ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ GLUU»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Маницький В.Є.
(прізвище та ініціали)
Керівник Гахов С.О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ - 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ……. 9

ВСТУП ……..…… 10

1 **АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ** …...……..……. 13

1.1 Аналіз проблеми керування користувачами в інформаційній системі організації …… 13
1.2 Роль, структура та функції технологій управління користувачами, їх доступом та ідентифікацією. Основні поняття. 19
1.3 Аналіз існуючих рішень для управління ідентифікацією та доступом користувачів до інформаційної системи організації…. 25

2 **ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ GLUU**…… 33

2.1 Призначення, можливості та функції рішення Gluu Identity and Access Management ……..…… 33
2.2 Компоненти та архітектура Gluu Identity and Access Management……..... 39
2.3 Можливості щодо адміністрування Gluu Identity and Access Management…… 47

3 **ПОРЯДОК ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ GLUU**…… 56

3.1 Порядок розгортання рішення Gluu Identity and Access Management …… 56
3.2 Інтеграція LDAP в Gluu з Fortigate NGFW ……..…… 61
3.3 Загальні рекомендації щодо застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи організації …… 71

ВИСНОВКИ ……. 75

ПЕРЕЛІК ПОСИЛАНЬ 77

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 79

ВСТУП

Актуальність використання технологій управління ідентифікацією та доступом користувачів. Централізована авторизація користувачів, керування їх доступами використовується майже у всіх компаніях. Це пов’язано як з безпекою так і зі зручністю.

Як простий приклад: працівник звільнився або був звільнений, в нього був свій акаунт для VPN, пошти, RDP і внутрішніх сервісів. Після звільнення ці доступи необхідно видалити, щоб колишній співробітник не мав змоги продовжувати користуватись внутрішніми ресурсами компанії. Щоб адміністратор не заходив на кожен сервер і вручну не видаляв користувача, витрачаючи свій час і ризикуючи пропустити щось через звичайний людський фактор, існують рішення для керування ідентифікацією та доступом, звідки і ведеться керування користувачами.

Також важливо, щоб працівники мали відповідні рівні доступів всередині інформаційної системи організації. За керування цими доступами як раз і відповідають сервіси, що будуть описані в даній роботі. Адміністратор може створити гру-пи користувачів і надати права одразу до групи. Тобто, існує дві групи, перша - високий рівень доступу, друга - низький. Для більш зручного і безпечного конт-ролю рівнів доступів користувачів, адміністратор просто додає їх у відповідні гру-пи, не маючи необхідності налаштовувати права для кожного користувача окремо.

З огляду на ці питання, стає зрозуміло, що проблема управління ідентифікацією та доступом користувачів буде залишатись актуальною завжди. Саме тому з’являються нові сервіси для розв’язування цих питань. Покращується зручність використання сервісу, гнучкість налаштувань та можливості інтеграції з іншими продуктами. Існують як комерційні, так і Open-Source варіанти, і в наш час актив-ного розвитку, безкоштовні або умовно безкоштовні варіанти з відкритим кодом, намагаються нічім не поступатись у функціоналі платним проектам. При

виборі сервісу, що буде відповідати за управління ідентифікацією та доступом користувачів в компанії, на Open-Source продукти обов'язково варто звернути увагу.

Прикладом такого продукту може бути Gluu Identity and Access Management. Він підтримує найпоширеніші протоколи: LDAP, RADIUS, SAML, тощо. Простий в установці і налаштуванні. Має досить зручний GUI (graphical user interface) для створення користувачів, груп, моніторингу подій та невдалих спроб входу.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження щодо технології управління ідентифікацією та доступом користувачів до інформаційної системи організації на базі рішення Gluu.

Об'єкт дослідження - процес забезпечення управління ідентифікацією та доступом користувачів до інформаційної системи організації на базі рішення Gluu

Предмет дослідження - технологія управління ідентифікацією та доступом користувачів до інформаційної системи організації

Мета роботи - розробити порядок застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи організації та рекомендації щодо його реалізації.

Наукові завдання:

дослідити сутність проблеми управління ідентифікацією та доступом користувачів до інформаційної системи організації;

встановити сутність завдання управління ідентифікацією та доступом користувачів до інформаційної системи організації;

проаналізувати існуючі технології управління ідентифікацією та доступом користувачів до інформаційної системи організації;

проаналізувати методи та засоби управління ідентифікацією та доступом користувачів до інформаційної системи організації;

розкрити порядок реалізації технології управління ідентифікацією та доступом користувачів до інформаційної системи організації;

Методи дослідження - опрацювання літератури за даною темою, аналіз

експлуатаційної документації, міжнародних стандартів, їх порівняння та проведення експерименту.

Практичне значення одержаних результатів: запропоновано порядок застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи організації на базі рішення Gluu, а також розроблено рекомендації фахівцям з кібербезпеки щодо застосування технологій управління ідентифікацією та доступом користувачів.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на Всеукраїнській науково-технічній конференції «Актуальні проблеми кібербезпеки», Навчально-науковий інститут захисту інформації, 27 жовтня 2022 р., 154-156 стр.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Аналіз проблеми керування користувачами в інформаційній системі організації

Питання проблеми керування користувачами, їх доступами не втрачає свою актуальність і навряд колись втратить. Чим більше в системі користувачів і об’єктів до яких вони мають/не мають отримувати доступ, тим більше задач постає перед адміністраторами і фахівцями з кібербезпеки. Адже важливі аспекти, це не лише зручне керування, а й безпека. Тут ці два пункти дуже тісно пов’язані, адже при налаштуванні системи керування користувачами, зручність може як бути додатковим плюсом з боку безпеки так і мінусом.

Якщо взяти в загальному визначенні централізоване керування користувачами, воно має на увазі наявність серверу або серверів, що зберігають дані користувачів для входу в систему. Користувач заходить в додаток, він відправляє запит на центральний сервер з даними входу, і якщо сервер знаходить ці дані в своїй базі, надається доступ користувачу. Приблизно так виглядає схема при використанні LDAP (рис. 1.1).

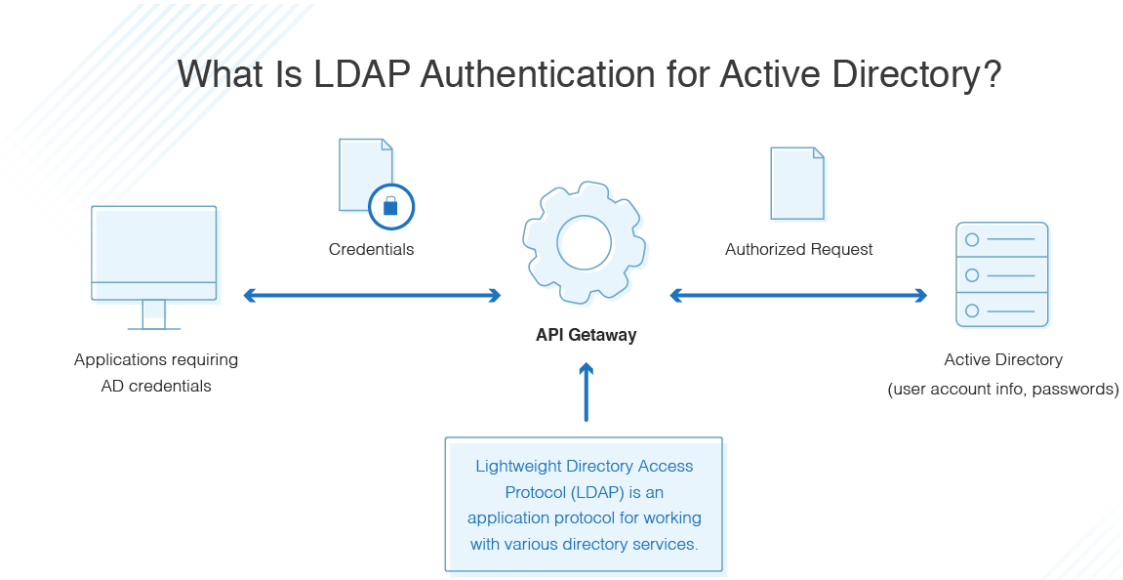


Рис. 1.1. Приклад авторизації користувача на основі LDAP серверу.

Інший популярний протокол RADIUS має схожу схему при авторизації до мережевого девайсу(рис. 1.2).

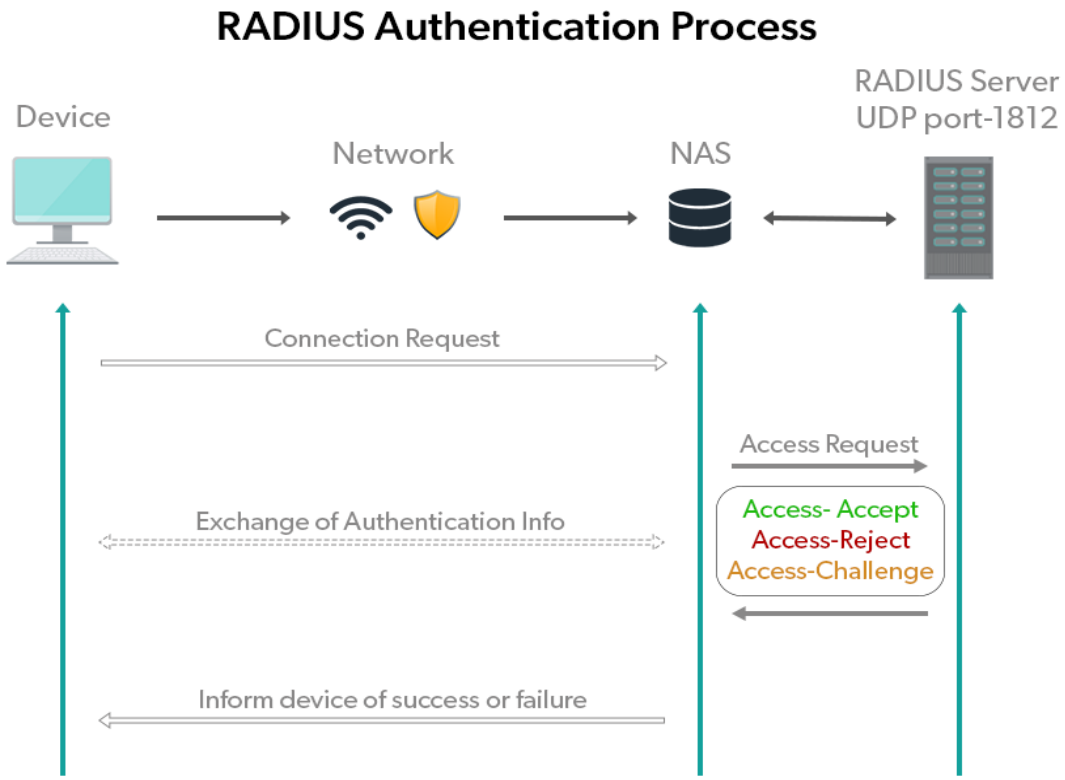


Рис. 1.2. Приклад авторизації користувача на основі RADIUS серверу.

Основна перевага - зручність в управлінні. Як було загадано раніше, якщо необхідно змінити якісь дані користувача, його рівні доступу, пароль тощо, адміністратору достатньо зробити це на одному сервері де зберігається база даних. А всі інші, сервіси, додатки, сервери, ПК, які під'єднані мережевим протоколом до центрального сервера автоматично оновлять налаштування. Це дуже зручно, і виключає людський фактор, у вигляді адміністратора який міг забути прибрати користувача з якогось сервера, чи видати йому некоректні права доступу до якогось додатку. Також, для зв'язку між клієнтом та сервером авторизації слід використовуються захищенні протоколи, що майже унеможливлюють спробу зловмисника розшифрувати дані навіть при успішному перехопленні.

Але з'являється логічне питання. Якщо всі дані зберігаються на одному сервері, чи значить, що якщо зловмисник отримає доступ до цього самого серверу він отримає доступ до системи? Взагалі - так. Саме тому домені контролери, сервера авторизації потребують додаткового захисту у вигляді Firewall, IDS, IPS, обмеження доступу тощо.

Із зручністю і ефективністю все просто - керування відбувається на одному сервері, а далі сервіси і додатки отримують ці дані. Але що з безпекою, окрім раніше згаданих функцій Firewall, які саме протоколи допомагають захисти дані при обміні? Мінімально, що має налаштувати адміністратор, для підвищення безпеки обмінну даними між клієнтом і сервером це шифрування трафіку, у вигляді SSL або TLS, як у випаду з LDAP. Такий протокол називають LDAPS. LDAPS не є принципово іншим протоколом: це той самий старий LDAP, тільки упакований інакше. LDAPS дозволяє шифрувати дані LDAP (включно з обліковими даними користувача) під час передачі під час будь-якого зв'язку з сервером LDAP (як прив'язка каталогу), таким чином захищаючи від крадіжки облікових даних.

Тобто дві проблеми які мають вирішувати технології керування користувачами в інформаційній системі організації - це зручність і безпека. І ці два питання мають стояти поруч. Адже якщо десь нехтувати безпекою заради зручності, під загрозу потрапляє майже вся ІС організації. Як приклад,

адміністратор налаштував обмін між клієнтом і сервером без протоколів шифрування, для більш швидкого налаштування. Або встановив простий пароль на сервер авторизації, щоб простіше на нього потрапляти. Коли дані входу користувачів будуть скомпрометовані, лише питання часу. Не варто і забувати про парольну політику для користувачів. Адже вони також досить часто можуть використовувати прості однакові паролі. Близько 81% витоку даних компанії відбувається саме через слабкі паролі, які було успішно зламано зловмисником (рис.1.3).

Рис. 1.3. Статистика зламу паролів

Якщо встановити контроль надійності паролів для кожного користувача, цей відсоток суттєво покращиться. Але для більш надійного захисту рекомендується також використовувати 2х факторну аутентифікацію. В 2020му році, компанія Microsoft надала статистику, за якою 99.9% парольних атак було заблоковано за допомогою багатофакторної аутентифікації при її наявності. Тому про неї трохи детальніше. Багатофакторна автентифікація (MFA) - це метод автентифікації, який вимагає від користувача надати два або більше факторів перевірки, щоб отримати доступ до ресурсу, наприклад програми, онлайн-облікового запису або VPN. MFA є основним компонентом надійної політики керування ідентифікацією та доступом. Замість простого запиту імені користувача та пароля MFA вимагає один або кілька

додаткових факторів перевірки, що зменшує ймовірність успішної кібератаки(рис.1.4).

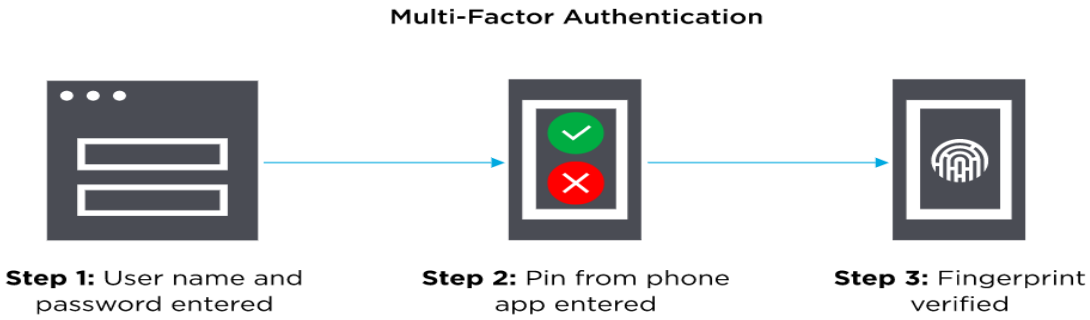


Рис. 1.4 Мультифакторна автентифікація користувача в системі

MFA працює, вимагаючи додаткової перевірочної інформації (факторів). Одним із найпоширеніших факторів MFA, з якими стикаються користувачі, є одноразові паролі (OTP) . Одноразові паролі - це 4-8-значні коди, які ви часто отримуєте електронною поштою, SMS або за допомогою мобільного додатка. За допомогою OTP новий код генерується періодично або кожного разу, коли надсилається запит на автентифікацію. Код генерується на основі початкового значення, яке призначається користувачеві під час першої реєстрації, а також іншого фактора, який може бути просто лічильником, що збільшується, або значенням часу.

Ну і звісно ж проблематика контролю доступу користувачів. Контроль доступу забезпечує дотримання політики таким чином, щоб користувачі не могли діяти поза межами призначених дозволів. Збої, як правило, призводять до неавторизованого розкриття інформації, модифікації чи знищення всіх даних або виконання бізнес-функцій за межами обмежень користувача. Це дуже поширена проблема. В рейтингу OWASP TOP 10 - Broken Access Control піднявся з 5ої сходинки на першу, якщо порівнювати 2017 і 2021 рік (рис.1.5).

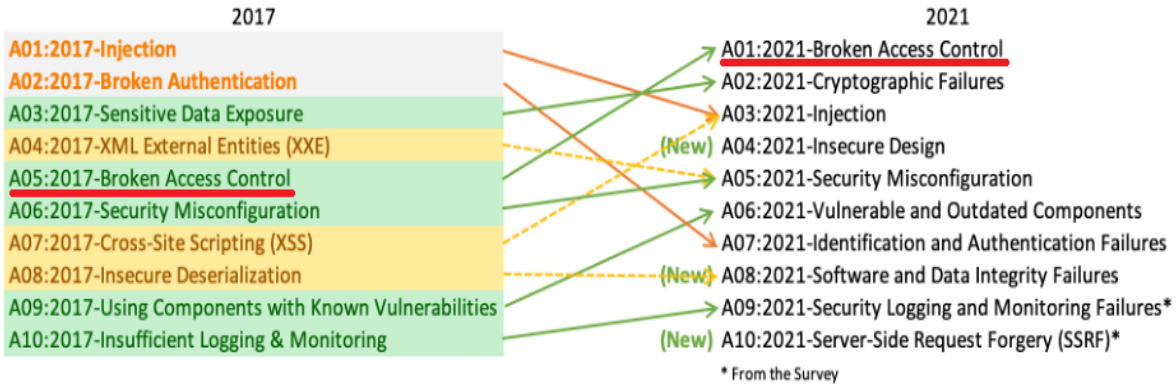


Рис.1.5. Broken Access Control в 2017 та 2022

Тепер, на рахунок того, якщо нехтувати зручністю та швидкістю, з якою можуть вноситись зміни в базу користувачів, то це може вплинути на продуктивність виконання задач організацією. Уявімо, що було вирішено, відмовитись від централізованої авторизації в компанії. В компанію прийшло 10 нових людей. Можна тільки уявити, скільки часу потрібно буде витратити адміністратору, щоб додати цих користувачів на всі сервери і сервіси вручну. І весь цей час вони не можуть виконувати свої обов'язки. А адміністратор витратить купу часу, який необхідно було б витратити на більш критичні питання. І небезпека людського фактору, адже тяжко проконтролювати і запам'ятати всі доступи в ручному режимі. А маючи сервіс для керування користувачами в організації, який вже інтегрований з іншими внутрішніми сервісами, йому буде достатньо додати і налаштувати цих користувачів лише на «центральний» сервер, а всі інші отримають дані за допомогою, як приклад, раніше згаданого LDAP-протоколу.

Тобто проблеми і їх вирішення за допомогою технологій управління ідентифікацією та доступом користувачів досить очевидні, але потребують детального вивчення перед їх впровадженням в саму систему. Потрібно розставити правильно пріоритети, визначити найкритичніші фактори для організації і на основі цього обирати продукт, розробляти політики доступу користувачів до системи. Звісно, стандартний набір правил і рекомендації у всіх випадках буде приблизно однаковий, але в залежності від потреб та напрямку організації і будуть виникати певні відмінності.

1.2. Роль, структура та функції технології управління користувачами, їх доступом та ідентифікацією. Основні поняття.

У сучасному світі, коли все стрімко змінюється, росте, інформаційні технології стали невід'ємною частиною нашого життя, не могла не виникнути потреба у технологіях, які будуть призначення для управління користувачами в системі певного бізнесу, компанії, організації. Адже будь-яка компанія має різні дані, з різними рівнями доступу, різні групи працівників, що потребують доступи до цих даних. Як згадувалось раніше, це все може стрімко змінюватись. Можуть змінитись працівники, або їх рівень доступу, тому технології контролю доступу та керування їх ідентифікацією у інформаційній системи організації - одне з найважливіших питань при побудові цієї самої системи. Далі - детальніше про всі ці поняття та їх важливість.

Ідентифікація - процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора, наприклад, логіну) або іншої інформації про нього, яка сприймається системою. Звісно ж існує декілька типів ідентифікації.

1. Парольна ідентифікація. Довгий час була основним і ледь не єдиним типом ідентифікації. Вона має просу реалізацію, та ще простіше використання. Не складно здогадатись, що її сутність полягає у використанні паролів. При реєстрації в системі користувач отримує або створює унікальну пару типу логін-пароль. Ця пара потім використовується при вході у систему. Система перевіряє, що вказаний унікальний логін відповідає паролю, що зберігається в її базі і надає користувачу доступ. Головний недолік - прості паролі. Якщо користувач використовує простий пароль, є висока вірогідність його вгадати або підібрати.

2. Апаратна ідентифікація. Тут користувач визначається по якомусь предмету, що перебуває в його власності і може бути використаний для розпізнавання в системі. Це може бути електронний ключ, токен, магнітна карта, спеціальна карта доступу, яка підключається напряму до ПК. Тут існує два недоліки. Перший - користувач може втратити свою карту або її можуть викрасти

для отримання несанкціонованого доступу. Для цього не треба особливих знань в сфері кібербезпеки, достатнього звичайної грубої сили. А також висока ціна реалізації цього типу ідентифікації.

3. Біометрична ідентифікація. Біометрія - це ідентифікація людини по унікальним, властивим тільки їй біологічним ознакам. Тобто користувач в системі розпізнається за допомогою відбитку пальця, сканеру очей. Цей вид ідентифікації теж потребує великих фінансових витрат, але має досить високий рівень надійності. Адже неймовірно мала ймовірність знайти людину з ідентичним відбитком пальця.

Можна додати, що для підвищення рівня безпеки, ці типи ідентифікації можна використовувати в комплексі. Наприклад встановлення додаткового пароля на використання електронної карти при підключенні до ПК. В такому випадку, навіть якщо зловмисник отримає доступ до карти, він все ще не зможе ідентифікувати себе в системі як користувач і отримати доступ до даних. Це називається багатофакторна автентифікація.

Щодо управління доступом вже ідентифікованих користувачів. Цей процес можна описати як авторизація. Авторизація - це те, що користувачу дозволяється робити після входу. Це надання і перевірка прав на вчинення будь-яких дій в системі. У багатокористувацьких комп’ютерних системах системний адміністратор визначає для системи, яким користувачам дозволено доступ до системи та які привілеї використання (наприклад, доступ до яких каталогів файлів, години доступу, обсяг виділеного місця для зберігання тощо). Якщо припустити, що хтось увійшов до комп’ютерної операційної системи чи програми , система чи програма може захотіти визначити, які ресурси можна надати користувачеві під час цього сеансу. Таким чином, авторизація іноді розглядається як попереднє налаштування дозволів системним адміністратором і фактична перевірка значень дозволів, які були встановлені, коли користувач отримує доступ. Розглянемо на прикладі операційної системи Linux, принцип роботи і налаштування прав доступу до файлів, каталогів тощо. В цій системі права доступу дозволяють надавати доступ до каталогів і файлів на основі облікових записів користувачів або груп

користувачів. Кожен об'єкт файлової системи зберігає таку інформацію:

Тип файлу;

Власника файлу та його групу;

потрійні права доступу для власника(того хто створив файл), його групи, та інших - користувачів, що не належать до групи власника - r (читання), w (запис) і x (запуск);

При роботі з об'єктами файлової системи застосовуються наступні правила:

Новостворений об'єкт належить користувачу, який його створив, і основній групі цього користувача;

Новостворений об'єкт одразу має права доступу за замовчуванням, призначені командою umask;

Права доступу до файлу, каталогу може змінювати власник або адміністратор серверу (root);

Власника може змінювати тільки root. Є виключення залежно від налаштування;

Групу може змінювати тільки root. Є виключення залежно від налаштування;

Права записуються за допомогою вісімкової системи числення або символьного запису. Отримане значення є сумою значень кожного дозволу у кожній трійці. Тут читання - r - 4, запис - w - 2, виконання(запуск) - x - 1. Тобто, якщо нам треба встановити, наприклад, повний доступ на папку для власника, але тільки на читання і виконання для групи і інших користувачів - запис буде мати вигляд - 755. 7 - (1+2+4) 5 - (1+4) 5 - (1+4).

Це простий приклад стандартних налаштувань прав доступу в Linux системах і їх принципів роботи.

У Windows системах розглянемо приклад - Group Policy Object (GPO) в Active Directory.

Спочатку, що таке Active Directory. LDAP-сумісна реалізація інтелектуальної служби каталогів корпорації Microsoft. Включає в себе базу даних і набір служб, які з’єднують користувачів із мережевими ресурсами, необхідними для виконання роботи. База даних (або каталог) містить критично важливу інформацію про ваше середовище, включно з тим, які користувачі та комп’ютери існують і хто має право

робити що. Наприклад, база даних може містити 100 облікових записів користувачів із такими деталями, як посада, номер телефону та пароль кожної особи. Для керування можуть використовуватись групові політики, вони ж Group Policy(GP). Перш за все, що таке групова політика? Групова політика - це функція Windows, яка забезпечує широкий спектр розширених налаштувань, які адміністратори мережі можуть використовувати для керування робочим середовищем користувачів і облікових записів комп'ютерів у Active Directory. По суті, це централізоване місце для адміністраторів, де вони можуть керувати та налаштовувати операційні системи, програми та параметри користувачів. Правильне використання групових політик може дозволити вам підвищити безпеку комп'ютерів користувачів і допомогти захистити як від внутрішніх загроз, так і від зовнішніх атак.

Об'єкт групової політики (GPO) - це група налаштувань, створених за допомогою редактора групової політики Microsoft Management Console (MMC). Об'єкти групової політики можуть бути пов'язані з одним або кількома контейнерами Active Directory, включаючи сайти, домени або організаційні підрозділи (OU). MMC дозволяє користувачам створювати GPO, які визначають політики на основі реєстру, параметри безпеки, встановлення програмного забезпечення та багато іншого. Тобто адміністратор налаштовує певну політику на сервері Active Directory, і ця політка автоматично застосовується до ПК, серверів, що приєднані до домену (рис1.6).

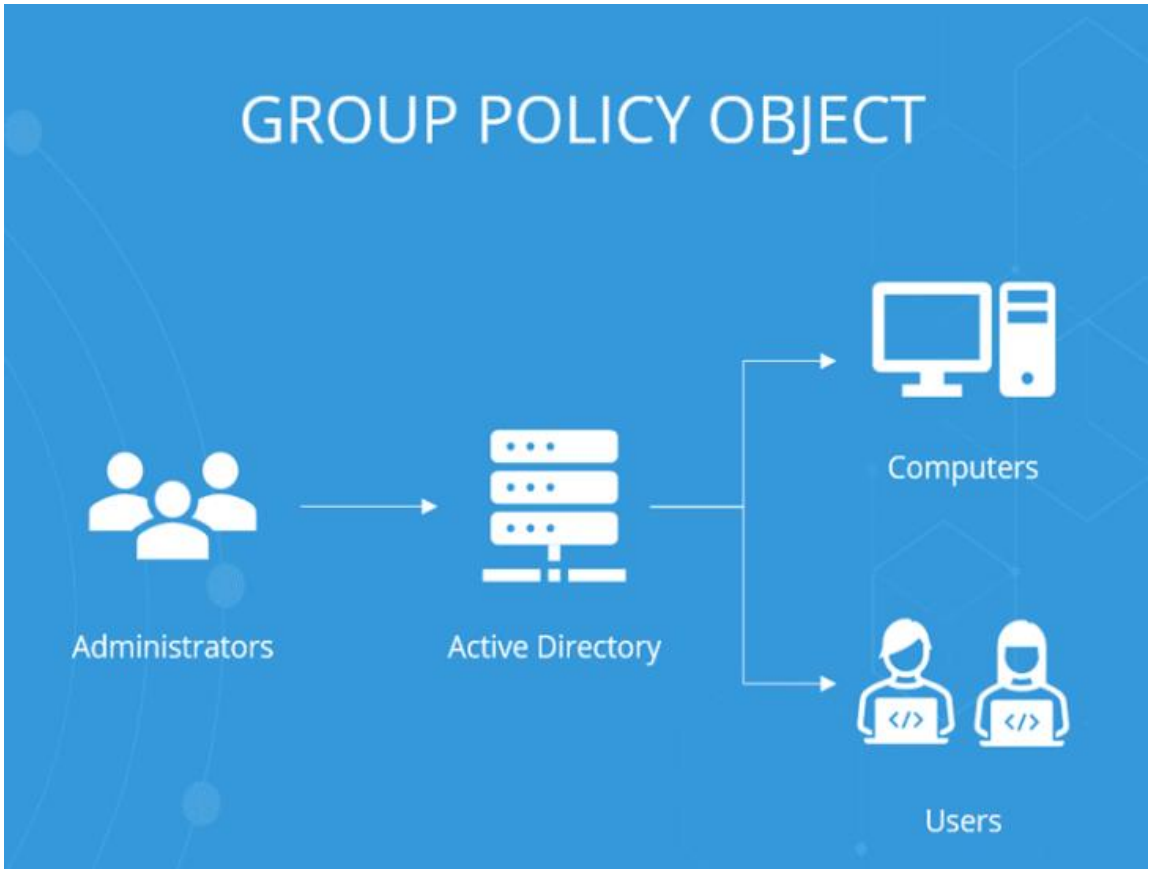


Рис.1.6. Застосування політики у AD.

Типи GPO

Є три типи GPO: локальні, нелокальні та початкові.

Об’єкти локальної групової політики. Об’єкт локальної групової політики стосується набору параметрів групової політики, які застосовуються лише до локального комп’ютера та користувачів, які входять до цього комп’ютера. Локальні GPO використовуються, коли параметри політики потрібно застосувати до одного комп’ютера або користувача Windows. Локальні GPO існують за замовчуванням на всіх комп’ютерах Windows.

Нелокальні об’єкти групової політики. Нелокальний об’єкт групової політики використовується, коли параметри політики мають застосовуватися до одного або кількох комп’ютерів або користувачів Windows. Нелокальні об’єкти групової політики застосовуються до комп’ютерів або користувачів Windows після того, як їх пов’язано з об’єктами Active Directory, такими як сайти, домени чи організаційні підрозділи.

Початкові об’єкти групової політики. Початкові об’єкти групової політики, представлені в Windows Server 2008, є шаблонами для параметрів групової політики. Ці об’єкти дозволяють адміністратору створювати та мати попередньо налаштовану групу налаштувань, які представляють базову лінію для будь-якої майбутньої політики, яка буде створена.

Існують деякі параметри групової політики, які можуть допомогти захистити мережу компанії. Наприклад, за допомогою групової політики організація може запускати сценарії, забороняти користувачам доступ до певних ресурсів і виконувати прості завдання, такі як примусове відкриття певної домашньої сторінки для кожного користувача мережі.

Деякі з цих заходів безпеки включають:

Обмеження доступу до панелі керування - за допомогою панелі керування компанія може контролювати всі аспекти комп’ютера. Обмеження доступу до комп’ютера дозволяє організаціям захищати дані та інші ресурси.

Вимкнення командного рядка - компанія може використовувати командні рядки для запуску команд, які надають високорівневий доступ користувачам і обходять інші системні обмеження. Ось чому доцільно вимкнути командний рядок, щоб забезпечити безпеку системних ресурсів. Якщо користувач спробує відкрити командне вікно після вимкнення командного рядка, система відобразить повідомлення про те, що деякі параметри перешкоджають цьому.

Запобігання встановленню програмного забезпечення - якщо користувачам дозволено встановлювати програмне забезпечення, вони можуть інсталювати небажані програми або зловмисне програмне забезпечення, яке може скомпрометувати систему компанії. Таким чином, краще запобігти встановленню програмного забезпечення за допомогою групової політики.

Як згадувалось раніше, при роботі з сервісами, що надають централізовану можливість управління ідентифікацією та доступом користувачів у всій системі використовуються мережеві протоколи. Один з найпоширеніших - це LDAP. Відносно простий протокол використовує TCP/IP і дозволяє проводити операції аутентифікації (bind), пошуку (search) та порівняння (compare), а також операції

додавання, зміни або видалення записів. Зазвичай LDAP використовується як центральне місце для автентифікації, тобто він зберігає імена користувачів і паролі. Потім LDAP можна використовувати в різних програмах або службах для перевірки користувачів за допомогою плагіна, що з'єднає програму з базою LDAP. Наприклад, LDAP можна використовувати для перевірки імен користувачів і паролів на серверах Docker , Jenkins , Kubernetes , Open VPN і Linux Samba. Єдиний вхід LDAP також може використовуватися системними адміністраторами для контролю доступу до бази даних LDAP.

Також поширеним є мережевий протокол Remote Authentication Dial-In User Service (RADIUS). Він складається з клієнта та сервера. Клієнт RADIUS (або сервер доступу до мережі) - це мережевий пристрій (наприклад, концентратор VPN, маршрутизатор, комутатор), який використовується для автентифікації користувачів. Сервер RADIUS - це фоновий процес, який виконується на сервері UNIX або Windows. Це дозволяє підтримувати профілі користувачів у центральній базі даних. Отже, якщо у вас є сервер RADIUS, ви можете контролювати, хто може підключатися до вашої мережі. Коли користувач намагається підключитися до клієнта RADIUS, клієнт надсилає запити на сервер RADIUS. Користувач може підключитися до клієнта RADIUS, лише якщо сервер RADIUS автентифікує та авторизує користувача.

Тобто для зручного і надійного керування користувачами, їх доступами в системі, компанії використовують сервіси які виконують ці дії централізовано.

1.3. Аналіз існуючих рішень для управління ідентифікацією та доступом користувачів до інформаційної системи організації

Враховуючи попит на сервіси для управління користувачами, існує досить багато різних продуктів, як Open-source так і ні. Один з найвідоміших продуктів - це Azure Active Directory від Microsoft. Також уваги заслуговують і open-source продукти, такі як 389 Directory Server і FreeIPA. Варто проаналізувати кожен з них, для

розуміння їх переваг або недоліків. Якщо беремо продукт з відкритим кодом, то його головна перевага - він безкоштовний, або умовно безкоштовний. А головний недолік - відсутність постійної підтримки і можлива низька інтенсивність випуску оновлень. У випадку з комерційним продуктом як Azure Active Directory - ситуація повністю протилежна. Тому залежно від пріоритетів і можливостей компанії і обирається продукт. Спочатку розглянемо Azure Active Directory.

Azure Active Directory (Azure AD) - це хмарна служба керування ідентифікацією та доступом. Наступна гілка еволюції Active Directory, що має в собі розширені хмарні можливості. Ця служба допомагає вашим співробітникам отримувати доступ до зовнішніх ресурсів, таких як Microsoft 365, портал Azure і тисячі інших програм SaaS. Azure Active Directory також допомагає їм отримувати доступ до внутрішніх ресурсів, таких як програми у вашій корпоративній інтранет-мережі, а також будь-які хмарні програми, розроблені для вашої організації.

Azure AD призначений для:

IT-адміністраторів: IT-адміністратор використовує Azure AD, щоб контролювати доступ до своїх програм і ресурсів програм відповідно до вимог вашого бізнесу. Наприклад, ви можете використовувати Azure AD, щоб вимагати багатофакторну автентифікацію під час доступу до важливих організаційних ресурсів. Ви також можете використовувати Azure AD для автоматизації ініціалізації користувачів між існуючою Windows Server AD і хмарними програмами, включаючи Microsoft 365. Нарешті, Azure AD надає вам потужні інструменти, які автоматично допомагають захистити ідентифікаційні дані та облікові дані користувачів і відповідати вашим вимогам щодо керування доступом.

Розробники додатків : як розробник додатків, ви можете використовувати Azure AD як підхід на основі стандартів для додавання єдиного входу (SSO) до свого додатка, дозволяючи йому працювати з уже існуючими обліковими даними користувача. Azure AD також надає API, які можуть допомогти вам створювати персоналізовані програми, використовуючи існуючі організаційні дані.

Так як це здебільшого хмарний сервіс, він має свою схему використання

автентифікації додатків чи користувачів, що також підтримує поширений LDAP (рис. 1.7).

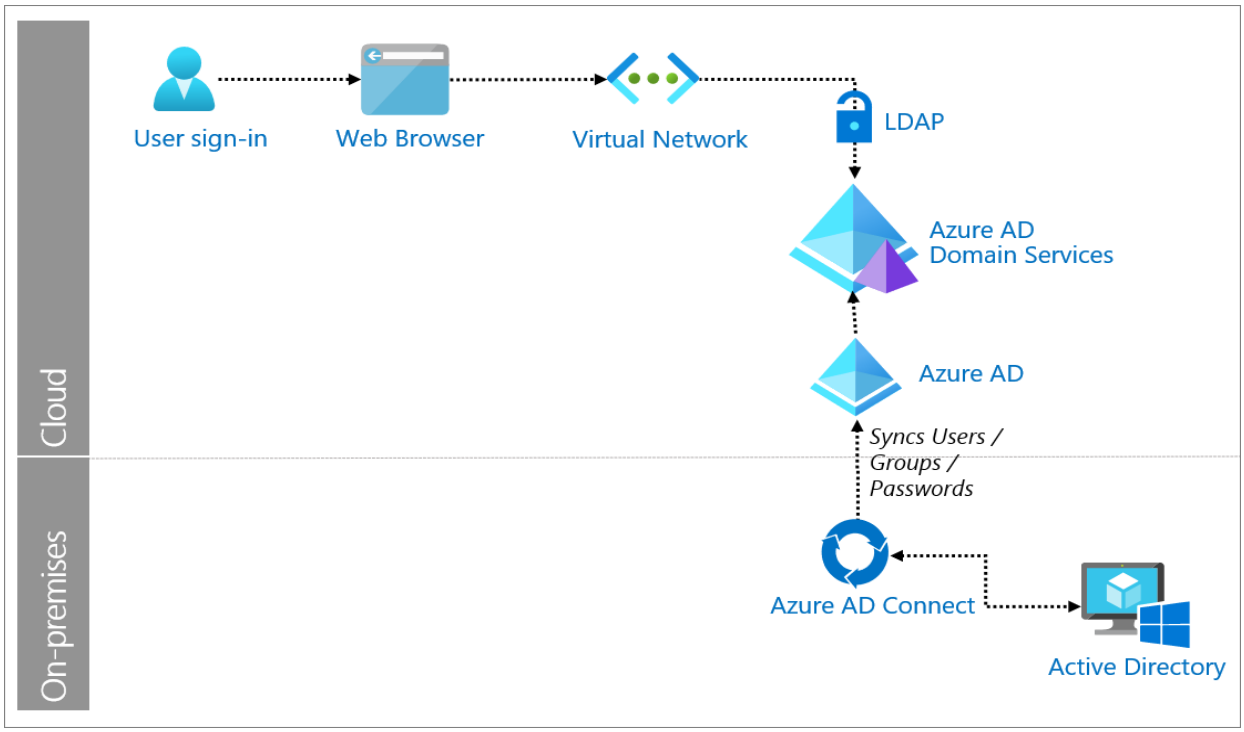


Рис. 1.7. Схема авторизації сервісів у Azure AD.

Компоненти системи:

Користувач : доступ до програм, що використовують LDAP, через браузер;

Веб-браузер: інтерфейс, з яким взаємодіє користувач для доступу до зовнішньої URL-адреси програми;

Віртуальна мережа : приватна мережа в Azure, через яку програма може використовувати служби LDAP;

Програми : програми або серверні робочі навантаження, які вимагають розгортання LDAP у віртуальній мережі в Azure;

Azure AD : синхронізує ідентифікаційну інформацію з локального каталогу організації через Azure AD Connect;

Служби домену Azure AD (AD DS) : виконує односторонню синхронізацію з Azure AD, щоб надати доступ до центрального набору користувачів, груп і облікових даних;

Azure AD Connect : інструмент для локальної синхронізації ідентифікаційної інформації з Microsoft Azure AD;

Active Directory : Служба каталогів, яка зберігає локальну ідентифікаційну інформацію, таку як інформація про користувача та обліковий запис , а також інформацію про безпеку, як-от паролі.

Azure AD має такі ціни на підписку: Azure Premium P1 - $6 **user/month**

Azure Premium P2 - $9 **user/month**.

Преміум P1

Преміум-версія Azure Active Directory, розроблена для розширення можливостей організацій із більш вимогливими потребами в ідентифікації та керуванні доступом, додає багатофункціональні можливості керування ідентифікацією корпоративного рівня та дозволяє гібридним користувачам безперешкодно отримувати доступ до локальних і хмарних можливостей.

Преміум P2

Azure Active Directory Premium P2 містить усі функції всіх інших версій Azure Active Directory, покращені розширеним захистом ідентичності та привілейованими можливостями керування ідентифікацією.

Продукт має широкий спектр функціоналу, для керування користувачами, їх доступами тощо. Але і ціна за послуги відповідна.

Наступний на черзі open-source продукт - 389 Directory Server.

Сервер каталогів рівня підприємства, що створюється спільнотою за спонсорської підтримки Red Hat. Базою для нього послужив Netscape Directory Server, що розробляється з 1996 року. Він отримав нове ім'я Fedora Directory Server після того, як права на нього в 2005 році придбала Red Hat. У 2009 році проект знову змінив назву на 389 Directory Server (389 - за номером порту служби LDAP). Причина проста: FDS нерозривно асоціювався з Fedora, що, на думку розробників, гальмувало розвиток, зокрема, інтеграцію в інші дистрибутиви. На основі 389DS Red Hat випустила комерційну версію Red Hat Directory Server (RHDS) із техпідтримкою 24/7. Можливості 389DS включають повну підтримку протоколу LDAPv3, SSL/TLS- та SASL-автентифікацію, синхронізацію даних (користувач, група, пароль) з Active Directory (за умови, що на КД Win2k3/2k8 встановлено компонент Windows Sync), розмежування доступу аж до окремих атрибутів (ім'я,

група, IP тощо). Як криптодвижок використовується бібліотека NSS від Mozilla Project. Конструктивно 389DS складається із сервера каталогів (Core Directory Server, CDS) та сервера адміністрування (Admin Server). Завдання останнього - управління всіма доступними CDS, для чого пропонується графічна консоль (389-console) та утиліти командного рядка. У Linux консоль встановлюється автоматично (написана Java). Для керування під Win2k3/2k8 на сайті проекту слід завантажити пакет Windows Console. Конструктивно 389DS складається із сервера каталогів (Core Directory Server, CDS) та сервера адміністрування (Admin Server). Завдання останнього - управління всіма доступними CDS, для чого пропонується графічна консоль (389-console) та утиліти командного рядка. У Linux консоль встановлюється автоматично (написана Java).

Сама консоль має «стандртний» вигляд, без зайвих вкладок та налаштування, що допомагає інтуїтивно розібратись з керуванням(рис. 1.8).

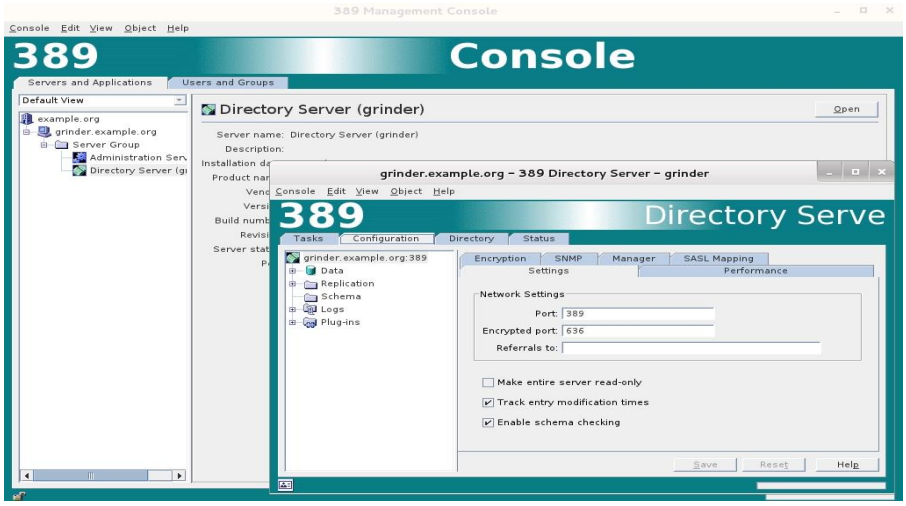


Рис. 1.8. Консоль керування 389 Directory Server

FreeIPA. Мета проекту FreeIPA (Free Identity, Policy and Audit) - створення для Linux-систем середовища, що є альтернативою Active Directory і дозволяє централізовано керувати аутентифікацією користувачів, встановлювати політики доступу та аудиту. Фактично FreeIPA - це симбіоз кількох опенсорсних проектів, таких як дистрибутив Fedora, 389DS, MIT Kerberos, NTP та BIND. На цьому проекті, що розвивається за фінансової підтримки Red Hat, заснований продукт

IPA, що використовується в комерційному дистрибутиві, який Red Hat представила громадськості влітку 2008 року. Вперше код FreeIPA з'явився у складі Fedora 9 (травень 2008-го), проте нормальну синхронізацію з Active Directory на той момент ще не було реалізовано. Спочатку клієнти могли підключатися вручну, але це було незручно. У жовтні 2009-го розпочалася робота над новою гілкою 2.0. Її фінальну версію було представлено наприкінці березня 2011-го. День, в який був анонсований реліз, запам'ятався багатьом користувачам Linux як Fedora 15 Test Day, присвячений саме тестуванню FreeIPA2. В даний час реалізовано:

Централізоване управління обліковими записами користувачів, груп, комп'ютерів та сервісів;

Керування доступом до додатків, встановлення політик паролів та налаштувань Kerberos, керування правилами SUDO;

Автентифікація Kerberos для користувачів та вузлів;

Host Based Access Control - управління та зберігання ролей у LDAP;

Служба керування сертифікатами (Dogtag Certificate Server).

Мережа, побудована із застосуванням FreeIPA, функціонально може складатися з трьох типів систем: одного або кількох серверів, клієнтських машин та комп'ютера адміністратора. Останній, по суті, є звичайним клієнтським десктопом з консольними утилітами для віддаленого управління FreeIPA(рис. 1.9.) (до речі, використовувати їх зовсім не обов'язково - цілком можна обійтися веб-інтерфейсом, який написаний на Java).

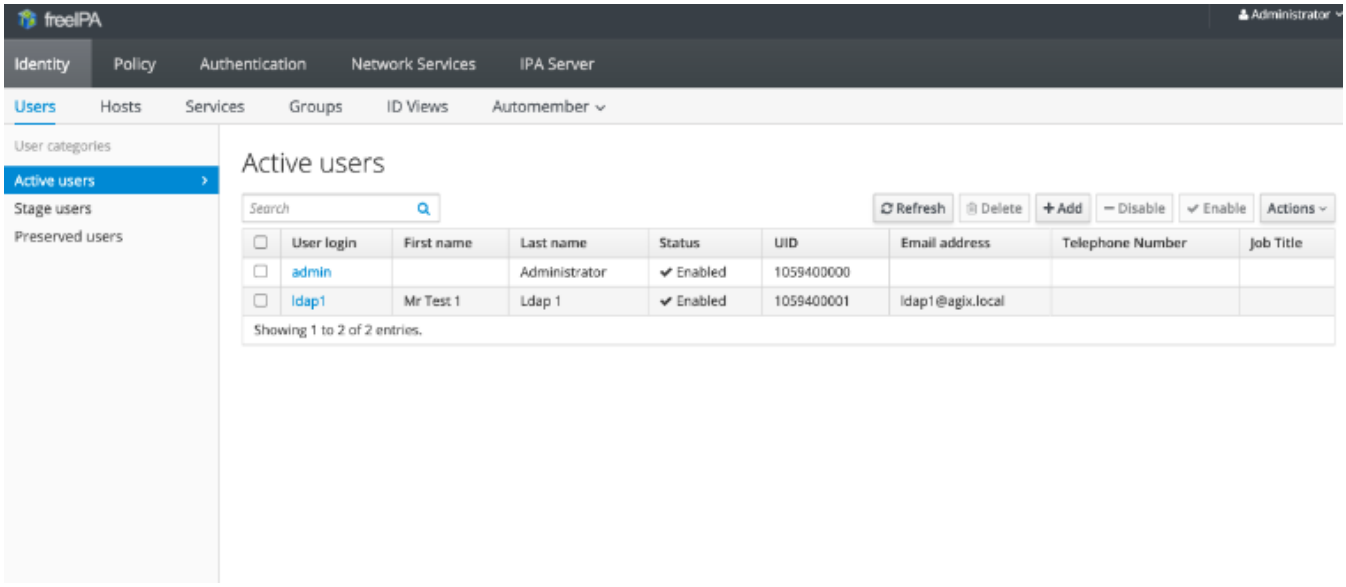


Рис. 1.9. Панель керування FreeIPA

Щоб знизити навантаження на канал, клієнт використовує локальний кеш (LDB і XML), отримуючи з нього налаштування навіть за відсутності доступу до сервера. На клієнтській системі встановлюється агент управління автентифікацією SSSD (System Security Services Daemon). Спеціальна програма (certmonger) спрощує створення сертифікатів та управління ними, автоматично генеруючи та отримуючи новий сертифікат після закінчення терміну дії старого. Опціонально можлива інтеграція з DNS-сервером на базі BIND (потрібний плагін LDAP BIND з динамічним оновленням через GSS-TSIG). Під час керування комп'ютерами та групами комп'ютерів повноваження підтверджуються за допомогою Kerberos keytab або сертифіката. Модульна архітектура серверної та клієнтської частини дозволяє без особливих проблем інтегрувати FreeIPA та будь-який продукт. Починаючи з версії 3.0.0, FreeIPA використовує Samba для інтеграції з Microsoft Active Directory за допомогою Cross Forest Trust. FreeIPA забезпечує підтримку комп’ютерів на базі Linux, Unix, Windows і Mac OS X. Зараз робота над проектом продовжується. Найновіша версія - 4.10.1 (3 листопада 2022).

Як видно, між цими продуктами дуже багато схожого, адже вони всі прагнуть вирішувати одні й ті самі проблеми, лише маючі певні відмінності у налаштуваннях і розмірі додаткового функіоналу, від чого і може залежити ціна.

З продуктів, що були наведені вище на данний момент один з

найпоширеніших є AD/Azure AD, через те - що в широкому загалі він один з перших увійшов на ринок і є продуктом IT-гіганту Microsoft. Він дуже зручно інтегрується з іншими сервісами, має активну підртимку і постійно покращується. Та чому ж в роботі за основу взятий інший продукт? Тому що, як було сказано раніше, головною причиною такої популярності є час коли продукт з’явився і ставши відомим, можливо, навіть еталоном, користувачі, компанії, адміністратори просто звикли до нього і його налаштувань, не бажаючи дивитись в сторону аналогів. Так, можливо на якомусь етапі особливо нічого було запропонувати, але поглянувши на готові рішення зараз, стає зрозуміло, що навіть Open-source продукти дуже часто нічим не поступаються одному з найвідоміших і найпоширеніших комерційних рішень. Майже всі продукти мають впевнений рівень підтримки протоколів, гнучкості налаштувань і «юзер-френдлі» інтерфейсів, які роблять роботу зручнішою і приємнішою. І також в епоху вільного доступу до інтернету, в якому вже існує величезна кількість інформації у відкритому доступі, мінус open-source у вигляді не такої активної підтримки, як у комерційних продуктів може частково бути стертрим, адже існує купа форумів, на яких скоріш за все хтось вже встиг зіткнутись з такою ж проблемою як у вас і з вискою вірогідністю її вирішити. Але стерти лише частоко, бо якшо проблема на стороні розробників, висока вірогідність, що доведеться чекати лише оновлень, які виправлять цю помилку. А вони можуть виходити досить не часто.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ GLUU

2.1. Призначення, можливості та функції рішення Gluu Identity and Access Management

Gluu Server - це програмне забезпечення з відкритим кодом для керування доступом від американського розробника Gluu. Завдяки Gluu Server вони пропонують платформу з відкритим кодом, яка допомагає компаніям контролювати доступ до власних ресурсів і ресурсів у партнерській мережі. Оскільки програмне забезпечення базується на протоколах SAML, OpenID Connect і OAuth2, можна підключити майже будь-яку програму. Таким чином, Gluu Server - це гнучке програмне забезпечення для керування доступом, яке може підвищити безпеку даних і зменшити витрати в довгостроковій перспективі. Єдиний вхід для всіх додатків значно покращує взаємодію з користувачем - навіть поза обмеженнями вищезгаданих протоколів.

Загальні випадки використання включають:

Єдиний вхід (SSO);

Мобільна автентифікація;

Керування доступом до API;

Двофакторна автентифікація (2FA);

Керування ідентифікацією клієнта та доступом (CIAM);

Федерація ідентичності;

Список веб-стандартів для автентифікації, авторизації, федеративної ідентифікації та керування ідентифікацією:

OAuth 2.0;

OpenID Connect;

Керований користувачем доступ 2.0 (UMA) ;

SAML 2.0;

Система міждоменного керування ідентифікацією (SCIM) ;

FIDO Universal 2nd Factor (U2F) ;

FIDO 2.0 / WebAuthn;

Легкий протокол доступу до каталогу (LDAP) ;

Служба віддаленої автентифікації за телефонним входом (RADIUS) ;

Трохи детальніше про функції які може виконувати Gluu і які можливості вони мають. Спочатку мова піде про Єдиний вхід (SSO). Єдиний вхід (SSO) - це служба автентифікації сеансу та користувача, яка дозволяє користувачеві використовувати один набір облікових даних для входу - наприклад, ім’я користувача та пароль - для доступу до кількох програм. SSO можуть використовувати підприємства, малі та середні організації, а також окремі особи, щоб спростити керування кількома обліковими даними.

Використання такої системи іноді називають федерацією ідентичності. Відкрита авторизація (OAuth) - це структура, яка дозволяє стороннім службам, таким як Facebook, використовувати інформацію облікового запису кінцевого користувача, не відкриваючи пароль користувача.

OAuth діє як посередник від імені кінцевого користувача, надаючи службі маркер доступу, який дозволяє передавати певну інформацію облікового запису. Коли користувач намагається отримати доступ до програми від постачальника послуг, постачальник послуг надсилає запит постачальнику ідентифікаційної інформації для автентифікації . Потім постачальник послуг перевіряє автентифікацію та авторизує користувача.

У базовій веб-службі SSO модуль агента на сервері додатків отримує конкретні облікові дані автентифікації для окремого користувача з виділеного сервера політики SSO, одночасно автентифікуючи користувача в сховищі користувачів, такому як каталог Lightweight Directory Access Protocol . Служба автентифікує кінцевого користувача для всіх програм, на які йому надано права, і усуває майбутні запити пароля для окремих програм під час того самого сеансу.

Види конфігурації і налаштувань SSO:

Деякі служби SSO використовують такі протоколи, як Kerberos або Security

Assertion Markup Language (SAML):

У налаштуванні на основі Kerberos після надання облікових даних користувача видається квиток надання квитка (TGT). TGT отримує сервісні квитки для інших програм, до яких користувач хоче отримати доступ, не вимагаючи від користувача повторного введення облікових даних.

SAML - це стандарт розширюваної мови розмітки, який полегшує обмін даними автентифікації та авторизації користувачів між безпечними доменами. Служби єдиного входу на основі SAML передбачають спілкування між користувачем, постачальником ідентифікаційної інформації, який підтримує каталог користувачів, і постачальником послуг.

Система єдиного входу на основі смарт-картки просить кінцевого користувача використати картку, яка містить облікові дані для входу, для першого входу. Після використання картки користувачеві не потрібно повторно вводити ім’я користувача чи пароль. Смарт-картки SSO зберігають або сертифікати, або паролі.

З огляду на зручність функціоналу SSO - не виникає жодних питань з поширеності його використання. Саме тому розробники Gluu додали його до свого продукти.

Далі - мобільна автентифікація. Використання мобільної програми автентифікації для MFA надає другий фактор автентифікації у формі одноразового пароля (OTP) або push-повідомлення, а також пропонує кілька варіантів для реалізації політики захисту програми та відповідності.

Мобільна програма автентифікації - це програмний маркер, який встановлюється на мобільний пристрій. Мобільна програма автентифікації використовує OTP або push-сповіщення, щоб підтвердити, що користувач володіє мобільним пристроєм. Лише мобільна програма автентифікації, яка володіє секретним ключем користувача, може згенерувати дійсний OTP.

Gluu пропонує власний додаток для мобільної автентифікації. Він має назву Super Gluu. Super Gluu використовує шифрування з відкритим ключем, як зазначено в стандарті автентифікації FIDO U2F (відкритий, бездрайверний

протокол для двофакторної автентифікації, заснований на виклик-відповідь автентифікації, що дозволяє інтернет-користувачам використовувати U2F пристроєм як другим чинником для автентифікації на великій кількості онлайн-служб) . Після реєстрації пристрою Super Gluu реєструє свій відкритий ключ на кінцевій точці FIDO U2F сервера Gluu. Коли відбувається автентифікація, виникає відповідь на виклик, щоб переконатися, що пристрій має відповідний закритий ключ. Для роботи потребує: доступний в Інтернеті (не внутрішній або локальний) сервер Gluu з DNS, що вказує на загальнодоступну адресу в інтернеті сервера; Super Gluu interception script - скрипт для роботи сервера з Super Gluu; пристрій Android або iOS із встановленим Super Gluu; якщо сервер Gluu використовує самопідписаний сертифікат, його потрібно ввімкнути в Super Gluu (відкрийте програму, перейдіть до Menu > Trust all (SSL) та ввімкніть). За замовчуванням користувачі проходять двоетапну двофакторну автентифікацію: спочатку ім'я користувача та пароль, а потім надсилання сповіщень через Super Gluu. Альтернативні робочі процеси автентифікації, наприклад автентифікацію без пароля, можна налаштувати за допомогою налаштування сценарію за потреби.

Керування доступом до API. API - це набір програмного коду, який забезпечує передачу даних між одним програмним продуктом та іншим. Він також містить умови цього обміну даними. Принцип роботи API зазвичай виражається через зв'язок запит-відповідь між клієнтом і сервером. Клієнт - це будь-яка зовнішня програма, з якою взаємодіє користувач. Сервер відповідає за серверну логіку та операції з базою даних. У цьому сценарії API працює як проміжний рівень між клієнтом і сервером, що дозволяє надсилати запити даних і відповіді. Gluu Server 4.1.x пропонує REST API для графічного інтерфейсу адміністратора oxTrust. За допомогою REST API можна автоматизувати конфігурації серверів, створювати нові графічні інтерфейси для надання певних функцій адміністратора та створювати інші інтеграції для порталу адміністратора Gluu. Також підтримка, SCIM API. SCIM, або система міждоменного керування ідентифікацією, є відкритим стандартом, який дозволяє автоматизувати надання доступу користувачам. Він був створений у 2011 році, коли стало зрозуміло, що технологія

майбутнього буде базуватися на хмарі. SCIM передає ідентифікаційні дані користувача між постачальниками ідентифікаційних даних (наприклад, компаніями з кількома окремими користувачами) та постачальниками послуг, яким потрібна ідентифікаційна інформація користувача (наприклад, корпоративні програми SaaS). IT-відділам більше не потрібно розробляти та постійно оновлювати спеціальні інтеграції, які підключають каталоги компанії до різноманітних зовнішніх інструментів і програм. Співробітники, які не належать до IT-спеціалістів, можуть скористатися перевагами системи єдиного входу (SSO). Сервер Gluu реалізує SCIM , щоб запропонувати REST API для виконання функцій CRUD (створення, читання, оновлення та видалення) щодо даних користувача. API SCIM можна використовувати для керування такими типами ресурсів: користувачами, групами та пристроями FIDO U2F / FIDO2. Також є підтримка UMA API - Керований користувачем доступ (UMA) - визначає, як власники ресурсів можуть маніпулювати ними, щоб захистити ресурси. OpenID Connect API - Ця сторінка надає інтерфейс для запиту авторизації через веб-служби REST.

Зручності в функціонал для користувачів також додає Gluu Casa. Це веб-портал самообслуговування. В ньому кінцеві користувачі можуть керувати своїми обліковими даними для автентифікації. Такі постачальники ідентифікаційних даних споживачів, як Google, дозволяють кінцевим користувачам переглядати, додавати та видаляти надійні облікові дані через веб-сторінку. Casa дозволяє вашій організації робити те саме. Дозволяючи користувачам реєструвати кілька надійних облікових даних, якщо вони втратять один, це не проблема. Вони можуть увійти, видалити втрачені облікові дані та зареєструвати заміну. Ви можете створювати власні плагіни для підтримки нових багатофакторних облікових даних або інших вимог.

Наприклад, коли люди взаємодіють із цифровими службами організації, їм може знадобитися:

Реєстрація, видалення або редагування облікових даних двофакторної автентифікації (2FA) для свого облікового запису (наприклад, ключі безпеки FIDO, мобільні програми, номери телефонів тощо) ;

Увімкнення або вимкнення 2FA;

Перегляд і керування зовнішніми програмами, яким надано доступ до особистих даних;

Перегляд надійних пристроїв;

Casa надає людям платформу для виконання цих функцій безпеки облікових записів тощо.

Тобто Основним варіантом використання Casa є 2FA для самообслуговування. Якщо людям потрібно дзвонити в службу підтримки кожного разу, коли вони отримують новий телефон або ключ безпеки, підтримка надійної автентифікації стає непомірно дорогою.

Заздалегідь Casa можна використовувати для реєстрації та керування такими автентифікаторами:

Ключі безпеки FIDO2/U2F, такі як Yubikeys;

Мобільний додаток для push-повідомлень U2F від Gluu, Super Gluu;

Апаратні карти OTP, як ці , або ключі, як ці;

Мобільні програми OTP, такі як Google Authenticator, FreeOTP тощо;

Номери мобільних телефонів, які можуть отримувати OTP через SMS;

Паролі (якщо зберігаються у відповідній локальній базі даних сервера Gluu, тобто не у серверній LDAP, як AD);

За замовчуванням панель адміністратора має корисний графік, який відображає кількість невдалих спроб входу(рис.2.1).

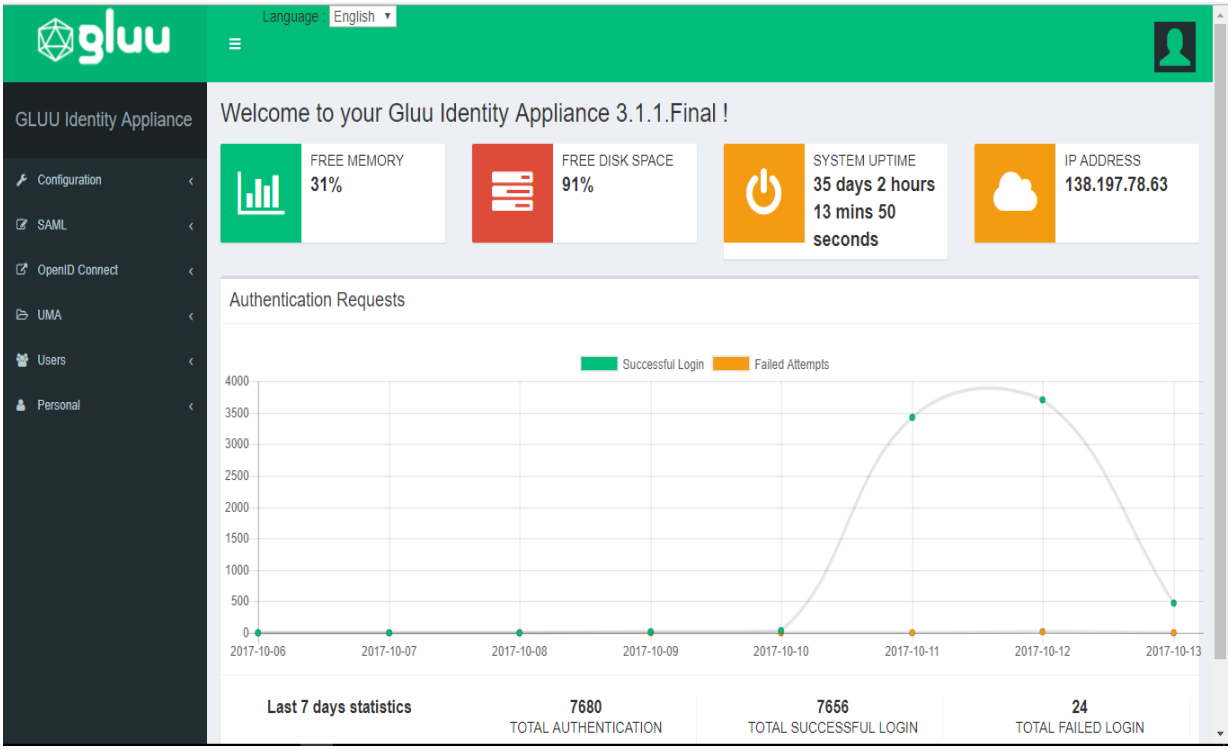


Рис. 2.1. Невдалі спроби входу на панелі адміністратора Gluu

Gluu справді має дуже широкий функціонал, який додає йому гнучкості і в цілому кожен може знайти в цьому продукті те, що сильно спростить виконання задач з управління ідентифікацією та доступом користувачів до інформаційної системи організації.

2.2. Компоненти та архітектура Gluu Identity and Access Management

Сервіс складається з декількох компонентів і кожен з них має свою роль у функціях, що були розглянуті в попередньому розділі. Але дуже важливо приділити увагу саме окремим компонентам і їх взаємодії між собою, для більш детального розуміння гнучкості налаштувань і спрощенні відлагоджування в майбутньому якщо виникають складнощі. Також розглянемо деякі рішення від Gluu, а саме Хмарний хостинг, Віртуальна машина або Cloud Native варіант.

Розберемо кожен компонент по-порядку. Деякі вже були згадані раніше, але поглянемо на них більш детально.

oxAuth - це компонент доступу з відкритим кодом, керований користувачем, і компонент OpenID Connect Provider сервера Gluu, який реалізує стек служб REST

OpenID Connect Core 1.0. Проект також включає код OpenID Connect Client, який можуть використовувати веб-сайти для перевірки токенів.

Наразі oxAuth реалізує всі необхідні аспекти стеку OpenID Connect, включаючи сервер авторизації OAuth 2.0, Simple Web Discovery, динамічну реєстрацію клієнта, веб-токени JSON, веб-ключі JSON та кінцеву точку інформації про користувача. oxAuth тісно пов'язаний з oxTrust. oxAuth є основним компонентом Gluu Server 4, який надає кінцеві точки OpenID Connect Provider і OAuth Authorization Server. oxAuth представляє сторінки входу, відстежує сеанси браузера та реалізує веб-потоки автентифікації та згоди.

oxTrust. Простими слова, це GUI(Graphical User Interface) для адміністрування Gluu севером. oxTrust - це єдина точка адміністрування для всіх компонентів серверів Gluu 4.x. Він включає механізм синхронізації ідентифікаційних даних для зовнішніх сховищ користувачів LDAP. Окрім веб-інтерфейсу, oxTrust також надає API для автоматизації багатьох завдань.

Gluu Server 4.x пропонує REST API для графічного інтерфейсу адміністратора oxTrust. За допомогою REST API можна автоматизувати конфігурації сервера, створювати нові графічні інтерфейси користувача для надання певних функцій адміністратора та створювати інші інтеграції для порталу адміністратора Gluu.

oxTrust дає змогу адміністраторам керувати інформацією про людей, яка надається партнерським веб-сайтам. oxTrust також є локальним інтерфейсом керування, який надає IT-адміністраторам механізм для підтримки людей в організації, які мають проблеми з доступом до веб-сайту чи мережевого ресурсу. Інтерфейс адміністрування сервера Gluu доступний, перейшовши до повного доменного імені, наданого під час налаштування.

Passport-JS. Сервер Gluu використовує цей компонент, щоб увімкнути вхід із соціальних мереж. Завдяки понад 300 існуючим «стратегіям» Passport надає краудсорсинговий підхід, щоб пропонувати користувачам вхід через соціальну мережу.

Для LDAP Gluu використовує OpenDJ. Це служба каталогів, сумісна з LDAPv3, розроблена для платформи Java, яка забезпечує високопродуктивне, високодоступне та безпечне сховище для ідентифікаційних даних, якими керує ваша організація. Простий процес встановлення в поєднанні з потужністю платформи Java робить OpenDJ найпростішим і найшвидшим каталогом для розгортання та керування. Gluu має можливість синхронізації AD/LDAP - синхронізація LDAP, також відома як Cache Refresh, - це процес підключення одного або кількох існуючих серверів LDAP, як-от Microsoft Active Directory, до локального сервера LDAP сервера Gluu. Користувачі, що додаються через OxTrust(рис.2.2) можуть також бути додані і переглянуті вручну через LDAP браузер(рис.2.3).

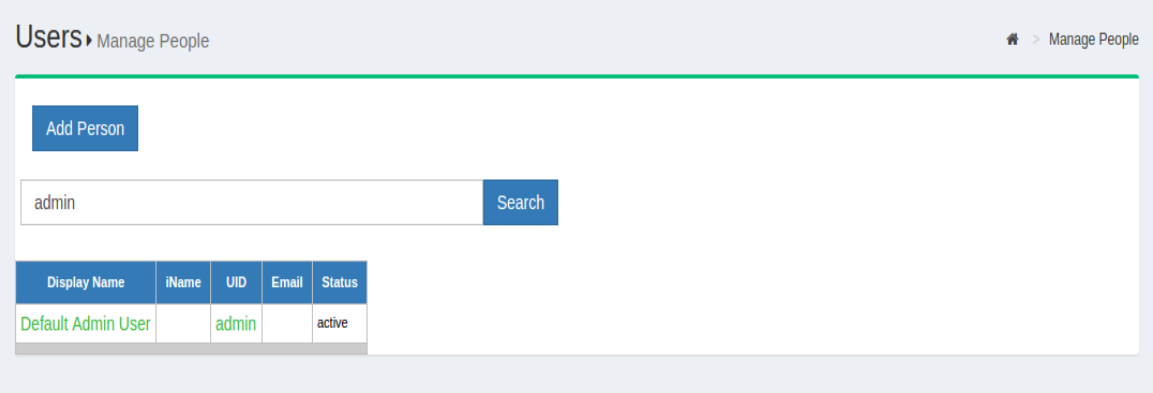
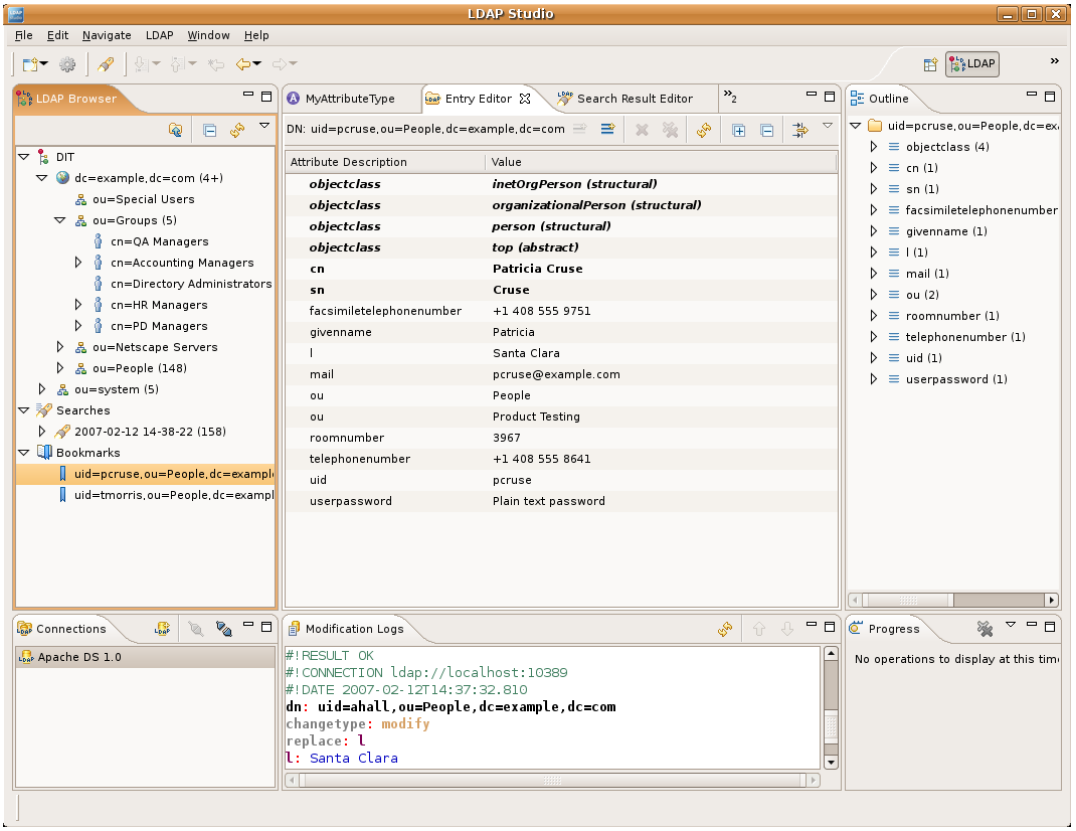


Рис.2.2. Додавання користувача через oxTrust



2.3. Користувачі через LDAP браузер

Наступний важливий компонент - Gluu 4 Cluster-Manager. Cluster Manager (CM) - це комерційно ліцензований інструмент графічного інтерфейсу користувача для встановлення високодоступної кластерної інфраструктури Gluu Server і керування нею на фізичних серверах або віртуальних машинах. HA-cluster створюється для того, щоб при виході з ладу одного сервера, інший одразу міг підхопити його функції. Тобто встановлюється два або більше серверів з налаштованим Gluu server, при цьому на них вмикається реплікація, щоб дані співпадали. Це досить поширена практика, щоб зменшити час недоступності сервсів, адже без ha-кластеру доступ буде втрачено, поки будуть тривати роботи по відновленню, а у випадку з кластером відбудеться автоматичне переключення на працюючий сервер. Також кластер може працювати у вигляді Active-Active, коли всі ноди кластеру виконують роботу. Трафік і навантаження рівномірно розділяється між нодами кластеру для уникнення перенавантаження. Робиться це за допомогою load balancer. Саме він діє як « дорожній поліцейський», який сидить перед вашими серверами та направляє клієнтські запити на всі сервери, здатні

виконувати ці запити таким чином, щоб максимізувати швидкість і використання потужності та гарантувати, що жоден сервер не буде перевантажений, що може погіршити продуктивність . Якщо один сервер виходить з ладу, балансувальник навантаження перенаправляє трафік на інші онлайн-сервери. Коли новий сервер додається до групи серверів, балансувальник навантаження автоматично починає надсилати йому запити. Кроки для налаштування досить детально описані у офіційній документації Gluu.

А от CM автоматизує багато завдань, пов’язаних зі створенням і роботою середовища HA/DR Gluu Server, зокрема:

Встановлення сервера Gluu;

Реплікація Gluu OpenDJ LDAP;

Керування кешем;

Моніторинг;

Центральне логування;

Наскрізне безпечне тунелювання між oxAuth і Redis;

Для налаштування кешу в кластері рекомендується використовувати Redis. Redis (що означає Remote Dictionary Serve) - це база даних NoSQL з відкритим вихідним кодом, яка відома як швидке сховище даних ключ-значення в пам’яті. На відміну від інших баз даних, Redis збергіє дані в оперативній пам’яті а не на диску, що дуже сильно прискорює доступ до даних. Кеш - це тимчасове сховище, де зберігаються дані, щоб у майбутньому отримати доступ до них швидше. Отже, кешування - це процес зберігання даних у кеші. Redis є хорошим вибором для впровадження високодоступного кешу в пам’яті, щоб зменшити затримку доступу до даних за допомогою HDD чи SSD, забезпечити високу пропускну здатність і зменшити навантаження на базу даних і програму. Кешування веб-сторінок, кешування результатів запитів до бази даних, постійне кешування сеансів і кешування часто використовуваних об’єктів, таких як зображення, файли та метадані, є популярними прикладами рішень кешування за допомогою Redis. Саму схему кластеризації розробник подає в такому вигляді(Рис.2.4).

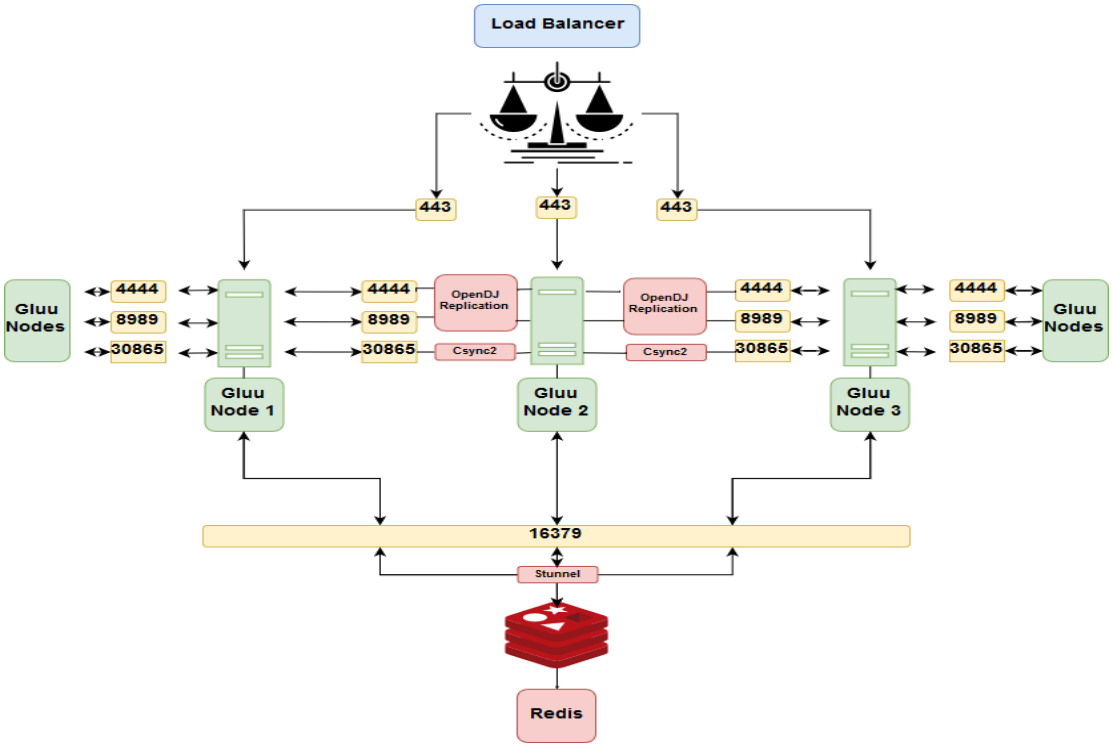


Рис.2.4. Схема кластеризації Gluu.

На схемі бачимо load balancer, який буде розділяти трафік і навантаження між нодами. Це може бути web-сервер NGINX з відповідною конфігурацією. Між нодами відбувається реплікація OpenDJ. Тобто синхронізація каталогів, що містять дані про користувачів, групи тощо. І також Redis сервер для кешування і швидкого доступу до кешу.

Gluu server може бути налаштований трьома типами. Хмарний хостинг, Віртуальна машина(self-hosted).

Хмарний хостинг. З хмарним рішенням, сервер gluu, як не дивно, буде знаходитись у хмарі і не буде потребувати турботи про сервер зі сторони IT-фахівців, як у випадку з віртуальною машиною(self-hosted), тобто локально розміщеного Gluu-server на серверах вашої компанії. Але звісно таке рішення платне, адже в оренду надаються хмарні ресурси.

Віртуальна машина(Self-hosted). Gluu публікує пакети Linux для Ubuntu, Debian, Centos і RedHat. Клієнти з VIP-підпискою також можуть використовувати існуючий інструмент розгортання Cluster Manager, щоб швидко налаштувати високодоступний кластер серверів Gluu.

В практичній частині буде розглянутий саме цей варіант. Gluu server не

потребує багато навичків і часу для встановлення, всі компоненти встановлюються і налаштовуються майже автоматично за допомогою скриптів, що економить час адміністратору. Мінімальні рекомендації при встановленні стандартних компонентів - це 2 ядра процесору, 4 ГБ оперативної пам’яті та 40ГБ диску. Також декілька додаткових згадок про вимоги:

При встановленні більшої кількості компонентів ніж за замовчуванням (тобто oxAuth, oxTrust і LDAP), розробник рекомендує використовувати сервер чи віртуальну машину із принаймні 8 ГБ оперативної пам’яті .

Gluu має бути розгорнуто на сервері або віртуальній машині зі статичною IP-адресою. Статична IP-адреса має резолвити на ім’я хоста комп’ютера, що можна отримати, додавши запис до DNS-сервера або в /etc/hosts.

Якщо налаштовувати віртуальну машину локально, розробник рекомендує використовувати VM Player. Хоча проблем і з іншими гіпервізорами виникати не має. В тестуванні, наприклад, з ProxMox проблем виявлено не було. Також для роботи всіх компонентів необхідно відкриті порти 80, 443 та 22.

Також важливий компонент, що з’явився з 4ої версії додатку Gluu server - це підтримка Radius. Сервер Gluu можна налаштувати для включення сервера RADIUS на основі бібліотеки Java TinyRadius . Реалізація ("Gluu Radius") підтримує автентифікацію RADIUS. При встановленні за допомогою скрипта просто необхідно вказати встановлення Radius. Можна налаштувати такі параметри:
Authentication Listen Port: це порт, на якому сервер прослуховує запити автентифікації;
Accounting Listen Port: це порт, на якому сервер прослуховує облікові запити;
Authentication Timeout: Це максимальний проміжок часу в мілісекундах між ініціюванням запиту на автентифікацію та підтвердженням автентифікації користувачем. Це стосується лише довготривалих запитів на основі двофакторної автентифікації (наприклад, Super-Gluu);

Якщо повернутися на декілька абзаців назад, видно, що мінімальним набором компонентів є oxAuth, oxTrust і LDAP(OpenDJ). В більшості випадків цього і справді достатньо. Тому такий варіант і буде детально розглянуто при

налаштуванні. Адміністратор за допомогою вікна авторизації oxAuth входить до графічного інтерфейсу Gluu server - oxTrust. А далі проводить маніпуляції з користувачами, групами тощо. Всі ці зміни відбуваються у внутрішніх базі Gluu server - OpenDj. Але графічний інтерфейс, має певні обмеження. Такі як кількість відображених користувачів за раз, для збереження ресурсів. Якшо адміністратору необхідно переглянути одночасно список всіх сервісів або ресурсів, він може скористатись будь яким LDAP браузером і переглянуи вміст директорії Users.

Як було згадано раніше - база Gluu OpenDJ може бути додатково синхронізована з базою AD, як приклад. Користувачі, групи можуть бути синхроніховані з бази Active Directory до бази OpenDJ. І Gluu сервер при зверненні користувача або сервіса до бази виконає синхронізацію із базою AD, для перевірки наявності користувача, групи, його прав тощо(Рис.2.5).

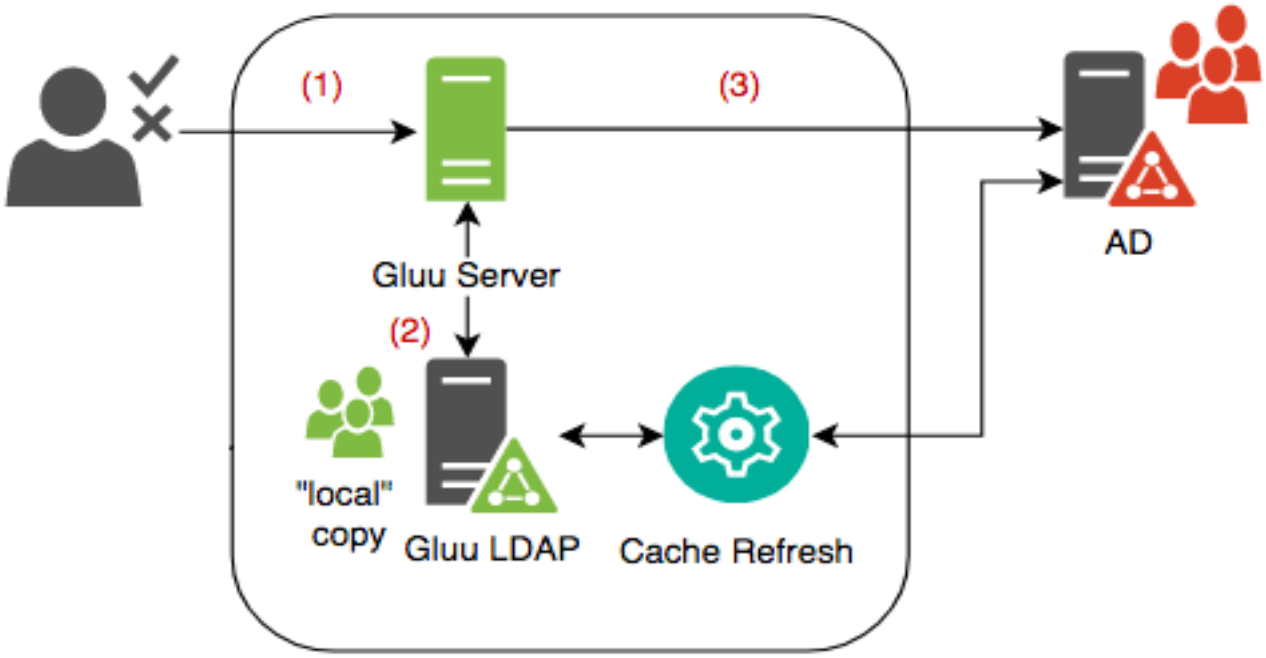


Рис.2.5. Схема звернення до бази Gluu та синхронізація з базою AD

В такому типі архітектури Gluu він може під’єднуватись та синхронізуватись з декількома вже існуючими базами на backend.

2.3. Можливості щодо адміністрування Gluu Identity and Access Management

Gluu server має дуже гнучкі налаштування, надаючи можливості кожному адміністратору змінити, додати певені параметри під свої вимоги, чи вимоги компанії. Але спочатку необхідно переглянути стандартні функції якими буду користуватись адміністратор при налаштуванні.

Почнемо з графічного інтерфейсу oxTrust. Коли адміністратор проходить авторизацію він потрапляє на панель адміністратора, що містить корисну інформацію для нього. Відображається деяка основна інформація про віртуальну машину/сервер, а також версію сервера, вільну пам'ять і місце на диску. Також відображається згаданий в попередніх розділах графік стастики авторизації користувачів.(Рис.2.6.)

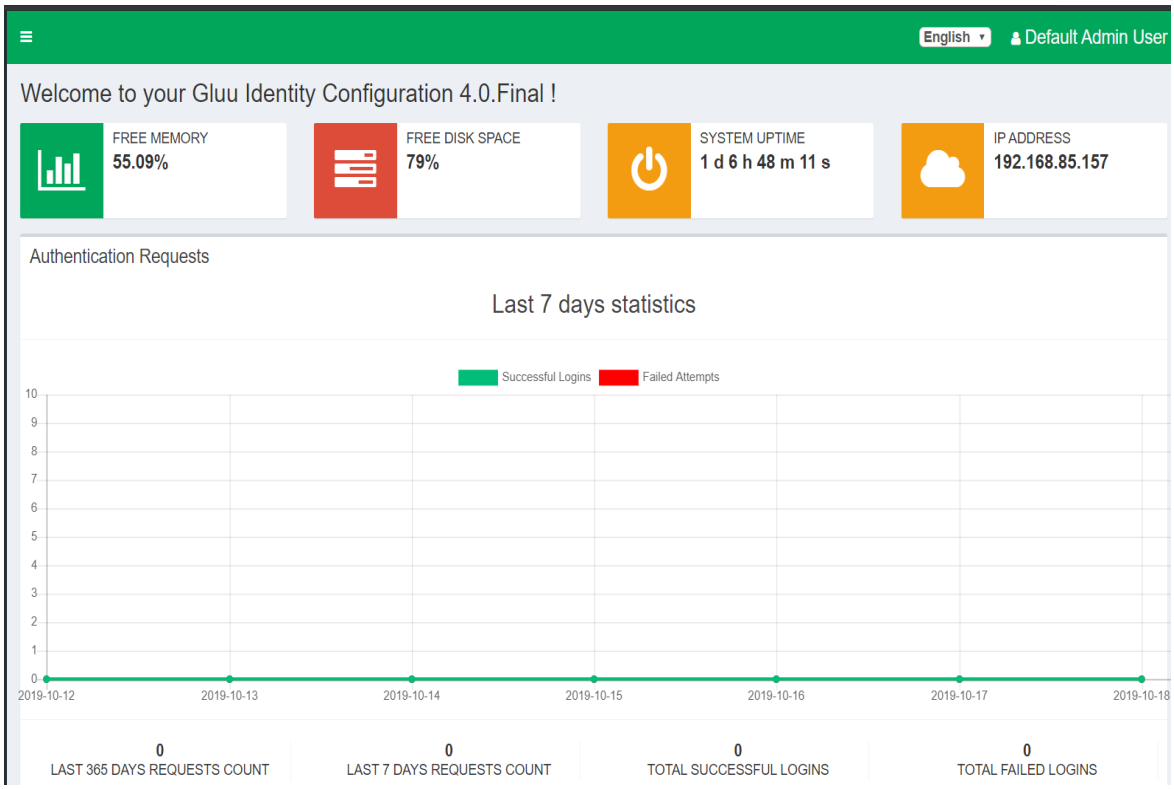


Рис.2.6. Панель адміністратора Gluu зі статистикою

Далі досить важлива вкладка - Configuration. На ній адміністратор може налаштувати таки пункти:

Самостійне скидання пароля. Користувачі зможуть власноруч відновити свій

пароль при його втраті не звертаючись то адміністратора, перейшовши за URL-адресою на зразок https://ваш.домен/identity/person/passwordReminder.htm. Новий пароль буде надіслано на електронну скриньку, яка вказується при створенні користувача у спеціальному атрибуті. Але щоб ця функція працювала для користувачів, адміністратору також потрібно буде виконати налаштування поштового сервера SMTP

Підтримка SCIM. Вона вмикається, якщо адміністратор планує використовувати цей протокол SCIM для обміну ідентифікаційними даними із програм до Gluu і навпаки.

Підтримка Passport.

DNS-сервер(и): якщо ця організація використовує будь-який спеціальний DNS Server, адміністратор додає сюди адресу, щоб Gluu сервер знав куди звертатись при резолві імені

Максимальний розмір журналу (в МБ): за умовчанням максимальний розмір файлу журналу становить 200 МБ. Це значення можна збільшити або зменшити залежно від вимог організації.

Користувач може редагувати власний профіль: oxTrust має розділ профілю для кожного користувача. Якщо цей параметр увімкнено, користувачі зможуть увійти в oxTrust і редагувати значення, пов’язані з їхніми даними

Контактна адреса електронної пошти: Спеціально налаштована адреса(напприклад, адміністратора) електронної пошти відображатиметься на всіх сторінках помилок, щоб користувач знав, куди звернутися за допомогою при виникненні проблем.

Щодо керування користувачами на сервері Gluu. Усі дані, створені сервером Gluu, зберігаються на локальному сервері LDAP, включеному в кожне розгортання. Один з методів - це підключення напряму до бази даних OpenDJ за допомогою LDAP браузеру. При стандартному налаштуванні параметри доступу будуть мати приблизно наступний вигяд:

bindDN: cn=directory manager

bindPassword: ваш пароль

servers: localhost:1636

Але існує певна особливість при підключенні таким методом. Небхідно налаштувати тунель, адже LDAP порт(1636) за замовчуванням не доступний з мережі в Gluu, а працює лише на localhost. Також можна додати правило перенаправлення трафіку, яке буде перенаправаляти пакети за локального ip gluu server на localhost. Після цього адміністратор може підключитись до LDAP северу і керувати користувачами.

Інший, більше “user-friendly” варіант - графічний інтерфейс oxTrust. В ньому можна додавати користувачів, їх атрибути, а також створювати групи і додавати користувачів до цих груп(рис.2.7).

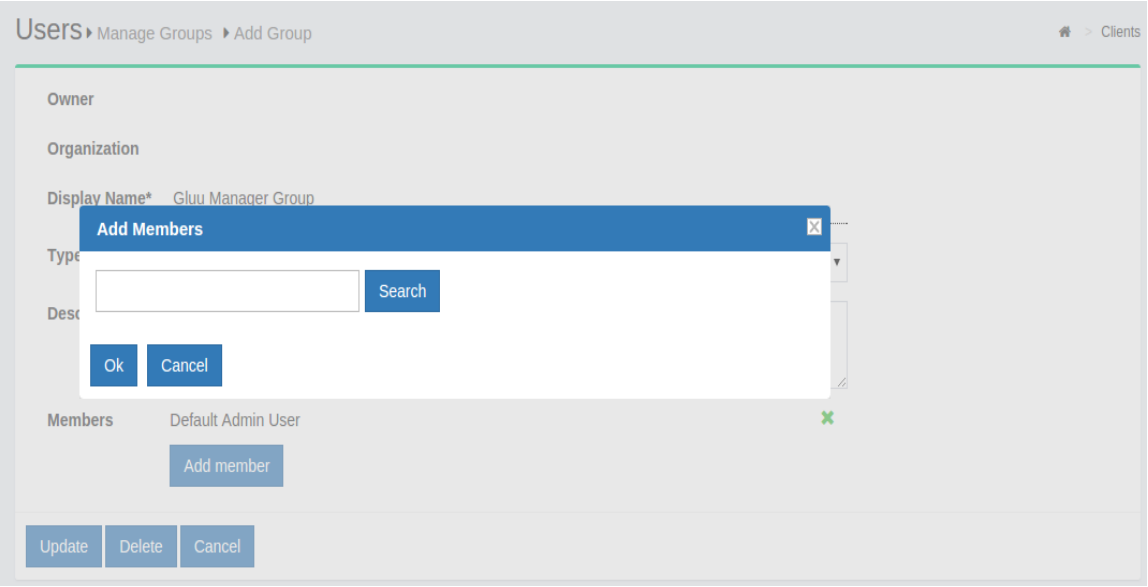


Рис.2.7. Панель додавання користувача до групи.

Важлива панель - Manage LDAP Authentication. Цей розділ дозволяє адміністратору сервера Gluu визначати, як і де сервер має підключатися для автентифікації користувачів. Якщо це віддалений сервер LDAP/Active Directory, параметри його підключення мають бути обов’язково вказані тут. Деталі джерела даних, яке буде підключено до сервера Gluu мають бути вказані в спеціальних полях. Наприклад, джерелом даних може бути ваш внутрішній каталог Active Directory або локальний сервер LDAP. При їх підключенні, налаштування відбувається в цілому за тією ж схемою, що і інтеграція будь якого сервісу з LDAP сервісом. Необхідно заповнити ті самі поля, та вказати параметри для підключення.

Після вдалого тестування підключення, адміністратор може починати працювати з групами, користувачами, їх доступами, тощо. Якщо розглядати більш детально парметри підключення Gluu до LDAP серверу, то панель має такі поля для налаштування(рис.2.8):

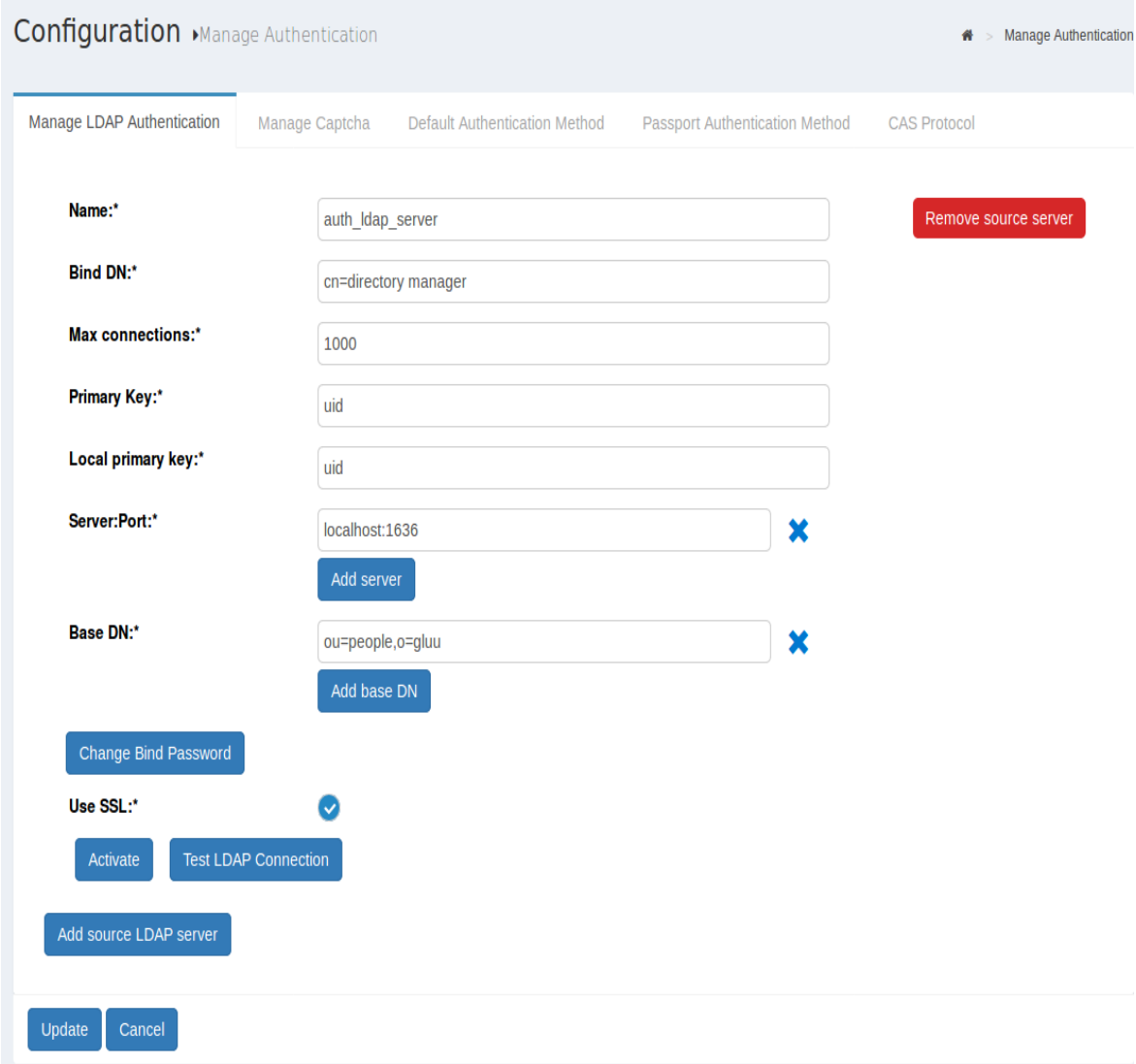


Рис.2.8. Підключення Gluu до LDAP северу

Name: це поле містить назву сервера автентифікації

Bind DN: ім’я користувача для сервера автентифікації

Max Connections: цей параметр можна використовувати для визначення загальної кількості одночасних підключень, дозволених для читання локального LDAP/віддаленого Active Directory/віддаленого LDAP

Primary key: це поле використовується в операціях пошуку та прив’язки до каталогу LDAP, який налаштовано на вкладці «Керування автентифікацією», який фактично перевіряє облікові дані, надані користувачем на сторінці входу. За замовчуванням він використовує внутрішній LDAP сервера Gluu, але можна використовувати будь-який сервер LDAP, уже налаштований у мережі, що дозволяє бездоганно інтегрувати сервер Gluu в будь-яке корпоративне середовище. Ключ може бути SAMAccountName , uid , mail тощо

Local primary key: це поле використовується під час пошуку у внутрішньому каталозі LDAP сервера Gluu, щоб перевірити, чи існує й активний запис локального користувача для цього користувача. Зазвичай ключем є uid або mail

Server: тут вказується унікальна назва сервера автентифікації та номер порту (наприклад, auth.company.org:636).

Base DN: Base DN вказується у цьому полі, щоб дозволити серверу Gluu підключатися та здійснювати пошук на сервері LDAP. Кожне дерево каталогів слід додавати окремо за допомогою параметра « Додати базове DN ».

Change Bind Password: ця кнопка вказує пароль для автентифікації

Use SSL: увімкнення SSL, якщо сервер автентифікації вимагає захищений порт (наприклад, 636)

Activate: ця кнопка вмикає та вимикає відповідний віддалений сервер LDAP як параметр автентифікації

Test LDAP connection: для перевірки, чи достатньо наданої інформації для підключення до сервера автентифікації. Сканування виконується в режимі реального часу

Досить зручна функція для адміністратора - імпорт користувачів. Імпорт може здійснюватись зі звичайного excel файлу через вкладку Users> Import People. Файл має бути такої структури:

Ім'я користувача (обов'язково);

Ім'я (обов'язково);

Прізвище (обов'язково);

Електронна пошта (обов'язково);

Пароль;

Статус користувача(активний/не активний). Якщо не вказати - за замовчуванням буде виставлений стан як не активний.

Також адміністратор може встановити правила при яких користувач буде заблоковано. Як приклад - перевищенний ліміт невдалих спроб входу. Дистрибутив Gluu Server за замовчуванням включає сценарій перехоплення для реалізації основної політики блокування облікового запису, яка деактивує обліковий запис користувача після встановленої кількості послідовних невдалих спроб входу. Сценарій використовує параметри автентифікації, надані на Manage LDAP Authentication вкладці в Configuration > Manage Authentication. Якщо досягнуто встановленого порогу невдалих входів, gluuStatus атрибут відповідного користувача буде встановлено на inactive а лічильник входів буде скинуто до нуля.

Якщо необхідно створити резервну копію - один з найпростіших методів - це tarball. Tarball - це утиліта комп'ютерного програмного забезпечення для збирання багатьох файлів в один архівний файл, який часто називають tarball, для розповсюдження або резервного копіювання. Тобто, створення архіву. Усі файли сервера Gluu зберігаються в одній папці: /opt. Усю папку Gluu Server CE chrootможна заархівувати за допомогою tar команди:

tar cvf gluu40-backup.tar /opt/gluu-server/.

-c - створити архів

-v - відображення процесу створення архіву

-f - вказати ім'я файлу

Попередньо зупинивши сервіс і запустивши його після успішного виконання бекапу.

Також графічний інтерфейс Gluu надає змогу зручного перегляду логів при виникненні проблем. Адміністратор може використовувати його, або підключитись напряму до серверу через ssh і переглядати логи в консолі. В першому варіанті необхідно зайти до Конфігурація --> Переглянути файл журналу. Тут можна встановити кількість рядків які необхідно вивести, наприклад якщо вказати значення 250 рядків, то графічний інтерфейс відобразить останні 250 рядків

логів. Через графічний інтерфейс можна відслідковувати повідомлення за такими рівнями:

Trace	Всі повідомлення
Debug	Debug рівень і вище
Info	Informational рівень і вище
Warn	Warning рівень і вище
Error	Error рівень і вище
Fatal	Тільки критичні помилки
off	Логування вимкнено

Адміністратор може налаштувати ці рівні у панелі Configuration > JSON Configuration > OxTrust Configuration Tab.

У зручний спосіб адміністртор може видалити користувачів за певними критеріями. Наприклад, ваш сервер підтримує вхід за допомогою Passport. Користувачі автоматично створюють локальні облікові записи на сервері Gluu під час автентифікації через зовнішніх постачальників ідентифікаційних даних, таких як соціальні мережі, тощо. І через якийсь час в базі може накопичитись досить багато записів, які не використовуються, для цього і існує інструмент у вигляді Python скрипта, який може допомогти видалити або декативувати цих користувачів. Для того, щоб ним скористатится необхідно в контейнері запустити скрипт python3 remove_external_people.py. Він має такі параметри:

remove: цей параметр вказується якщо користувачів необхідно саме видалити із бази. Якщо його не вказувати, користувачі будуть просто переведені в статус inactive. Це дає змогу в майбутньому швидше повернути користувачів назад за потреби;

provider-only: вимкнення чи видалення користувачів, що були зареєстровані саме через конкретний сервіс, який передав ідентифікаційні дані. Такі як github, Okta-1234 тощо;

last-logon: Видалення/дезактивація відбуватиметься після записів, час останнього входу яких раніше або дорівнює вказаному значенню. Приклад: 2022-11-30. Тобто

таке правило буде стосуватись всіх користувачів, що не використовували акаунт після 30 листопада;

Але є винятки. Якщо користувач підпадає під параметри, які адміністратор вказав при користуванні інструментом очистки, але він теж знаходиться в групі адміністраторів, то на нього очистка чи декативація не спрацюють.

Приклад використання інструменту. Перевіривши базу даних, адміністратор побачив там велику кількість користувачів, які вже не є активними. Наприклад, колишні співробітники компанії, або зайві створені облікові записи. Щоб швидко очистити ці записи, він може виконати команду: python3 remove_external_people.py -remove last-logon 2022-11-15. Після використання цього скрипта, всі користувачі, що жодного разу не входили до програм, сервісів звертаючись до бази Gluu сервер, будуть видалені. Або ж, якщо не до кінця впевнений кого варто видаляти, а кого ні, він може вказати команду без ключа -remove, тоді користувачі будуть просто деактивовані.

Це лише частина інструментів і можливостей які має адміністратор при керуванні Gluu-server, ті, що більше виступають, як необхідні або спрощують задачі. Також Gluu надає можливість змінювати візуальну частину панелі керування і входу, щоб вона більше пасувала під бренд і стиль компанії. Це складно назвати необхідністю, але точно може стати приємним бонусом. Також адміністратор має змогу додавати персоналізовані поля, які мають бути заповнені при створенні користувачів, що по-перше дозволяє зберігати більше інформації про користувача, а по-друге, надає в майбутньому можливість більшої гнучкості фільтрів, при необхідності знайти користувачів в базі, що відповідають певним вимогам. Наприклад, при реєстрації користувача, адміністратор може додати поле «відділ». Логічно було б припустити, що при налаштуванні доступів, все одно потрібні користувачі будуть додаватись до певних груп, по яким можна буде знайти потрібних користувачів, але додаткові атрибути можуть зробити цей пошук ще більше гнучким. Уявімо, є дві групи, розробники та інженери мережевої безпеки. Скоріш за все, за правами доступів до ресурсів, вони будуть відрізняться і будуть знаходитись в різних групах на сервері LDAP. Але всі вони у відділі IT, і ось за

допомогою додаткового атрибуту буде простіше знайти всіх працівників, що працюють у цьому відділі, якщо це знадобиться. Або ж додатковий атрибут який вказує модель робочої станції користувача. При виникненні проблеми із робочою станцією користувача, адміністратор зможе подивитись в кого з користувачів така ж станція і перевірити, чи присутня там така ж проблема, вирішивши її завчасно.

3 ПОРЯДОК ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ GLUU

3.1 Порядок розгортання рішення Gluu Identity and Access Management

Рішення Gluu Identity and Access Management дозволяє побудувати систему управління ідентифікацією та доступом користувачів до інформаційної системи організації використовуючи власний сервер. В даному випадку буде розглянутий Linux server - Ubuntu. Працює сервіс у вигляді chroot контейнеру. Chroot - в Unix-подібних операційних системах операція зміни кореневого каталогу. Програма, запущена зі зміненим кореневим каталогом, матиме доступ тільки до файлів, що містяться в цьому каталозі. Після його розгортання адміністратор може інтегрувати інші сервіси компанії з Gluu для використання централізованої авторизації. Це може бути VPN-шлюз, доступ до локальних сервері тощо.

Порядок розгортання сервісу Gluu на локальному сервері досить простий. Враховуючи, що ми використовуємо сервер з Ubuntu - встановлення буде проводитись за допомогою .deb пакетів. Необхідно виконати наступні команди:

1.echo "deb https://repo.gluu.org/ubuntu/ bionic main" > /etc/apt/sources.list.d/gluu-repo.list

2.curl https://repo.gluu.org/ubuntu/gluu-apt.key | apt-key add -

3.apt-get update

4.apt-get install gluu-server=4.0~bionic

Перша команда додасть репозиторій для подальшого встановлення сервісу Gluu Identity and Access Management шляхом додавання посилання на репозиторій до списку джерел з яких система бере пакети. Друга команда додасть ключ репозиторія до локальної бази, щоб перевірити його і зробити довіреним. Третя виконає оновлення пакеті і четверта проведе вже саме встановлення сервісу до системи.

Після встановлення необхідно запустити chroot контейнер сервісу та перейти до нього за допомогою команд /sbin/gluu-serverd start і /sbin/gluu-serverd login відповідно. Тепер проведення конфігурації сервісу. Відбувається воно за допомогою python скрипта, що встановлюється разом з пакетами. Його запуск - cd /install/community-edition-setup; ./setup.py. Після цього скрипт почне задавати певні питання, для генерації SSL-сертифікатів, які додаткові сервіси мають бути встановлені тощо. Ми проведемо мінімальну інсталяцію, що буде включати в себе панель адміністратора, внутрішню базу даних та LDAP сервер. Одне з питань при встановленні - це hostname, якщо ваш сервер не має власного доменого імені, можна вказати його IP(рис.3.1).

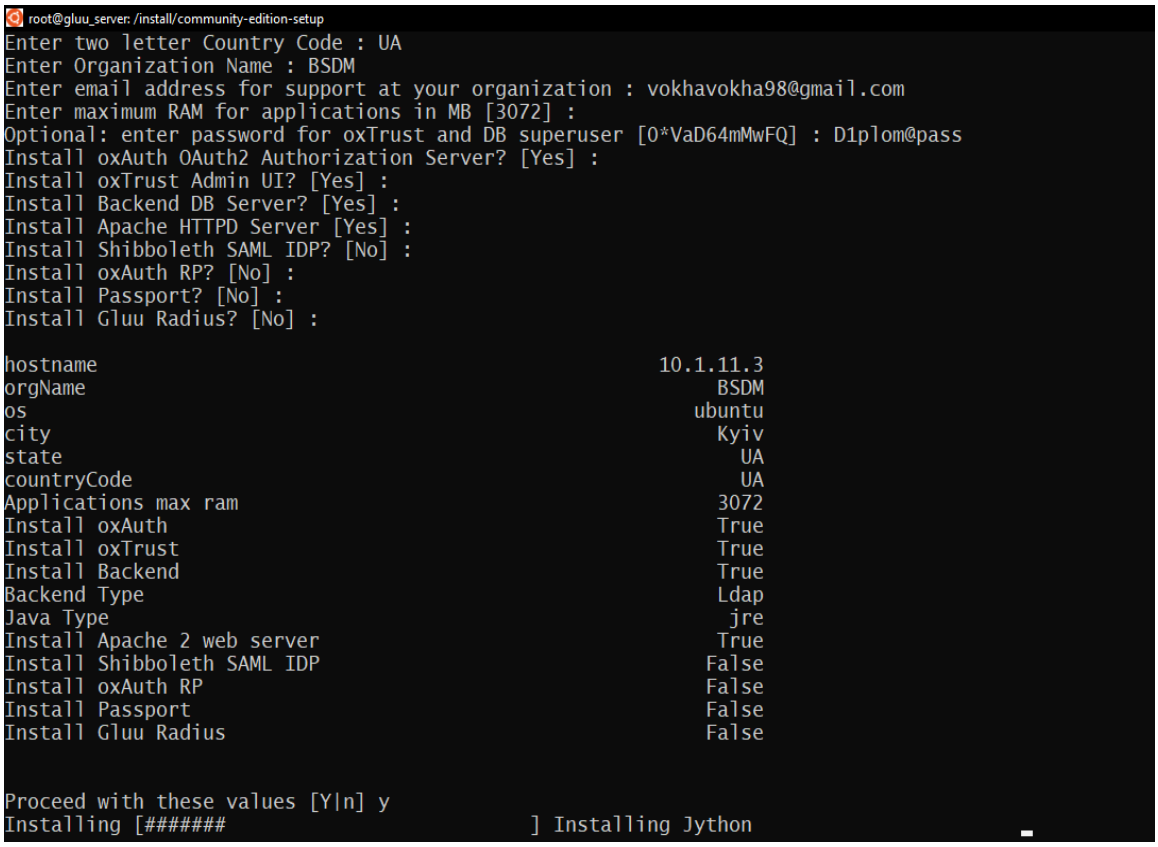


Рис.3.1. Конфігурація за допомогою скрипта.

Після відповіді на всі питання почнеться встановлення компонентів, що може тривати близько 10 хвилин. Буде проінформовано, що встановлення завершене і панель адміністратора доступна за такою-то адресою. Переходимо за нею, вводимо дані, що вказували під час конфігурації і отримуємо доступ(рис.3.2).

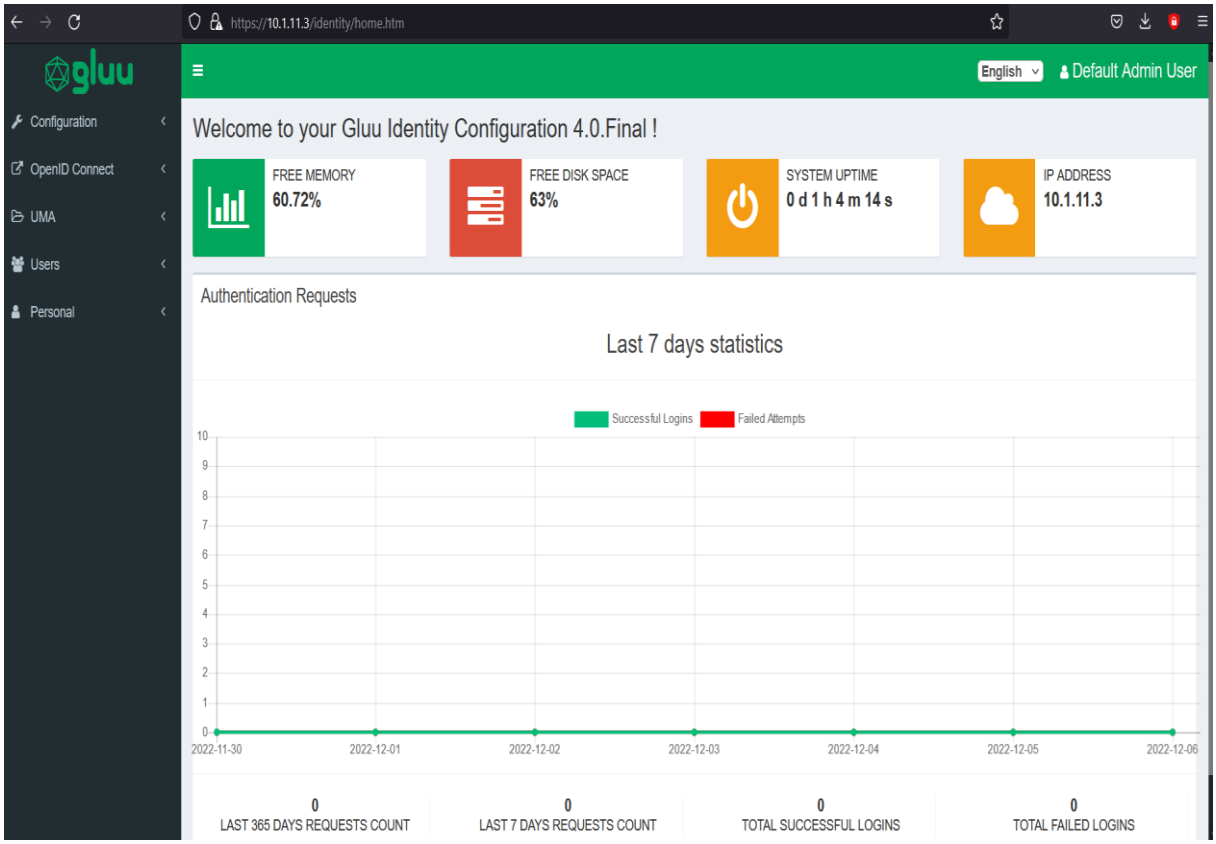


Рис.3.2. Встановлена панель адміністратора Gluu

На ній ми бачимо одразу статистику входів в систему та ресурси сервера. Основне налаштування на цьому завершено, але є певні тонкощі, які можуть спросити роботу в майбутньому. Після первинного налаштування Gluu, він має свій LDAP сервер на основі OpenDJ на порту 1636, але якщо спробувати підключитись до нього з віддаленого сервера, нічого не вийде, а проблема в тому, що слухає OpenDJ лише на localhost. Щоб мати змогу підключатись, необхідно зробити або ssh-тунель, або port-forwarding, який буде перенаправляти пакети, що приходять зовні на localhost. Використаємо другий варіант. Для його реалізації нам потрібен IPTABLES. Iptables - інструмент адміністрування для фільтрації пакетів IPv4 і NAT.

Виконаємо наступні команди:

sysctl net.ipv4.ip_forward=1

sysctl -w net.ipv4.conf.ens160.route_localnet=1

iptables -t nat -A PREROUTING -p tcp --dport 1636 -j DNAT --to-destination 127.0.0.1:1636

Якщо необхідно, щоб після перезавантаженні серверу ці налаштування залишались дійсними і не виконувати їх кожного разу в ручному режимі, треба виконати ще декілька додаткових дій.

Відкрити файл конфігурації /etc/sysctl.conf та дописати в нього раніше згадані рядки налаштувань sysctl. Після цього виконати команду sysctl -p, вона збереже ці налаштування і використає їх зараз.

Наступна дія - додаткове налаштування iptables. Для цього знадобиться пакет iptables-persistent. При перезавантаженні серверу система буде перечитувати рядки правил у файлах /etc/iptables/rules.v4. та /etc/iptables/rules.v6. Так як ми використовуємо IPv4, то вносимо наші зміни в перший файл. Тепер якщо сервер буде перезавантажено, то доступ до LDAP серверу Gluu з’явиться автоматично.

Команди sysctl дозволили системі перенаправляти пакети, а команда iptables створила правило, для розуміння які пакети і куди. Тепер ми можемо за допомогою команди telnet перевірити, що порт доступний, або під’єднатись за допомогою LDAP браузера для перевірки, що все працює(рис.3.3). Це дає змогу працювати з базою, якщо, наприклад нема доступу до oxTrust, або якщо необхідне більш детальне ознайомлення з атрибутами які мають групи чи користувачі. Також їх можна буде редагувати за необхідності. Використовувати можна будь-який браузер, що підтримує протокол LDAPS. В даному випадку - це Apache Directory Studio.

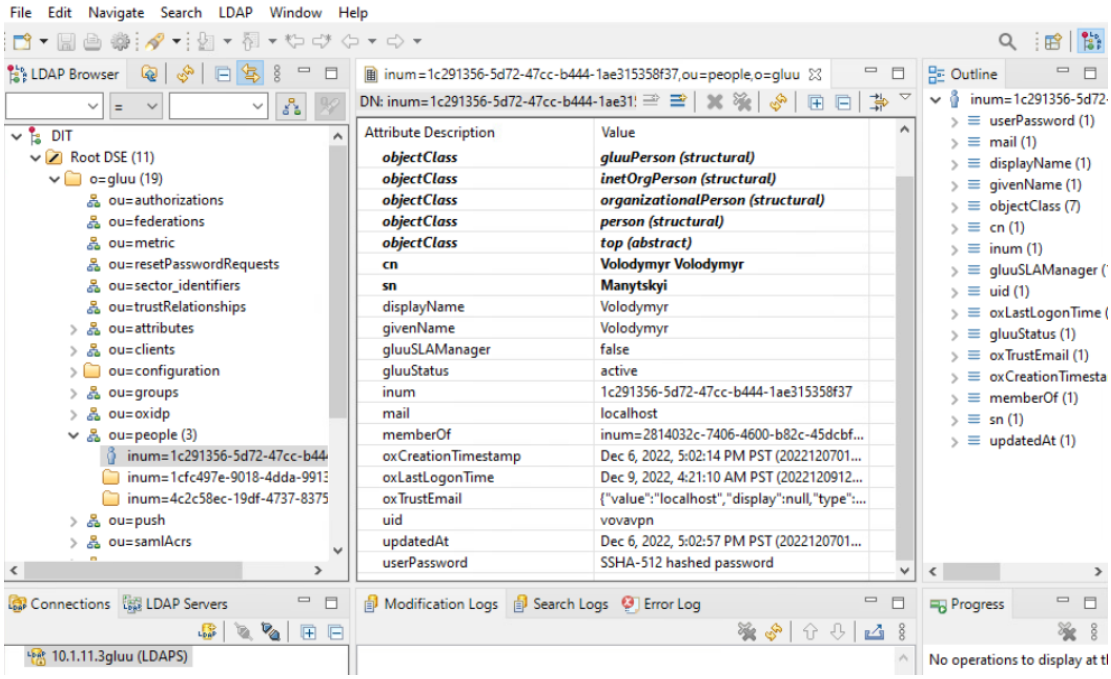


Рис.3.3. Підключення через LDAP бразуер

І ще одна важлива деталь, яку бажано налаштувати заздалегідь. Це додати атрибут для користувачів, що створюються в Gluu. Більшість сервісів саме за ним розуміє, що цей об’єкт саме користувач, а не група, папка тощо. У панелі адміністратора на вкладці Json Configuration додаємо атрибут InetOrgPerson. Тепер при створенні нових користувачів, цей параметр буде додаватись автоматично і сервіси будуть розуміти, що користувач - це користувач. За замовченням Gluu створює користувача з атрибутом gluuCustomPerson. Для впевненості забігаємо трохи наперед, та перевіряємо яких користувачів бачить Fortigate за допомогою LDAP. Стандартний користувач(admin) не мав цього атрибуту, а новий(with_org) був створений вже з ним. І якщо після підключення до серверу перейти в папку people - нам відобразиться лише користувач with_org(рис.3.4). Адже за схемою за замовчуванням тільки він зараз розглядається як коректний користувач з яким можуть проводитись певні дії для налаштування авторизації в системі. Якщо якийсь сервіс буде шукати користувачів за іншим атрибутом, його можна додати як ще один, не прибираючи старий, що дасть змогу всім необхідним сервісам знайти потрібні об’єкти.

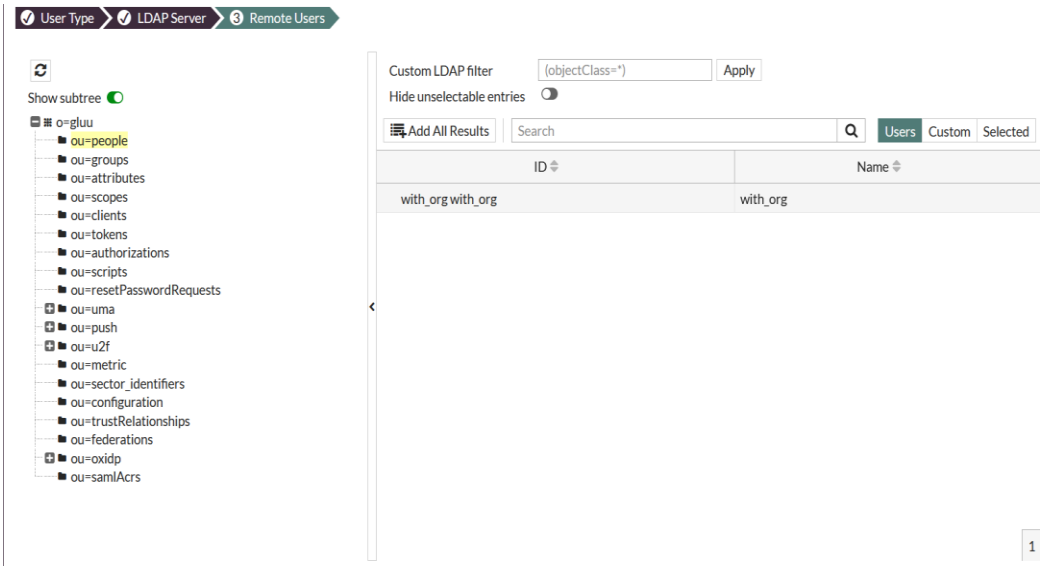


Рис.3.4. Пошук користувачів з атрибутом InetOrgPerson

Звісно можна використати Custom LDAP filter, але кожного разу це буде забирати час і заважати автоматизації.

Тепер налаштування і справді можна вважати завершеним. LDAP сервер доступний для зовнішніх сервісів, користувачі створюються з коректними атрибутами, для їх зручного пошуку. Тепер адміністратор може починати інтегрувати різні сервіси з Gluu для управління ідентифікацією та доступом користувачів до інформаційної системи організації.

3.2 Інтеграція LDAP в Gluu з Fortigate NGFW

Необхідно на конкретному прикладі розглянути можливість інтеграції продуктів з Gluu для керування ідентифікацією користувачів, їх доступами. За основу взято Fortigate NGFW і створення на ньому користувачів за допомогою LDAP серверу з подальшим використанням цих налаштувань для підключення через VPN. У звичайній схемі Fortigate має можливість створення локальних користувачів. Після цього налаштовується VPN-шлюз, створюються політики доступу, до яких додаються користувачі, яким необхідно мати доступ до віртуальної приватної мережі. В такій схемі адміністратору кожного окремого користувача необхідно додавати вручну, створюючи логін та пароль. Інтеграція з Gluu сильно спрощує цю задачу. Необхідно після підключення до LDAP серверу

просто обрати користувача, якого необхідно додати і Fortigate отримає від бази даних Gluu дані для його входу. Цей варіант буде розглянуто, але і він не найзручніший, адже адміністратору все одно необхідно буде кожного разу заходити на Fortigate і вручну додавати користувачів, які були додані на Gluu сервер, лише економлячи час на додаванні логіну і паролю.

Тому необхідно піти ще далі і налаштувати доступ за допомогою групи. Це буде працювати наступним чином. Fortigate буде мати підключену групу з LDAP серверу і постійно оновлювати дані про наявних в ній користувачів. Тобто та система до якої ми і прагнемо, керування користувачами, їх ідентифікацією буде відбуватись на стороні централізованого сервера, а саме Gluu.

Отже спочатку необхідно підключити Fortigate до LDAP серверу Gluu. Так як ми вже налаштували port forwarding на сервері, проблем виникнути не має. Заходимо до вкладки Users & Authentication > LDAP Servers та задаємо параметри підключення(рис.3.5).

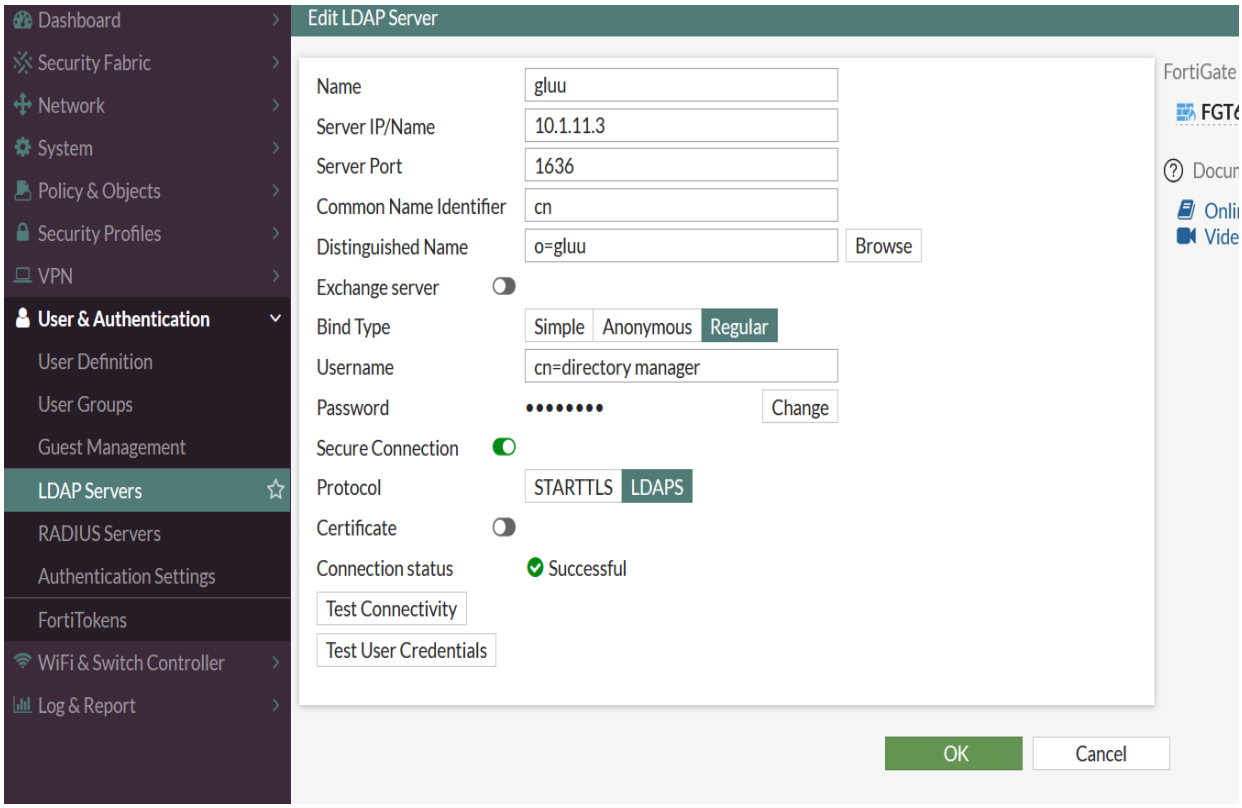


Рис.3.5. Підключення fortigate до LDAP-серверу

Так як LDAP в Gluu за замовченням працює через захищений протокол, то вмикаємо LDAPS. Також бажано змінити Common Name Identifier на uid, тоді як

логін буде використовуватись саме username. Далі необхідно натиснути Test Connectivity для розуміння, що всі дані введено вірно, та натиснути OK. Тепер зв'язок між Fortigate та LDAP сервером встановлено. Необхідно створити користувача, який буде використовувати VPN. В Gluu сервері за це відповідає вкладка User Management. Так як ми налаштовуємо авторизацію через LDAP, то саме вона для цього і потрібна. Отже, створюємо користувача з username - vovavpn, заповнюємо необхідні для реєстрації дані(рис.3.6), адже саме його необхідно буде налаштувати для доступу до мережі за допомогою VPN використовуючи сервер LDAP, як сервер централізованої авторизації.

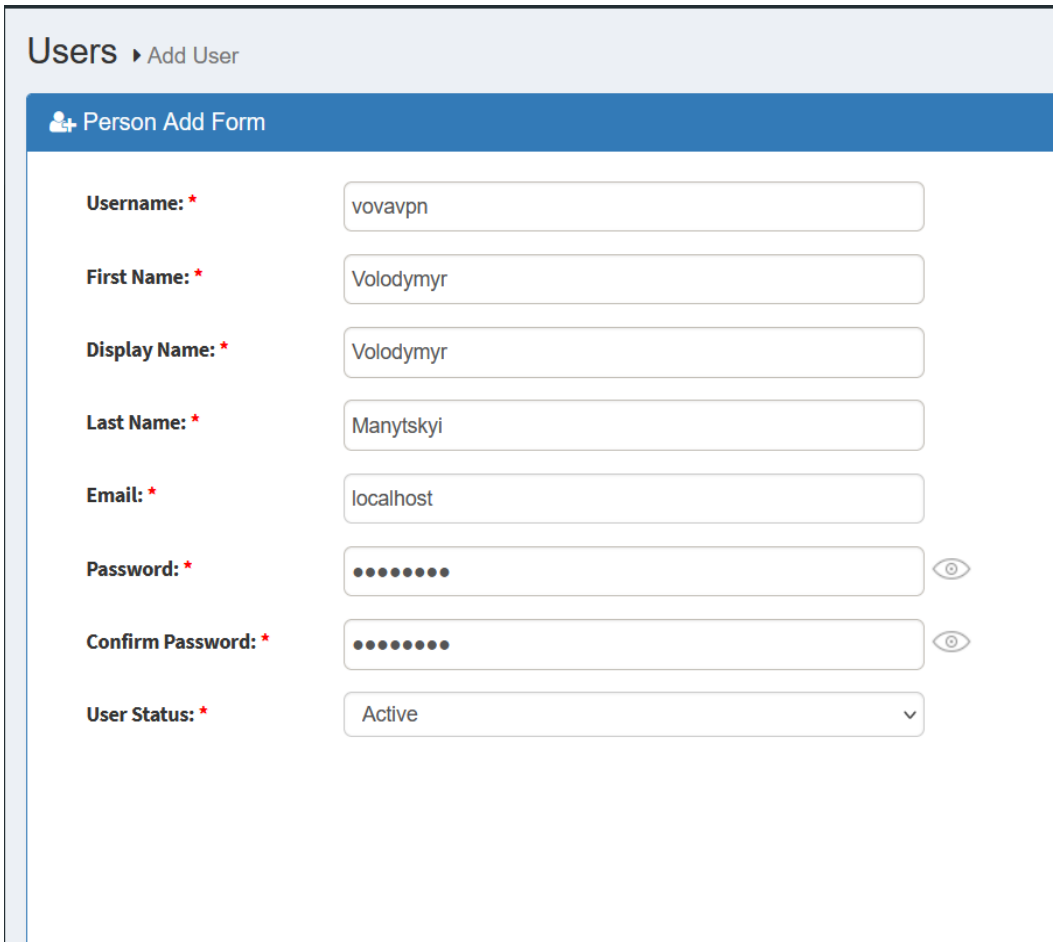


Рис.3.6. Створення користувача на Gluu сервері.

Після цього, для більш зручного керування необхідно створити групу користувачів. В даному випадку ця група буде основана на тому, для чого будуть використовуватись юзери. Назва - vpnusers і додаємо туди вже раніше створеного користувача - vovavpn(рис.3.7).

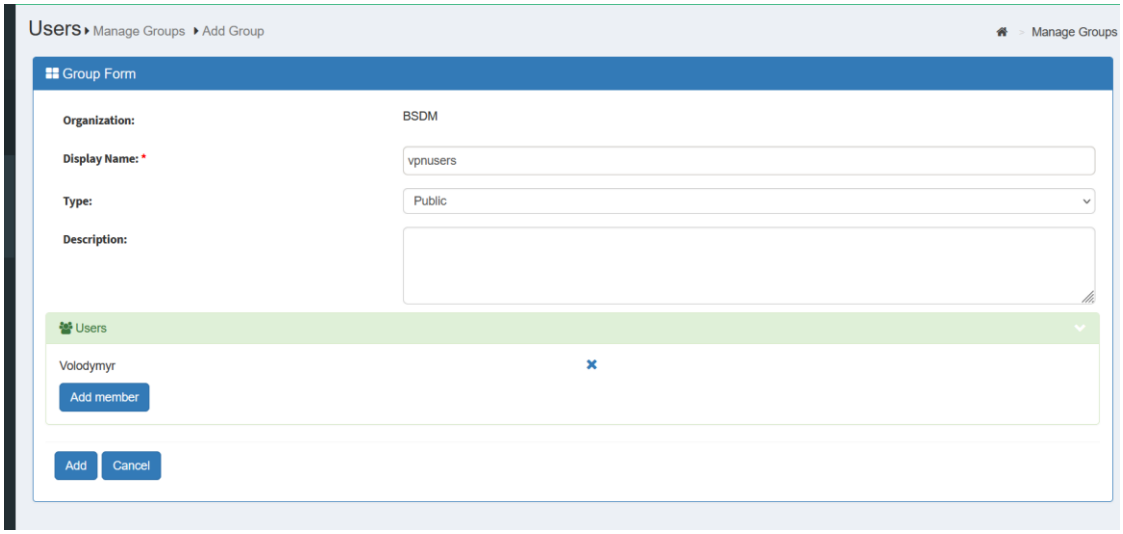


Рис.3.7. Створення групи і додавання користувача до неї

Тепер є два варіанти налаштувань на стороні Fortigate. Перший, як було згадано раніше, просто додати користувача, якого Fortigate може отримати з LDAP серверу. Це варіант не потребує особливо додаткової конфігурації і виконується простим чином. Адміністратор заходить у вкладку Users & Authentication > User Definition та починає створювати користувача, як звичайного локального, але на моменті вибору типу користувача обирає Remote LDAP User(рис.3.8)

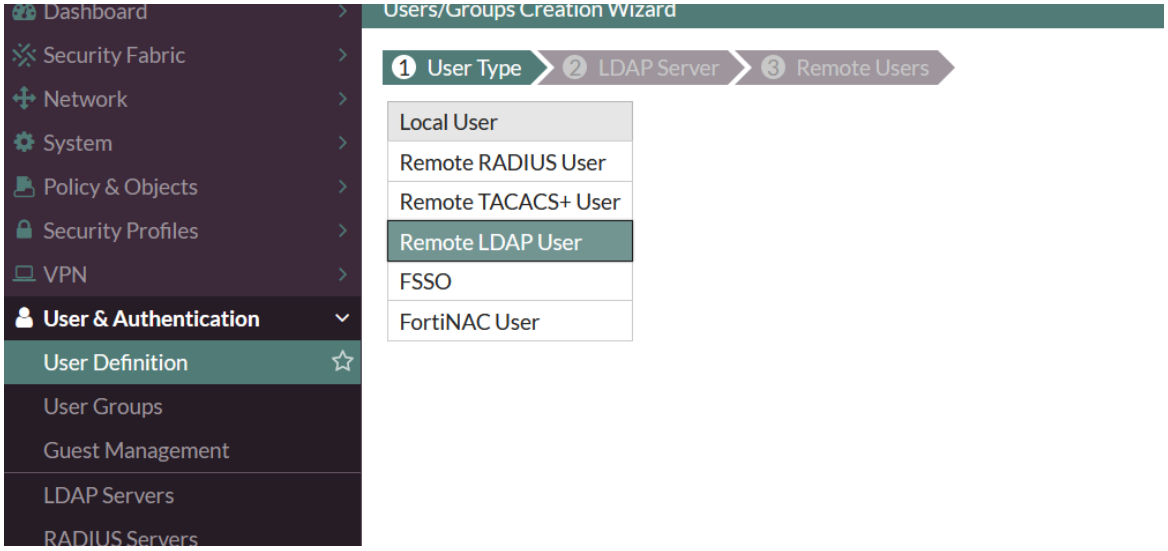


Рис.3.8. Перший етап створення користувача за допомогою LDAP

На наступній вкладці обираємо раніше створений LDAP сервер і переходимо на вкладку пошуку користувачів. Завдяки раніше доданому

атрибуту(InetOrgPerson), наш юзер одразу з’явиться в списку - vovavpn. Обираємо його і натискаємо Submit(рис.3.9).

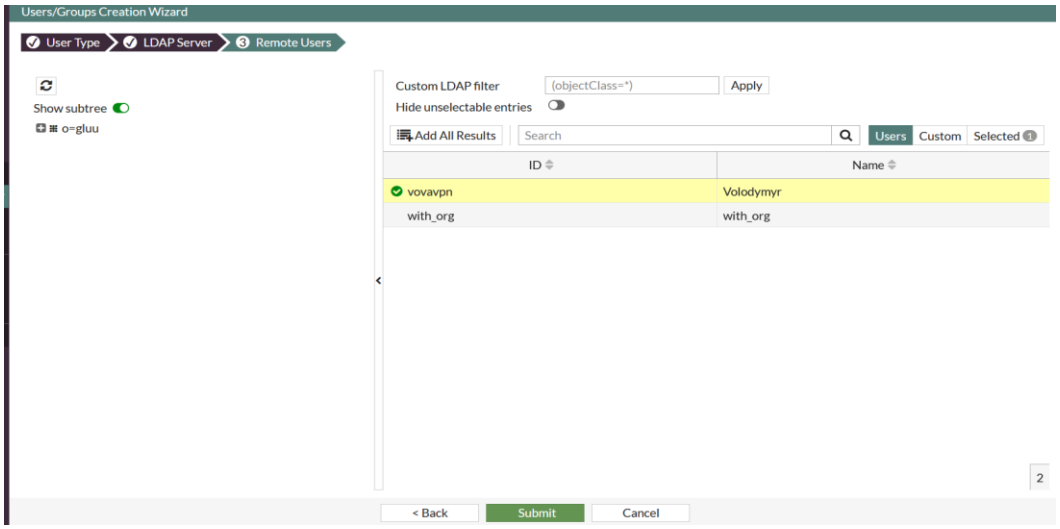


Рис.3.9. Завершення створення користувача

Описаний вище метод більш простий, але при великій кількості користувачів має свій недолік. Це витрата часу на додавання кожного користувача до систему. Тому дослідивши можливості Fortigate та Gluu був знайдений більш зручний і швидкий варіант, що допоможе зекономити час і зробити повноцінну автоматизацію. Але враховуючи певні особливості в атрибутах і схемі Gluu, цей метод потребує більш детального розгляду і додаткових налаштувань зі сторони Fortigate. Проблема полягає в тому, що при створенні користувачів і додавання їх до групи, Gluu має свій атрибут того, що такий-то користувач належить до такої групи, а також за замовчуванням fortigate має параметр перевірки того, що користувач належить до групи, такий, що не підходить для роботи в парі з Gluu. Тому необхідно налаштувати LDAP підключення зі сторони Fortigate.

Спочатку підключення самої групи до Fortigate. Для цього знову ж таки необхідно зайти у Users & Authentication, але у вкладку User Groups. Групи необхідно дати ім’я, обрати тип Firewall, а після цього у вікні Remote Groups підключити групу з Gluu серверу(рис.3.10).

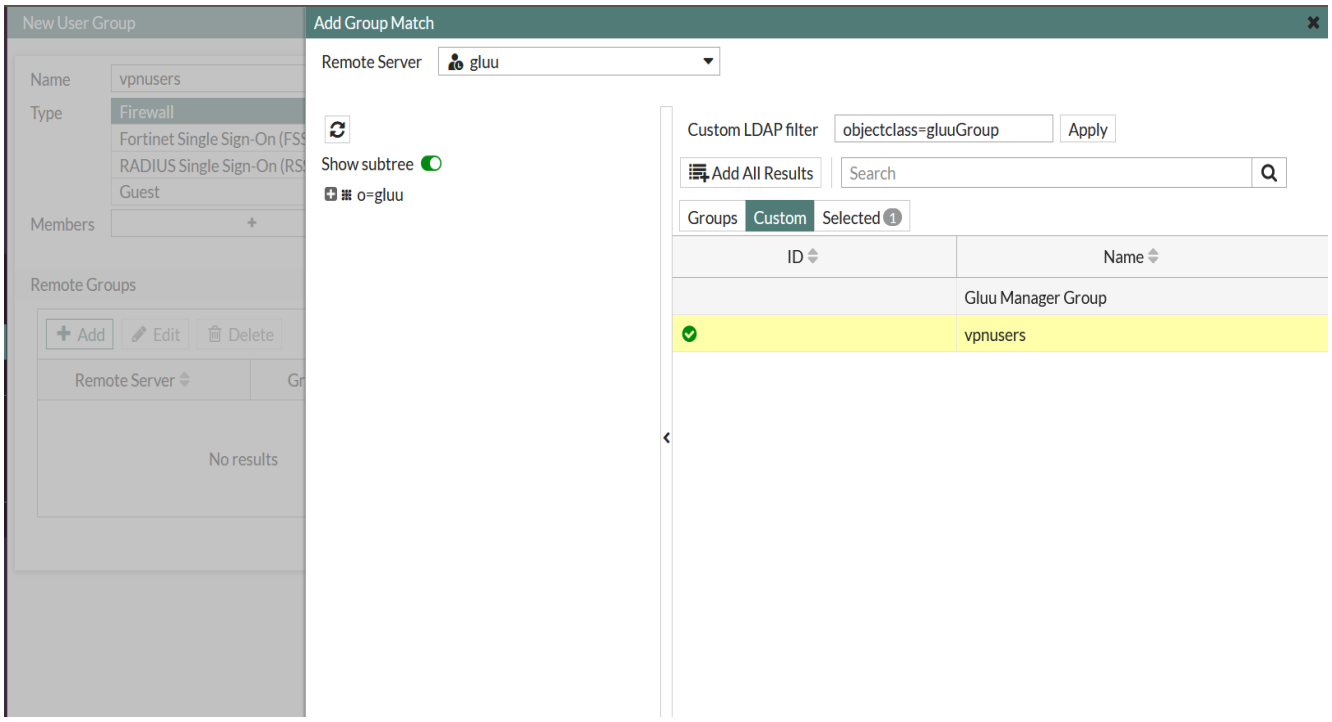


Рис.3.10. Підключення групи Gluu до Fortigate.

Також важливий нюанс, це фільтр для пошуку груп - gluuGroup. Його можна додати також в налаштуваннях через CLI як стандартний. Тепер цю групу здавалось би просто необхідно додати до політики, яка надає доступ користувачам, до ресурсів VPN. І при спробі підключення користувача, Fortigate просто буде перевіряти, чи є такий користувач у групі LDAP і у разі його наявності, надавати доступ. Але ні, якщо додати і спробувати увійти, користувач отримає ось таке вікно(рис.3.11). В ньому він побачить відмову в доступі з пропозицією перевірити налаштування. Зазвичай таке повідомлення зникає коли некоректно вказано пароль користувача або такого користувача взагалі не існує в системі. Зараз саме цей випадок, Fortigate просто не може знайти користувача і через це не надає доступ. Причина проста, але потребує додаткових змін і налаштувань.

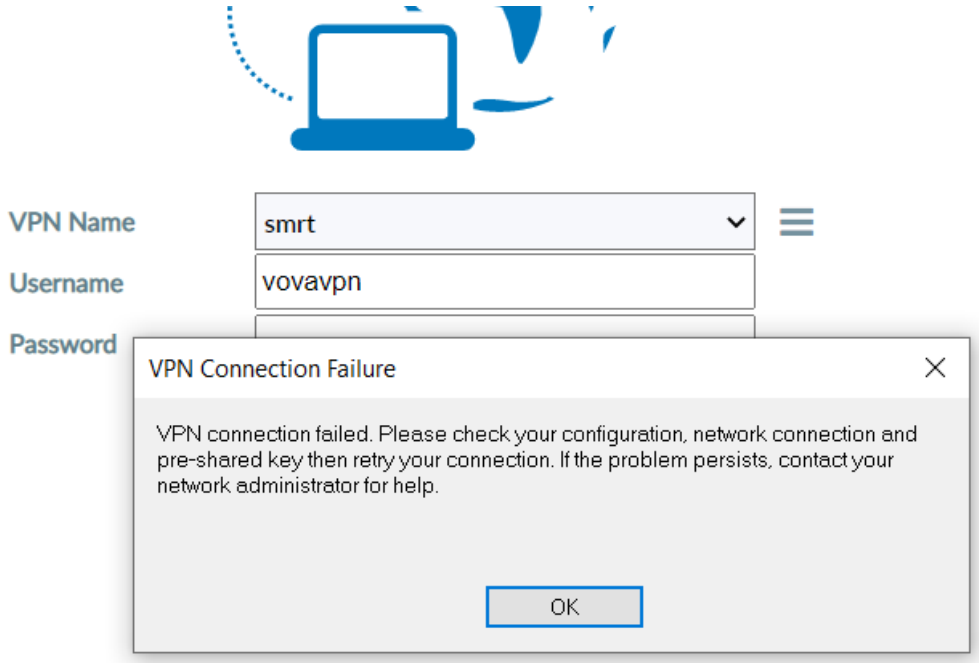


Рис.3.11. Невдала спроба підключення.

Це може стати питанням для адміністратора. Адже користувач є, його логін і пароль вірні, група додана у всі політики, але доступу все одно нема. То в чому ж все-таки проблема? Ознайомившись з можливостями налаштування LDAP зі сторони Fortigate можна знайти ось такий рядок налаштувань:

set group-member-check {user-attr | group-object | posix-group-object}

і пояснення до нього

Group member checking methods.

user-attr - User attribute checking.

group-object - Group object checking.

posix-group-object - POSIX group object checking.

І ось що це значить. За замовчуванням, використовується параметр user-attr, і він має принцип роботи, який дослівно написаний. Тобто він шукає у користувача в атрибутах рядок в якому написано, що цей користувач є членом такої групи, і далі вже звіряє дані зі свої сторони. Але через деякі особливості стандартних атрибутів у Gluu, Fortigate не може зрозуміти значення цього атрибуту і підтвердити, що користувач справді входить до групи у якої є дозвіл на доступ до системи. І найпростіший спосіб це підправити, змінити цей самий метод перевірки. Для цього

виконуємо набір команд. Спочатку заходимо на Fortigate в режим CLI, там переходимо до налаштувань LDAP серверу(Рис.3.12).

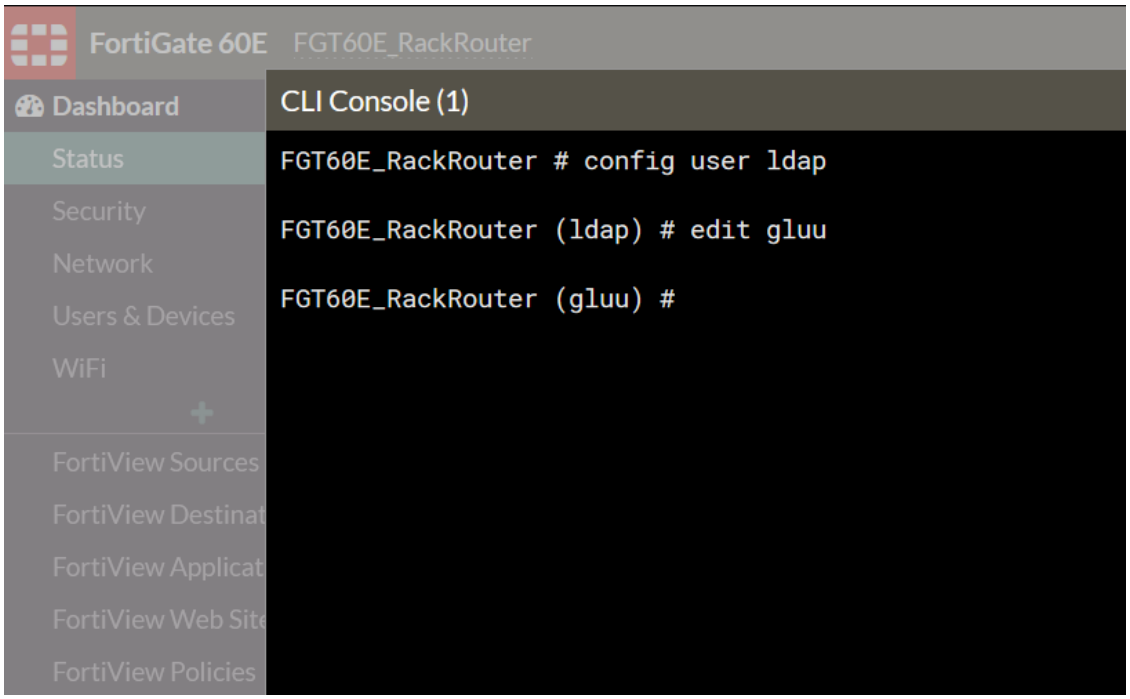


Рис.3.12. Налаштування LDAP серверу за допомогою CLI.

А далі виконаємо ці команди:

set group-member-check group-object

next

end - Щоб зберегти змінені налаштування.

За такою схемою Gluu почне працювати так, як необхідно адміністратору. Тобто, при вході користувача, він буде перевіряти чи є в потрібній групі користувач, який намагається увійти в систему і в разі позитивної відповіді надавати йому доступ до системи.

Провівши ці налаштування, спробуємо ще раз підключитись до мережі VPN компанії. Використаємо ті ж самі логін і пароль, що були створені на Gluu сервері(рис.3.13). Та почекаємо на підключення(Рис.3.14).

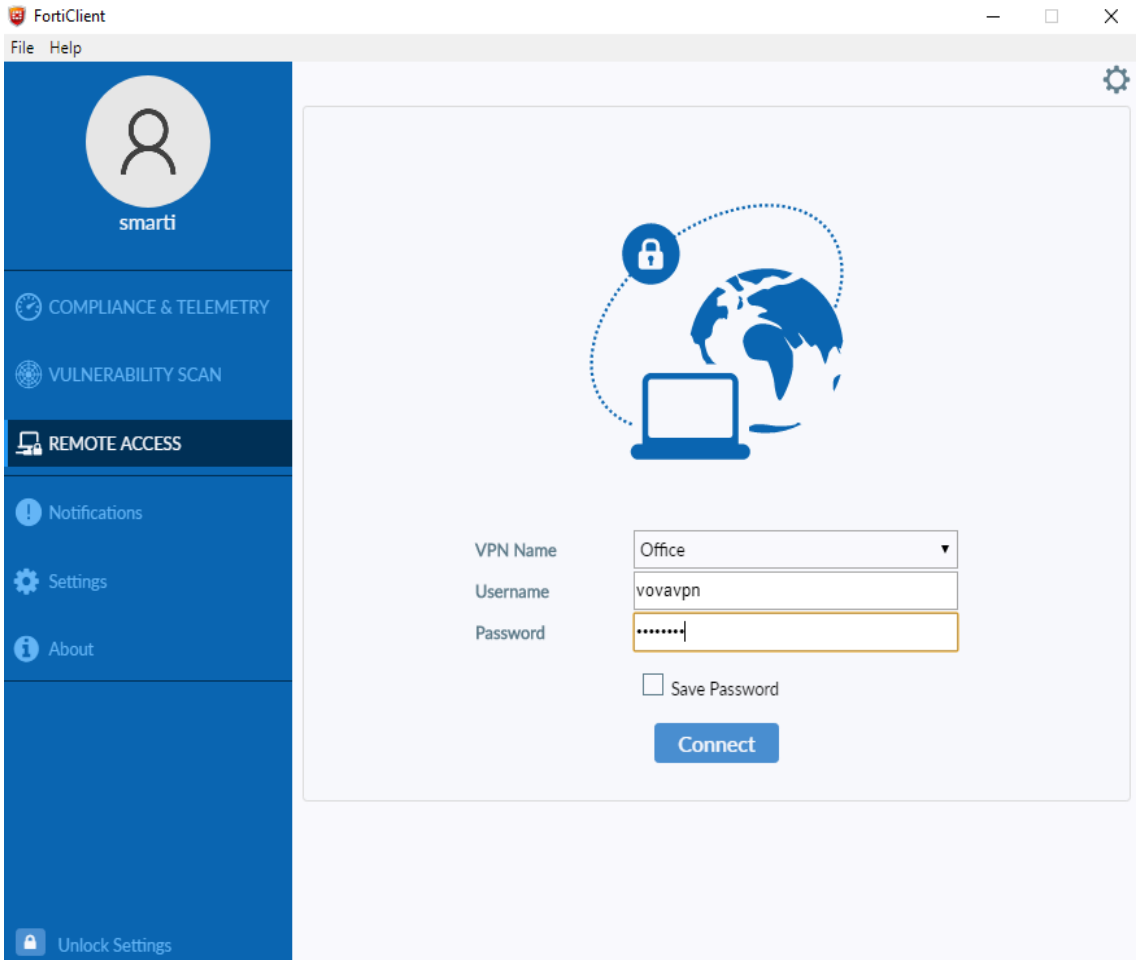


Рис.3.14. Спроба підключення після внесення змін

Рис.3.14. Успішне підключення

Тепер, після зміни методу, за допомого якого Fortigate перевіряє чи надавати користувачу доступ до системи, підключення через VPN виявилось успішним, користувач пройшов авторизацію і отримав доступ. В майбутньому, адміністратору буде достатньо додавати користувачів лише на сервері централізованої авторизації - тобто Gluu і всі вони автоматично будуть синхронізуватись із Fortigate. У випадку їх видалення чи деактивації на сервері Gluu, користувачі так само будуть ставати неактивними для вхожу на Fortigate. При спробі входу, відбуватиметься перевірка, що користувач досі є в цій групі і якщо відповідь негативна, доступ не буде надано.

Спочатку заходимо на Gluu сервер і деактивуємо користувача у вікні його налаштувань. Users > User Management > vovavpn > Inactive. Тепер користувач вимкнений в системі і його дані для входу мають бути неактивні. Цей пункт також потребує ретельної перевірки. Спробуємо підключитись за допомогою VPN знову і отримаємо відмову у доступі. Якщо поглянути в журнали Fortigate, то видно, що цього разу, користувач з таким username не був допущений до системи, адже він деактивований на сервері Gluu(Рис.3.15).

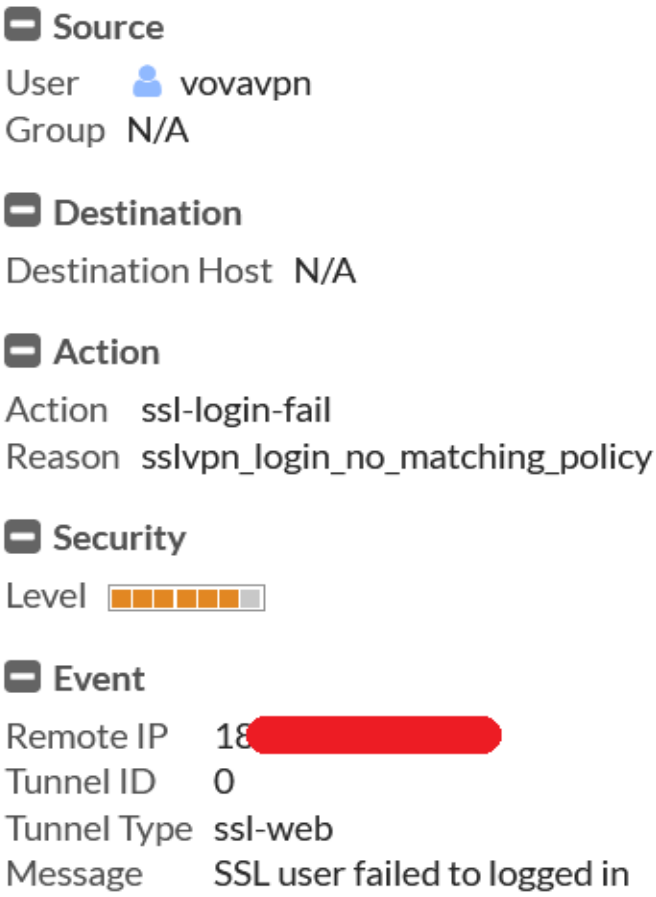


Рис.3.15. Спроба входу після деактивації

Це досить важлива частина перевірки налаштувань, адже у випадку, якщо б статус користувачів перевірявся некоректно, то при певних умовах, користувач, що вже, як приклад, не працює в компанії міг би мати доступ до мережі компанії, що становить загрозу внутрішнім даним.

За рахунок того, що Gluu підтримує протокол LDAP, він може використовуватись майже з будь-яким продуктом, адже цей протокол дуже

поширений, і велика кількість сервісів і додатків за замовчуванням підтримують авторизацію за допомогою LDAP.

3.3 Загальні рекомендації щодо застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи організації

Для того, щоб організація могла правильно розставити пріоритети при виборі продукту для управління ідентифікацією і доступом користувачів необхідно знайти основні критерії, яким він має відповідати. Також необхідно розглянути в цілому основні пункти, що мають бути враховані при розгортанні технології управління ідентифікацією та доступом користувачів до інформаційної системи організації.

1. Керування користувачами на основі ролей

Керування користувачами - це процес керування обліковими записами користувачів на рівні підприємства та за його межами. Ініціалізація користувачів включає в себе наступне:

Типи користувачів, якими керуватиме організація;

Системи, програми та інші бізнес-ресурси, до яких потрібен доступ користувачам;

Рівні доступу до цих ресурсів;

Створення, оновлення та видалення облікових записів користувачів;

Розрахунок адміністративних витрат, пов’язаних з керуванням користувачами;

Показники успіху;

Ініціалізація користувачів надає належні ресурси користувачам за мінімальних витрат. Відбувається керування робочим циклом користувача, включаючи такі речі, як створення облікових записів у різних системах в середині організації, доступ до зовнішніх служб і додатків, а також призупинення доступу або остаточне видалення облікових записів. Ефективне керування користувачами зменшує ризики безпеки, такі як слабкі паролі, і, як згадувалось раніше, керування користувачами мінімізує перешкоди для ефективної роботи користувачів. Керування користувачами також надає можливості централізованого керування та

автоматизації за допомогою створення облікових записів на основі ролей і прав доступу.

2. Управління ідентифікацією користувача

Організації можуть ідентифікувати різні типи користувачів відповідно до того, які функції вони виконують у організації, такі як: співробітники, клієнти, постачальники, партнери тощо. Кожен користувач у цих групах має окрему онлайн-ідентифікацію, якою можна ефективно керувати, щоб знизити ризики безпеки.

Набагато легше керувати ідентифікатором одного користувача в системі, ніж намагатися вслідкувати за всіма ідентифікаторами, які можуть відноситись до одного користувача.

Всередині організації IT-відділ зазвичай реалізує власні інструменти надання доступу користувачам та інтегрує їх із програмою управління. Окремі ролі користувачів повинні мати заздалегідь визначені права доступу. Коли працівник приєднується до компанії і отримує певну роль(посаду), його дозволи на доступ до ресурсів організації мають динамічно оновлюватися відповідно до налаштувань і дозволів, що були попередньо встановлені адміністраторами. Такий підхід в кінцевому підсумку знижує витрати та ефективно автоматизує процеси всередині організації.

У випадку коли організація співпрацює з клієнтом, постачальником чи партнером, необхідно, щоб процес реєстрації користувача та його взаємодії є простим, дружнім, безпечним і захищеним. Щоб користувач відчував комфорт при роботі, а також знав, що його данні надійно захищені і конфіденційні.

3. Інфраструктура каталогів

Каталоги дозволяють підприємствам групувати інформацію про співробітників у легкодоступну ієрархічну структуру. Потужність цієї архітектури дозволяє каталогам синхронізувати, копіювати та зв’язувати інформацію між сховищами інформації в нескладному розподіленому середовищі. Каталоги забезпечують надзвичайно швидкі можливості пошуку в географічно розподілених місцях.

4. Аутентифікація користувача

Організаціями бажано використовувати додаткові, надійні методи автентифікації для підтвердження ідентичності користувачів, такі як біометрія, смарт-картки та цифрові сертифікати. Звісно, це може бути запроваджене у вигляді багатофакторної аутентифікації. Спочатку користувач вводить звичайний логін та пароль, а після цього проводить додаткове підтвердження за допомогою смарт-картики. Організації можуть перевіряти інформацію, забезпечуючи при цьому конфіденційність зв'язку між компанією та користувачем, встановлюючи рівень довіри між двома сторонами.

5. Єдиний вхід(SSO) і безпечний доступ

Спрощений доступ до додатків забезпечується завдяки технології єдиного входу(SSO). Єдиний вхід позбавляє необхідності запам'ятовувати багато паролів при роботі в середині організації. Увійшовши до свого акаунту, користувач може вільно переміщатись між іншими ресурсами компанії без необхідності повторно вводити пароль, або входити до іншого облікового запису(рис.3.16). Це дуже сильно спрощує роботу і підіймає її ефективність, адже велика кількість процесів, що пов'язана з додаванням користувачів, їх керуванням автоматизується. Причому як і для самого користувача так і для працівника IT-відділу.

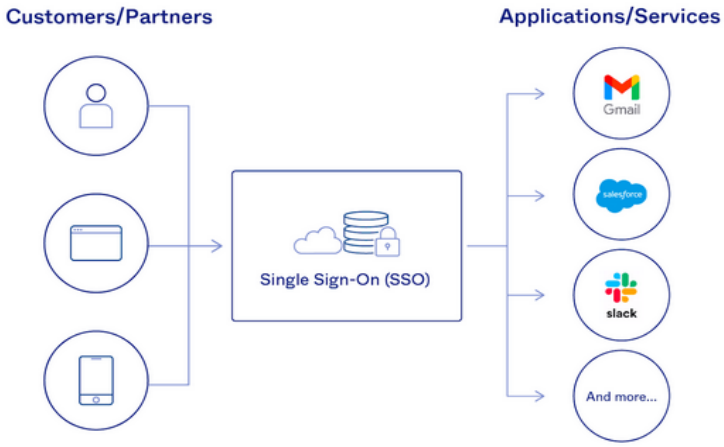


Рис.3.17. Схема входу через SSO.

6. Самореєстрація та самоуправління

Як не дивно, але краще за все про потреби користувача знає сам користувач. Самостійна реєстрація та самостійне адміністрування зменшують накладні витрати

та підвищують продуктивність користувачів, делегуючи керування користувачеві. Наприклад, користувач може самостійно зареєструватися в компанії, надіславши веб-форму. Або скидання паролів, що може забирати дорогоцінний час у відділу IT, можливість для користувачів скидати власні забуті паролі за допомогою пошти, або СМС, зменшує робоче навантаження IT-відділу та підвищує продуктивність користувачів.

7. Мобільність облікових записів

Одна з основних вимог до технології керування ідентифікацією полягає в тому, щоб облікові записи користувачів залишалися мобільними. Співробітники можуть часто їздити в робочі відрядження, подорожувати, або взагалі повністю працювати віддалено. Однак користувачам обов'язково потрібен однаковий рівень доступу, незалежно від місця підключення до мережі організації. Інфраструктура керування ідентифікацією має бути достатньо гнучкою, щоб відповідати такому типу мобільності.

Інфраструктура керування ідентифікацією також має бути відкритою та розширюваною для підтримки майбутніх служб та сервісів, та готова інтеграції з іншими бізнес-середовищами.

Найкращий спосіб протистояти проблемам керування ідентифікацією, з якими стикається більшість організацій - це централізовано керувати життєвим циклом користувача(створення, редагування, вимкнення, видалення), та забезпечувати самообслуговування користувачів у межах організації та за її межами. До речі, раніше описаний сервіс Gluu відповідає цим вимогам. Пошук системи керування ідентифікацією, яка враховує вищезазначені пункти, не тільки зробить керування ідентифікацією більш ефективною, але й забезпечить більш ефективну роботу всіх процесів в середині організації.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми використання технологій управління ідентифікацією та доступом користувачів до інформаційної системи організації, встановлена сутність завдань цього управління.

Gluu Identity and Access Management - це Open-source продукт який має багато можливостей для вирішення цієї проблеми. Підтримка всіх поширених протоколів, гнучкість налаштувань та просте встановлення і налаштування скриптів робить цей продукт дуже вдалим безкоштовним рішенням для оргранізації.

В роботі було проаналізовано вже існуючі технології управління ідентифікацією та доступом користувачів. Досліджена технологія управління ідентифікацією та доступом користувачів до інформаційної системи на основі рішення Gluu Identity and Access Management.

Встановлено основні функції і та принципи роботи продукту Gluu Identity and Access Management. Gluu - це сервіс, що реалізує технологію управління ідентифікацією та доступом користувачів. Користувацькі програми з відкритим вихідним кодом і комерційні веб та мобільні програми можуть використовувати сервер Gluu для автентифікації користувачів, ідентифікаційної інформації та налаштувань політик доступу.

Gluu за замовчуванням має власну базу і підтримку протоколу LDAP, що надає змогу інтеграції з більшістю продуктів, через поширеність цього протоколу. Також за замовчуванням цей протокол працює у захищеному режимі з використанням TLS(LDAPS).

При налаштуванні Gluu пропонує встановити підтримку RADIUS, що надає змогу використання цього протоколу для аутентифікації, авторизації та обліку сервісів беручі за основу внутрішню базу користувачів Gluu.

Gluu має підтримку функціоналу OAuth 2.0. Це схема авторизації дозволяє використовувати дані інших сервісів, наприклад, Facebook, для входу у систему без необхідності створювати додатковий акаунт.

Для використання Gluu іншими сервісами як сервісу управління ідентифікацією та доступом користувачів до інформаційної системи необхідно спочатку провести деякі додаткові налаштування для більш зручного користування і універсальності підключень.

У роботі запропоновано порядок розгортання та застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи на основі рішення Gluu. Продемонстрована можливість його інтеграції з таким продуктом як Fortigate NGFW. Також розроблено рекомендації щодо застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи організації.

Таким чином, правильна реалізація технології управління ідентифікацією та доступом користувачів до інформаційної системи організації має підвищити ефективність роботи організації, а також рівень безпеки її даних.

ПЕРЕЛІК ПОСИЛАНЬ

1. Gluu Server Documentation, Режим доступу: World Wide Web - URL - https://gluu.org/docs/gluu-server/4.0/
2. OWASP Top 10:2021, Режим доступу: World Wide Web - URL - https://owasp.org/Top10/A01_2021-Broken_Access_Control/
3. Seven tips for effective identity management, Режим доступу: World Wide Web. - URL - https://www.computerworld.com/article/2566203/seven-tips-effective-identity-management.html
4. What is Single Sign On, Режим доступу: World Wide Web. - URL - https://cloudinfrastructureservices.co.uk/what-is-single-sign-on-and-how-does-sso-work/
5. What is Azure Active Directory, Режим доступу: World Wide Web. - URL - https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis
6. LDAP, Режим доступу: World Wide Web. - URL - https://www.okta.com/identity-101/what-is-ldap/
7. RADIUS Server, Режим доступу: World Wide Web. - URL - https://www.foxpass.com/blog/radius-server-and-how-it-works
8. Local User Managment, Режим доступу: World Wide Web. - URL - https://gluu.org/docs/gluu-server/4.1/user-management/local-user-management/
9. User ldap, Режим доступу: World Wide Web. - URL - https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/15405/user-ldap
10. Account Lockout, Режим доступу: World Wide Web. - URL - https://gluu.org/docs/gluu-server/4.0/authn-guide/lockout/
11. Clustering for HA, Режим доступу: World Wide Web. - URL - https://gluu.org/docs/gluu-server/4.0/installation-guide/cluster/
12. Password Reset, Режим доступу: World Wide Web. - URL - https://gluu.org/docs/gluu-server/4.0/authn-guide/pw-reset/
13. oxTrust Admin GUI, Режим доступу: World Wide Web. - URL - https://gluu.org/docs/gluu-server/4.1/admin-guide/oxtrust-ui/

14. FIDO U2F, Режим доступу: World Wide Web. - URL - https://gluu.org/docs/gluu-server/4.1/authn-guide/U2F/

15. Gluu Server Backup, Режим доступу: World Wide Web. - URL - https://gluu.org/docs/gluu-server/4.1/operation/backup/

16. TAR command in Linux, Режим доступу: World Wide Web. - URL - https://www.geeksforgeeks.org/tar-command-linux-examples/

17. What is OTP/2FA/MFA, Режим доступу: World Wide Web. - URL - https://www.authonet.com/authentication.php

18. Gluu Server clean up, Режим доступу: World Wide Web. - URL - https://gluu.org/docs/gluu-server/4.1/operation/cleanup/

19. Fortigate viewing event logs, Режим доступу: World Wide Web. - URL - https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/536166/viewing-event-logs

20. Маницький Володимир Євгенійович. Керування ідентифікацією та доступом на базі рішення Gluu. ВСЕУКРАЇНСЬКА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ», Державний Університет Телекомунікацій. 27 жовтня 2022 р., Тези доповідей С. 154-156. https://dut.edu.ua/uploads/p_2121_20358827.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Магістерська робота
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ GLUU»

Виконав: Маницький Володимир Євгенійович

Керівник: ГАХОВ Сергій Олександрович, к.в.н., доц

2

Об'єкт дослідження – управління ідентифікацією та доступом користувачів до інформаційної системи організації на базі рішення Gluu.

Предмет дослідження – технологія управління ідентифікацією та доступом користувачів до інформаційної системи організації.

Мета роботи – розробити порядок застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи організації та рекомендації щодо його реалізації на базі Gluu

Наукові завдання:

- дослідити сутність проблеми управління ідентифікацією та доступом користувачів до інформаційної системи організації;
- встановити сутність завдання управління ідентифікацією та доступом користувачів до інформаційної системи організації;
- проаналізувати існуючі технології управління ідентифікацією та доступом користувачів до інформаційної системи організації;
- проаналізувати методи та засоби управління ідентифікацією та доступом користувачів до інформаційної системи організації;
- розкрити порядок реалізації технології управління ідентифікацією та доступом користувачів до інформаційної системи організації;

Аналіз проблеми керування користувачами в інформаційній системі організації

3

Питання проблеми керування користувачами, їх доступами не втрачає свою актуальність і навряд колись втратить. Чим більше в системі користувачів і об'єктів до яких вони мають/не мають отримувати доступ, тим більше задач постає перед адміністраторами і фахівцями з кібербезпеки. Адже важливі аспекти, це не лише зручне керування, а й безпека. Тут ці два пункти дуже тісно пов'язані, адже при налаштуванні системи керування користувачами, зручність може як бути додатковим плюсом з боку безпеки так і мінусом.

Рис.1 приклад централізованої авторизації за допомогою протоколу LDAP та AD

Як простий приклад: працівник звільнився або був звільнений, в нього був свій акаунт для VPN, пошти, RDP і внутрішніх сервісів. Після звільнення ці доступи необхідно видалити, щоб колишній співробітник не мав змоги продовжувати користуватись внутрішніми ресурсами компанії. Щоб адміністратор не заходив на кожен сервер і вручну не видаляв користувача, витрачаючи свій час і ризикуючи пропустити щось через звичайний людський фактор, існують рішення для керування ідентифікацією та доступом, звідки і ведеться керування користувачами.

На рисунку 1 зображено приклад централізованої авторизації за допомогою протоколу LDAP та AD

Що може Gluu

4

- OAuth 2.0
- OpenID Connect
- User Managed Access 2.0 (UMA)
- SAML 2.0
- System for Cross-domain Identity Management (SCIM)
- FIDO Universal 2nd Factor (U2F)
- FIDO 2.0 / WebAuthn
- Lightweight Directory Access Protocol (LDAP)
- Remote Authentication Dial-In User Service (RADIUS)

Розгортання і базове налаштування Gluu IAM

5

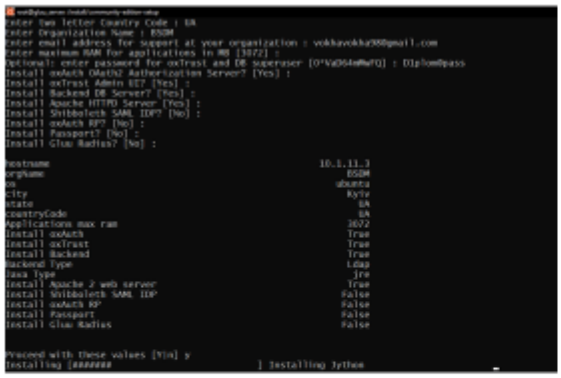
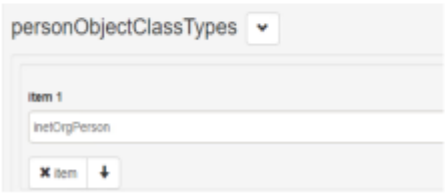


Рис. 2 Встановлення Gluu за допомогою скрипта

Рис. 3 Панель адміністратора



sysctl net.ipv4.ip_forward=1
sysctl -w net.ipv4.conf.ens160.route_localnet=1
iptables -t nat -A PREROUTING -p tcp --dport 1636 -j DNAT --to-destination 127.0.0.1:1636

Рис. 4 Додавання параметру для об'єкту користувачів у Gluu

Результат аналізу налаштувань для інтеграції Fortigate з Gluu

6

Рис. 4 Підлкючення Fortigate до Gluu

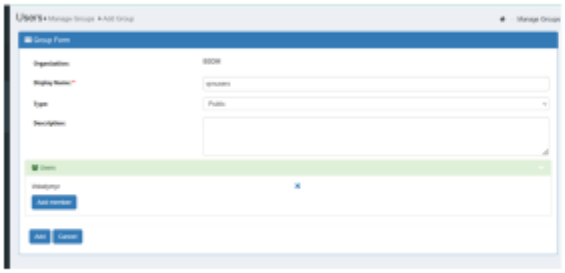


Рис. 6 Створення групи в Gluu

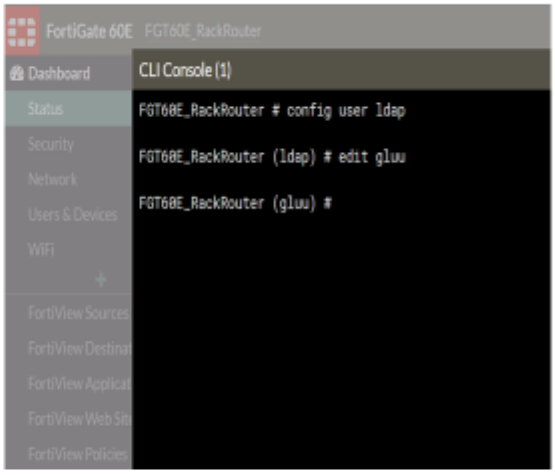


Рис. 5 Розширені налаштування LDAP

set group-member-check group-object

next
end

Робота Fortigate NGFW з Gluu 7

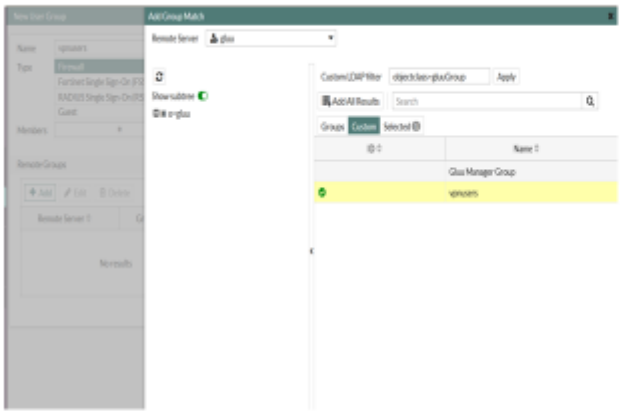


Рис. 7 Підключення Gluu групи до груп Fortigate

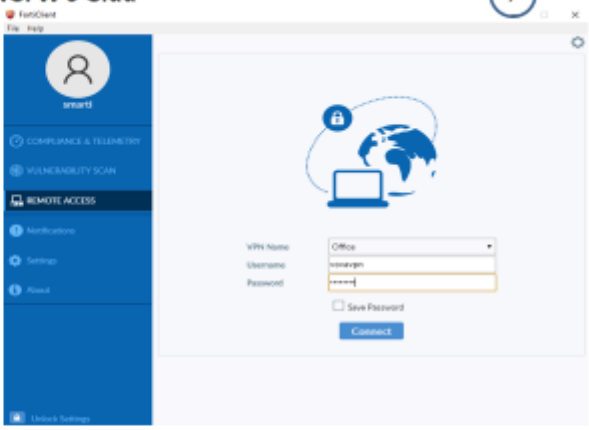


Рис. 8 Підключення до VPN

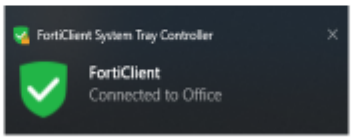


Рис. 9 Успішне підключення

Деактивація користувача в Gluu 8

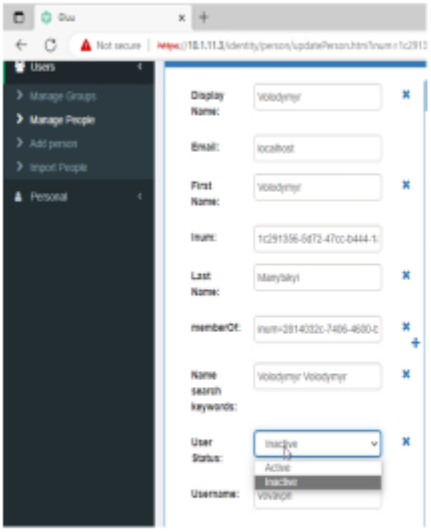


Рис. 10 Дективація Gluu користувача

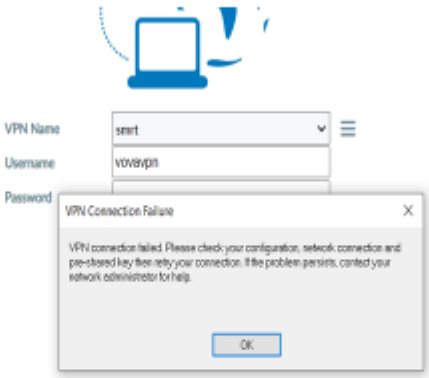


Рис. 11 Відмова в підключені

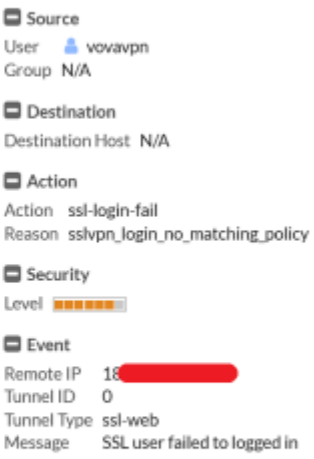


Рис. 12 Запис в логах Fortigate

Висновки

1. В роботі було проаналізовано вже існуючі технології управління ідентифікацією та доступом користувачів. Досліджена технологія управління ідентифікацією та доступом користувачів до інформаційної системи на основі рішення Gluu Identity and Access Management.
2. Встановлено основні функції і та принципи роботи продукту Gluu Identity and Access Management. Сервіс реалізує технологію управління ідентифікацією та доступом користувачів. Користувацькі програми з відкритим вихідним кодом і комерційні веб та мобільні програми можуть використовувати сервер Gluu для автентифікації користувачів, ідентифікаційної інформації та налаштувань політик доступу.
3. Gluu за замовчуванням має власну базу і підтримку протоколу LDAP, що надає змогу інтеграції з більшістю продуктів, через поширеність цього протоколу. Також за замовчуванням цей протокол працює у захищеному режимі з використанням TLS(LDAPS).
4. Для використання Gluu іншими сервісами як сервісу управління ідентифікацією та доступом користувачів до інформаційної системи необхідно спочатку провести деякі додаткові налаштування для більш зручного користування і універсальності підключень.
5. У роботі запропоновано порядок розгортання та застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи на основі рішення Gluu. Продемонстрована можливість його інтеграції з таким продуктом як Fortigate NGFW. Також розроблено рекомендації щодо застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи організації.

Апробація

1. Маницький В.Є., Всеукраїнська науково-технічна конференція «Актуальні проблеми кібербезпеки», Навчально-науковий інститут захисту інформації, 27 жовтня 2022 р., 154-156 стр.

Кінець доповіді
Дякую за увагу!