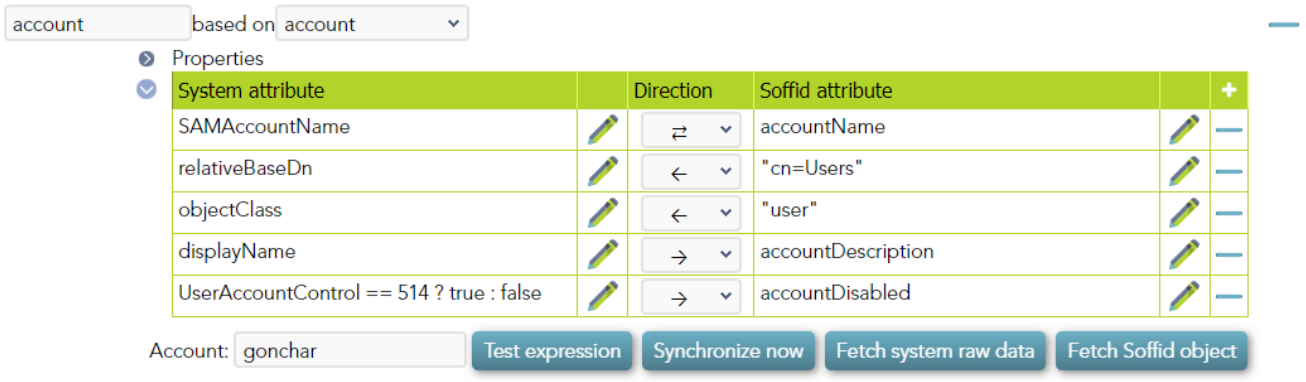


Рисунок 3.53 Тестування агента Active Directory

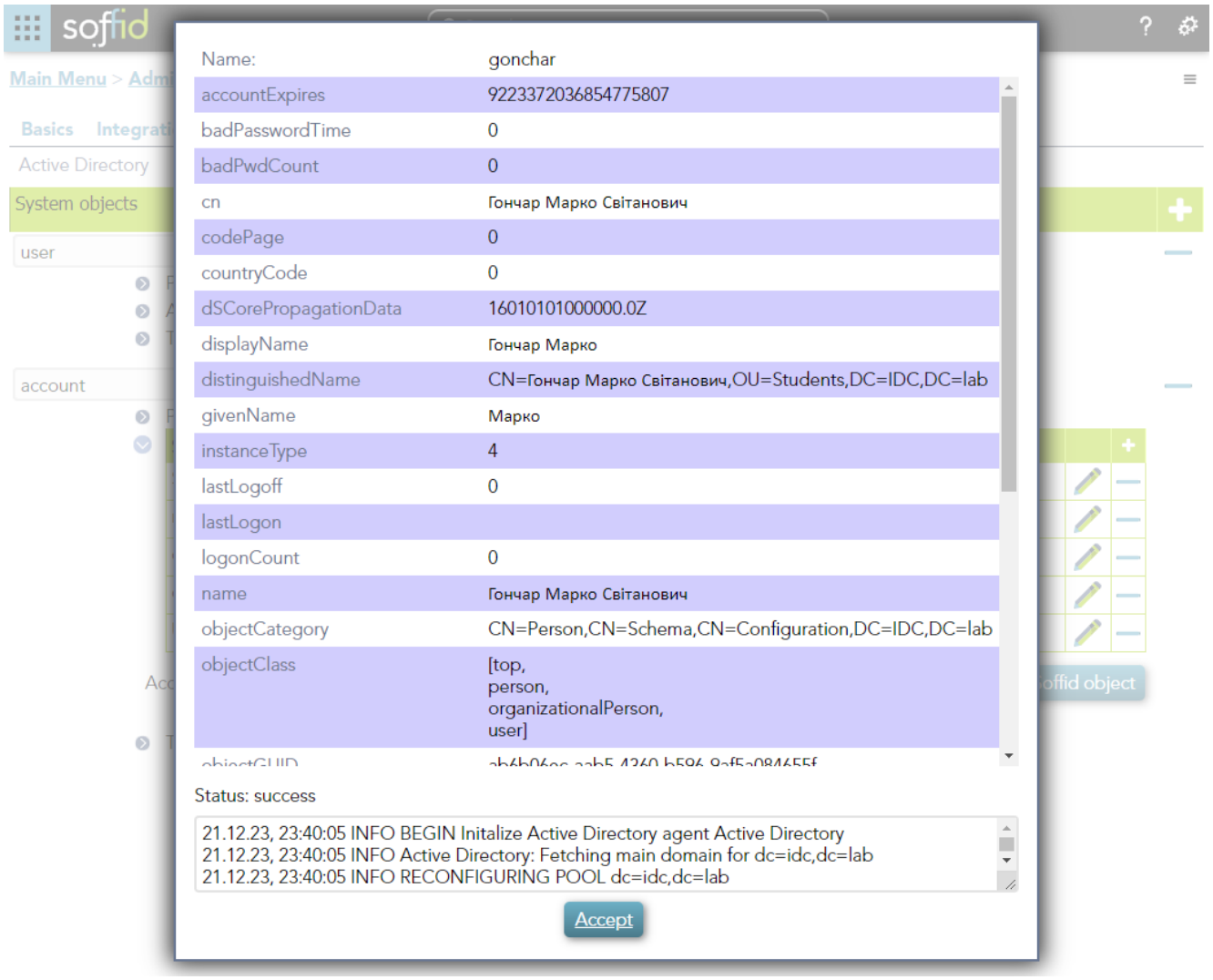


Рисунок 3.54 Результат тестування агента

Тепер нам потрібно додати ще один системний об'єкт – user. Для цього натискаємо плюс у рядку System objects та вводимо ім'я об'єкта user based on user.

Далі за аналогією з account додамо для user властивість rename (табл. 3.3)

Таблиця 3.3 Властивості об'єкта user

Property	Value
rename	false

І потім заповнимо його атрибути (табл. 3.4)

Таблиця 3.4 Атрибути об'єкта user

System attribute	Direction	Soffid attribute
sAMAccountName	↔	userName
givenName	↔	lastName
sn	↔	firstName
relativeBaseDn	←	"cn=Users"
objectClass	←	"user"
displayName	←	accountDescription
cn	←	userName
(userAccountControl & 2) == 0	→	active

Збережемо зміни, натиснувши дискету у правому верхньому кутку.

Ще раз протестуємо роботу агента, цього разу для об'єкта user. Натиснемо на кнопку Test і введемо відоме нам ім'я користувача, яке присутнє на контролері домену. І натиснемо на кнопку Fetch system raw data.

Ми повинні побачити таке саме вікно, як на рисунку 3.54.

Продовжимо налаштування агента та перейдемо на вкладку Load triggers. Тут знаходяться дві опції - Full reconciliation та Propagate changes.

Перша опція Full reconciliation (Повне узгодження) відповідає за повну синхронізацію об'єктів Soffid з контролером домену, включаючи видалення об'єктів на стороні Soffid, якщо вони були видалені на контролері домену. У зв'язку з цим цю опцію не можна включати, якщо планується використовувати Active Directory як джерело для всіх користувачів (опція Authoritative Identity Source). У цьому випадку всі користувачі, які відсутні на контролері домену, будуть автоматично заблоковані або видалені в Soffid. В результаті є ризик втратити доступ до консолі Soffid, оскільки адміністративного облікового запису Soffid немає на контролері домену, і він буде вимкнений.

Друга опція Propagate changes (Розповсюдження змін) відповідає за те, що зміни, що прийшли з контролера домену, будуть передані на інші керовані системи за допомогою створення та виконання задач – Synchronization tasks.

Збережемо зміни, натиснувши дискету у верхньому правому кутку. Результат представлений на рисунку 3.55.

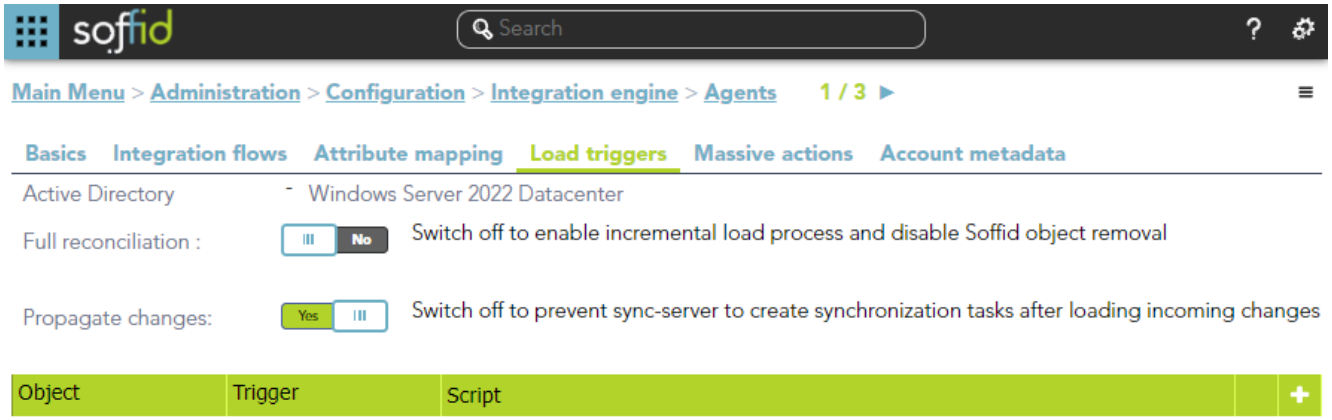


Рисунок 3.55 Налаштування Load triggers агента Active Directory

На цьому налаштування агента контролера домену закінчено. Переходимо до підключення до серверу Soffid поштового сервера Zimbra.

3.3 Підключення поштового сервера Zimbra до Soffid

3.3.1 Встановлення Java JDK

Перед тим, як приступити до установки Soffid Sync Server, нам знадобиться скачати і встановити Java. Починаючи з версії 3.3.2, розробники перейшли на

використання Java 11. У репозиторії Ubuntu 20.04 є потрібний пакет java, який називається openjdk-11-jre. Встановимо його за допомогою команди (рис. 3.56)

```
# sudo apt install openjdk-11-jre
```

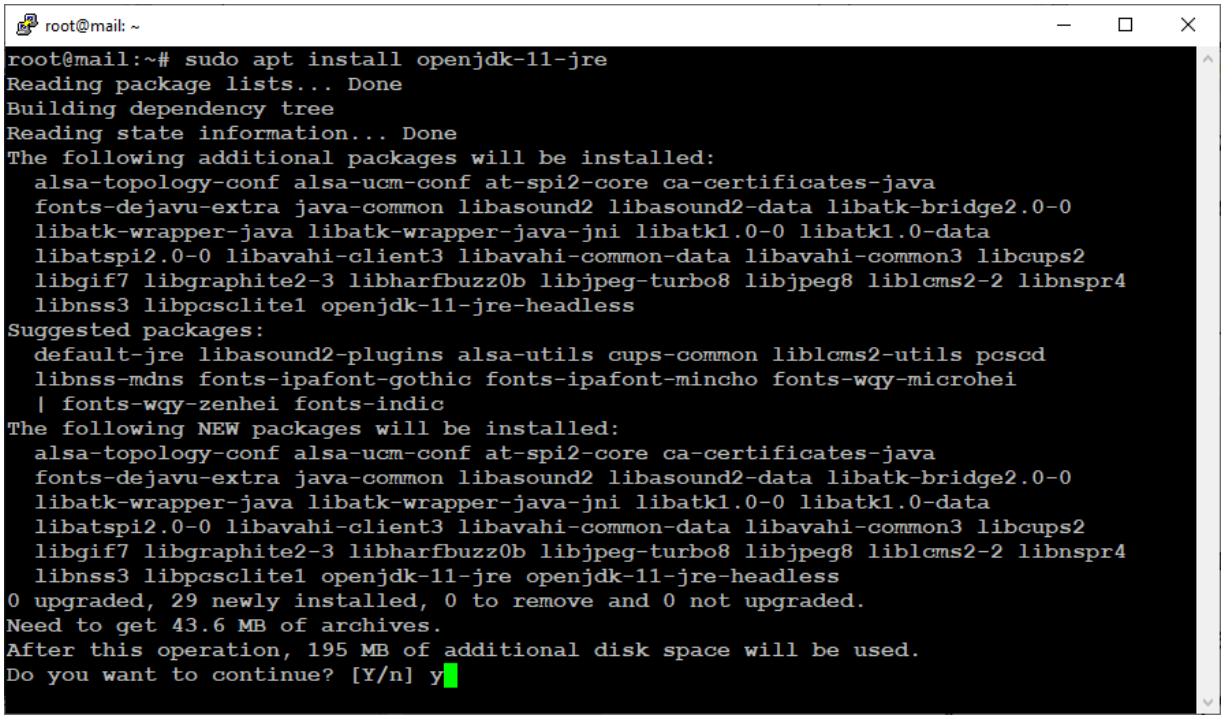


Рисунок 3.56 Встановлення Java JDK на сервер Ubuntu

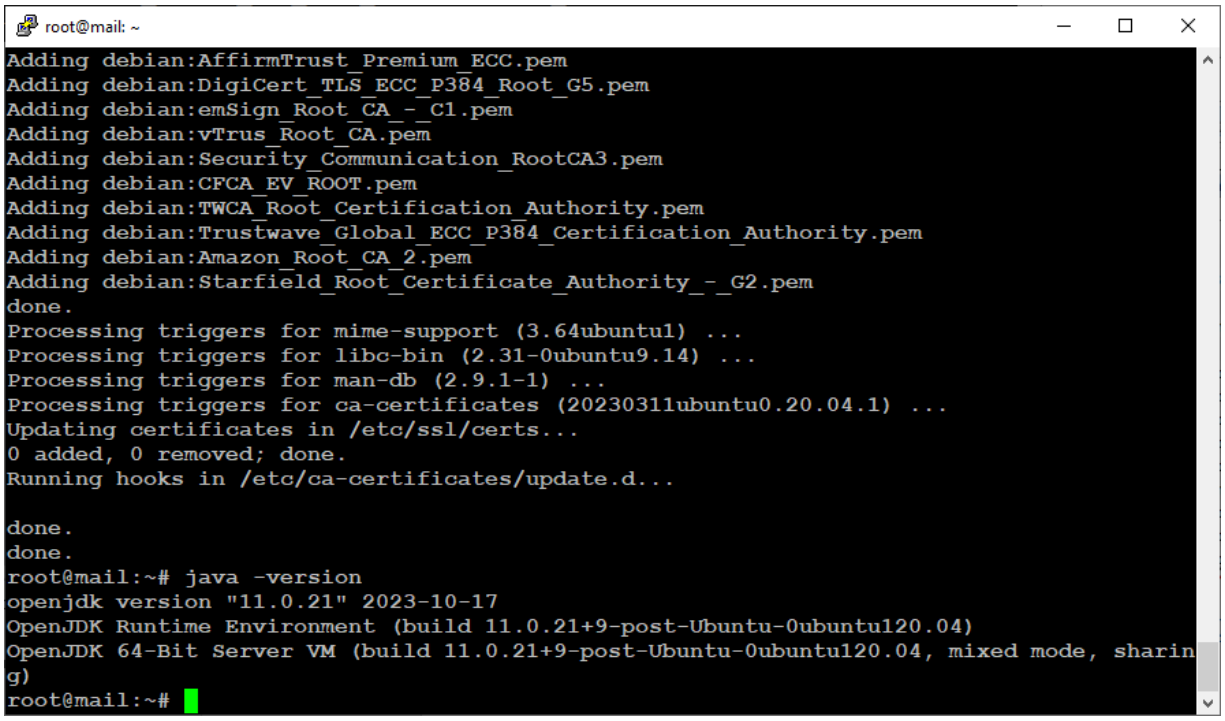


Рисунок 3.57 Перевірка версії Java на сервері Ubuntu

Потім перевіримо результат виконання командою (рис. 3.57)

```
# java -version
```

3.3.2 Встановлення Soffid Sync Server на сервер Zimbra

Наш поштовий сервер Zimbra працює під керуванням операційної системи Ubuntu 20.04. Тому для установки Sync Server на сервер Zimbra нам знадобиться інсталятор Soffid 3 Sync server для Ubuntu. Зайдемо на сторінку Soffid Download http://download.soffid.com/download/ та завантажимо відповідну версію (рис. 3.58).

Рисунок 3.58 Завантаження Soffid Sync server для сервера Zimbra

Отриманий файл SOFFID 3 Sync server-Debian_Ubuntu installer-3.5.5.deb завантажуємо на сервер Zimbra. Для цього найпростіше скористатися програмою WinSCP.

Перед тим, як запустити інсталяцію, переконаємося, що із сервера Zimbra можна підключитися до сервера Soffid з використанням його імені, а не ip адреси. Якщо в якості імені сервера використовується FQDN, яке система зможе перетворити за допомогою сервера DNS, то тоді нічого додатково робити не потрібно. Але в нашій моделі, яка розроблена для демонстрації процесу інтеграції,

використовується неіснуюче доменне ім’я. Тому нам необхідно додати на сервері Zimbra у файл hosts рядок, за допомогою якого система зможе перетворити ім'я сервера на ip адресу (рис. 3.59). Для цього достатньо виконати команду:

```
# sudo echo '192.168.2.201 soffid' >> /etc/hosts
```

Результат можна перевірити командою:

```
# cat /etc/hosts
```

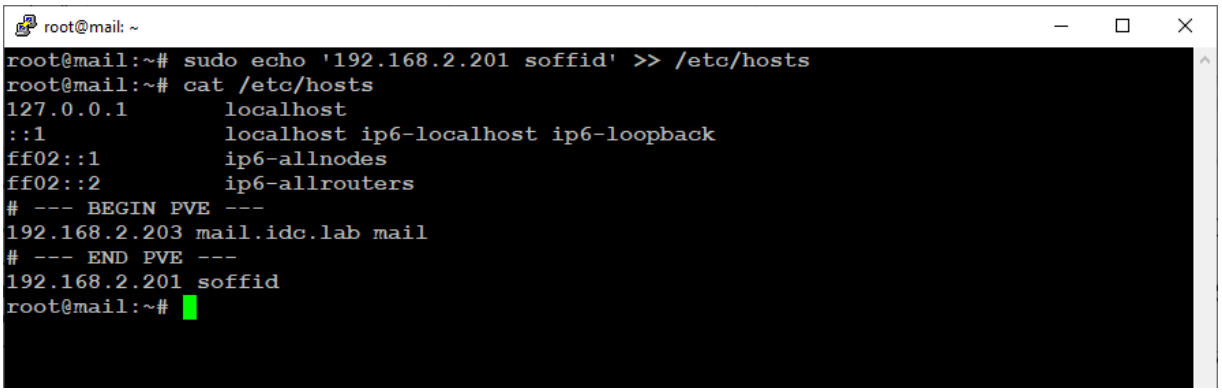


Рисунок 3.59 Додавання запису до файлу hosts на сервері Zimbra

На сервері Zimbra перейдемо в каталог, куди ми завантажили файл інсталятора Soffid 3 Sync server, і запустимо його за допомогою команди:

```
# sudo dpkg -i 'SOFFID 3 Sync server-Debian_Ubuntu installer-3.5.5.deb'
```

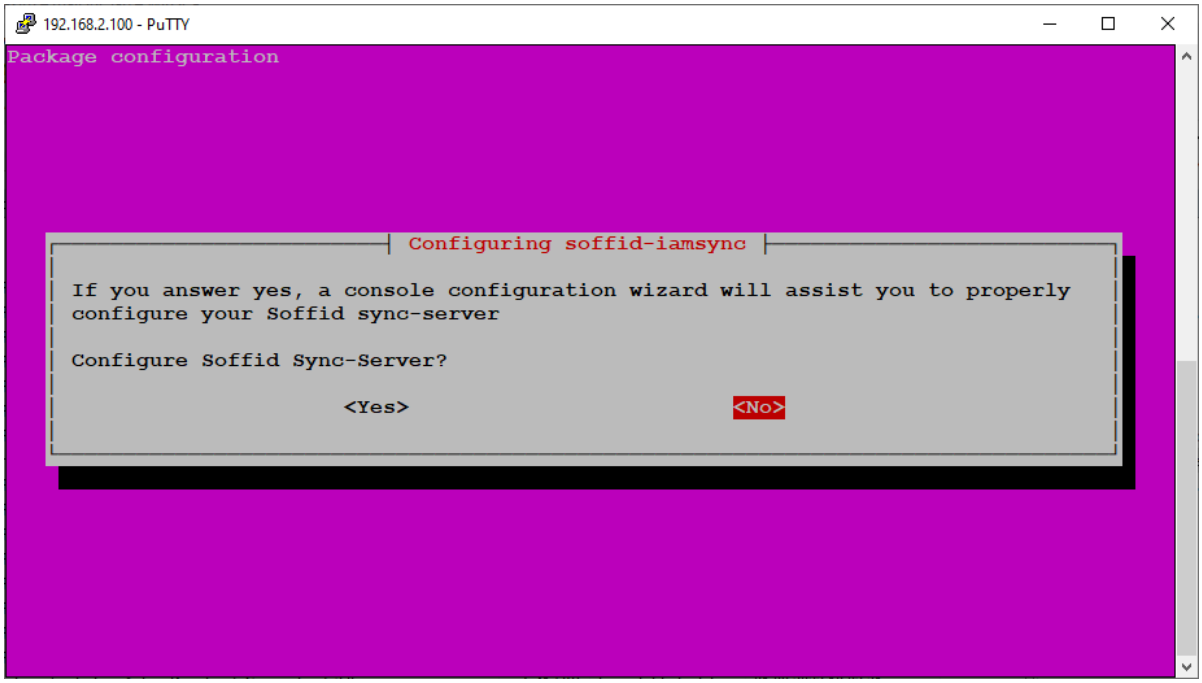


Рисунок 3.60 Установка Soffid Sync Server на сервер Ubuntu

Під час інсталяції на екрані з'явиться запитання: Configure Soffid Sync-Server? (рис. 3.60). Відповімо Ні (No). Ми запустимо скрипт для конфігурування Sync server самостійно. Але перед цим зупинимо службу soffid-iamsync командою:

```
# service soffid-iamsync stop
```

Тепер можна починати конфігурацію sync server.

3.3.3 Налаштування Soffid Sync Server

Запустимо скрипт конфігурації Soffid Sync Server. Робити це потрібно від імені користувача soffid, щоб створювані файли конфігурації були доступні цьому користувачеві надалі.

Запускаємо configuration wizard командою:

```
# sudo -u soffid /opt/soffid/iam-sync/bin/configure
```

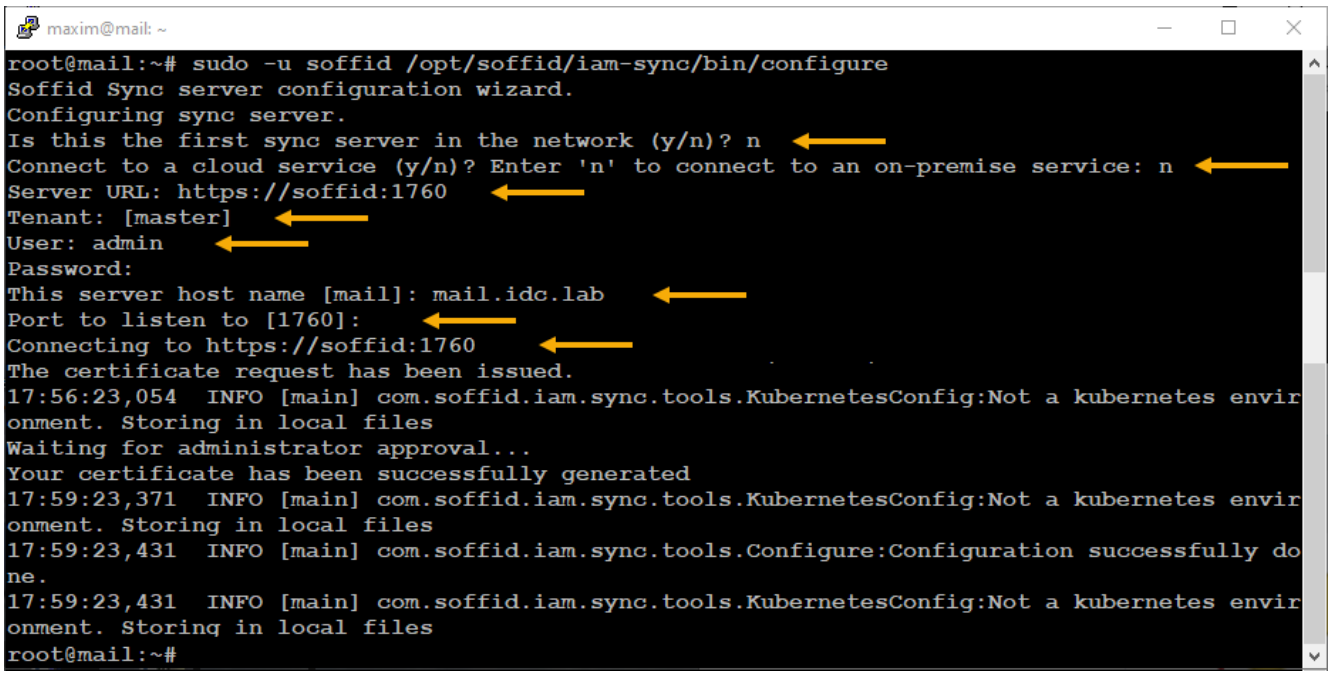


Рисунок 3.61 Налаштування Sync server на сервері Ubuntu

Відповідаємо на запитання Soffid Sync server configuration wizard (рис. 3.61):

1) Is this the first sync server in the network? – Це ваш перший Sync server у мережі? Для всіх керованих систем, які підключаються до Soffid, на це питання слід відповідати Hi. Відповімо n (No).
2) Connect to a cloud service? Enter ‘n’ to connect to an on-premise service: n (Нет) – Приєднатись до хмарного сервісу? Введіть 'n', щоб підключитися до сервера підприємства. У нашому випадку ми використовуємо свій сервер Soffid та хочемо підключитися до нього. Тому відповідаємо Hi.
3) Server URL: https://soffid:1760
4) Tenant: [master] Залишимо значення за замовчуванням (натиснемо Enter)
5) User: Користувач Soffid. Введемо користувача admin, якого ми використовуємо для входу до веб-інтерфейсу Soffid.
6) Password: пароль від цього користувача.
7) This server host name: потрібно ввести повне ім'я сервера з доменом. IP адресу тут вказувати не можна.
8) Port to listen to [1760]: номер TCP порту, на якому працюватиме служба Sync server. Рекомендовано використовувати значення за замовчуванням, тому залишимо його, натиснувши Enter.

Після відповіді на останнє запитання, майстер налаштування спробує підключитися до сервера Soffid, вказаного в рядку Server URL. Якщо з'єднання буде успішним, на екрані з'явиться напис

```
Waiting for administrator approval…
```

У цей момент потрібно перейти до веб консолі Soffid – там має з'явитися нова задача для адміністратора.

Увійдемо в консоль користувачем admin і перейдемо до меню Main Menu > My tasks. У списку завдань з'явиться нове завдання, яке потрібно схвалити (рис. 3.62).

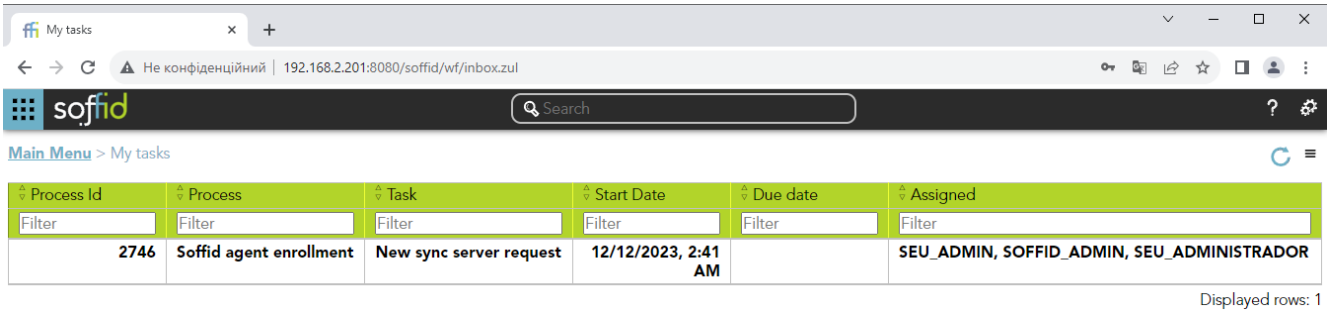


Рисунок 3.62 Запит на підключення поштового сервера Zimbra

За аналогією з тим, як ми давали добро на підключення сервера контролера домену, нам потрібно дозволити підключення нової системи до сервера Soffid. Для цього відкриємо завдання, двічі клацнувши по ньому кнопкою миші. У вікні, що відкриється, натиснемо кнопку Take ownership. Далі у списку поля Approve виберемо Підтвердити (Approve) і натиснемо кнопку End, щоб закрити вікно. Запит підтверджений.

Тепер повертаємось у консоль сервера Zimbra, де ми запускали майстер конфігурування Sync server. Там процес налаштування Soffid Sync server має успішно завершитись (рис. 3.61).

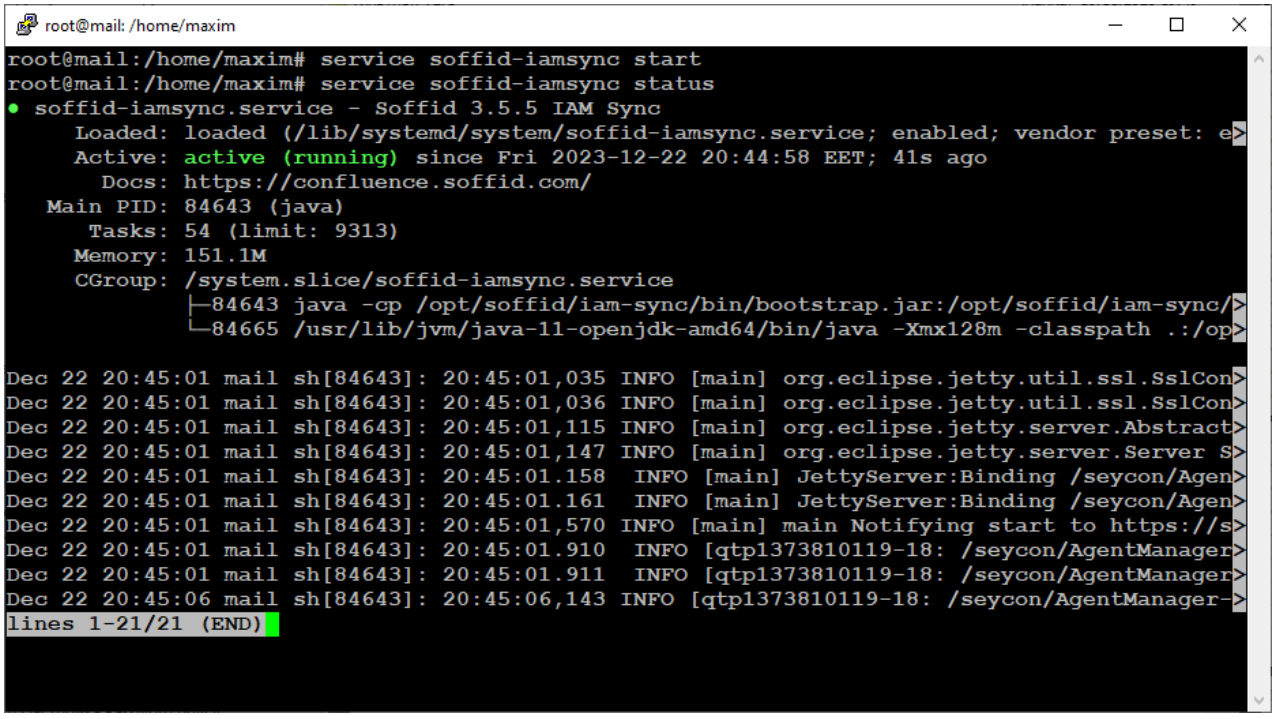


Рисунок 3.63 Запуск Sync server та перевірка його статусу

Після закінчення процесу конфігурації запустимо службу soffid-iamsync та перевіримо її статус (рис. 3.63):

```
# service soffid-iamsync start
# service soffid-iamsync status
```

Інші корисні команди для керування службою sync server, які можуть стати в нагоді:

```
# systemctl enable soffid-iamsync
# systemctl restart soffid-iamsync
```

Перша команда додасть службу soffid syncserver в автозапуск, якщо цього не було зроблено в процесі інсталяції. Друга команда використовується для перезапуску служби сервера синхронізації.

На цьому налаштування Soffid на стороні системи, що підключається, завершується.

3.3.4 Встановлення плагіна для Zimbra

Тепер перейдемо до налаштування агента на стороні сервера Soffid. Налаштування агента починається з установки плагіна. Зайдемо на сторінку завантаження Soffid http://download.soffid.com/download/ та знайдемо там Zimbra connector. На момент написання роботи поточною версією Zimbra plugin була Version 1.0.7. Завантажуємо її (рис. 3.64).

В результаті отримаємо файл Zimbra connector-Zimbra plugin-1.0.7.jar.

Відкриємо веб консоль Soffid і перейдемо в меню Main Menu > Administration > Configuration > Global Settings > Plugins.

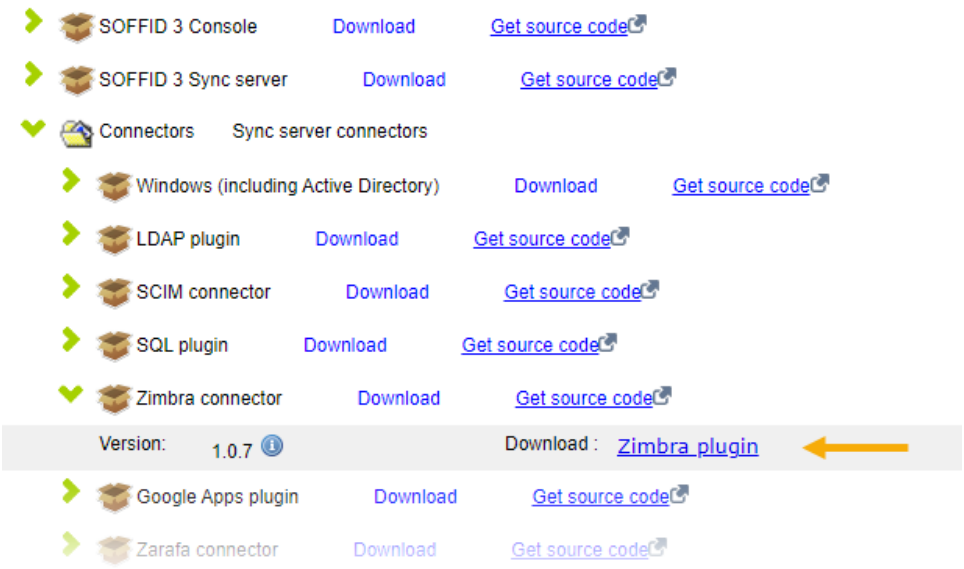


Рисунок 3.64 Завантаження плагіна Soffid для Zimbra

Натиснемо + (додати новий плагін), Pick a file та виберемо файл плагіну. Файл завантажиться на сервер і у списку з'явиться новий плагін (рис. 3.65).

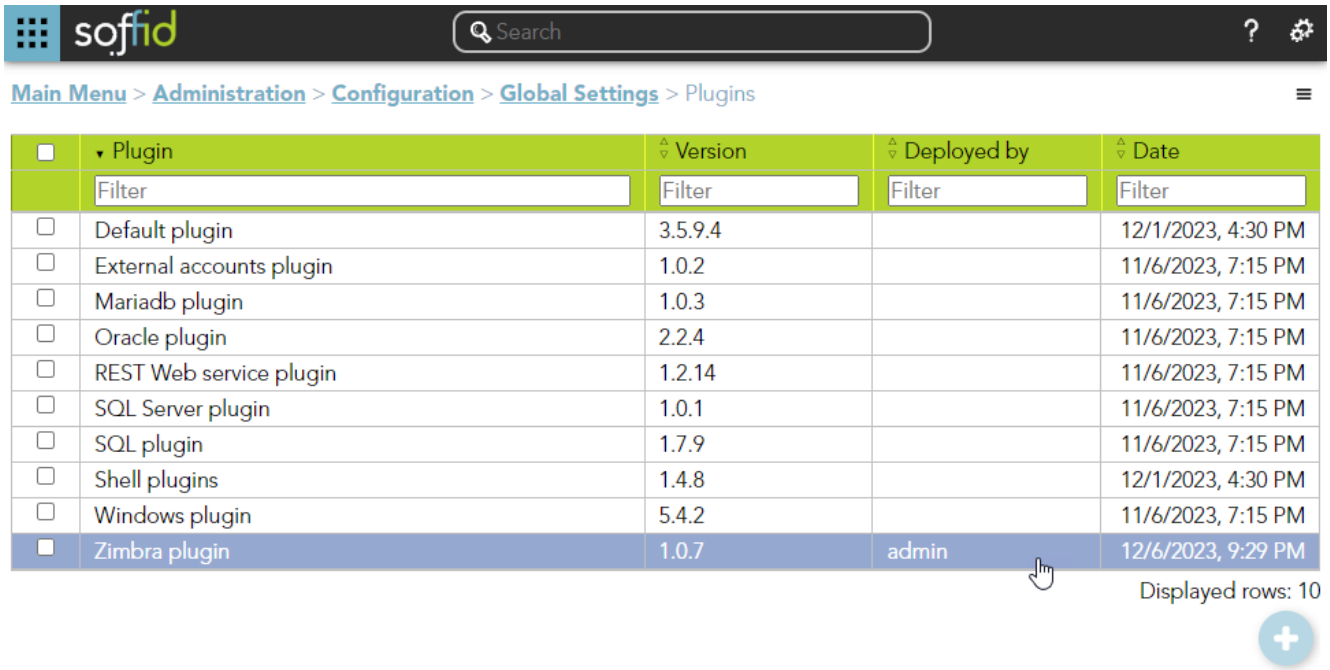


Рисунок 3.65 Установка плагіна для Zimbra

Перед тим, як продовжити, переконаємося, що з сервера Soffid можна підключитися до сервера Zimbra за допомогою його імені, а не ip адреси. Якщо ім'я поштового сервера правильно розпізнається сервером DNS, то тоді нічого додатково робити не потрібно. Але бувають варіанти, коли все одно доводиться

вносити зміни до файлу hosts. Наприклад, у нашій фізичній моделі використовується неіснуючий поштовий домен mail.idc.lab, який не може бути розпізнаний сервером DNS. Тому для того, щоб сервер Soffid зміг попри це перетворити домен mail.idc.lab на ip адресу, додамо у файл hosts сервера Soffid відповідний рядок (рис. 3.66).

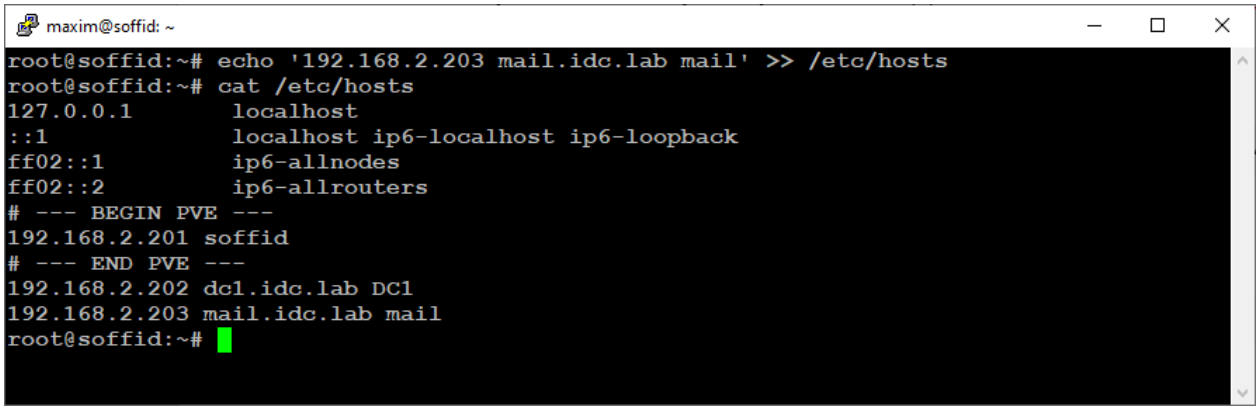


Рисунок 3.66 Додавання рядка до файлу hosts сервера

Виконаємо наступну команду з консолі root сервера:

```
# echo '192.168.2.203 mail.idc.lab mail' >> /etc/hosts
```

Результат можна перевірити командою:

```
# cat /etc/hosts
```

3.3.5 Додавання правила Zimbra user domain

Перш ніж додавати агента, необхідно створити правило, за яким буде генеруватися ім'я для нових користувачів Zimbra. Воно знадобиться під час створення агента.

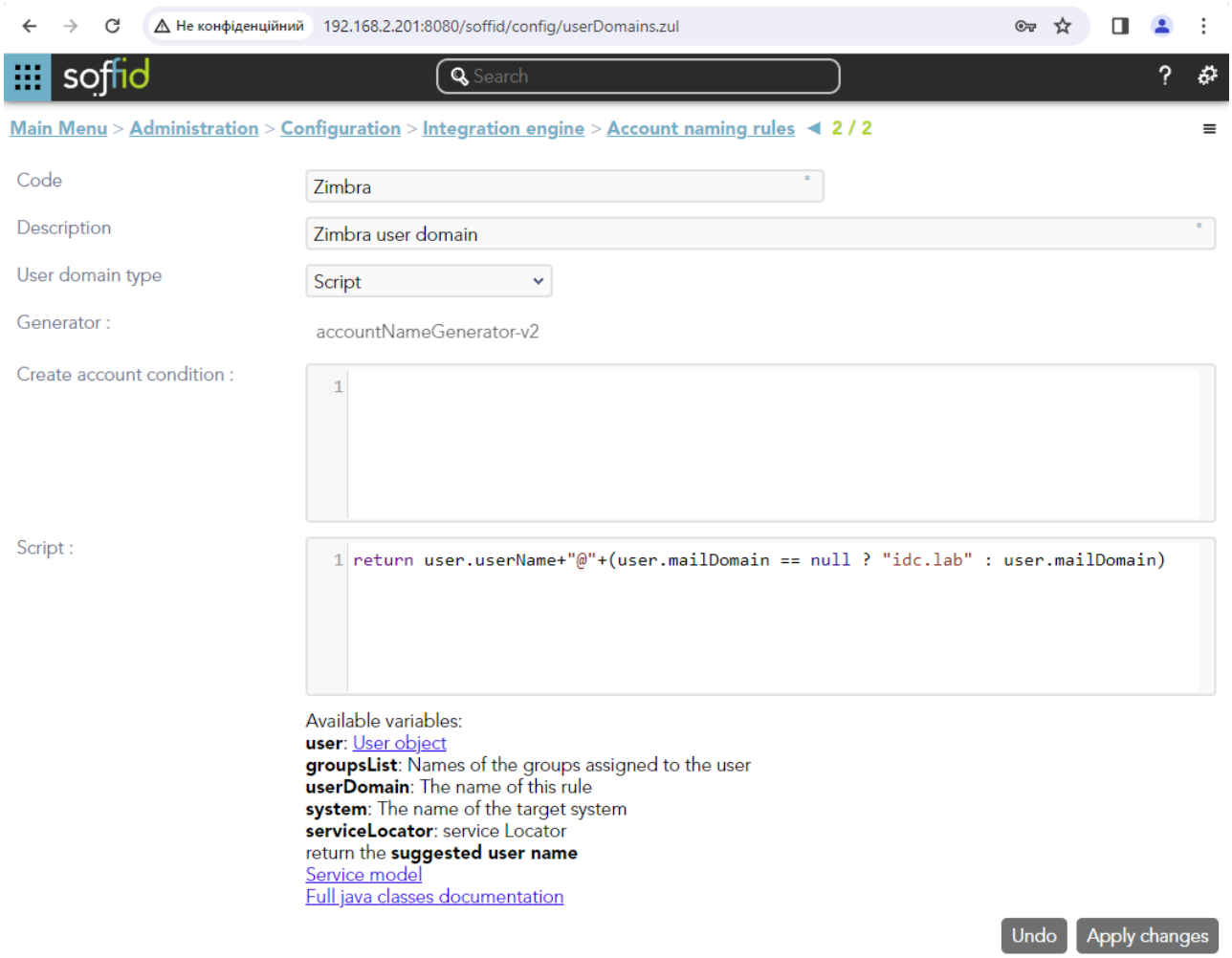


Рисунок 3.67 Правило Zimbra user domain

Перейдемо в меню Main Menu > Administration > Configuration > Integration engine > Account naming rules та створимо нове правило, натиснувши на іконку з плюсом. З'явиться вікно з новим правилом. Заповнимо поля.

Code: Zimbra

Description: Zimbra user domain

User domain type: Script (вибрати зі списку)

У полі Script введемо наступний код:

```
return user.userName+"@"+(user.mailDomain == null ? "idc.lab" : user.mailDomain)
```

В результаті має вийти, як зображено на рисунку 3.67.

Натисніть Apply Changes щоб зберегти зміни та закрити вікно.

Нове правило з'явиться у списку після збереження (рис. 3.68).

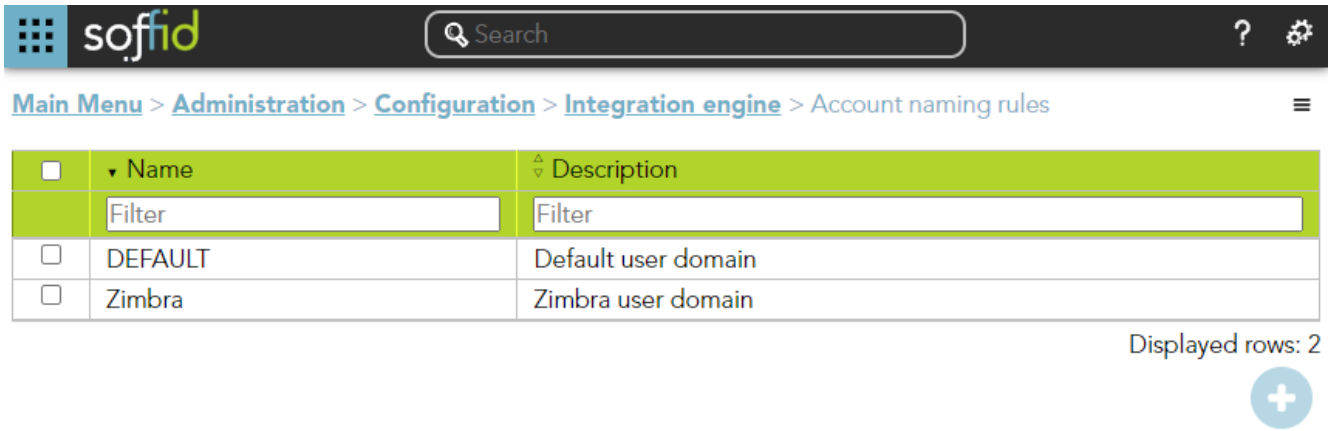


Рисунок 3.68 Список правил Account naming rules

3.3.6 Додавання агента Zimbra

Тепер можна приступати до налаштування агента. Відкриємо веб консоль Soffid і пройдемо в наступний пункт меню – Main Menu > Administration > Configuration > Integration engine > Agents. Натисніть на іконку у вигляді лупи – відобразяться встановлені агенти. Для додавання нового агента натиснемо на іконку із плюсом. Відкриється діалог створення нового агента.

Заповнимо поля.

Name: Zimbra

Description: Zimbra mail server

Type: Customizable Zimbra Agent (виберемо з списку, що випадає)

Server: mail.idc.lab – тут зі списку вибираємо сервер синхронізації, який ми налаштовували на два кроки раніше (п. 3.3.3).

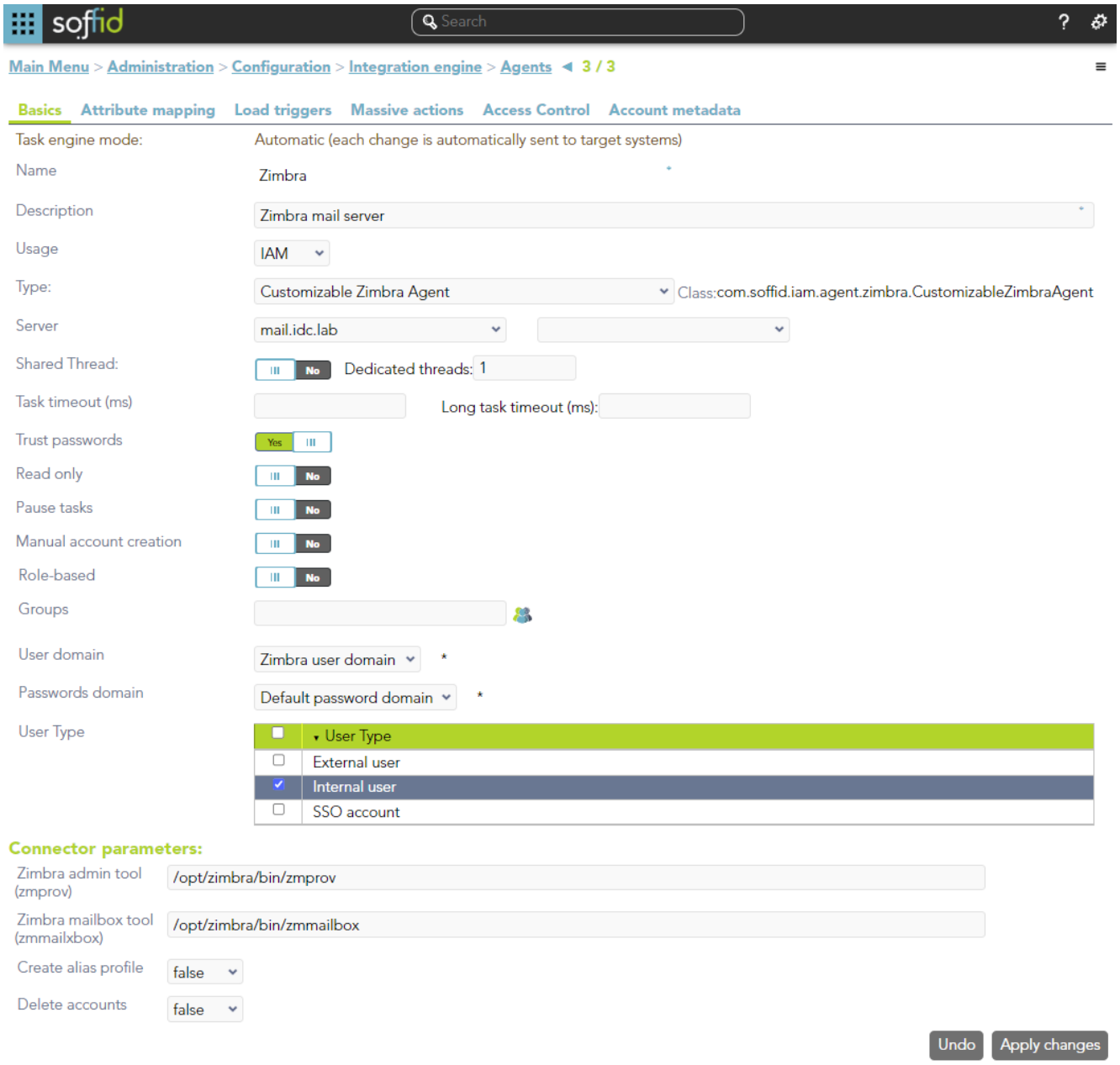


Рисунок 3.69 Додавання агента Zimbra

Trust passwords: Yes – тут ми даємо вказівку серверу довіряти паролям, якщо вони були змінені на стороні керованої системи.

Read only: No

Якщо увімкнути цю опцію, то жодних змін на стороні керованої системи вноситись не буде. Буде дозволено лише зчитувати дані із підключеної системи. Це може виявитися корисним на етапі тестування в продакшн оточенні. Однак у нашій тестовій моделі ми не будемо використовувати дану опцію і залишимо її вимкненою.

Manual account creation: No

Ця опція відповідає за автоматичне створення облікових записів. Якщо відповісти Ні (No), Soffid буде автоматично створювати акаунти для нових користувачів. У випадку, якщо Soffid не повинен цього робити і планується створювати облікові записи вручну, опцію треба включити.

User domain: Zimbra user domain (вибрати зі списку) – оберемо те саме правило, яке ми створили на попередньому кроці (п. 3.3.5).

Password domain: Default password domain (вибрати зі списку)

User type: Internal user

Connector parameters:

Zimbra admin tool (zmprov): /opt/zimbra/bin/zmprov

Zimbra mailbox tool (zmmailxbox): /opt/zimbra/bin/zmmailbox

Інші поля залишаємо без змін (рис. 3.69).

Збережемо налаштування – натиснемо кнопку Apply changes або на іконку з дискетою в правому верхньому кутку.

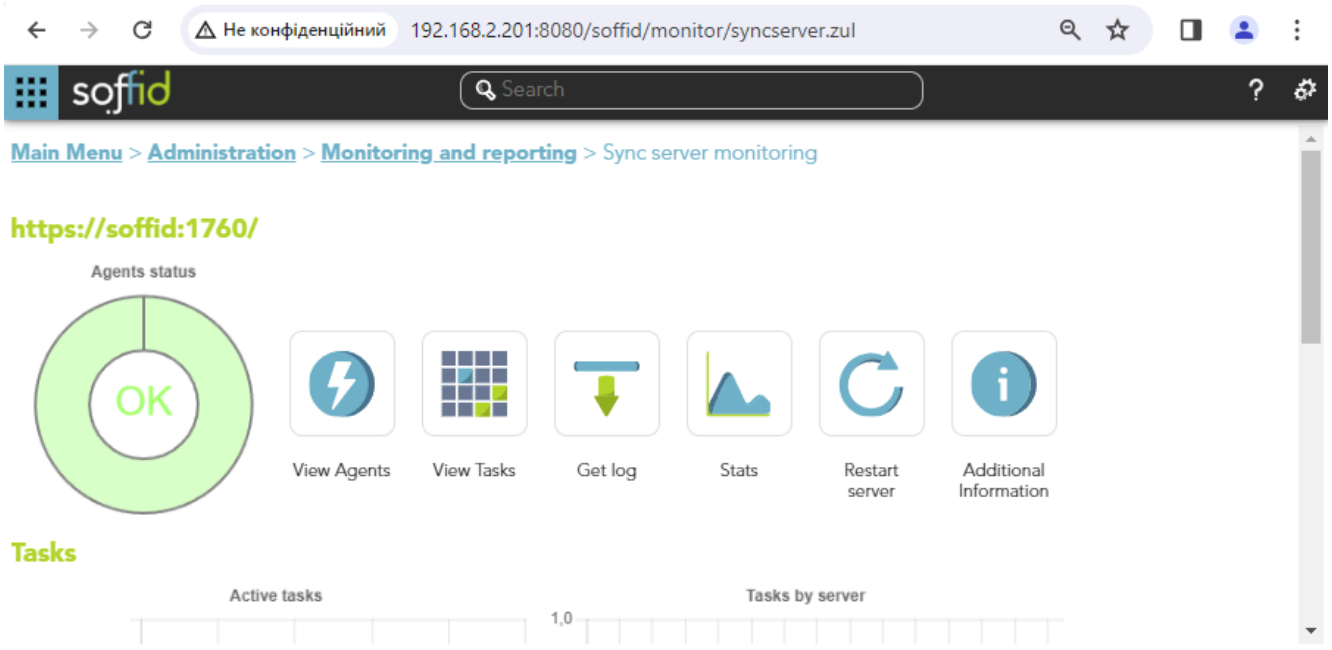


Рисунок 3.70 Моніторинг статусу Soffid Sync сервера

Перевіримо результат. Перейдемо в меню Main Menu > Administration > Monitoring and reporting > Sync server monitoring. Тут ми маємо побачити повністю зелене коло з написом ОК у центрі (рис. 3.70).

Натисніть кнопку View Agents, щоб перевірити стан агентів.

У рядку агента Zimbra має бути статус Connected.

Однак в останніх версіях Soffid Sync Server агент Zimbra не працює із коробки. Тобто ймовірно, що на сторінці View Agents у рядку Zimbra з'явиться статус Disconnected. Щоб побачити причину цього, натиснемо на цей рядок лівою кнопкою миші. З'явиться вікно з інформацією про помилку: failed to initialize LDAP client (рис. 3.71).

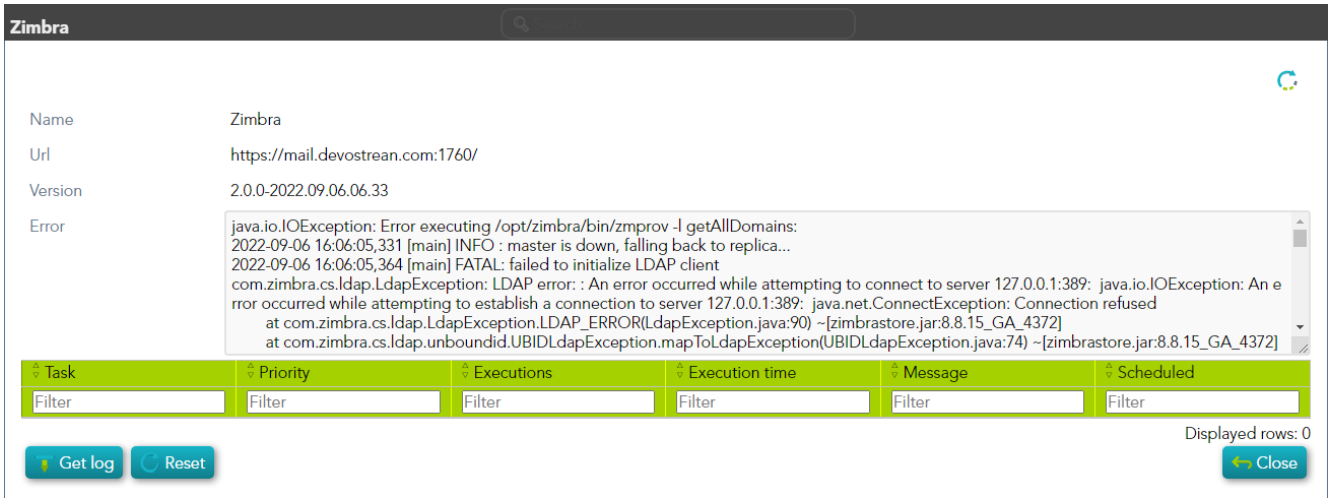


Рисунок 3.71 Помилка failed to initialize LDAP client

Щоб виправити цю помилку, доведеться внести зміни до налаштувань Zimbra.

По-перше, треба налаштувати сервер Zimbra таким чином, щоб сервіс ldap приймав підключення на інтерфейсі 127.0.0.1. За замовчуванням він працює тільки на головному мережевому інтерфейсі (якщо не встановлено інше значення в налаштуваннях zmlocalconfig). Щоб з'ясувати, на якому інтерфейсі працює ldap, виконаємо команду:

```
# netstat -tulpn | grep 389
```

Результат виконання команди представлений на рисунку 3.72.

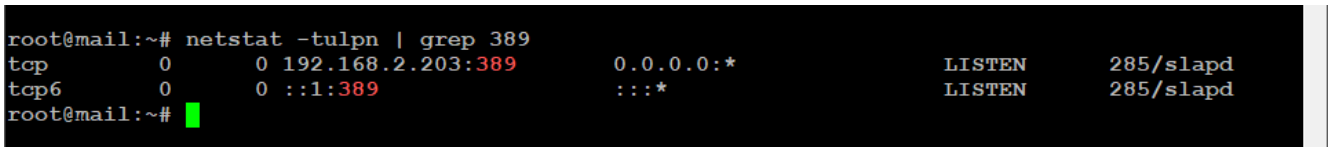


Рисунок 3.72 Виведення інформації про інтерфейси сервісу ldap

Тут видно, що сервіс ldap працює на інтерфейсі 192.168.2.203, а агент soffid намагається підключитися до адреси 127.0.0.1. Цю проблему можна виправити, якщо скоригувати параметр ldap_bind_url сервера Zimbra.

Зайдемо в консоль поштового сервера та виконаємо декілька команд від імені користувача zimbra.

```
# su - zimbra
# zmlocalconfig | grep ldap_bind_url
```

Ця команда покаже поточне значення параметра ldap_bind_url. Нам потрібно до поточного значення додати рядок ldap://localhost:389, використовуючи як роздільник пробіл. Але тут є важливий момент. Навіть якщо поточне значення даного параметра виявиться порожнім, все одно потрібно залишити в ньому основний інтерфейс, який ми побачили у виводі команди netstat, інакше у нас перестане працювати Zimbra. Таким чином, команда для зміни параметра ldap_bind_url виглядатиме так:

```
# zmlocalconfig -e ldap_bind_url="ldap://192.168.2.203:389 ldap://localhost:389"
```

Після цього перевіримо результат командою:

```
# zmlocalconfig | grep ldap_bind_url
```

Ми маємо побачити нове значення параметра. Тепер перезапустимо сервіс ldap командою:

```
# ldap restart
```

За допомогою netstat перевіримо, на якому інтерфейсі ldap приймає підключення після перезапуску (рис. 3.73).

```
root@mail:~# netstat -tulpn | grep 389
tcp        0      0 127.0.0.1:389           0.0.0.0:*               LISTEN      285/slapd
tcp        0      0 192.168.2.203:389       0.0.0.0:*               LISTEN      285/slapd
tcp6       0      0 ::1:389                 :::*                    LISTEN      285/slapd
root@mail:~#
```

Рисунок 3.73 Інтерфейси ldap після внесення змін

Повернімося до веб консолі Soffid на сторінку Sync server monitoring і натиснемо там іконку View Agents, щоб перевірити статус агента Zimbra. Швидше за все, статус буде як і раніше Disconnected, проте помилка вже має бути інша. Натиснемо на рядок Zimbra, щоб побачити нову помилку (рис. 3.74).

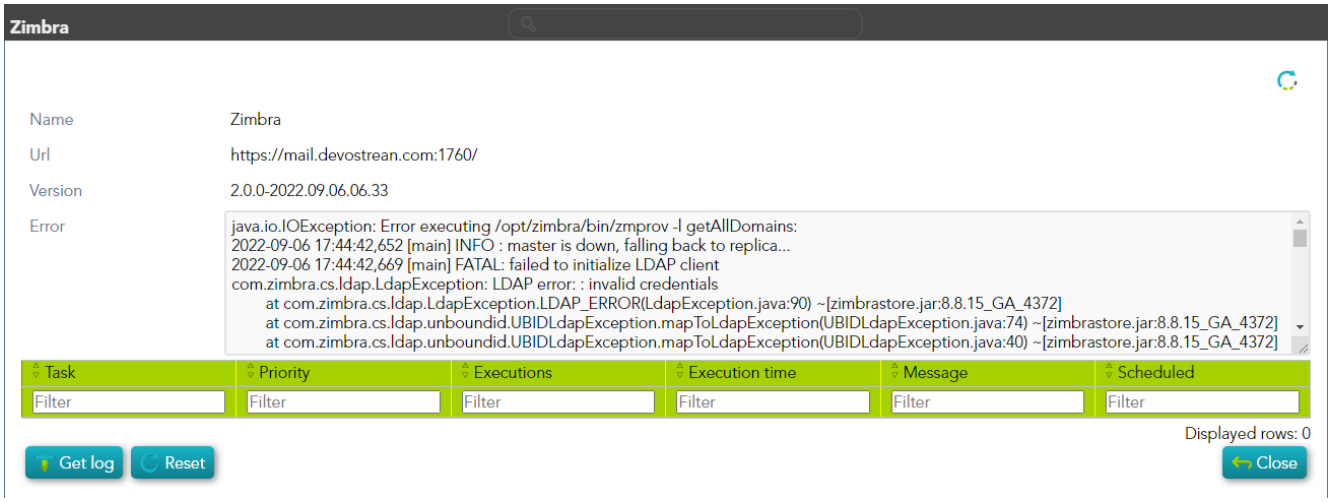


Рисунок 3.74 Помилка LDAP invalid credentials

Тепер сервер повідомляє нам про помилку LDAP invalid credentials. Ця помилка пов'язана з тим, що у користувача soffid, під яким працює агент, недостатньо прав для роботи з базою даних ldap. Додамо користувача soffid до групи zimbra, щоб вирішити проблему. Для цього в консолі Zimbra виконаємо команду:

```
# sudo usermod -aG zimbra soffid
```

Після цих змін перезапустимо Soffid Sync server командою:

```
# sudo service soffid-iamsync restart
```

Повернемося консоль Soffid в Main Menu > Administration > Monitoring and reporting > Sync server monitoring > View Agents. Помилка має зникнути. Статус агента повинен змінитись на Connected (рис. 3.75).

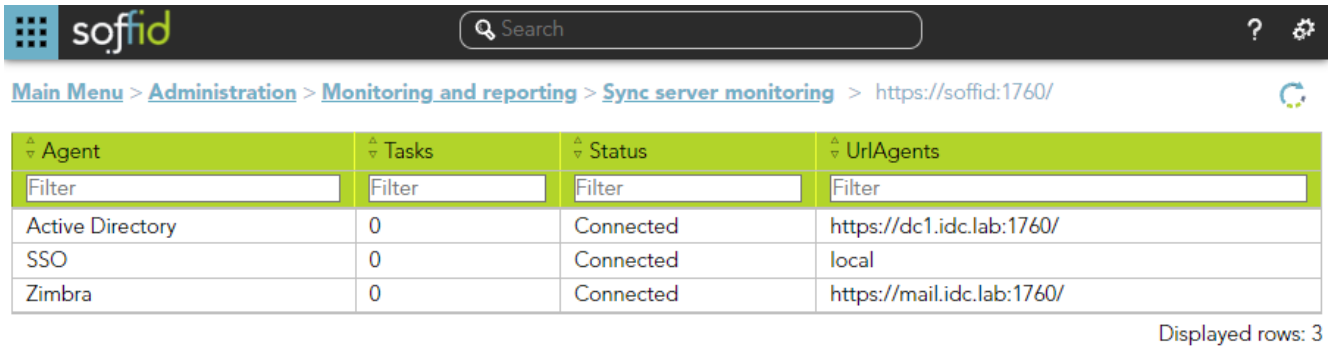


Рисунок 3.75 View agents – Перевірка статусу агентів

3.3.7 Налаштування агента Zimbra

Тепер нам треба налаштувати, яким чином атрибути користувача Zimbra будуть перетворюватися на атрибути Soffid. Для цього в Soffid є спеціальне налаштування – Attribute mapping. Перейдемо в меню Main Menu > Administration > Configuration > Integration engine > Agents та натиснемо на іконку у вигляді лупи праворуч, щоб відобразити список зареєстрованих агентів. Потім знайдемо рядок з агентом Zimbra і клацнемо по ньому – відкриється сторінка налаштувань агента. Перейдемо на вкладку Attribute mapping.

Тут нам потрібно налаштувати атрибути для двох системних об'єктів – account та user. Натиснемо плюс у рядку System objects, щоб додати новий об'єкт. Для початку створимо об'єкт account based on account.

Заповнимо системні атрибути. Розкриємо список System attribute, натиснувши на стрілочку зліва. І натиснемо кнопку плюс для додавання нового атрибуту. Усього необхідно додати три атрибути (табл. 3.5).

Таблиця 3.5 Атрибути об'єкта account агента Zimbra

System attribute	Direction	Soffid attribute
zimbraAccountStatus	←	accountDisabled ? "closed": "active"
zimbraAccount	↔	accountName
displayName	→	accountDescription

Збережемо зміни, натиснувши дискету у правому верхньому кутку.

Тепер нам потрібно додати другий системний об'єкт – user. Для цього натиснемо плюс у рядку System objects та введемо ім'я об'єкта user based on user.

Заповнимо його атрибути (табл. 3.6).

Натиснемо дискету у правому верхньому кутку, щоб зберегти зміни. Результат налаштування Attribute mapping представлений на рисунку 3.76.

Таблиця 3.6 Атрибути об'єкта user агента Zimbra

System attribute	Direction	Soffid attribute
displayName	←	firstName+" "+lastName
givenName	←	lastName
Sn	←	firstName
zimbraAccountStatus	←	accountDisabled ? "closed": "active"

Тепер перейдемо на вкладку Load triggers.

Першу опцію Full reconciliation необхідно вимкнути, щоб у процесі синхронізації Soffid не видаляв вимкнені об'єкти. Другу опцію Propagate changes слід увімкнути. Вона відповідає за автоматичне розповсюдження отриманих змін по іншим керованим системам (рис. 3.77).

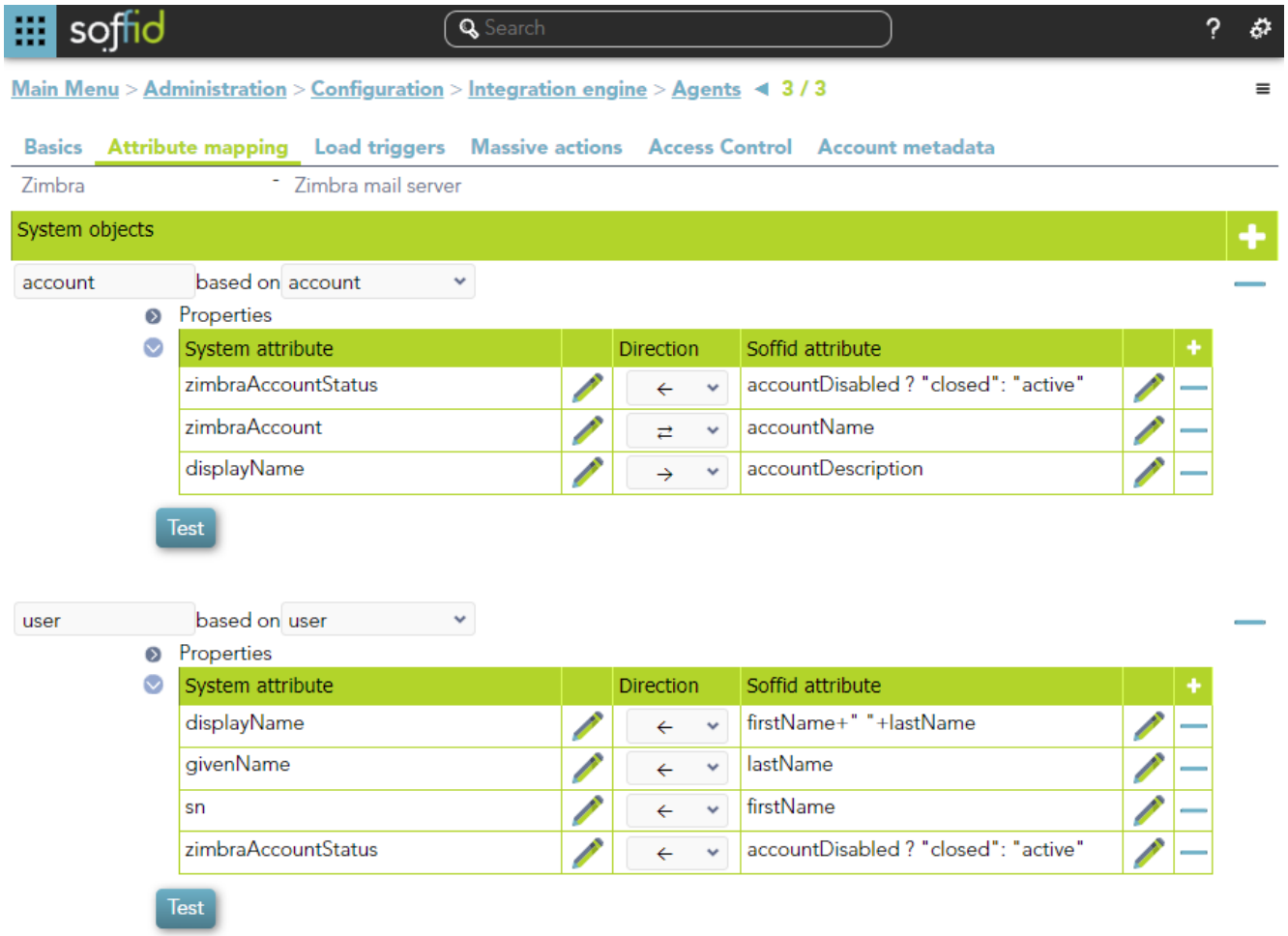


Рисунок 3.76 Налаштування Attribute mapping агента Zimbra

Натиснемо іконку у вигляді дискети у верхньому правому кутку, щоб зберегти налаштування.

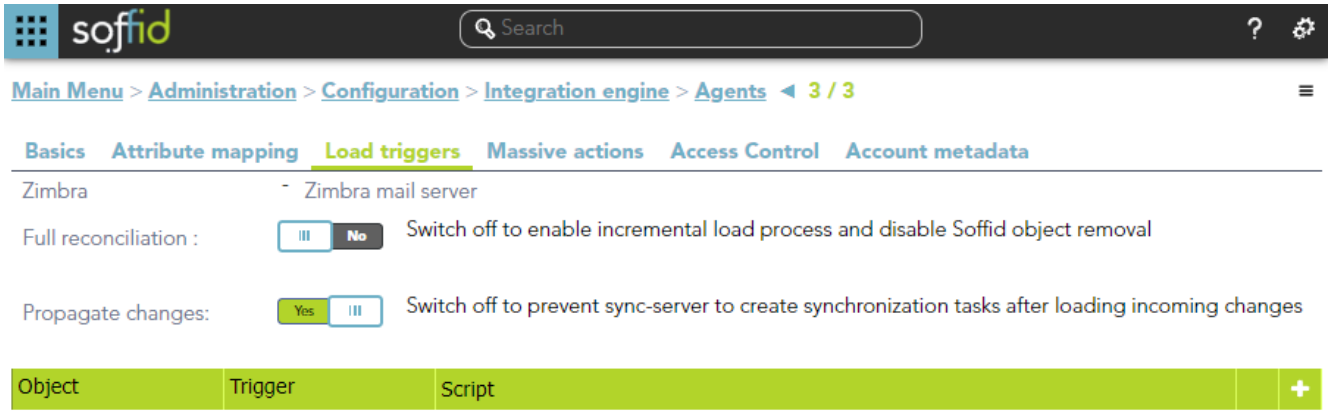


Рисунок 3.77 Налаштування Load triggers агента Zimbra

3.4 Імпорт користувачів з контролера домену в Soffid

Припустимо, що на даному етапі до Soffid було підключено всі керовані системи підприємства. Також ми вважаємо, що система моніторингу показує статус OK, і всі агенти знаходяться в стані Connected. У цьому випадку можна розпочинати початковий імпорт користувачів у Soffid IAM.

Можливо, що така задача не буде ставитися, адже всіх користувачів можна ввести до бази даних Soffid вручну. Але якщо підприємство велике, на кілька сотень користувачів, то обов'язково постане питання про те, як можна перенести всіх старих користувачів у Soffid автоматично. У такому випадку найреальніший сценарій – це коли облік користувачів на підприємстві до впровадження системи IAM вівся на контролері домену. Це найпопулярніше сховище ідентичностей у середовищі Windows. А оскільки більшість підприємств використовує на своїх комп'ютерах операційну систему Windows, то з великою ймовірністю можна припустити, що майже на кожному великому підприємстві є свій контролер домену, на якому зберігається інформація про всіх його користувачів.

У нашій моделі ми розглянемо процедуру імпорту всіх користувачів із контролера домену до системи Soffid IAM. При цьому в процесі імпорту для цих користувачів буде створено облікові записи в інших керованих системах. У нашому випадку ми маємо лише одну систему для розповсюдження облікових записів з контролера домену – це поштовий сервер Zimbra. Тому в процесі імпорту за допомогою задач синхронізації Soffid створить для кожного користувача персональну поштову скриньку на сервері Zimbra. При необхідності цю процедуру можна вимкнути – наприклад, якщо користувачі вже мають облікові записи на сервері Zimbra. Тоді слід обмежитися лише імпортом користувачів, а далі окремо проімпортувати облікові записи з кожної з керованих систем і потім прив'язати кожен обліковий запис до користувача. На жаль, ця процедура зв'язування облікових записів з користувачами може бути виконана тільки вручну. Але її

необхідно зробити лише один раз – на етапі впровадження. Надалі всі операції зі створення, редагування та управління користувачами будуть здійснюватися з консолі Soffid і всі внесені зміни будуть поширюватися на керовані системи автоматично.

Для того, щоб проімпортувати користувачів з контролера домену в Soffid увійдемо в консоль і перейдемо до налаштувань агента Main Menu > Administration > Configuration > Integration engine > Agents. Натиснемо значок у вигляді лупи, щоб оновити список агентів. Знайдемо агент Active Directory і натиснемо на нього лівою кнопкою миші. Відкриються налаштування агента. Перейдемо на вкладку Massive actions.

На цій вкладці знаходиться кілька кнопок, за допомогою яких можна запустити ті чи інші дії щодо синхронізації об'єктів між Soffid та керованою системою вручну. Зазвичай у цьому немає потреби, оскільки всі основні процеси запускаються автоматично, без участі адміністратора. Але деякі дії, такі як початковий імпорт об'єктів із керованої системи, запускаються вручну.

Щоб розпочати імпорт користувачів з контролера домену, потрібно натиснути кнопку Load authoritative data for identities and groups. Ця кнопка з'являється на вкладці Massive action тільки в тому випадку, якщо агент вибрано як джерело облікових даних – на вкладці Basic повинна бути включена опція Authoritative identity source (рис. 3.49).

Але перш, ніж розпочати імпорт, змінимо деякі налаштування Soffid, щоб оптимізувати процес синхронізації. Перейдемо в меню Main Menu > Administration > Configuration > Integration engine > Smart engine settings. У цьому вікні внесемо такі зміни (рис. 3.78).

Task engine mode: Automatic (each change is automatically sent to target systems) – виберемо зі списку значення Automatic. У цьому режимі всі зміни автоматично надсилаються на керовані системи.

Tasks limit per transaction: 100 – якщо окрема транзакція створює велику кількість задач, то всі задачі понад це число ставляться на паузу і чекають, поки адміністратор не запустить їх вручну. Цей параметр – захист від перевантаження сервера, коли надто велика кількість задач може паралізувати роботу сервера Soffid.

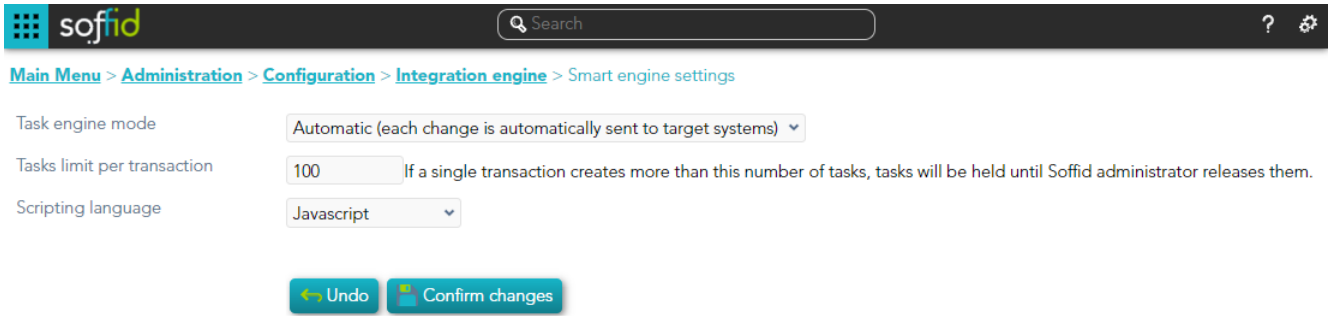


Рисунок 3.78 Smart engine settings – Параметри синхронізації

Натисніть кнопку Confirm changes щоб зберегти зміни та закрити вікно.

Тепер можна приступати до процедури імпорту. Повернемось до агента Active Directory на вкладку Massive actions (рис. 3.79). Якщо натиснути кнопку Reconcile (load target system objects), то у Soffid завантажаться акаунти з керованої системи – контролера домену. Якщо ж натиснути кнопку Load authoritative data for identities and groups – з контролера домену буде імпортовано користувачів.

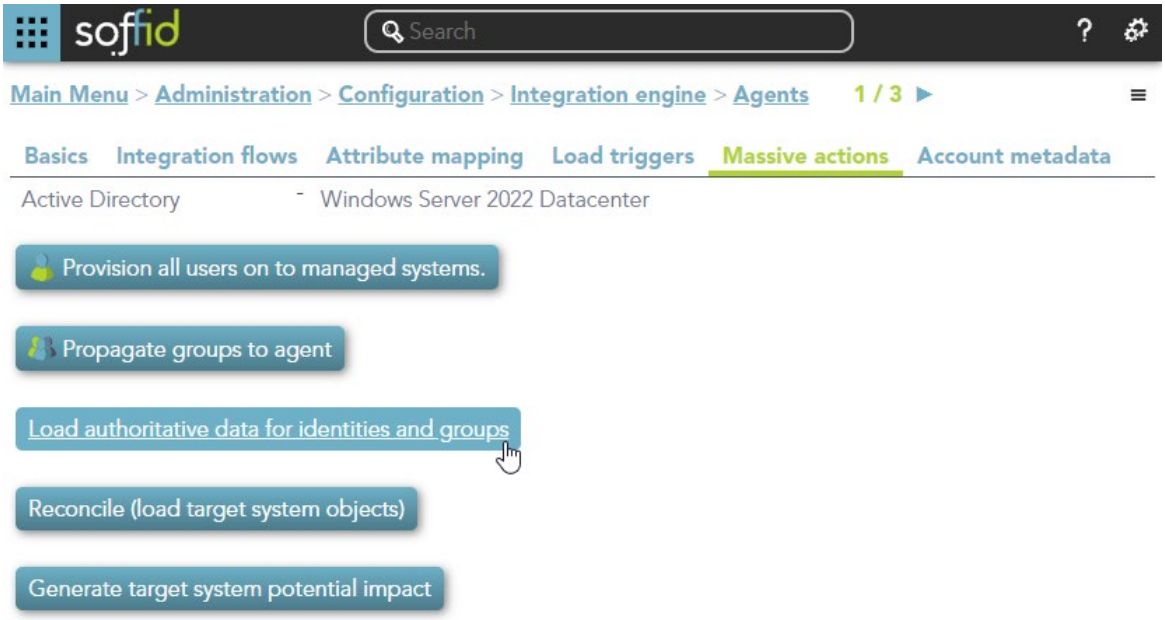


Рисунок 3.79 Запуск імпорту даних із Active Directory

Натиснемо кнопку Load authoritative data for identities and groups. Перед запуском процедури нам буде запропоновано вказати сервер, на який імпортуватимуться облікові дані. Тут потрібно вибрати основний сервер синхронізації. У нашій моделі в списку, що випадає, буде доступний тільки один варіант – soffid (рис. 3.80).

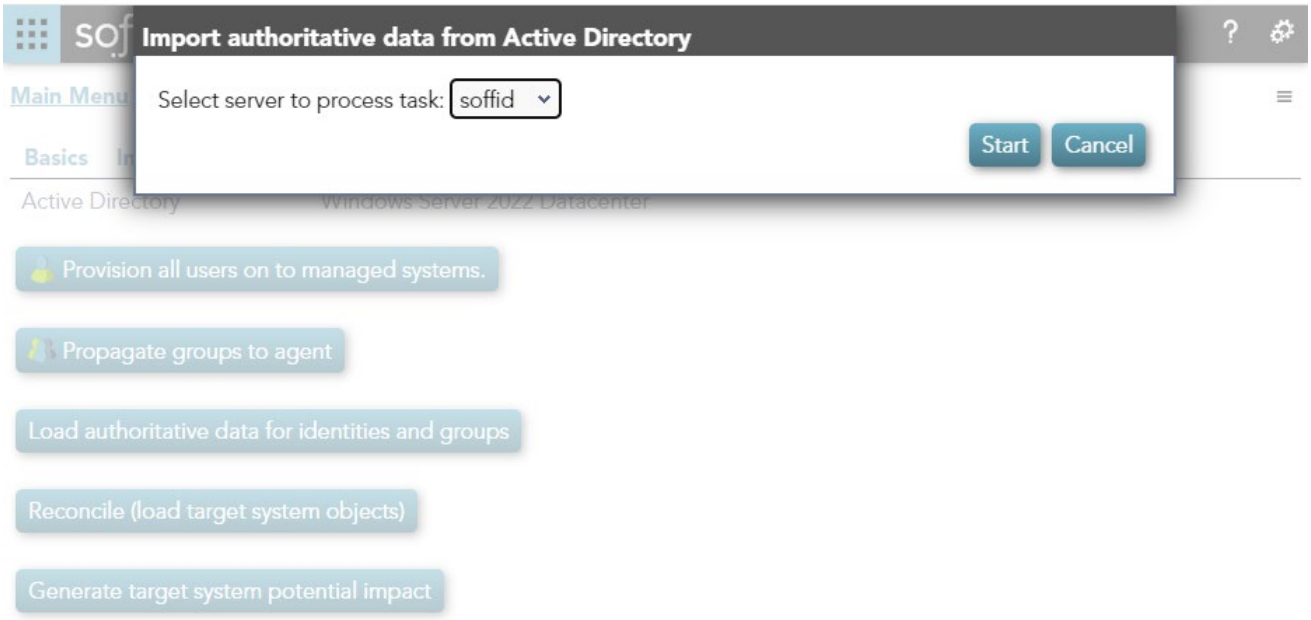


Рисунок 3.80 Вибір сервера для імпорту

Виберемо у списку soffid і натиснемо Start.

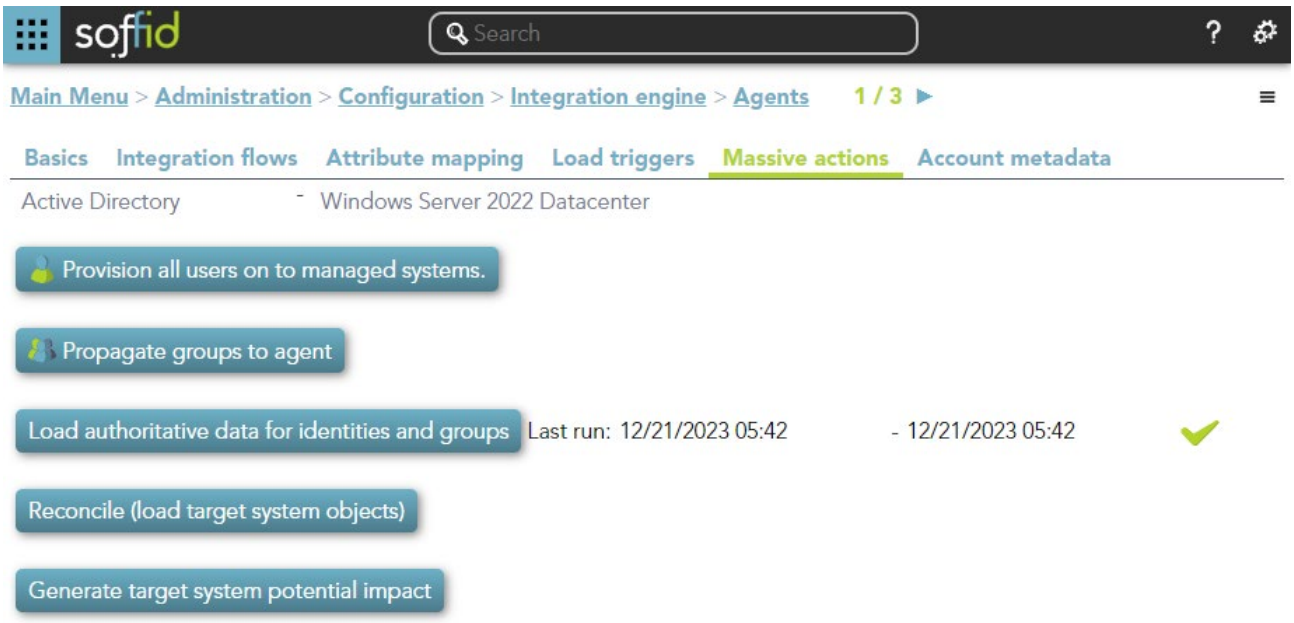


Рисунок 3.81 Результат процедури імпорту користувачів

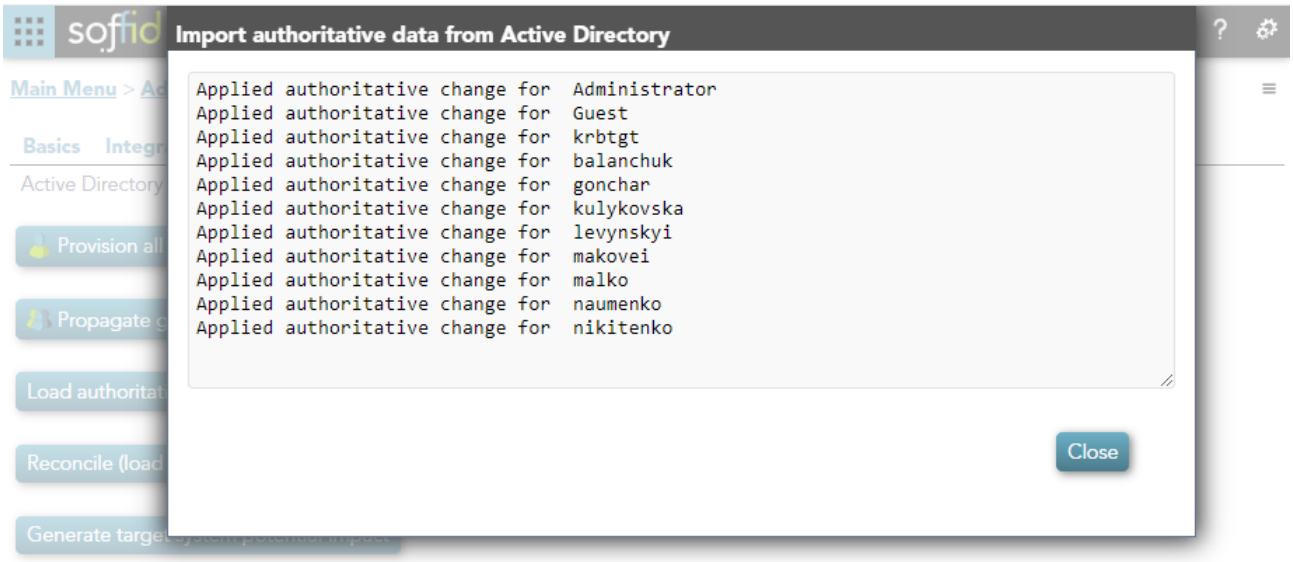


Рисунок 3.82 Звіт про імпорт користувачів із Active Directory

Почнеться імпорт облікових даних з контролера домену в Soffid відповідно до правил перетворення атрибутів, налаштованих в агенті. Після закінчення процедури поруч із кнопкою Load authoritative data for identities and groups з'явиться запис про дату та час останнього запуску цієї опції. Якщо операція була успішною, справа у рядку з'явиться зелена галочка (рис. 3.81). Натиснемо на цю галочку, щоб побачити звіт Soffid про імпортованих користувачів (рис. 3.82).

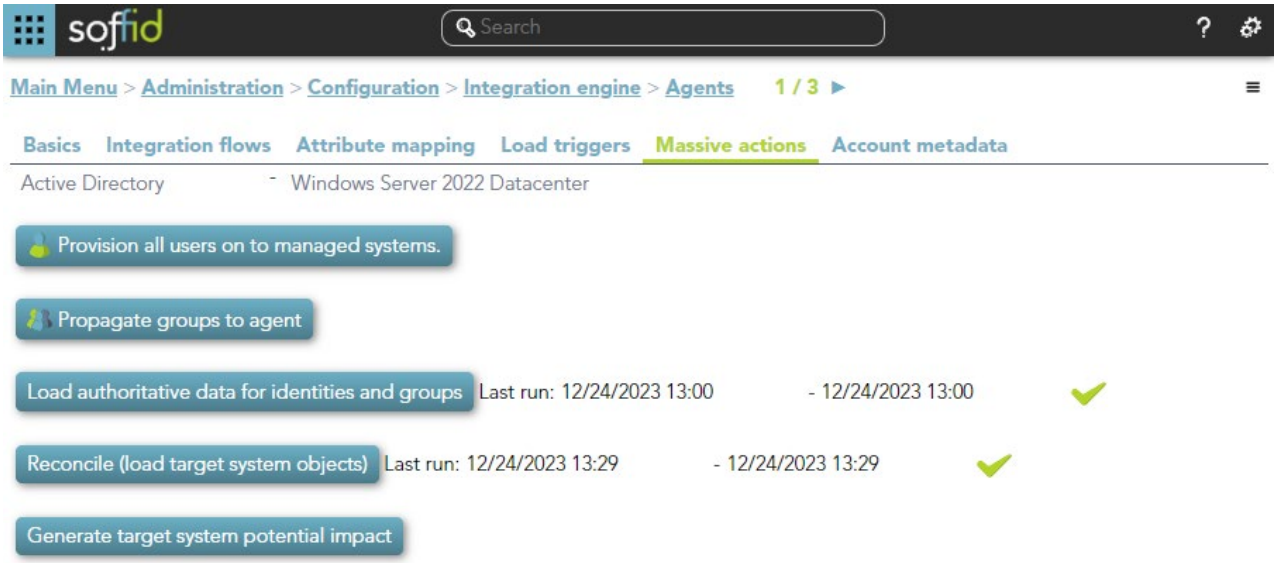


Рисунок 3.83 Результат процедури імпорту акаунтів

Після цього натиснемо кнопку Reconcile (load target system objects), щоб проімпортувати акаунти з Active Directory. За аналогією з процедурою імпорту

користувачів вкажемо цільовий сервер для імпорту акаунтів (рис. 3.80). Після закінчення процесу імпорту поряд з кнопкою з'явиться відповідний запис з часом виконання та відміткою у вигляді зеленої галки (рис. 3.83). Натиснемо на зелену галочку, щоб відкрити звіт про завантажені акаунти (рис. 3.84).

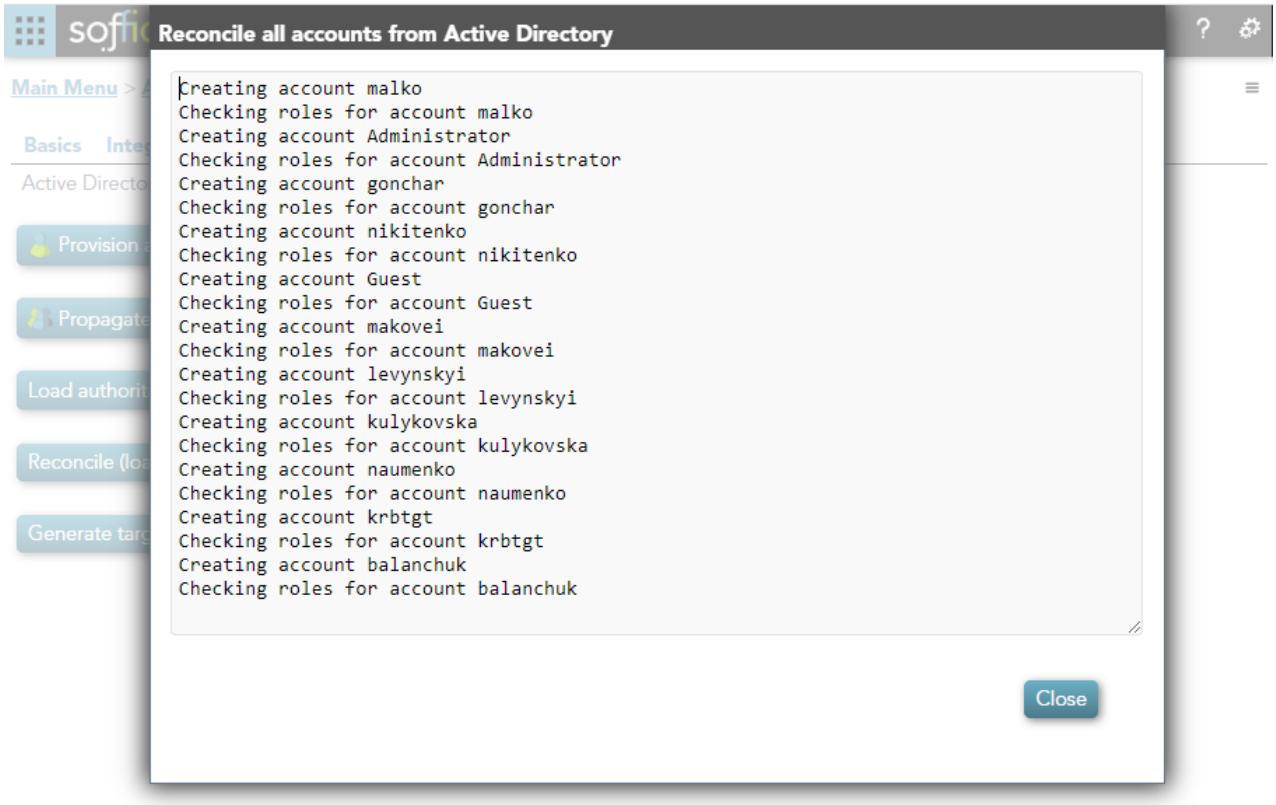


Рисунок 3.84 Звіт про імпорт акаунтів з Active Directory

Тепер перейдемо в меню Main Menu > Administration > Resources > Users та перевіримо, чи з'явилися там нові користувачі. Натиснемо на іконку у вигляді лупи поруч із кнопкою Add criteria – з'явиться список користувачів (рис. 3.85).

Так само потрібно перевірити список акаунтів. Перейдемо в меню Main Menu > Administration > Resources > Accounts та натиснемо на іконку у вигляді лупи біля кнопки Add criteria. Відобразяться акаунти Soffid (рис. 3.86).

За замовчуванням Soffid виводить на екран некеровані акаунти – це акаунти, які не пов'язані з жодним обліковим записом користувача Soffid (вони відображаються шрифтом сірого кольору). Оскільки ці акаунти були імпортовані з

керованої системи, вони поки що не прив'язані до користувачів. Прив'язку акаунтів до користувачів необхідно проводити вручну. Це разова операція, яку потрібно зробити на етапі впровадження Soffid IAM. В подальшому, якщо користувачі та облікові записи будуть створюватися безпосередньо в Soffid, прив'язка облікових записів до користувачів буде здійснюватися автоматично.

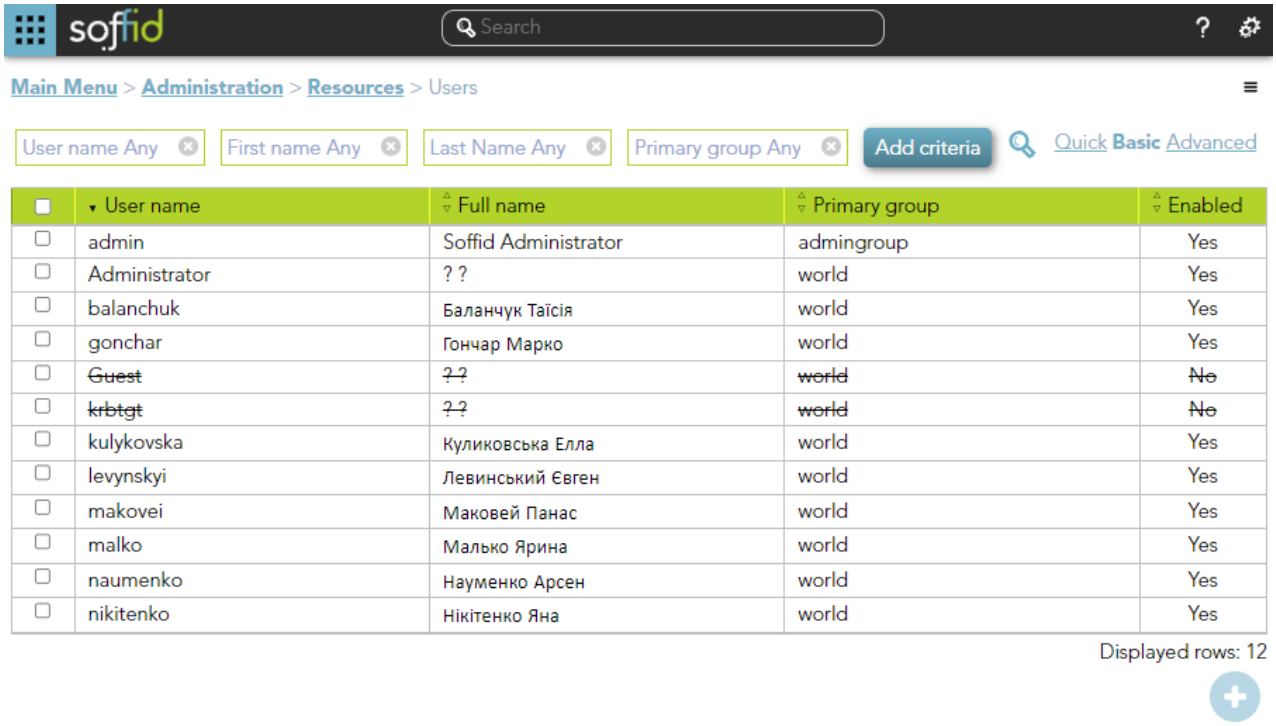


Рисунок 3.85 Список користувачів Soffid

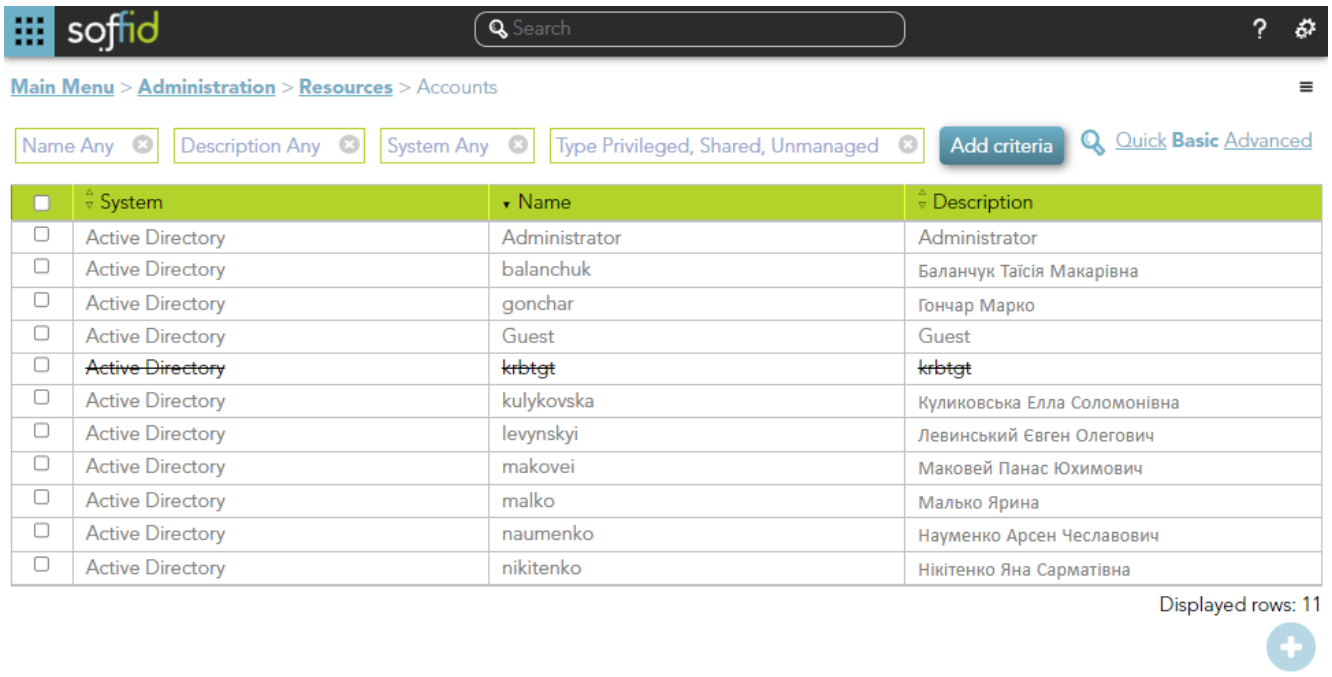


Рисунок 3.86 Список некерованих акаунтів Soffid

У процесі імпорту користувачів з контролера домену Soffid повинен був для цих користувачів створити акаунти на поштовому сервері Zimbra. Але зараз ми бачимо лише акаунти Active Directory. Щоб побачити акаунти Zimbra, зминемо фільтр у полі Type вгорі сторінки. Увімкнемо в ньому тип Single user, а інші типи відключимо (рис. 3.87). І натиснемо кнопку Accept.

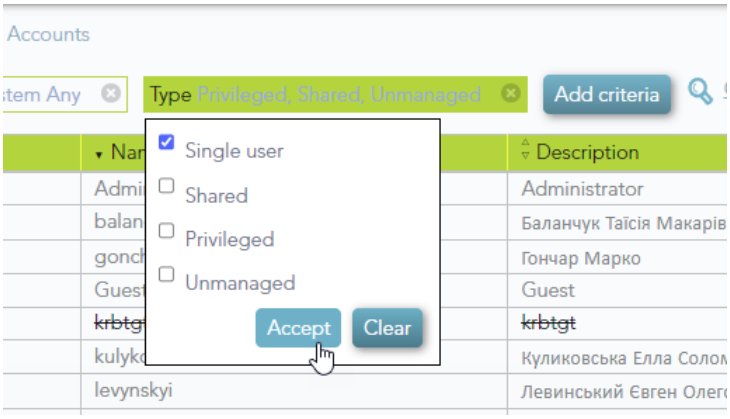


Рисунок 3.87 Фільтр за типом акаунта в консолі Soffid

Відобразяться акаунти Zimbra, створені в процесі імпортування користувачів з контролера домену (рис. 3.88). Ці облікові записи вже пов'язані з користувачами, тому вони відображаються шрифтом чорного кольору, на відміну від облікових записів Active Directory (рис. 3.84).

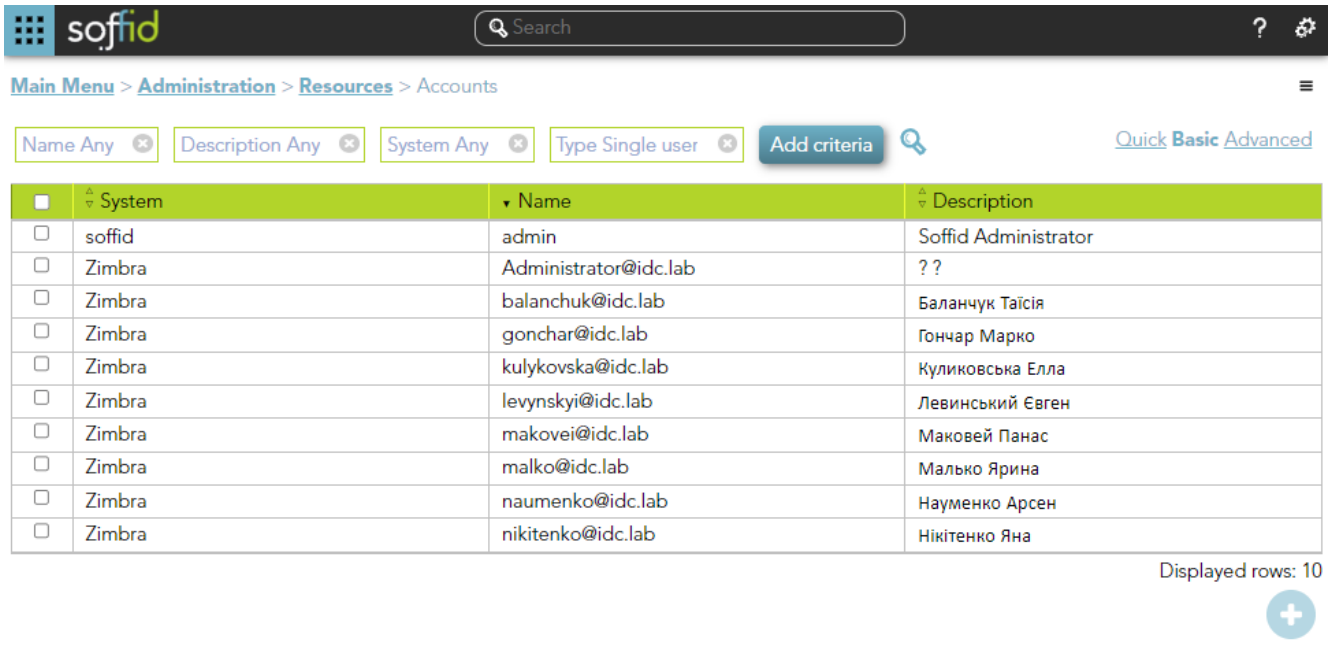


Рисунок 3.88 Список акаунтів поштового сервера Zimbra

Зайдемо до адміністративної панелі Zimbra і перевіримо, чи з'явилися там поштові скриньки, створені агентом синхронізації Soffid. Зайдемо в меню Керування – Облікові записи. Ми побачимо, що у списку облікових записів Zimbra з'явилися поштові скриньки з іменами користувачів Soffid (рис. 3.89). Це означає, що процедура синхронізації між сервером Soffid та поштовим сервером Zimbra працює.

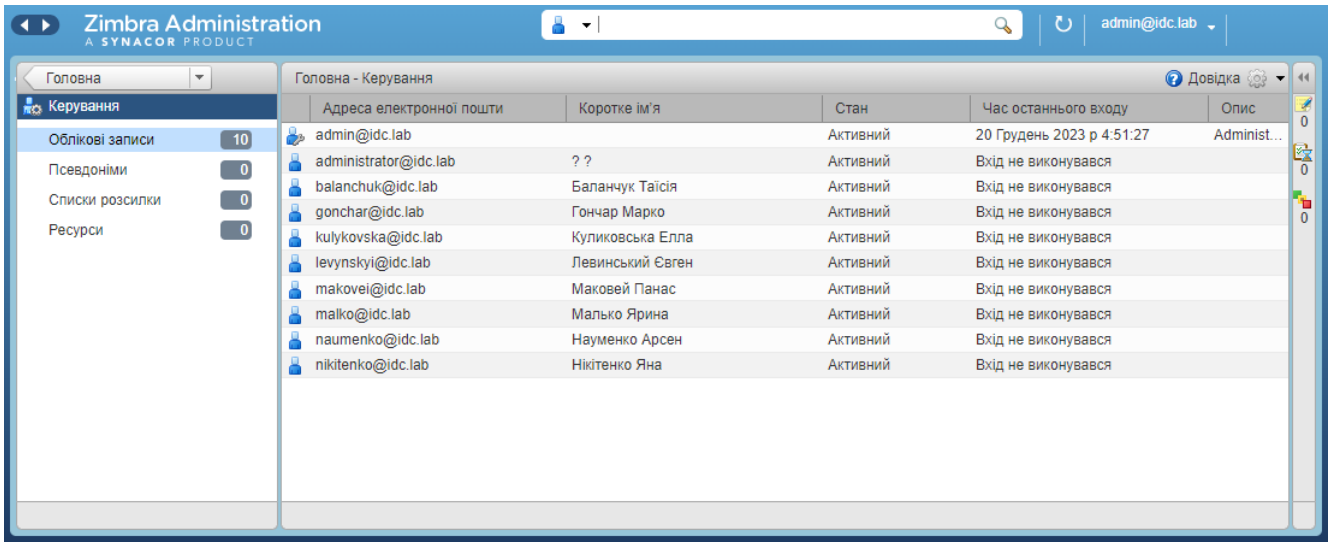


Рисунок 3.89 Список облікових записів в панелі керування Zimbra

На цьому процес початкової інтеграції Soffid IAM до існуючої інфраструктури підприємства можна вважати завершеним.

ВИСНОВКИ

Впровадження IAM системи допоможе прискорити надання доступу до ресурсів підприємства новим співробітникам, підвищить безпеку наявних інформаційних систем, спростить співробітникам процедуру входу до тієї чи іншої системи перед початком роботи з ними.

У ході роботи над завданням було проведено детальний аналіз різних систем керування ідентичністю та доступом та зроблено вибір на користь системи Soffid IAM. Ця система одночасно задовольняє багатьом критеріям – вона багатофункціональна, гнучка, сумісна з багатьма платформами і відноситься до категорії вільного програмного забезпечення з відкритим кодом.

Для вирішення поставлених завдань було розроблено модель із використанням системи віртуалізації Proxmox VE. Ця модель, що складається з трьох віртуальних машин, добре зарекомендувала себе і може використовуватися для інших подібних досліджень.

У ході вирішення поставлених завдань було виявлено низку проблем, які виникли під час встановлення та налаштування програмного забезпечення Soffid IAM. Дослідження показали, що знайти рішення тієї чи іншої проблеми в інтернеті, включаючи сайт розробників, практично неможливо. Це пов'язано з тим, що система Soffid ще не набула широкого поширення і спільнота його користувачів поки що дуже мала. Тим цінніше отриманий у цій роботі результат, оскільки він включає у тому числі вирішення проблем, які можуть виникнути під час встановлення та впровадження Soffid IAM.

Незважаючи на складнощі, пов'язані з впровадженням Soffid IAM, та що процес впровадження може зайняти тривалий час, плюси від отриманого результату безумовно компенсують усі ті ресурси, що знадобяться на етапі впровадження.

ПЕРЕЛІК ПОСИЛАНЬ

1. Що таке система керування ідентичністю та доступом? [Електронний ресурс] – 2023. – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-identity-access-management-iam (дата звернення: 17.11.2023). – Назва з екрана.
2. Identity and Access Management (IAM) [Електронний ресурс] – 2023. – Режим доступу: https://www.oracle.com/ca-en/security/identity-management (дата звернення: 17.11.2023). – Назва з екрана.
3. Identity and Access Management або система управління обліковими даними. Рішення Microsoft Azure AD [Електронний ресурс] – 2023. – Режим доступу: https://www.globallogic.com/ua/insights/blogs/identity-and-access-management-azure-ad (дата звернення: 18.11.2023). – Назва з екрана.
4. Soffid 3 Reference guide. [Електронний ресурс] – 2023. – Режим доступу: https://bookstack.soffid.com/books/soffid-3-reference-guide (дата звернення: 18.12.2023). – Назва з екрана.
5. Gittlen S., Rosencrance L. What is identity and access management? Guide to IAM [Електронний ресурс] / S. Gittlen, L. Rosencrance – 2021. – Режим доступу: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system (дата звернення: 28.10.2023). – Назва з екрана.
6. Ruchini C. Introduction to Identity and Access Management [Електронний ресурс] / C. Ruchini – 2021. – Режим доступу: https://medium.com/identity-beyond-borders/introduction-to-identity-and-access-management-2f3b80862647 (дата звернення: 21.10.2023). – Назва з екрана.
7. Understanding the Importance of IAM (Identity and Access Management) [Електронний ресурс] – 2021. – Режим доступу: https://www.auditboard.com/blog/importance-of-iam/ (дата звернення: 22.10.2023). – Назва з екрана.
8. Strom D. What is IAM? Identity and access management explained [Електронний ресурс] / D. Strom – 2021. – Режим доступу:

https://www.mufgamericas.com/insights-and-experience/what-iam-identity-and-access-management-explained (дата звернення: 14.10.2023). – Назва з екрана.

9. 5 keys to success when implementing Identity and Access Management [Електронний ресурс] – 2022. – Режим доступу: https://www.trustbuilder.com/articles/5-keys-to-success-when-implementing-iam/ (дата звернення: 10.11.2023). – Назва з екрана.
10. Brooks S. Tips for Getting IAM Implementation Right [Електронний ресурс] / S. Brooks – 2023. – Режим доступу: https://convergetp.com/2023/05/09/tips-for-getting-iam-implementation-right/ (дата звернення: 15.10.2023). – Назва з екрана.
11. Moyle E. How to build an effective IAM architecture [Електронний ресурс] / E. Moyle – 2020. – Режим доступу: https://www.techtarget.com/searchsecurity/feature/How-to-build-an-identity-and-access-management-architecture (дата звернення: 11.11.2023). – Назва з екрана.
12. Magnusson A. Identity and Access Management (IAM) Best Practices [Електронний ресурс] / A. Magnusson – 2022. – Режим доступу: https://www.strongdm.com/blog/iam-best-practices (дата звернення: 12.11.2023). – Назва з екрана.
13. Build Access Management Platform with Free Identity Server [Електронний ресурс] – 2023. – Режим доступу: https://products.containerize.com/single-sign-on/wso2/ (дата звернення: 19.12.2023). – Назва з екрана.
14. McDade M. The Top 11 Identity And Access Management Solutions [Електронний ресурс] / M. McDade – 2023. – Режим доступу: https://expertinsights.com/insights/top-10-identity-and-access-management-solutions/ (дата звернення: 27.11.2023). – Назва з екрана.
15. Step by Step guide to setup LDAPS on Windows Server [Електронний ресурс] – 2023. – Режим доступу: https://www.miniorange.com/guide-to-setup-ldaps-on-windows-server (дата звернення: 27.10.2023). – Назва з екрана.
16. Canner B. The 10 Best Free and Open-Source Identity Management Tools [Електронний ресурс] / B. Canner – 2022. – Режим доступу:

https://solutionsreview.com/identity-management/the-best-free-and-open-source-identity-management-tools/ (дата звернення: 28.11.2023). – Назва з екрана.

17. Top Identity and Access Management Systems | IAM | Open Source | Enterprise [Електронний ресурс] – 2022. – Режим доступу: https://medium.com/@devops.ent/top-identity-and-access-management-systems-iam-open-source-enterprise-92cf66560a55 (дата звернення: 10.11.2023). – Назва з екрана.
18. Diener D. How to run unstable packages on Debian Stable [Електронний ресурс] / D. Diener – 2023. – Режим доступу: https://www.addictivetips.com/ubuntu-linux-tips/how-to-run-unstable-packages-on-debian-stable/ (дата звернення: 08.12.2023). – Назва з екрана.
19. Köller J. What Is Identity and Access Management? The Beginner's Guide to IAM [Електронний ресурс] / J. Köller – 2023. – Режим доступу: https://www.tenfold-security.com/en/identity-and-access-management/ (дата звернення: 14.11.2023). – Назва з екрана.
20. Nelson B. How do you Implement IAM? One Bite at a Time [Електронний ресурс] / B. Nelson – 2022. – Режим доступу: https://www.identityfusion.com/blog/iam-implementation-approach (дата звернення: 26.11.2023). – Назва з екрана.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

Державний університет інформаційно-комунікаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження ефективності застосування IAM систем на підприємстві на прикладі впровадження Soffid IAM»

на здобуття освітнього ступеня магістра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Виконав: здобувач вищої освіти гр. ІСДМ-61
Максим БАКЛИКОВ

Керівник: доктор філософії (PhD), доцент
Аліна ТУШИЧ

Київ - 2023

Актуальність теми: на підприємствах з великою кількістю працівників та багатьма сервісами та ресурсами, до яких співробітникам надається персональний доступ (за логіном та паролем) стає актуальним питання обліку ідентифікаційних даних, а також керування рівнями доступу, які отримують співробітники залежно від своїх посад. Основна проблема, з якою постійно стикаються адміністратори великих підприємств, – зробити так, щоб користувачі отримували доступ до необхідних ресурсів, але в жодному разі не мали доступу до конфіденційної інформації, яка їм не потрібна. Ці задачі вирішуються впровадженням на підприємстві системи IAM (Identity and Access Management).

Об`єкт дослідження: процес обліку ідентифікаційних даних.

Предмет дослідження: система керування ідентичністю та доступом.

Мета дослідження: автоматизувати процес обліку ідентифікаційних даних та керування доступом співробітників до ресурсів компанії за рахунок впровадження в існуючу IT інфраструктуру системи IAM.

Завдання дослідження:

- здійснити аналіз наявних на ринку IAM рішень;
- дослідити технології, що застосовуються у сучасних системах IAM;
- обрати систему IAM та обґрунтувати цей вибір;
- встановити серверну частину Soffid IAM;
- підключити до сервера Soffid керовані системи-сателіти на прикладі контролера домену Active Directory та поштового сервера Zimbra;
- перенести користувачів контролера домену до Soffid IAM.


IDENTITY AND ACCESS MANAGEMENT
Автоматичне створення та видалення акаунтів
Ефективне адміністрування
Контроль доступу на основі ролей
Запити самообслуговування
Чіткі та детальні звіти про дозволи
Регулярні перевірки доступу
Підвищена кібербезпека
Централізоване керування користувачами
Покращена відповідність вимогам

Компоненти IAM систем

- **Ідентифікація** – це можливість однозначно ідентифікувати користувача системи або додаток, що виконується в системі.
- **Аутентифікація** – це можливість довести, що користувач або програма дійсно є тими, за кого вони себе видають.
- **Авторизація** – це надання чи делегування дозволів певній особі чи групі користувачів.

Технології IAM

- **ESSO або SSO** – технологія корпоративного єдиного входу – Enterprise Single Sign-On або Single Sign-On;
- **IdP або Web SSO** – технологія постачальника ідентифікації – Identity Provider або Web Single Sign-On.

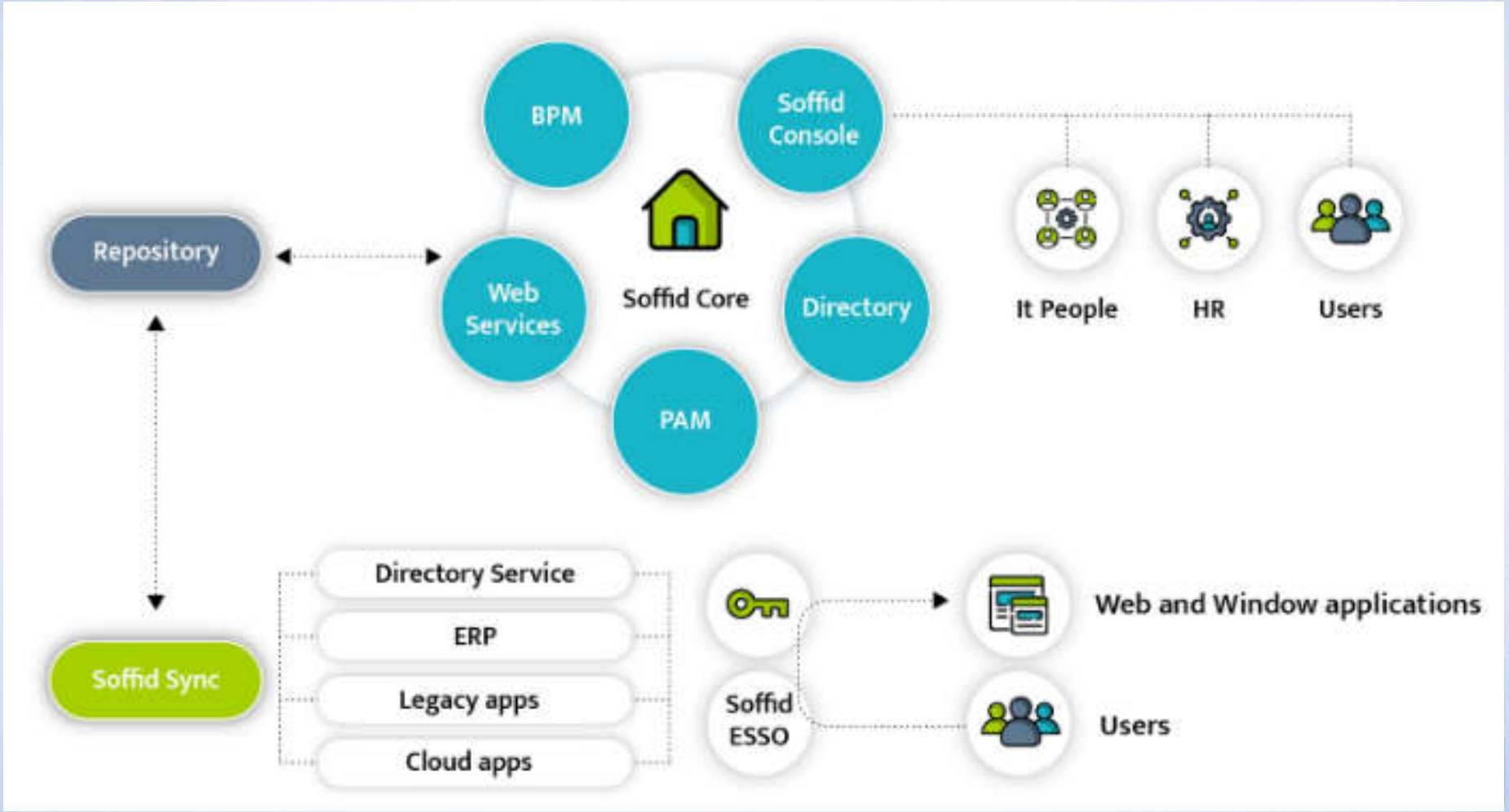
Переваги IAM з відкритим початковим кодом

- наявність доступу до початкового коду;
- підтримка спільнотою;
- швидкий процес впровадження та реалізації;
- розширюваність та масштабування;
- більш повна участь IT-команди підприємства;
- відсутність прив'язки до постачальника;
- **безкоштовність.**

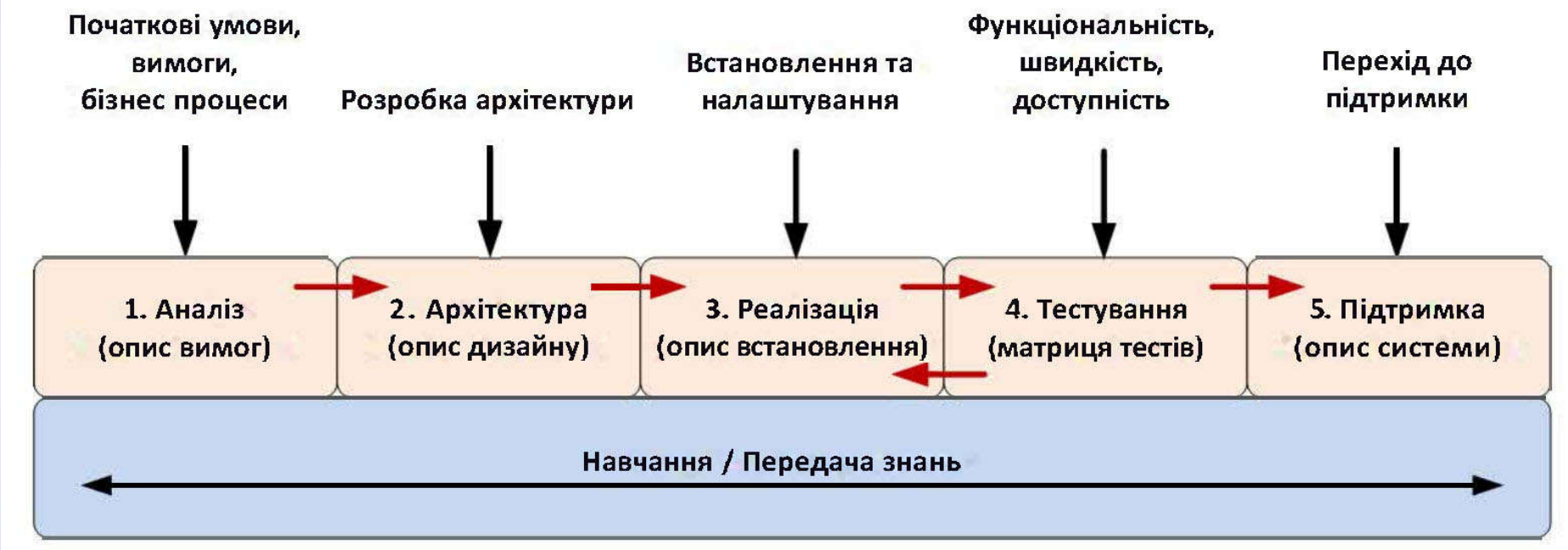
IAM системи з відкритим початковим кодом для підприємств

- Keycloak
- Apache Syncope
- OpenIAM
- WSO2
- **Soffid**

Архітектура Soffid

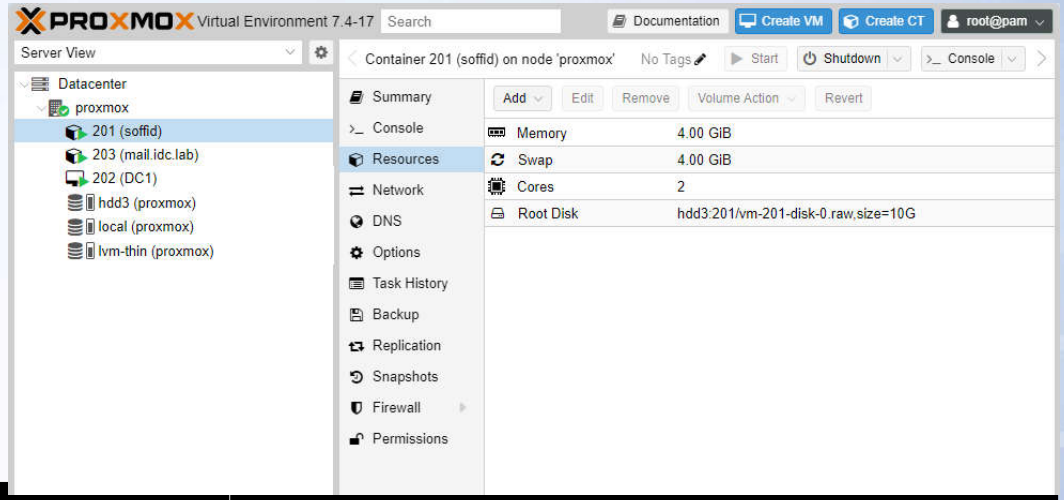


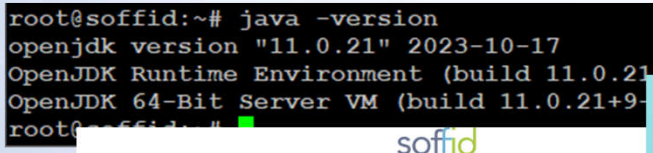
Етапи впровадження IAM системи

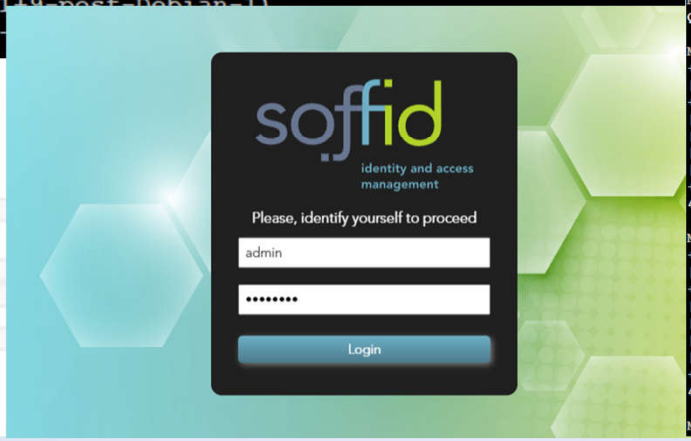


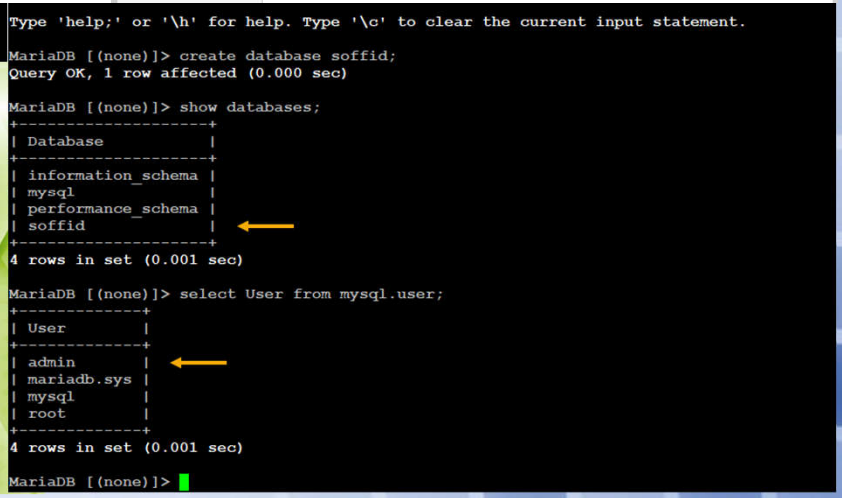
Встановлення серверної частини Soffid

1. Встановлення та підготовка бази даних
2. Встановлення Java JDK
3. Встановлення Soffid IAM Console
4. Первинне налаштування Soffid Console
5. Встановлення Soffid Sync Server
6. Налаштування Password policy





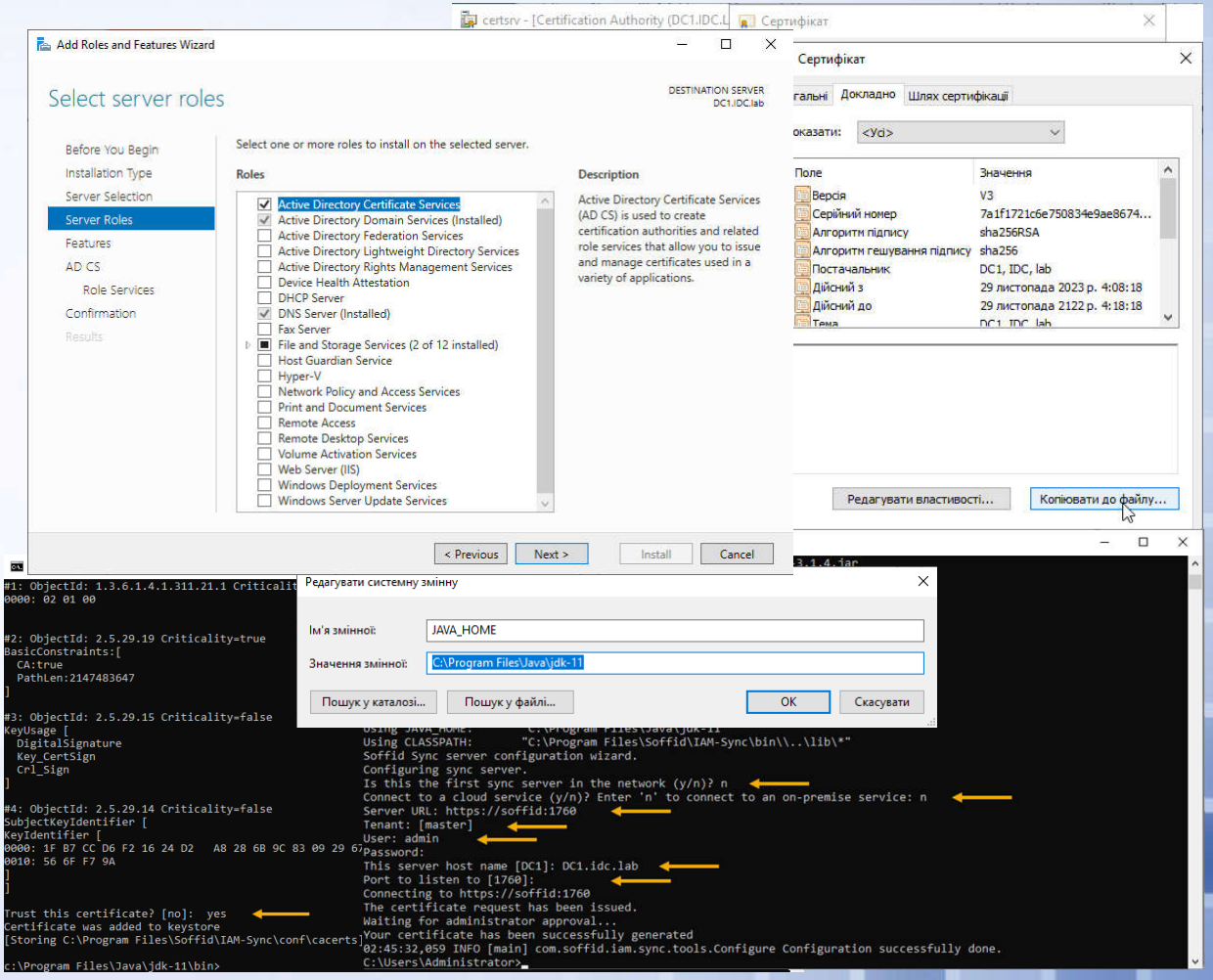




Підключення контролера домену до Soffid

Крок 1. Встановлення Soffid Sync Server на Windows Server 2022

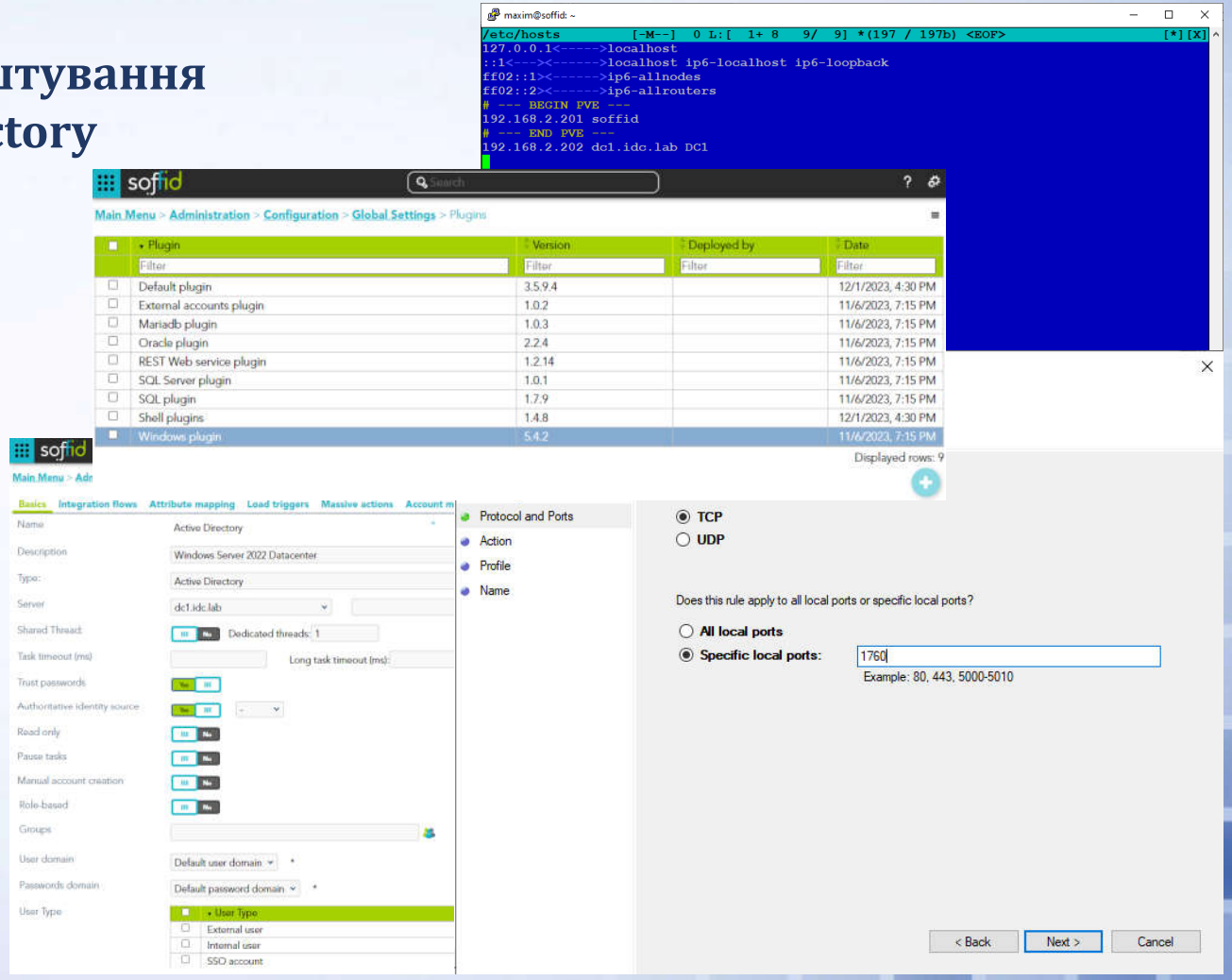
1. Налаштування захищеного протоколу LDAPS (LDAP over SSL)
   a) Додавання ролі Служби сертифікатів Active Directory
   b) Налаштування центру сертифікації та кореневого сертифіката
   c) Експорт сертифіката у файл
2. Встановлення Java на Windows Server
3. Встановлення та налаштування Soffid Sync Server
4. Імпорт сертифіката домену до сховища IAM Sync Server



Підключення контролера домену до Soffid

Крок 2. Встановлення та налаштування конектора для Active Directory

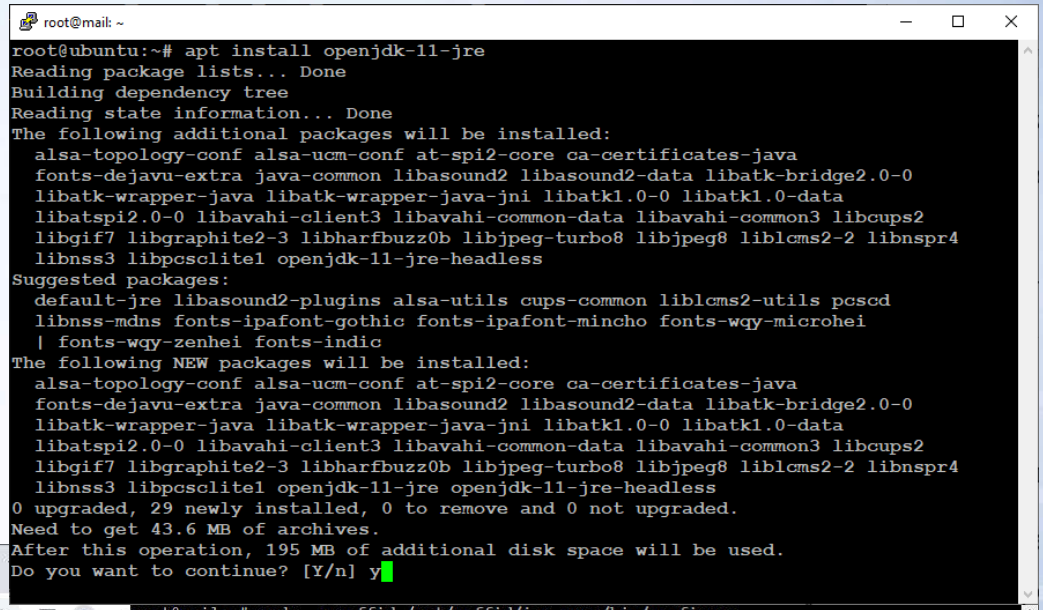
1. Встановлення плагіна для Active Directory
2. Оновлення файлу hosts на сервері (опціонально)
3. Відкриття порту 1760 на сервері Windows
4. Додавання агента Active Directory
5. Налаштування агента Active Directory

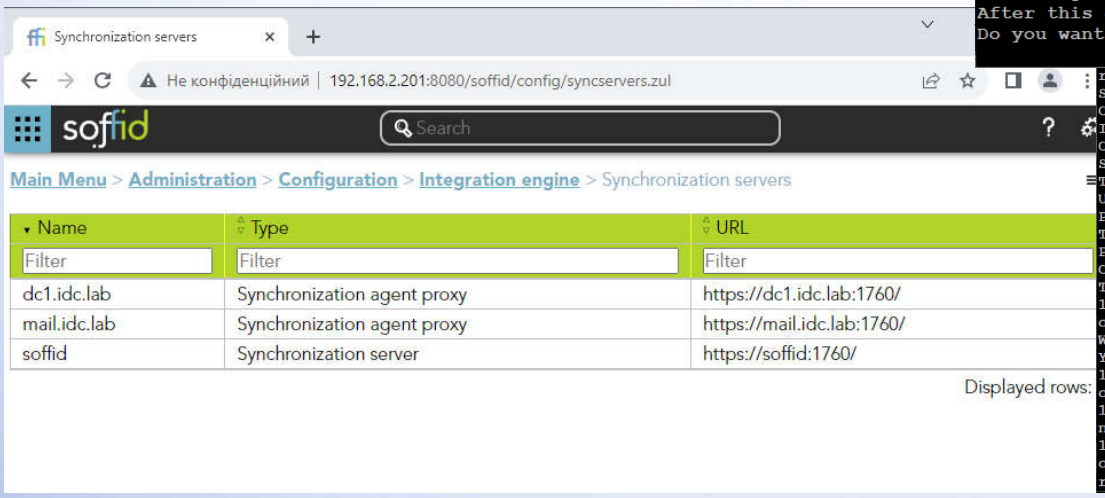


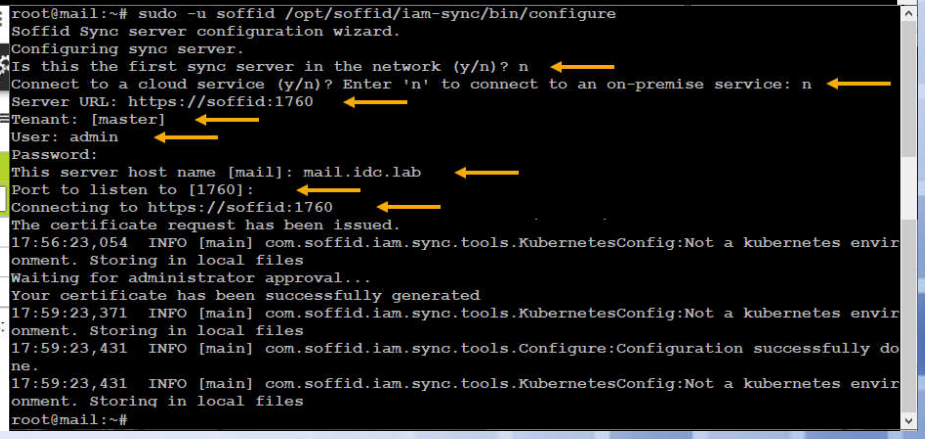
Підключення поштового сервера Zimbra до Soffid

Крок 1. Встановлення Soffid Sync Server на сервер Zimbra

1. Встановлення Java JDK
2. Оновлення файлу hosts (опціонально)
3. Встановлення та налаштування Soffid Sync server



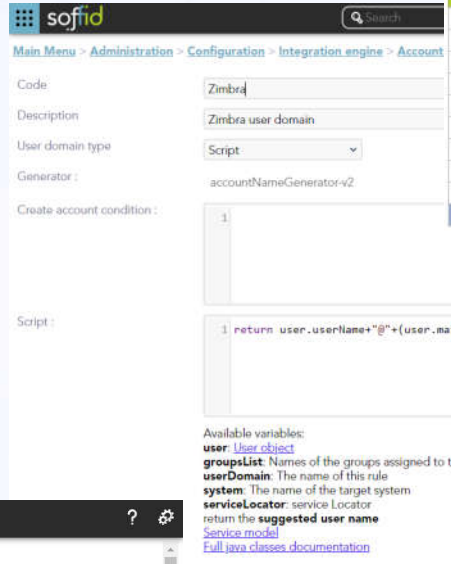


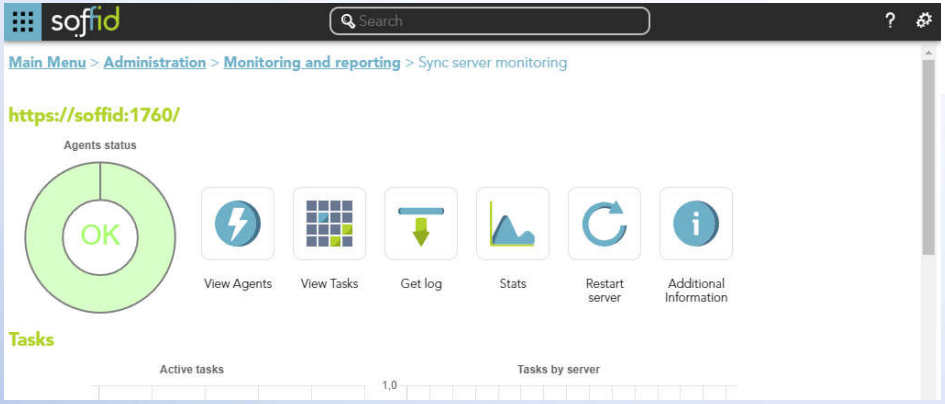


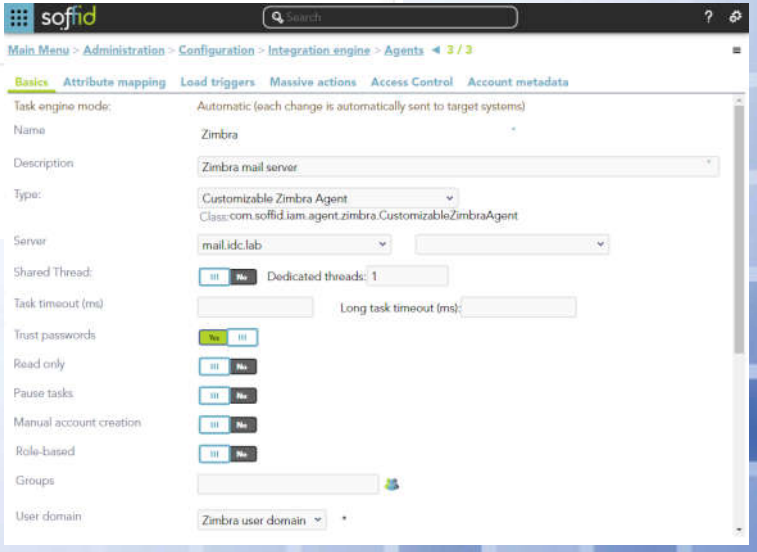
Підключення поштового сервера Zimbra до Soffid

Крок 2. Встановлення та налаштування конектора для Zimbra

1. Встановлення плагіна для Zimbra
2. Оновлення файлу hosts на сервері (опціонально)
3. Додавання Zimbra user domain
4. Додавання агента Zimbra
5. Налаштування агента Zimbra

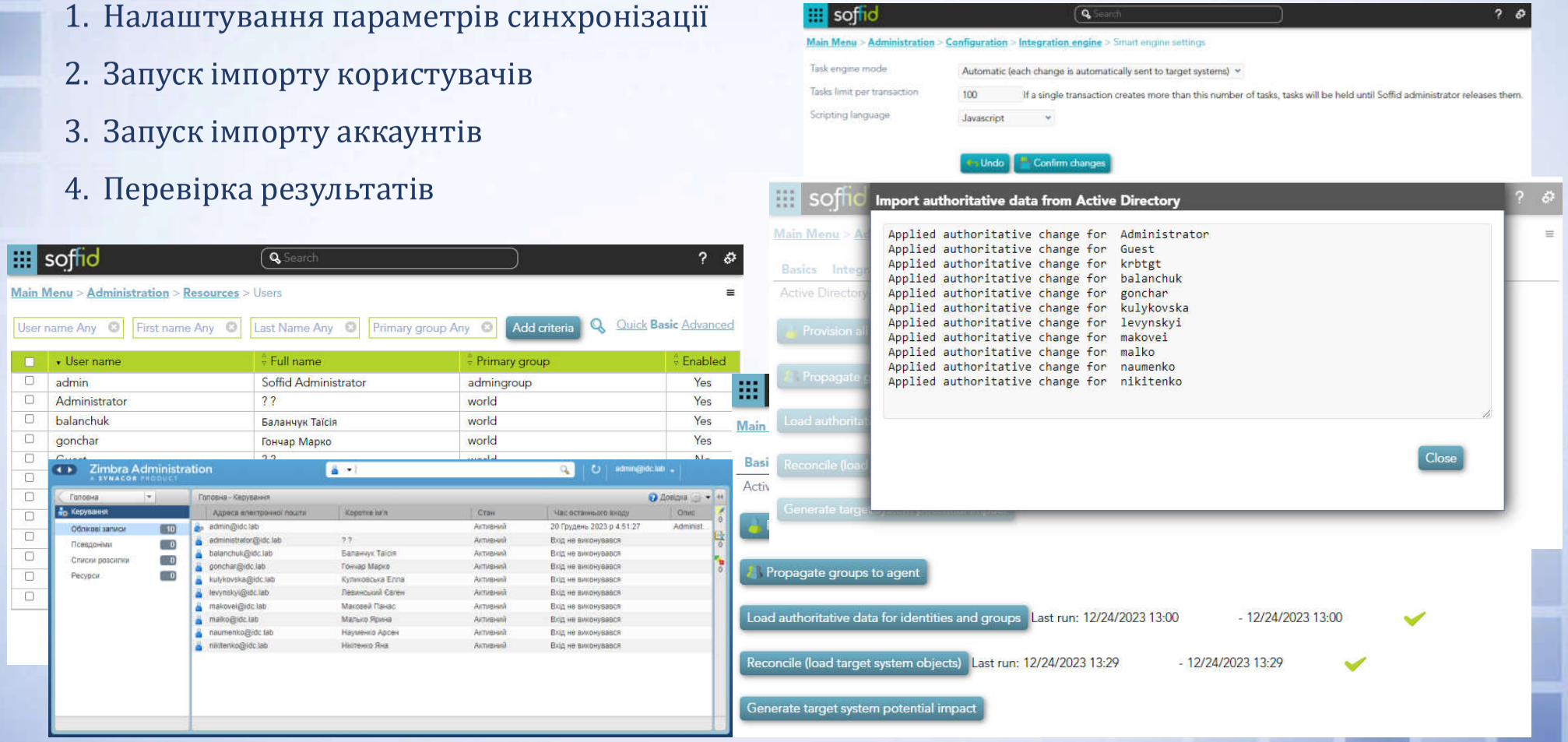






Імпорт користувачів з контролера домену в Soffid

1. Налаштування параметрів синхронізації
2. Запуск імпорту користувачів
3. Запуск імпорту аккаунтів
4. Перевірка результатів



Висновки

Впровадження IAM системи допоможе прискорити надання доступу до ресурсів підприємства новим співробітникам, підвищить безпеку наявних інформаційних систем, спростить співробітникам процедуру входу до тієї чи іншої системи перед початком роботи з ними.

Незважаючи на складнощі, пов'язані з впровадженням IAM систем, та що процес впровадження може зайняти тривалий час, плюси від отриманого результату безумовно компенсують усі ті ресурси, що знадобяться на етапі впровадження.

Апробація результатів дослідження

1. Бакликов М.І. «Ефективність застосування ІАМ системи на підприємстві». Тези доповіді на Всеукраїнської науково-технічної конференції «Сучасний стан та перспективи розвитку ІОТ». – Київ, 7 квітня 2023 р.

Дякую за увагу!