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 ACTIVE DIRECTORY»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Гребенюк В.О.
(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

MFA - Multi-Factor Authentication

SSO - Single-Sign-On

ШІ - Штучний Інтелект

IAM - Identity and Access Management

AD - Active Directory

ВСТУП

Актуальність проблеми. Централізоване управління ідентифікацією, автентифікацією та керування доступом користувачів використовується майже у всіх компаніях. Це пов’язано як з безпекою так і зі зручністю.

Управління ідентифікацією та доступом (з англ. Identity and Access Management) - це система бізнес-процесів, політик і технологій, яка полегшує управління електронною або цифровою ідентифікацією користувачів. За допомогою систем управління ідентифікацією та доступом, менеджери з інформаційних технологій можуть контролювати доступ користувачів до інформації різного ступеня критичності в своїх організаціях. Системи IAM надають можливості використання єдиного входу(Single Sign-On), багатофакторну автентифікацію та управління привілейованим доступом. Ці технології також забезпечують можливість безпечного зберігання даних про особу та профілі, а також функції управління даними, щоб гарантувати, що тільки ті дані, які є необхідними та релевантними, є доступними для спільного використання.

Системи управління ідентифікацією та доступом користувачів будуть актуальними завжди, бо кожний набір інфраструктури організації, використовуваних рішень та технологій є з схожим та унікальним в один момент і потребує власного підходу до управління ідентифікацією та доступом користувачів.

Існують як комерційні, так і Open-Source варіанти, тому до вибору IAM системи потрібно підходити вдумливо, в наш час активного розвитку, безкоштовні або умовно безкоштовні варіанти з відкритим кодом, зазвичай відрізняються більшою гнучкістю налаштування, але і в той час пропонують обмежену технічну підтримку або продукт доступний тільки без сервісної підтримки. При виборі сервісу, що буде відповідати за управління ідентифікацією та доступом користувачів в компанії треба звернути увагу на вбудований сервіс у Windows-домені під назвою Active Directory та його хмарний варіант Azure Active Directory.

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 Active Directory.

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

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;

проаналізувати основні функції та принципи реалізації 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 Active Directory, а також

розроблено рекомендації фахівцям з кібербезпеки щодо застосування технологій управління ідентифікацією та доступом користувачів.

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

1.1. Аналіз проблеми ідентифікації та управління доступом користувачів до інформаційної системи організації

У сучасному віці технологій, системи управління ідентифікацією та доступом користувачів є невід'ємною частиною бізнес-процесів, тому що керівники підприємств та IT-відділи перебувають під посиленим регуляторним та організаційним тиском щодо захисту доступу до корпоративних ресурсів і з часом цей регуляторний тиск посилюється. В результаті вони більше не можуть покладатися на ручні та схильні до помилок процеси призначення та відстеження привілеїв користувачів. Системи управління ідентифікацією та доступом користувачів(далі IAM - Identity and Access Management) автоматизує ці завдання і дозволяє здійснювати детальний контроль доступу та аудит всіх корпоративних активів у фізичних приміщеннях і в хмарному середовищі.

Системи IAM - це системи політик і технологій, що гарантують, що потрібні користувачі (які є частиною екосистеми, пов'язаної з підприємством або всередині нього) мають відповідний доступ до технологічних ресурсів. Системи управління ідентифікацією та доступом ідентифікують, автентифікують та контролюють доступ для осіб, які будуть використовувати IT-ресурси.

Цифрові ідентифікатори призначені не тільки для людей; IAM може управляти цифровими ідентифікаторами пристроїв і додатків, щоб допомогти встановити довіру.

Система IAM дозволяє IT-спеціалістам контролювати доступ користувачів до критично важливої інформації в організаціях. Продукти IAM пропонують управління доступом на основі ролей, що дозволяє системним адміністраторам регулювати доступ до систем або мереж на основі ролей окремих користувачів на підприємстві.

У цьому контексті доступ - це можливість окремого користувача виконувати певне завдання, наприклад, переглядати, створювати або модифікувати файл. Ролі визначаються відповідно до посади, повноважень та відповідальності в межах підприємства.

Системи IAM повинні виконувати наступні функції: збирати та реєструвати реєстраційні дані користувачів, керувати корпоративною базою даних ідентифікаційних даних користувачів, а також організовувати призначення та скасування привілеїв доступу.

Це означає, що системи, які використовуються для IAM, повинні забезпечувати централізовану службу каталогів з наглядом і видимістю всіх аспектів бази користувачів компанії.

Види цифрової автентифікації - за допомогою IAM підприємства можуть впроваджувати ряд методів цифрової автентифікації для підтвердження цифрової ідентичності та авторизації доступу до корпоративних ресурсів:

Унікальні паролі. Найпоширенішим типом цифрової автентифікації є унікальний пароль. Щоб зробити паролі більш безпечними, деякі організації вимагають більш довгих або складних паролів, які вимагають комбінації букв, символів і цифр. Якщо користувачі не можуть автоматично збирати свою колекцію паролів за єдиною точкою входу в систему, вони, як правило, вважають, що запам'ятовування унікальних паролів є обтяжливим.

Попередньо відкритий ключ (PSK). PSK - це ще один тип цифрової автентифікації, де пароль є спільним для користувачів, які мають доступ до одних і тих же ресурсів - уявіть собі пароль до Wi-Fi у філії. Цей тип автентифікації менш безпечний, ніж індивідуальні паролі.

Поведінкова автентифікація. При роботі з високочутливою інформацією та системами організації можуть використовувати поведінкову автентифікацію, щоб отримати набагато більш детальну інформацію та проаналізувати динаміку натискання клавіш або характеристики використання миші. Застосовуючи штучний інтелект, тренд в системах IAM, організації можуть швидко розпізнати, якщо поведінка користувача або машини виходить за рамки норми, і можуть

автоматично заблокувати системи.

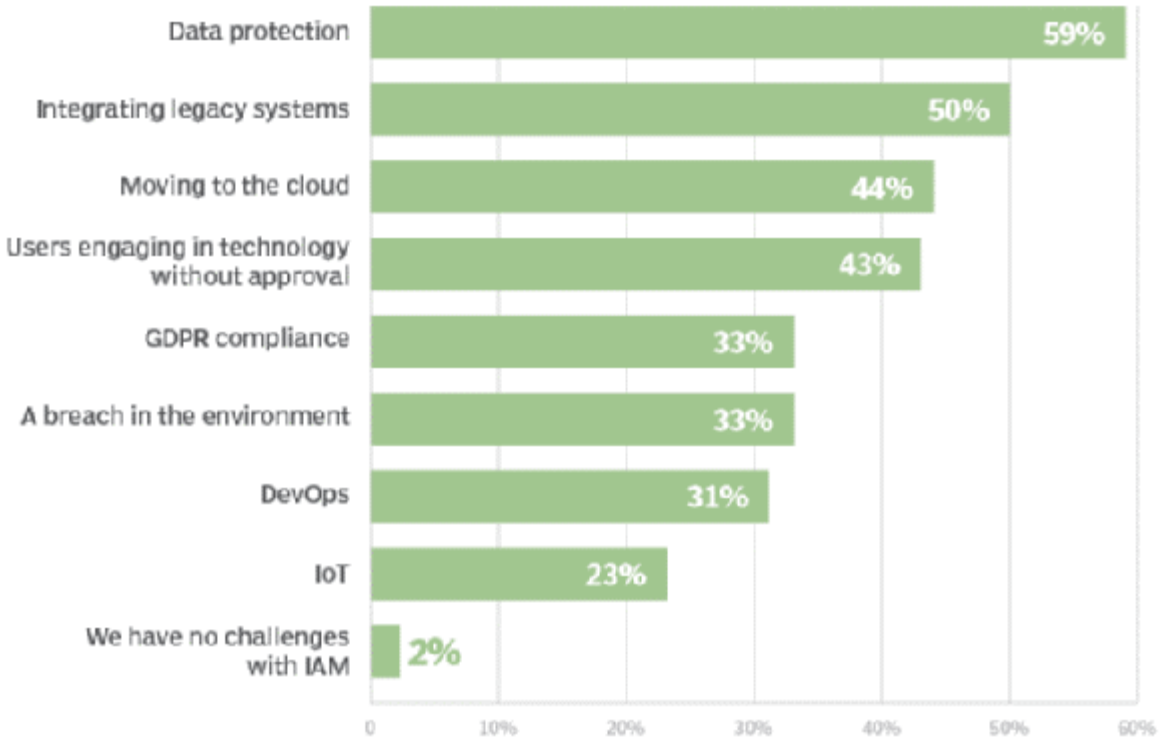


Рис.1.1. Основні вектори захисту за допомогою систем IAM

При зборі та використанні біометричних характеристик компанії повинні враховувати етику в наступних сферах:

безпека даних (доступ, використання та зберігання біометричних даних);

прозорість (впровадження легкого для розуміння розкриття інформації);

необов'язковість (надання клієнтам можливості вибору - приєднатися або відмовитися);

конфіденційність біометричних даних (розуміння того, що є приватними даними, та наявність правил щодо обміну ними з партнерами).

Рис.1.2. Можливості та функції IAM систем

Як кіберзлочинці компрометують привілейовані облікові записи?

Шлях до компрометації привілейованого облікового запису часто відбувається за наступною схемою:

Компрометація локального облікового запису. Злочинні хакери використовують шкідливе програмне забезпечення або соціальну інженерію, щоб отримати доступ до настільних комп'ютерів, ноутбуків або серверів. Співробітники обманюються фішинговими атаками, які виглядають як законні запити від

менеджера, керівника компанії або іншого довіреного джерела. Вони можуть несвідомо натиснути на шкідливе посилання, завантажити програмне забезпечення з прихованим шкідливим програмним забезпеченням або ввести свої облікові дані на фальшивих веб-сайтах.

Захоплення привілейованого облікового запису. Основна мета зловмисника - отримати привілейований обліковий запис (наприклад, локальний обліковий запис адміністратора Windows) для переміщення. Після того, як пароль співробітника перехоплений, зловмисник може увійти в мережу і просто обійти багато традиційних засобів контролю IT-безпеки, оскільки він виглядає як користувач з законними повноваженнями. Поширені методи включають атаки типу "людина посередині" або "передача хешу" для підвищення привілеїв.

Сховатися і спостерігати. Досвідчені злочинні хакери терплячі, вважаючи за краще залишатися непоміченими, ніж зламувати і прориватися. Після того, як зловмисники виявляють пролом, вони зазвичай використовують скомпрометовані привілейовані облікові записи для проведення розвідки і вивчення звичайних процедур роботи IT-команд. Це включає спостереження за регулярними розкладами, заходами безпеки та потоком мережевого трафіку. Вони використовують ці спостереження для того, щоб влитися в мережу і переконатися, що вони не викликають жодних сигналів тривоги мережевої безпеки. Зрештою, вони можуть отримати точну картину всієї мережі та її роботи.

Видавати себе за співробітників. Зловмисник, який має доступ до привілейованого облікового запису, може видавати себе за довіреного співробітника або систему і, таким чином, може здійснювати шкідливу діяльність, не будучи виявленим як зловмисник. Коли зловмисники компрометують привілейований обліковий запис, вони можуть діяти непоміченими протягом тижнів або місяців. Оскільки скомпрометований привілейований обліковий запис здається законним користувачем, дуже важко знайти першопричину або провести цифрову криміналістичну експертизу, коли порушення в кінцевому підсумку буде виявлено.

Встановлення постійного доступу. Наступним кроком зловмисника часто є

встановлення постійного доступу шляхом встановлення інструментів віддаленого доступу, що дозволяє йому повернутися в будь-який час і виконати зловмисні дії, не викликаючи тривоги.

Заподіяння шкоди. Залежно від мотиву зловмисників, вони можуть використовувати привілейовані облікові записи для таких дій, як:

пошкодити функції системи або відключити доступ IT-адміністратора;

викрасти конфіденційні дані для шахрайства або нанесення шкоди репутації;

впровадити шкідливий код;

отруїти дані.

Після того, як ви відчуєте переваги системи управління привілейованим доступом, важливо підтримувати її в ідеальному стані та планувати постійні вдосконалення.

Аудит та аналіз активності привілейованих облікових записів. Поєднання аудиту та аналітики може знизити ризик використання привілейованих облікових записів. Аудит привілейованих облікових записів дає вам метрики, які надають керівникам життєво важливу інформацію для прийняття більш обґрунтованих рішень, а також демонструють відповідність політикам і правилам.

Продовження виявлення привілейованих облікових записів. Впровадьте процес і автоматизовані інструменти для постійного виявлення нових привілейованих облікових записів і змін облікових записів, зроблених у вашій мережі. Це єдиний практичний спосіб підтримувати видимість і контроль, необхідні для захисту ваших критично важливих інформаційних активів.

Запобігання розростанню. Автоматизоване управління службовими обліковими записами запобігає розростанню службових облікових записів, керуючи життєвим циклом службових облікових записів від надання до виведення з експлуатації.

Інтеграція PAM з іншими IT-системами та системами безпеки. Інтегруйте PAM з іншими системами безпеки та IT-системами організації для реалізації стратегії глибокого захисту. Інтеграція PAM як частини більш широкої категорії управління ідентифікацією та доступом (IAM) забезпечує автоматизований

контроль над забезпеченням користувачів разом з кращими практиками безпеки для захисту всіх ідентифікаційних даних користувачів. Безпека PAM також повинна бути інтегрована з рішеннями з управління інформацією та подіями безпеки (SIEM). Це забезпечує більш повну картину подій безпеки, пов'язаних з привілейованими обліковими записами, і дає вашим співробітникам служби IT-безпеки краще зрозуміти проблеми безпеки, які необхідно виправити, або ті, які вимагають додаткового аналізу.

PAM також може бути використаний для поліпшення розуміння оцінки вразливостей, сканування інвентаризації IT-мережі, безпеки віртуального середовища, а також адміністрування та аналізу поведінки. Приділяючи особливу увагу безпеці привілейованих облікових записів, ви можете посилити всю свою кібербезпеку, щоб захистити свою організацію найбільш ефективним і дієвим способом.

Розширення існуючих каталогів, таких як Active Directory, на Unix/Linux. Збільшення видимості локальних і привілейованих користувачів і облікових записів в різних операційних системах і платформах для спрощення управління і звітності.

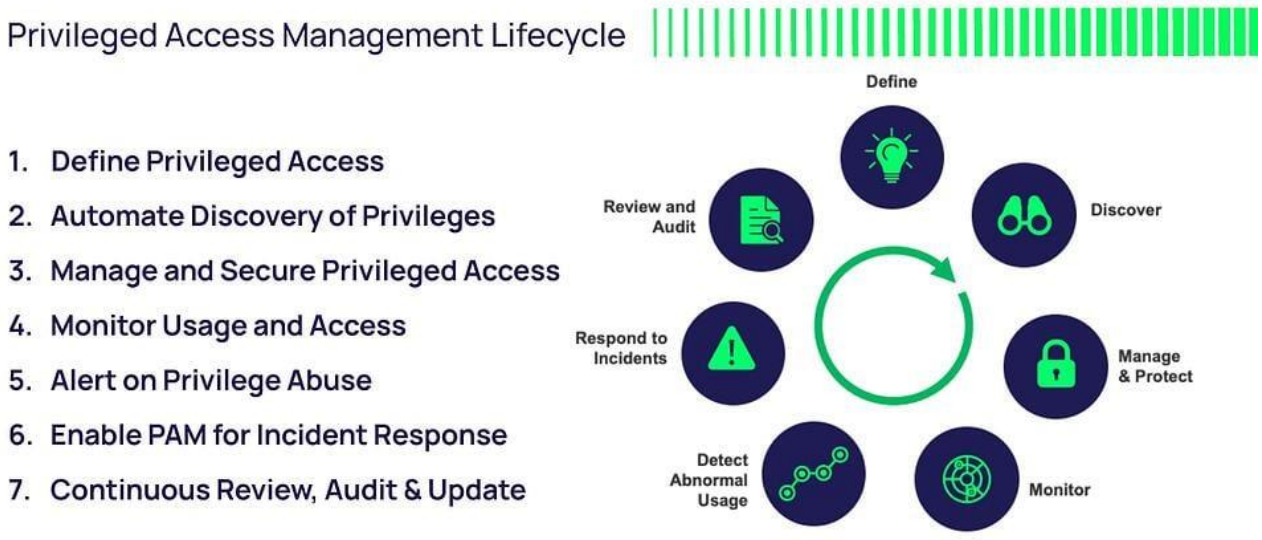


Рис.1.3. Життєвий процес PAM

1.2. Аналіз основних засобів управління ідентифікацією та доступом користувачів в інформаційній системі організації

Інновацій навколо IAM багато, і підприємства є бенефіціарами нових стратегій, які підкріплені продуктами і функціями.

Багато нових технологій IAM призначені для зменшення ризиків шляхом зберігання інформації, що ідентифікує особу, у власника цієї інформації, а не розподіленої між базами даних, вразливими до зломів і крадіжок.

Легко подумати, що поліпшення безпеки - це просто акт нагромадження більшої кількості процесів безпеки, але, як писали штатний автор Шерон Шей і експерт Рендалл Гембі, безпека "полягає в тому, щоб продемонструвати, що ці процеси і технології дійсно забезпечують більш безпечне середовище".

IAM відповідає цьому стандарту, дотримуючись принципу найменших привілеїв, коли користувачеві надаються тільки ті права доступу, які необхідні для виконання його робочих обов'язків, і розподілу обов'язків, коли одна людина ніколи не відповідає за кожне завдання. Завдяки поєднанню попередньо визначеного контролю доступу та контролю доступу в режимі реального часу, IAM дозволяє організаціям виконувати свої регуляторні, ризик-менеджмент та compliance мандати.

Сучасні технології IAM здатні підтвердити відповідність організації критично важливим вимогам, включаючи HIPAA, Закон Сарбейнса-Окслі, Закон про права на сімейну освіту та конфіденційність, а також керівні принципи NIST та інші.

Сучасні інструменти управління ідентифікацією та доступом допомагають фахівцям з IT-безпеки централізовано керувати доступом до всіх додатків і файлів для співробітників, клієнтів, партнерів та інших авторизованих груп. Таке управління, що забезпечується IAM, масштабується по всій корпоративній інфраструктурі, включаючи корпоративну локальну мережу, бездротову локальну мережу, глобальну мережу, і навіть в публічні і приватні хмари і точки присутності периферійних обчислень. У багатьох випадках IAM є обов'язковим для ресурсів, які підпадають під регуляторні правила.

Два базових принципа, які мають бути імплементовані для безпечного доступу до цифрових активів.

IAM підтверджує, що користувач, програмне або апаратне забезпечення є тим, за кого себе видає, шляхом перевірки його облікових даних у базі даних. Хмарні інструменти ідентифікації IAM є більш безпечними та гнучкими, ніж традиційні рішення з використанням імен користувачів та паролів.

Системи управління доступом на основі ідентифікаційних даних надають лише відповідний рівень доступу. Замість того, щоб використовувати ім'я користувача та пароль для доступу до всього програмного забезпечення, IAM дозволяє розділити доступ на вузькі сегменти, наприклад, редактор, глядач та коментатор в системі управління контентом.

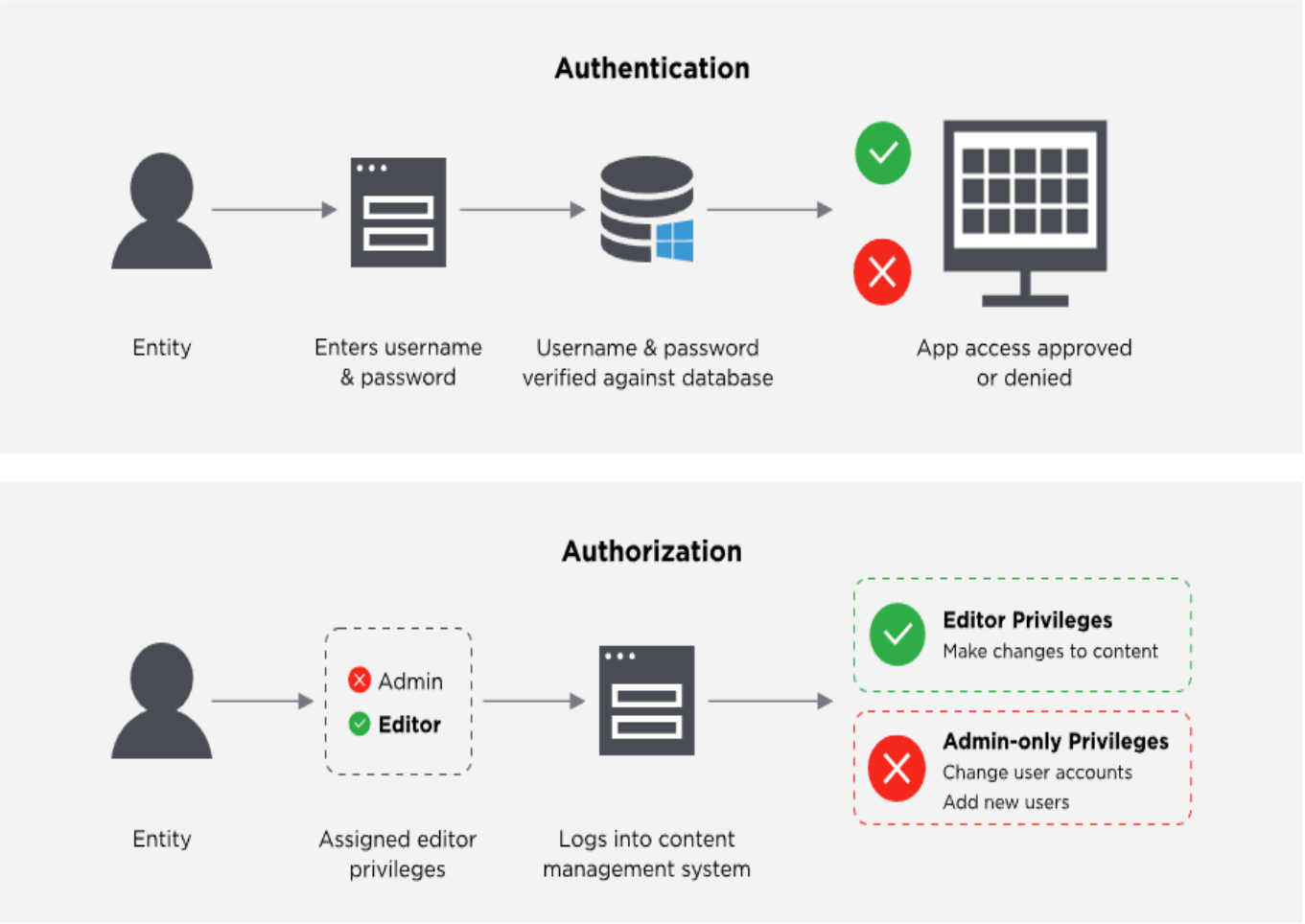


Рис. 1.4. процес авторизації та аутентифікації

Основні інструменти управління ідентифікацією та доступом користувачів є широкоохоплюючими та взаємодоповнюючими.

Налаштування користувачів - ці інструменти спрощують процес створення облікового запису користувача та призначення ролей авторизації, які визначають, до яких ресурсів користувач може отримати доступ.

Централізоване управління доступом - незалежно від того, де знаходяться додатки та дані, IAM централізує управління цими ресурсами, щоб адміністратори могли уніфіковано керувати контролем доступу та авторизацією по всій інфраструктурі.

Єдиний вхід (SSO) - це низка процесів, які дозволяють користувачам один раз пройти автентифікацію через централізований портал, а потім отримати повний доступ до ресурсів, на які вони мають право, без необхідності проходити додаткові етапи автентифікації. Це досягається шляхом передачі єдиної наданої автентифікації від системи до системи за необхідності.

Багатофакторна автентифікація (MFA) - це використання більш ніж одного методу для автентифікації користувача або пристрою. MFA забезпечує кращу гарантію того, що автентифікатори є тими, за кого вони себе видають.

Відповідність/контроль за діяльністю користувачів - це дозволяє організації скористатися можливостями IAM для захисту та виявлення ризиків діяльності, пов'язаних з конфіденційністю та захистом даних, які підпадають під суворі регуляторні правила відповідності.

Управління ідентифікацією - це підхід, заснований на політиці, передбачений багатьма регуляторними правилами відповідності, який вимагає від платформи демонстрації того, що вона управляє ідентифікацією та доступом належним чином відповідно до конкретних вимог відповідності.

Керована безпека - у міру зростання компаній одна з найбільших проблем пов'язана з підтримкою масштабованої системи автентифікації та контролю доступу. Платформи IAM досягають цього на централізованій платформі, якою набагато простіше керувати в порівнянні з розрізненою автентифікацією і контролем доступу на основі кожного додатка або пристрою.

Сервіс порталу доступу - для великих організацій портал самообслуговування може заощадити величезну кількість людино-годин. Співробітники та клієнти можуть використовувати портали для самореєстрації, скидання паролів, управління профілями, запитів на доступ та інших подібних завдань.

API - хоча більшість платформ IAM забезпечують попередньо створені інтеграції з сотнями або тисячами сторонніх додатків для аутентифікації та надання доступу, деякі компанії використовують застарілі або створені на замовлення додатки, які вимагають трохи більше роботи. У цих випадках API може створити користувальницький інтерфейс, щоб дозволити додатку аутентифікувати і контролювати доступ за допомогою IAM. Потім шлюз API перенаправляє всі виклики API до внутрішньої системи IAM, щоб вона могла належним чином ідентифікувати користувачів та надавати/забороняти доступ.

Аналітика ризиків - деякі платформи IAM збирають дані про автентифікацію користувачів та поведінку ідентифікаторів доступу з плином часу. Крім того, збираються відповідні дані, включаючи місце доступу кінцевого користувача, час доби і тип бажаного доступу. Використовуючи ШІ, IAM може використовувати цю базову інформацію для виявлення аномалій в поведінці користувачів, які можуть вказувати на зловживання або атаки. Тригери можуть бути налаштовані для попередження адміністраторів безпеки або для повного блокування доступу, поки IT-персонал не завершить подальші розслідування.

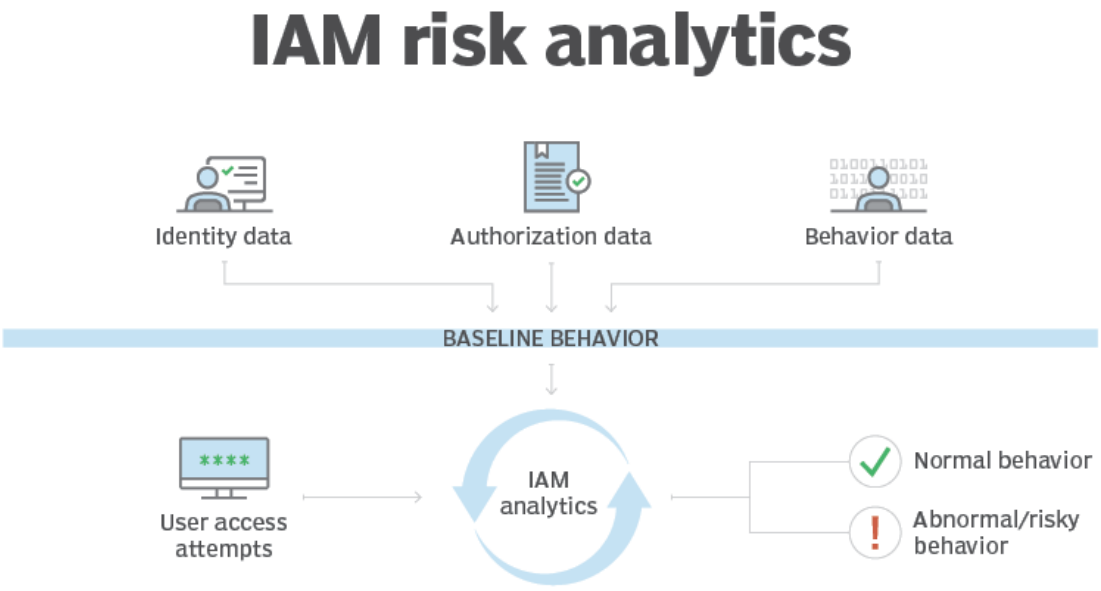


Рис.1.5. Аналіз поведінки користувача

Не менш важливим аспектом використання IAM систем є стратегії їх впровадження. Як наріжний камінь архітектури нульової довіри, рішення IAM повинно бути реалізовано з використанням принципів нульової довіри, таких як доступ з найменшими привілеями та політики безпеки на основі ідентифікаційних даних.

Централізоване управління ідентифікацією - ключовим принципом нульової довіри є управління доступом до ресурсів на рівні ідентифікаційних даних, тому централізоване управління цими ідентифікаційними даними може значно спростити цей підхід. Це може означати міграцію користувачів з інших систем або, принаймні, синхронізацію вашого IAM з іншими каталогами користувачів у вашому середовищі, наприклад, з каталогом відділу кадрів.

Безпечний доступ - оскільки захист на рівні ідентичності є ключовим, IAM повинен переконатися, що він підтверджує ідентичність тих, хто входить в систему. Це може означати впровадження MFA або комбінації MFA і адаптивної автентифікації, щоб мати можливість враховувати контекст спроби входу: місце розташування, час, пристрій і т.д.

Контроль на основі політик - користувачам слід надавати повноваження лише для виконання необхідних завдань і не більше привілеїв, ніж це необхідно.

IAM повинна бути спроектована таким чином, щоб надавати користувачам доступ до ресурсів на основі їх посадових обов'язків, підрозділу або будь-яких інших атрибутів, які здаються доцільними. Як частина централізованого рішення для ідентифікації, ці політики можуть забезпечити безпеку ресурсів незалежно від того, звідки здійснюється доступ до них.

Політика нульової довіри - політика нульової довіри означає, що рішення IAM організації постійно контролює і захищає ідентифікаційні дані користувачів і точки доступу. У минулому організації працювали за принципом "як тільки ви увійшли, у вас є доступ", але політика нульової довіри гарантує, що кожен член організації постійно ідентифікується і його доступ знаходиться під управлінням.

Захищені привілейовані облікові записи - не всі облікові записи в системі управління доступом створені рівними. Обліковим записам зі спеціальними інструментами або привілейованим доступом до конфіденційної інформації може бути наданий рівень безпеки та підтримки, який відповідає їх статусу в організації.

Навчання та підтримка - провайдери IAM проводять навчання для користувачів, які будуть найбільш активно працювати з продуктом, включаючи користувачів і адміністраторів, і часто надають послуги з обслуговування клієнтів для забезпечення довгострокової працездатності вашої установки IAM і її користувачів.

Очікується, що система IAM зможе інтегруватися з багатьма різними системами. Через це існують певні стандарти або технології, які повинні підтримувати всі системи IAM: Security Access Markup Language, OpenID Connect та Система управління міждоменною ідентифікацією.

Мова розмітки доступу до безпеки (Security Access Markup Language, SAML) - це відкритий стандарт, який використовується для обміну інформацією про автентифікацію та авторизацію між системою постачальника ідентифікаційних даних, такою як IAM, та сервісом або додатком. Це найбільш часто використовуваний метод для IAM, щоб надати користувачеві можливість входу в додаток, який був інтегрований з платформою IAM.

OpenID Connect (OIDC) - це новий відкритий стандарт, який також дозволяє користувачам входити в свій додаток від постачальника ідентифікаційних даних. Він дуже схожий на SAML, але побудований на стандартах OAuth 2.0 і використовує JSON для передачі даних замість XML, який використовується в SAML.

Система управління міждоменною ідентифікацією (SCIM) - це стандарт, який використовується для автоматичного обміну ідентифікаційною інформацією між двома системами. Хоча і SAML, і OIDC можуть передавати ідентифікаційну інформацію додатку під час процесу автентифікації, SCIM використовується для підтримання інформації про користувача в актуальному стані щоразу, коли нові користувачі призначаються до служби або додатку, оновлюються дані користувача або видаляються користувачі. SCIM є ключовим компонентом забезпечення користувачів у просторі IAM.

Не менш важливим є відповідність регуляторним стандартам та нормам. IAM система повинна забезпечувати наступні контролі у організації:

унікальні ID - унікальні ідентифікатори для кожного користувача у системі;

механізми ідентифікації користувачів та систем, до яких вони мають доступ;

опис процесу авторизації та рівнів доступу, які були надані користувачу;

процес створення, модифікації та видалення аккаунтів та їх доступів і облікових даних;

опис критеріїв для видалення неактивних аккаунтів після визначеного часу неактивності;

можливість відкликання прав у акаунтів у випадках необхідності(звільнення, зміна посади, компрометація аккаунту);

управління привілейованими обліковими записами, визначення критеріїв для надання доступу до привілейованих облікових записів або їх створення для працівників організації;

визначення критеріїв для надання віддаленого доступу до ресурсів організації;

розділення обов’язків та створення правил для надання лише необхідних

доступів;

визначення критеріїв для надання доступу до ресурсів організації авторизованими вендорами;

визначення критеріїв та факторів автентифікації, успішне проходження яких надає право доступу до ресурсів організації;

процес для забезпечення завершеності процесу автентифікації до того як буде надано будь-який доступ до ресурсів організації;

процес управління паролями.

IAM controls for compliance

IAM CONTROL	DESCRIPTION
General requirements	Address access to systems and data, access privileges based on role and assignment of access privileges
Unique access IDs	Assign a unique ID to each user
Assignment of accounts	Mechanism to identify users and the resources they have access to
Access approvals	Define the process for authorizing access and the level(s) of access granted
Management of accounts	Addresses creation, modification and deletion of accounts and associated credentials
Access review and recertification	Processes for reviewing and updating user accounts based on role changes and other criteria
Inactive accounts	Criteria for deleting inactive accounts after a specific period of inactivity
Access revocation and disablement	Address changes in access privileges due to change in access needs, employee terminations or identification of compromised accounts
Privileged account management	Defines criteria for assigning privileged accounts and IDs
Remote access by administrators	Defines criteria for remote administrative access to systems and resources
Segregation of duties	Sets rules to ensure segregation of duties when assigning access privileges
Vendor access to resources	Defines criteria for assigning access to authorized vendors accessing system resources
Access authentication	Assigns criteria for granting permission to system resources through a series of authentication factors
User validation	Process to ensure user authentication is established before any transactions are performed
Password management	Addresses criteria for creating passwords
Authentication of mobile devices	Establishes access criteria for mobile devices
Access to voicemail	Defines criteria for access to voicemail accounts
User session management	Establishes criteria for termination of a session after a defined period of inactivity and criteria for multiple concurrent sessions by a user
Notification of system use	Criteria for displaying a visual message delineating access data prior to granting session access
Remote access	Establishes criteria for granting remote access to system resources
Data protection access	Governs access to data and resources that are considered mission-critical to the organization
Identification and validation of devices	Criteria for identifying all devices before connecting to system resources
Policies and procedures	Approved documents that specify how the organization ensures the confidentiality, integrity and availability of information

Рис.1.6. Основні регуляторні правила, які потребуються від системи IAM

Використання IAM систем є дуже необхідним для побудови та забезпечення процесу захищеності інформаційних ресурсів підприємства. Відповідно до OWASP TOP - 10 2021, де вектор атаки на контроль доступу є найпоширенішим, до поширених вразливостей контролю доступу відносяться: Контроль доступу забезпечує дотримання політики таким чином, щоб користувачі не могли діяти поза межами наданих їм дозволів. Збої, як правило, призводять до несанкціонованого розкриття інформації, модифікації або знищення всіх даних або виконання бізнес-функцій за межами дозволених користувачеві повноважень. До поширених вразливостей контролю доступу відносяться:

порушення принципу найменших привілеїв або заборони за замовчуванням, коли доступ повинен надаватися тільки для певних можливостей, ролей або користувачів, але надається будь-кому;

обхід перевірок контролю доступу шляхом модифікації URL-адреси (підміна параметрів або примусовий перегляд), внутрішнього стану додатку або HTML-сторінки, або за допомогою інструменту атаки, що модифікує запити API;

дозвіл на перегляд або редагування чужого облікового запису, шляхом надання його унікального ідентифікатора (незахищені прямі посилання на об'єкти);

доступ до API з відсутніми елементами управління доступом для POST, PUT та DELETE;

підвищення привілеїв. Виконання дій від імені користувача без авторизації або від імені адміністратора при авторизації від імені користувача;

маніпуляції з метаданими, такі як відтворення або підробка токену контролю доступу JSON Web Token (JWT), куки або прихованого поля, маніпуляції з метою підвищення привілеїв або зловживання недійсністю JWT;

неправильна конфігурація CORS потенційно призводить як до отримання несанкціонованого доступу до внутрішніх ресурсів, так і до викрадення даних сесій користувача

примусовий перегляд аутентифікованих сторінок від імені неавторизованого користувача або привілейованих сторінок від імені стандартного користувача.

Відповідно, OWASP приводить також список можливих заходів для

дотримання процедури безпечного контролю за доступом користувачів. Ці процедури включають в себе:

контроль доступу - він ефективний тільки в довіреному серверному коді або безсерверному API, де зловмисник не може змінити перевірку контролю доступу або метадані;

заборона доступу за замовчуванням, окрім публічних ресурсів;

впровадження механізмів контролю один раз і їх повторне використання у всьому додатку, включаючи правильну конфігурацію з використанням Cross-Origin Resource Sharing (CORS);

моделі контролю доступу повинні забезпечувати право власності на записи, а не допускати, що користувач може створювати, читати, оновлювати або видаляти будь-який запис;

відключення лістинг каталогів веб-серверів та забезпечення відсутності метаданих файлів (наприклад, .git) та файлів резервних копій у кореневих каталогах веб-серверів;

реєстрування збоїв контролю доступу, сповіщення адміністраторів, коли це доречно (наприклад, повторні збої);

обмеження доступу до API та контролерів, щоб мінімізувати шкоду від автоматизованих інструментів атак;

ідентифікатори сеансів повинні бути анульовані на сервері після виходу з системи. Токени JWT без статусу повинні бути скоріше короткоживучими, щоб звести до мінімуму вікно можливостей для зловмисника. Для довготривалих JWT настійно рекомендується дотримуватися стандартів OAuth для відкликання доступу;

механізми захисту від атак типу переповнення буферу.

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

Існує дуже багато IAM систем, як комерційних так і open-source. Серед комерційних рішень одними з найвідоміших є рішення IBM, Microsoft, Okta,

OneLogin, Oracle та інші.

Наприклад, IBM пропонує хмарну IAM - продукт на основі принципу SaaS(software-as-a-service) який працює майже з усіма платформами - на землі, в хмарі та їх гібридні варіанти. Також їх система пропонує інструменти для управління ідентифікацією та привілейованим доступом додатково до можливостей використання MFA та SSO.

Продукт добре працює як для додатків, орієнтованих на співробітників, так і на клієнтів. Оскільки IBM добре обізнана в галузі штучного інтелекту, великих даних та глибокої аналітики, Cloud IAM включає ці передові функції в продукт, що допомагає автоматизувати модифікацію контролів/лімітів доступу користувачів та ідентифікувати аномальні або ризиковані рівні доступу.

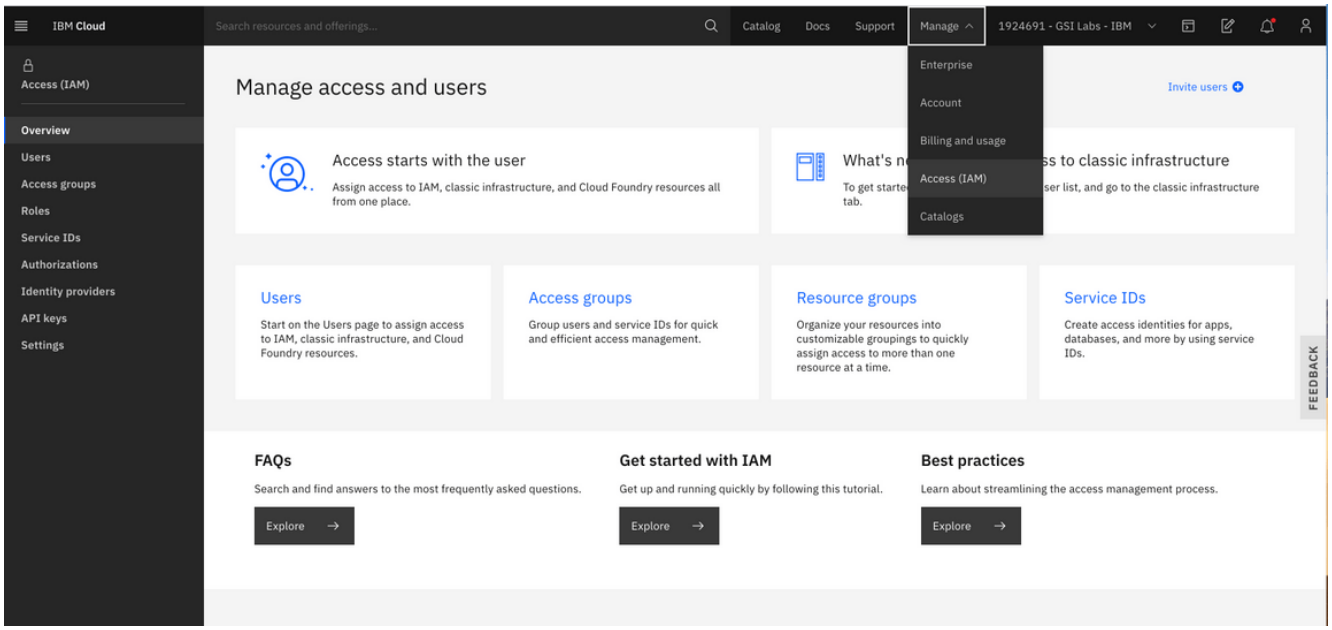


Рис.1.7. Вигляд консолі IBM Cloud IAM

Компанія "Окта", постачальник послуг "чистої гри", вважається піонером на ринку IAM на основі SaaS. Як нейтральна до постачальників платформа, вона може добре функціонувати незалежно від типів використовуваних базових інфраструктурних технологій. Хоча Okta найбільш відома завдяки IAM для клієнтів, вона будує міцну ринкову базу IAM для персоналу, а також для корпоративних хмарних та гібридних хмарних середовищ. Універсальний каталог користувачів/груп/пристроїв Okta може отримувати дані з декількох джерел каталогів.

Платформа також включає в себе Okta Access Gateway, додаток для безпечної аутентифікації користувачів і надання доступу до локальних додатків без необхідності віддаленого доступу через VPN-з'єднання.

Нарешті, функція Okta ThreatInsight блокує відомі зловмисні IP-адреси, які намагаються вкрасти облікові дані, одночасно обмежуючи швидкість інших джерел для запобігання розподіленим атакам на відмову в обслуговуванні.

Як ще один постачальник чистих послуг, Ping Identity добре відомий в сфері IAM і є першопрохідцем в SSO і MFA. Насправді, широко відомо, що Ping - єдиний постачальник, з яким компанія Microsoft співпрацює, щоб запропонувати використання служб ідентифікації в рамках пропозиції Microsoft Azure AD Premium. Ping Identity доступний в декількох різних пакетних пропозиціях, в залежності від того, чи потрібні компанії послуги IAM для внутрішніх співробітників, зовнішніх клієнтів або їх комбінації.

Ping також пропонує кілька корисних коінтегрованих систем під ключ для компаній, які мають специфічні потреби в IAM. Деякі приклади платформ під ключ включають IAM для Microsoft AD Federation Services, AWS, Google Cloud, Zscaler Internet Access і Zoom.

Незалежно від того, чи є середовище локальним, гібридним хмарним або повністю SaaS, RSA SecurID Suite є хорошим універсальним вибором, оскільки платформа пропонує гнучкі варіанти розгортання. Це особливо актуально, якщо підприємству необхідна гнучкість MFA. Цей продукт також включає в себе всі необхідні функції для великих організацій.

Програма RSA Ready - це технологічний партнерський портал, який дозволяє стороннім постачальникам програмного забезпечення пропонувати інтеграцію своїх продуктів в SecurID Suite. Наразі в програмі беруть участь понад 500 партнерів з більш ніж 1 000 сертифікованих RSA інтеграцій.

Також слід пам'ятати, що RSA є дочірньою компанією Dell EMC. Таким чином, для підприємств, які вже мають значні інвестиції в інші технології Dell EMC або RSA, вибір RSA SecurID Suite має сенс з точки зору інтеграції та підтримки.

SailPoint - ще один провайдер IAM в чистому вигляді. Це також одна з

найменших компаній в цьому списку. Проте, те, чого їй не вистачає у розмірі, вона компенсує функціональністю IAM та загальною гнучкістю для роботи в рамках будь-якої архітектури підприємства. Компанія стверджує, що її платформа IdentityIQ дозволяє підприємствам підключати в середньому до 99% всіх поточних додатків і даних за допомогою спрощених майстрів інтеграції та попередньо налаштованих робочих процесів.

Ще одна важлива деталь полягає в тому, що клієнти можуть відокремити основні функції IAM від своїх більш просунутих аналітичних компонентів, керованих штучним інтелектом. ШІ-частина продукту відома як Predictive Identity. Клієнти можуть придбати Predictive Identity і негайно інтегрувати його з іншими частинами IdentityIQ, або ж додати цю можливість пізніше або взагалі не додавати її.

Це чудова модель для тих компаній, які в даний час не мають власного персоналу для належного управління аналітичною частиною продукту, але бажають включити її колись у майбутньому.

На початку 2019 року Centrify виділила свій IAM-бізнес в окрему компанію Idaptive, яка через рік була придбана компанією CyberArk і ребрендована в CyberArk Workforce Identity. Цей продукт пропонує платформу IAM на основі SaaS, використовує структуру нульової довіри в якості основи і доступний для хмарних, локальних або мобільних додатків і послуг.

CyberArk Workforce Identity добре інтегрується з існуючими сховищами ідентифікаційних даних, які вже можуть мати багато малих і великих організацій, включаючи Microsoft Active Directory (AD), Lightweight Directory Access Protocol (LDAP) і Google Workspace. Крім того, платформа використовує форму MFA з підтримкою штучного інтелекту, відому як адаптивна MFA. Це дозволяє клієнтам використовувати кілька методів вторинної автентифікації, а також ШІ для моніторингу та потенційного блокування доступу до критично важливих додатків за допомогою методів, заснованих на поведінці.

Цей варіант також відрізняється чітко розробленою інформаційною панеллю, де адміністратори можуть швидко виявляти такі речі, як помилки в інтеграції,

потенційні загрози та інші проблеми, які IT-адміністратори повинні швидко вирішувати.

У 2016 році компанія ForgeRock комерціалізувала популярну платформу управління ідентифікацією та доступом OpenAM з відкритим вихідним кодом і значно розширила зручність використання та функції управління для корпоративних середовищ. Для IT-фахівців, знайомих з OpenAM або подібними форками з відкритим вихідним кодом, платформа Identity Platform від ForgeRock є чудовим варіантом.

ForgeRock пропонує такі функції, як Intelligent Access, який персоналізує аутентифікацію та налаштування доступу на гранулярному рівні за допомогою спрощеного інтерфейсу управління перетягуванням. Інтелектуальний доступ також надає можливість самообслуговування реєстрації та скидання облікових даних, які безпосередньо інтегровані в єдину систему входу в систему.

Потенційним покупцям варто звернути увагу на можливості машинного навчання та штучного інтелекту, які вигідно відрізняють продукт від багатьох конкурентів. Функція ШІ може допомогти виміряти видимість ризиків і підвищити операційну ефективність за рахунок усунення багатьох процесів управління, інцидентів і звітності, які раніше адміністраторам безпеки доводилося виконувати вручну.

Існуючі клієнти Oracle, ймовірно, віддадуть перевагу платформі Identity Cloud Service від Oracle для своїх потреб IAM. Identity Cloud Service ідеально підходить для гібридних хмарних архітектур і особливо корисна для управління ідентифікацією та доступом в багатокористувацьких сценаріях. Oracle Identity Cloud Service також пропонує дуже широкий API для інтеграції користувацьких додатків, які ще не мають попередньо створених інтеграцій. Нарешті, Oracle продовжує працювати над загальною продуктивністю платформи, що робить її однією з найнадійніших і найшвидших платформ на ринку.

Платформа OneLogin Workforce Identity є надійним варіантом для корпоративних організацій, яким необхідно синхронізувати користувачів і групи, розташовані в декількох каталогах, включаючи AD, LDAP, Workday і Google

Workspace. Адміністратори можуть посилатися на атрибути користувачів і передавати їх в наступні додатки для отримання доступу за допомогою мови розмітки Security Assertion Markup Language або через API.

У цій роботі ми зупинимось на одному з основних рішень щодо управління ідентифікацією та доступом користувачів під назвою Microsoft Active Directory та хмарного варіанту Azure AD.

Microsoft AD користується популярністю на підприємствах для забезпечення автентифікації та контролю доступу в доменах Windows. Azure AD IAM може похвалитися тисячами готових інтеграцій сторонніх додатків, які охоплюють цілий ряд бізнес-сервісів, включаючи наступні:

хмарне сховище;

інструменти управління;

співпраця;

CRM;

електронна комерція;

ERP.

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

2.1. Призначення та основні функції Active Directory

Active Directory - це ієрархічно організоване сховище даних про об'єкти мережі, що забезпечує зручні засоби для пошуку та використання цих даних. Комп'ютер, на якому працює Active Directory, називається контролером домену. З Active Directory пов'язані майже всі адміністративні завдання. Active Directory дозволяє адміністраторам використовувати групові політики (GPO) для забезпечення подібного налаштування користувацького робочого середовища, розгортати ПЗ на великій кількості комп'ютерів (через групові політики або за допомогою System Center Configuration Manager), встановлювати оновлення ОС, прикладного та серверного ПЗ на всіх комп'ютерах в мережі(WSUS).

Active Directory (AD) має ієрархічну структуру, що складається з об'єктів. Об'єкти поділяються на три основні категорії:

ресурси (наприклад, принтери);

служби (наприклад, електронна пошта);

люди (облікові записи користувачів і груп користувачів).

Active Directory виконує наступні функції:

надає інформацію про об'єкти;

дозволяє організовувати об'єкти;

дозволяє керувати доступом до об'єктів;

встановлює правила безпеки.

Об'єкти являють собою окремі сутності (користувача, комп'ютер, принтер, програму або спільну мережеву папку) і їхні атрибути. Об'єкти також можуть бути контейнерами для інших об'єктів. Об'єкт унікально ідентифікується своєю назвою і має набір атрибутів:

характеристик;

даних, які об'єкт може містити.

Дані, які об'єкт може містити, у свою чергу, залежать від типу об'єкта. Атрибути є складовою базової структури об'єкта і визначаються схемою Active Directory. Схема визначає, які типи об'єктів можуть існувати в Active Directory.

Сама схема складається з двох типів об'єктів схеми:

класів схеми;

атрибутів схеми.

Один клас схеми визначає один тип об'єкта Active Directory (наприклад, об'єкт «Користувач»), а один атрибут схеми визначає атрибут, який об'єкт може мати.

Кожен атрибут може бути використаний в декількох різних класах схеми. Ці об'єкти називаються об'єктами схеми (або метаданими) і дозволяють змінювати і доповнювати схему, коли це необхідно. Проте, кожен об'єкт схеми є частиною визначень об'єктів Active Directory, тому деактивація або зміна цих об'єктів можуть мати серйозні наслідки, тому що в результаті цих дій буде змінена структура Active Directory. Зміна об'єкта схеми автоматично поширюється в Active Directory. Будучи одного разу створеним, об'єкт схеми не може бути вилучений, його можна лише активізувати. Зазвичай всі зміни схеми ретельно плануються.

Контейнер є аналогічним до об'єкта в тому сенсі, що він також має атрибути та належить простору імен, але, на відміну від об'єкта, контейнер не означає нічого конкретного: контейнер може лише містити групу об'єктів або інші контейнери.

За допомогою служби Active Directory створюються облікові записи комп'ютерів, здійснюється підключення до домену, здійснюється управління комп'ютерами, контролерами домену та організаційними підрозділами (ОП).

Для керування Active Directory призначені засоби адміністрування та підтримки. Наведені нижче інструменти реалізовані і у вигляді оснасток консолі MMC (Microsoft Management Console):

Active Directory - користувачі та комп'ютери (Active Directory Users and Computers) - дозволяє керувати користувачами, групами, комп'ютерами та організаційними підрозділами (ОП). Active Directory Users and Computers, безумовно, найпопулярніший інструмент для доступу до AD, встановлюється на контролерах домену і додається в якості інструменту віддаленого доступу при установці відповідного інструменту в Windows 10, Windows 11 або інших серверах Windows, що входять до складу групи.

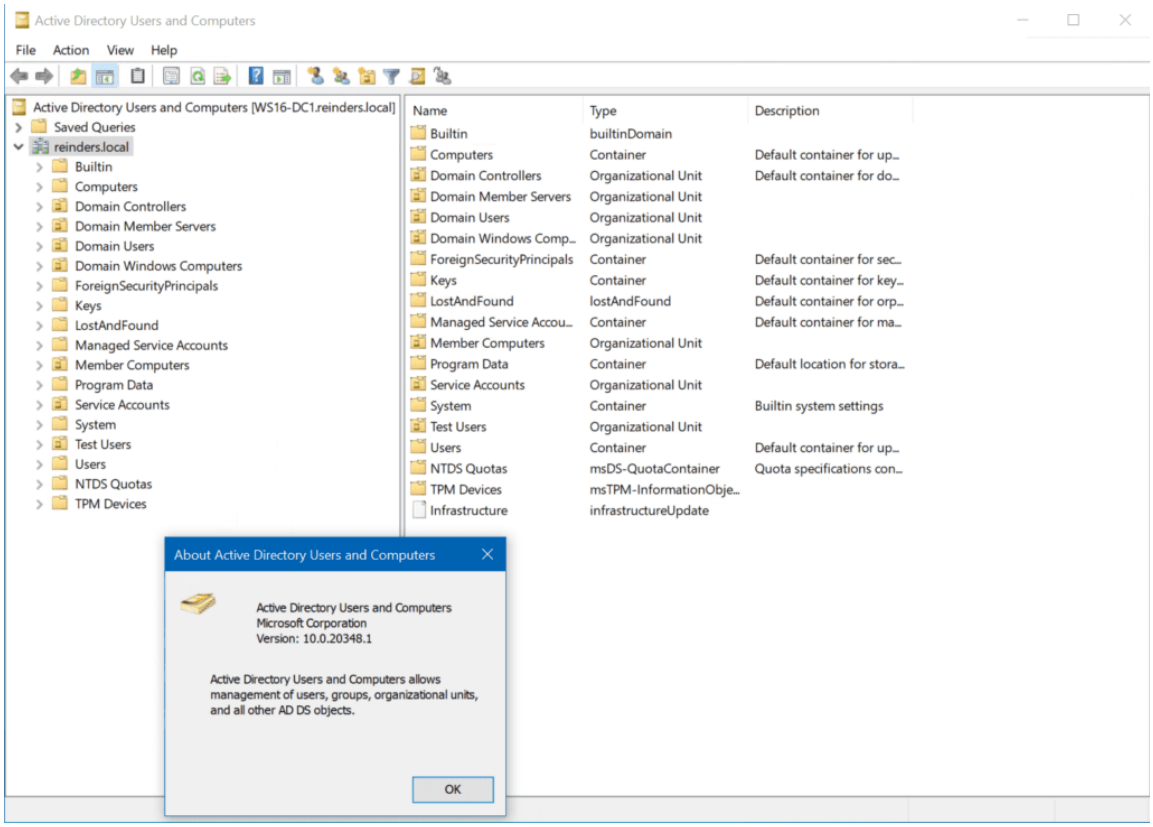


Рис.2.1. Active Directory Users and Computers

Active Directory - домени та довіра (Active Directory Domains and Trusts) - служить для роботи з доменами, деревами доменів та лісами доменів, адміністратори можуть використовувати Active Directory Domains and Trusts, Netdom і Nltest для виявлення, створення, видалення або зміни довірених осіб.

Active Directory - сайти та служби (Active Directory Sites and Services) - дозволяє керувати сайтами та підмережами. Active Directory Sites and Services (ADSS) використовується для управління логічною структурою мережі вашого домену AD. Саме тут ви створюєте та керуєте сайтами - логічними, часто географічними межами, визначеними мережевими IP-підмережами.

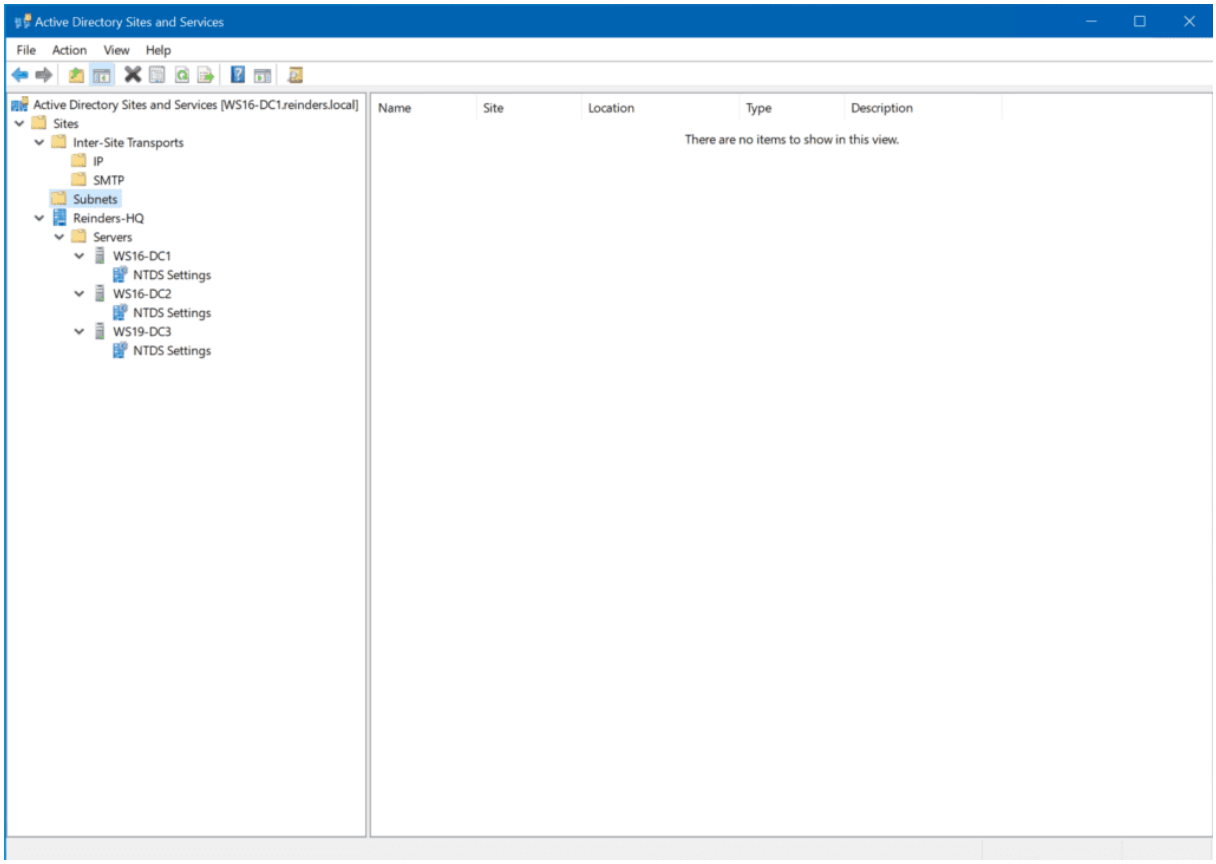


Рис.2.2. Active Directory Sites and Services

Результуюча політика (Resultant Set of Policy) - використовується для перегляду поточної політики користувача або системи та планування змін у політиці.

В Microsoft Windows 2003 Server можна отримати доступ до цих оснасток безпосередньо з меню Administrative Tools.

Для управління об'єктами Active Directory є засоби командного рядка, які дозволяють здійснювати широкий спектр адміністративних завдань:

DSADD - додає в Active Directory комп'ютери, контакти, групи, ОП та користувачів.

```
vlad:dsadd
Description:  This tool's commands add specific types of objects to the
directory. The dsadd commands:

dsadd computer - adds a computer to the directory.
dsadd contact - adds a contact to the directory.
dsadd group - adds a group to the directory.
dsadd ou - adds an organizational unit to the directory.
dsadd user - adds a user to the directory.
dsadd quota - adds a quota specification to a directory partition.
```

Рис.2.3. Вивід команди dsadd

DSGET - відображає властивості комп'ютерів, контактів, груп, ВП, користувачів, сайтів, підмереж та серверів, зареєстрованих у Active Directory.

DSMOD - змінює властивості комп'ютерів, контактів, груп, ОП, користувачів та серверів, зареєстрованих у Active Directory.

DSMOVE - переміщує одиночний об'єкт у нове розташування в межах домену або перейменовує об'єкт без переміщення.

DSQXJERY - здійснює пошук комп'ютерів, контактів, груп, ВП, користувачів, сайтів, підмереж та серверів в Active Directory за заданими критеріями.

DSRM - видаляє об'єкт із Active Directory.

NTDSUTIL - дозволяє переглядати інформацію про сайт, домен або сервер, управляти господарями операцій (operations masters) і обслуговувати базу даних Active Directory.

Ліс Active Directory визначає набір одного або декількох доменів, що використовують одні й ті самі схему, конфігурацію та глобальний каталог. Крім того, всі домени беруть участь у двосторонніх транзитивних відносинах довіри.

Звернемо увагу на терміни, що використовуються у визначенні лісу.

Домен - домен надає спосіб організації та захисту об'єктів, наприклад, користувачів та комп'ютерів, які є частиною одного простору ім‘я.com. Комп'ютери в кожному домені використовують однакову конфігурацію домену і можуть бути об'єктом застосування політик та обмежень, що встановлюються адміністратором домену. Використання доменів дозволяє спростити безпеку в масштабі підприємства.

Схема - схема Active Directory використовується спільно всіма доменами в межах лісу. Схема це конфігураційна інформація, яка управляє структурою та вмістом каталогу.

Конфігурація - конфігурація визначає логічну структуру лісу, наприклад, число та конфігурацію сайтів у межах лісу.

Глобальний каталог - світовий каталог можна сприймати у вигляді довідника для лісу. Глобальний каталог містить інформацію про всі об'єкти лісу, включаючи інформацію про розташування об'єктів. Крім того, глобальний каталог містить інформацію про членство в універсальних групах.

Довіра - довіра надає різним доменам можливість працювати разом. Без довіри домени працюють як окремі сутності, тобто користувачі з домену А не зможуть отримувати доступ до ресурсів домену В. Якщо ставлення довіри встановлюється між доменами таким чином, що домен В довіряє домену А, то користувачі домену А зможуть отримувати доступ до ресурсів домену В, якщо вони мають відповідні дозволи.

Існує три основні типи відносин довіри.

Транзитивні - транзитивні відносини довіри створюються автоматично між доменом одного лісу. Вони дозволяють користувачам будь-якого домену потенційно отримувати доступ до ресурсів будь-якого іншого домену цього лісу, якщо користувачі мають відповідні права доступу.

Shortcut - це відношення довіри між доменами одного лісу, які мають транзитивне відношення довіри. Таке ставлення довіри надає швидше аутентифікацію та перевірку доступу до ресурсів між несусідніми доменами лісу.

Зовнішні - зовнішні відносини довіри дозволяють доменам з різних лісів спільно використовувати ресурси. Такі відносини довіри не є транзитивними, тобто вони належать лише до тих доменів, котрим вони створювалися.

Основний вигляд структури Active Directory - верхнім рівнем структури є ліс - сукупність всіх об'єктів, атрибутів та правил (синтаксису атрибутів) в Active Directory. Ліс містить одне або кілька дерев, пов'язаних транзитивними стосунками довіри. Дерево містить один або декілька доменів, також пов'язаних в ієрархію транзитивними стосунками довіри. Домени ідентифікуються своїми структурами імен DNS — просторами імен.

Об'єкти в домені можуть бути згруповані у контейнери — підрозділи. Підрозділи дозволяють створювати ієрархію всередині домену, спрощують його адміністрування і дозволяють моделювати організаційну та/або географічну структури компанії в Active Directory. Підрозділи можуть містити інші підрозділи. Корпорація Майкрософт рекомендує використовувати якомога менше доменів в Active Directory, а для структурування AD і політик використовувати підрозділи. Часто групові політики застосовуються саме до підрозділів. Групові політики самі є об'єктами. Підрозділ є найнижчим рівнем, на якому можуть делегуватися адміністративні повноваження.

Іншим способом поділу AD є «сайти», які є способом фізичного (а не логічного) групування на основі підмереж IP. Сайти діляться на такі, що мають підключення низькошвидкісними каналами (наприклад, каналами глобальних мереж, за допомогою віртуальних приватних мереж), і таких, що підключені до високошвидкісних каналів (наприклад через локальні мережі). Сайт може містити один або декілька доменів, а домен може містити один або кілька сайтів. При проектуванні Active Directory важливо враховувати мережевий трафік, що

створюється при синхронізації даних AD між сайтами.

Ключовим рішенням при проектуванні AD є рішення щодо поділу інформаційної інфраструктури на ієрархічні домени та підрозділи верхнього рівня. Типовими моделями, що використовуються для такого поділу, є моделі поділу за функціональними підрозділами компанії, за географічним розташуванням, і за ролями в інформаційній інфраструктурі компанії. Часто використовуються комбінації цих моделей.

Azure Active Directory - це наступний етап еволюції рішень для управління посвідченнями та доступом для хмари. Майкрософт представила доменні служби Active Directory у Windows 2000, щоб дати організаціям можливість керувати кількома компонентами локальної інфраструктури та системами, використовуючи єдину ідентифікацію для кожного користувача. Azure AD виводить цей підхід на новий рівень, надаючи організаціям рішення "Ідентифікація як послуга" (IDaaS) для всіх своїх додатків у хмарі та локально. Більшість IT-адміністраторів знайомі з концепціями доменних служб Active Directory. Для прикладу, відмінності у Azure Active Directory від Active Directory:

існуючі організації AD використовують Azure AD Connect для синхронізації посвідчень із хмарою. В Azure AD додано підтримку автоматичного створення користувачів із хмарних HR-систем. Azure AD може надавати посвідчення в додатках SaaS з підтримкою SCIM, щоб автоматично надавати додаткам відомості, необхідні для надання доступу користувачам. На відмінність у Active Directory організації створюють внутрішніх користувачів вручну або використовують внутрішню чи автоматизовану систему підготовки;

Active Directory не підтримує додатки SaaS від самого початку і вимагає системи федерації, такої як AD FS. У Azure Active Directory додатки SaaS, що підтримують перевірку автентичності OAuth2, SAML і WS-*, можуть бути інтегровані для використання Azure AD для перевірки автентичності;

Active Directory від початку не підтримує мобільні пристрої без сторонніх рішень. Рішення Microsoft для управління мобільними пристроями, Microsoft

Intune, інтегровано з Azure AD. Microsoft Intune надає інформацію про стан пристрою системі ідентифікації для оцінки під час перевірки автентичності.

Active Directory від самого початку не підтримує ОС, відмінні від Windows, без сторонніх рішень, хоча комп'ютери Linux можна налаштувати для аутентифікації за допомогою Active Directory за допомогою Kerberos. Віртуальні машини Linux/Unix можуть використовувати керовані посвідчення для доступу до системи або ресурсів посвідчень. Деякі організації переносять ці робочі навантаження на технології хмарних контейнерів, які також можуть використовувати керовані посвідчення.

Фізично інформація AD зберігається на одному або декількох рівнозначних контролерах доменів, які замінили основний і резервні контролери домену (що використовувалися в Windows NT) (хоча для виконання деяких операцій зберігається і так званий сервер «операцій з одним головним сервером», який може емулювати головний контролер домену). Кожен контролер домену зберігає копію даних AD, призначену для читання та запису. Зміни, зроблені на одному контролері, синхронізуються на всі контролери домену при реплікації. Сервери, на яких сама служба Active Directory не встановлена, але які при цьому входять в домен AD, називаються рядовими серверами.

2.2. Архітектура Active Directory

Служба каталогів Active Directory, будучи частиною операційної системи Windows 2000/2003, забезпечує централізоване управління мережею. Ефективна робота складного корпоративного середовища досягається за допомогою таких можливостей, які надає служба каталогів Active Directory:

централізоване управління, що дає змогу адміністраторам зручно керувати всіма корпоративними ресурсами. Рутинні завдання адміністрування не потрібно повторювати для численних об'єктів мережі;

масштабованість - здатність служби охоплювати як один домен, так і безліч доменів, один контролер домену або безліч контролерів домену.

кілька доменів можна об'єднати в дерево доменів, а кілька дерев доменів можна зв'язати в ліс;

розширюваність каталогу, що забезпечує адміністраторам можливість додавання в схему каталогу нових класів об'єктів або додавати нові атрибути до наявних класів;

інтеграція з DNS (Domain Name Service), що дає змогу іменувати об'єкти Active Directory відповідно до угоди про доменні імена. Це забезпечує автоматичне перетворення доменних імен об'єктів на IP-адреси і дає змогу природно інтегрувати мережі на основі Windows 2000/2003 у глобальну мережу, як-от Internet;

адміністрування з використанням групових політик, що являють собою деяку сукупність налаштувань, які застосовуються до певної групи комп'ютера, користувачів, доменів або сайтів. Active Directory дає змогу встановлювати групову політику на кількох рівнях, що відкриває перед адміністратором широкі можливості управління;

єдина реєстрація в мережі, що дає змогу користувачам отримувати доступ до всіх мережевих ресурсів (серверів, принтерів, файлів тощо) незалежно від їх розташування в мережі;

безпека інформації, що досягається централізованим захистом мережі завдяки засобам автентифікації та управління доступом до ресурсів, вбудованим у службу Active Directory. Права доступу можна визначати не тільки для кожного об'єкта, а й для кожної властивості (атрибута) об'єкта;

гнучкість змін у службі каталогів відповідно до змін у структурі підприємства;

реплікація інформації за схемою з багатьма ведучими (multi-master), що дає

змогу модифікувати каталог на будь-якому контролері домену. За наявності в домені кількох контролерів це забезпечує високу відмовостійкість і можливість розподілу мережевого навантаження.

В основі архітектури Active Directory лежать такі технології:

Стандарти X.500 і X.509, що визначають інформаційну модель даних, синтаксис і формат цифрових сертифікатів, які використовуються для аутентифікації користувачів.

Стандартний протокол доступу до каталогів LDAP (Lightweight Directory Access Protocol), що дає змогу додаткам працювати з інформацією, яка міститься в каталозі.

Стек протоколів TCP/IP, що є основним при побудові мережі масштабу корпорації на основі ОС Windows 2000/2003.

Служба DNS (Domain Name Service), що використовується для дозволу доменних імен в IP-адреси. Дозвіл імен - це процес перетворення імені об'єкта в посилання на об'єкт. У цьому випадку це перетворення DNS-імені в IP-адресу. ОС Windows 2000/2003 використовує динамічну DNS (DDNS), що дає змогу клієнтським комп'ютерам із динамічними адресами реєструватися на сервері DNS.

Протокол динамічної конфігурації клієнта DHCP (Dynamic Host Configuration Protocol), що взаємодіє з DNS і дає змогу спростити процес конфігурації клієнтів мережі TCP/IP і полегшити розширення мережі.

Система Kerberos - протокол автентифікації користувачів, що використовується як основний засіб під час реалізації системи безпеки Windows 2000/2003.

У багаторівневій архітектурі Active Directory кожний рівень відповідає серверному процесу, що надає службу каталогу клієнтським додаткам. Архітектура AD включає три рівні служб, кілька інтерфейсів і протоколів. Рівні служб

(системний агент каталогу, рівень бази даних і розширюване ядро сховища) обробляють дані, необхідні для пошуку записів у базі даних (БД) каталогу. Над рівнями служб у цій архітектурі розташовані протоколи та інтерфейси, що забезпечують взаємодію клієнтів зі службою каталогів.

Вищим рівнем AD є системний агент каталогу (Directory System Agent, DSA), що надає API-інтерфейси для доступу до каталогу. DSA підтримує кілька інтерфейсів. Основний клієнтський інтерфейс - ADSI (Active Directory Service Interlaces) - є засобом абстрагування від API-інтерфейсу протоколу LDAP, що використовується в AD.

Інтерфейс REPL використовується службою реплікації для копіювання відомостей з AD через RPC (Remote Procedure Call - виклик віддалених процедур) поверх протоколів IP або SMTP зі стека протоколів TCP/IP. SMTP (Simple Mail Transport Protocol) застосовується тільки для міжсайтової реплікації. Виклик віддалених процедур RPC поверх IP використовується як для внутрішньосайтових, так і для міжсайтових реплікацій.

Ще два підтримуваних інтерфейси - SAM і MAPL - застосовуються для взаємодії з клієнтами, які використовують програмне забезпечення більш ранніх версій. Зокрема, SAM (Security Accounts Manager - диспетчер облікових записів) забезпечує низькорівневу сумісність для зв'язку доменів Windows 2000/2003 і Windows NT 4.0. Реплікація інформації з резервних контролерів доменів у домен змішаного режиму також здійснюється через інтерфейс SAM. ≪Застарілі≫ клієнти MAPI, наприклад клієнт MS Outlook, для обміну повідомленнями підключаються до DSA за допомогою MAPI (Messaging Application Programming Interface).

Наступний рівень архітектури AD - рівень бази даних - забезпечує об'єктне надання інформації бази даних шляхом застосування семантики схеми до записів БД та ізолювання верхніх рівнів служби каталогу від вихідної СУБД. Рівень БД є прихованим внутрішнім інтерфейсом.

Основною функцією бази даних є переведення кожного різного відносного

складеного імені об'єкта, що запитується клієнтом, у ціле число - тег, застосовуваний для всіх внутрішніх операцій доступу. Рівень БД гарантує унікальність тега DN (distinguished name - складене ім'я) для кожного запису в базі.

Усі дані, що описують об'єкт, містяться у вигляді набору атрибутів, що зберігаються у формі полів запису БД. Рівень БД відповідає за створення, витяг і видалення індивідуальних записів, полів записів і значень полів.

Нижній рівень архітектури AD представлений розширюваним ядром сховища.

Служби AP реалізовані поверх диспетчера таблиць ISAM (Indexed Sequential Access Method - метод індексно-послідовного доступу). У Windows 2000/2003 діє поліпшена версія диспетчера таблиць ESE (Extensible Storage Engine). Останній реалізує транзакційну БД, що застосовує файли журналу для підтвердження коректного виконання транзакції. ESE відповідає за зберігання всіх об'єктів AD і підтримує БД об'ємом до 16 Тбайт, теоретично здатну містити кілька мільйонів об'єктів для кожного домену.

ESE задовольняє потреби AD щодо зберігання інформації:

виконує операції оновлення у вигляді транзакції для підтримання стійкості та цілісності системи на випадок системних збоїв;

ефективно обробляє розріджені записи, в яких багатьом полям не присвоєно значення властивостей об'єктів.

Під час встановлення AD створюється стандартна схема, що визначає всі необхідні та допустимі атрибути для цього об'єкта. ESE залишає місце тільки для призначених об'єкту атрибутів, а не для всіх можливих атрибутів. Якщо надалі буде додано нові атрибути, для їх розміщення буде виділено додатковий обсяг.

Каталог Active Directory передбачає виділення в мережі двох структур - логічної та фізичної.

До логічної структури належать такі елементи:

об'єкт (object), що представляє деяку конкретну сутність (принтер, модем, папка, користувач та ін.), з відмінним набором іменованих атрибутів (характеристик об'єкта). Об'єкти є екземплярами деякого класу, що логічно групує об'єкти;

контейнер (container) або контейнерний об'єкт (container object);

логічне об'єднання, що групує об'єкти або інші контейнери за будь-якою ознакою. Цим контейнери схожі з папками файлової системи.

Проте контейнери теж є елементами деякого класу і мають певний набір атрибутів;

організаційний підрозділ (organizational unit);

деякий контейнерний об'єкт, що організовує об'єкти в логічні адміністративні групи в межах домену. Організаційний підрозділ ОП може містити такі об'єкти, як групи, комп'ютери, додатки тощо. Як правило, ОП відображають структуру підприємства;

домен (domain) - сукупність комп'ютерів, які спільно використовують загальну базу даних каталогу;

дерево доменів (domain tree) - угруповання одного або декількох доменів із суміжною структурою імен, що надають спільний доступ до ресурсів;

ліс доменів (domain forest) - об'єднання одного або більше дерев, які спільно використовують інформацію каталогу.

До фізичної структури мережі, представленої в Active Directory, належать такі елементи:

контролер домену - комп'ютер із серверною ОС Windows Server (Advanced Server, Datacenter Server), що зберігає розділ каталогу (локальну базу даних

домену);

підмережа (Subnet) - мережева група із заданою областю IP-адрес і мережевою маскою, яка має певне географічне місце;

сайт (site) - одна або кілька підмереж зі своєю безліччю областей IP-адрес. Комп'ютери приписуються сайтом залежно від місця розташування в підмережі або в наборі підмереж. В ідеалі сайти складаються з добре пов'язаних підмереж і комп'ютерів.

Визначення всіх об'єктів, які допустимо розміщувати в Active Directory AD, а також сукупність правил, що дають змогу керувати структурою і вмістом AD, містяться в схемі каталогу (Directory Schema). Схема є обов'язковим компонентом AD і зберігається в каталозі у вигляді двох класів об'єктів: об'єктів Class Schema і об'єктів Attribute Schema. Іншим обов'язковим компонентом є глобальний каталог (Global catalog), що виконує функції пошукового механізму.

Безліч об'єктів, що містяться в безлічі вкладених контейнерів, утворюють ієрархію - дерево (tree) AD. Листям цього дерева є об'єкти, а вузлами - контейнери. У загальному випадку мережа корпоративного підприємства представляється доменним деревом або доменним лісом. Кожен домен є розділом каталогу AD. У корені за допомогою довірчих відносин пов'язані дочірні домени. Кожен із них також може бути пов'язаний із доменами-нащадками. Повне ім'я домену, що входить до складу дерева, містить у собі за стандартами DNS імена всіх його предків, розділені символом крапки.

Домени, що використовують однакову схему іменування, утворюють дерево доменів, як показано на рис. У цьому випадку кажуть, що домени використовують суміжну структуру імен. Простір імен - набір правил іменування, що забезпечують ієрархічну структуру, або шлях у дереві. За стандартами DNS ім'я дочірнього домену доповнюється ім'ям батьківського.

Дерева розрізняють за низкою ознак:

ієрархії доменів;

безперервності простору імен;

довірчими відносинами між доменами;

загальною схемою;

здатності відображати будь-який об'єкт у списку глобального каталогу.

Однак суміжна структура імен необов'язкова. У цьому разі, якщо в корпорації є підрозділи, які працюють незалежно один від одного і використовують різні схеми іменування, їхні доменні дерева можуть бути об'єднані в ліс. Дерева в лісі забезпечують доступ до однакової схеми і правил спільної роботи об'єктів. Усі домени лісу мають єдиний глобальний каталог і конфігураційний контролер.

Домени в дереві зв'язуються один з одним, використовуючи двосторонні транзитивні довірчі відносини за протоколом Kerberos. Транзитивна довіра означає, що якщо домен А довіряє домену В і домен В довіряє домену С, то домен А довіряє домену С. Тому приєднаний до дерева домен одразу вступає в довірчі відносини з кожним деревом домену. Призначені для користувача облікові записи та групи, визначені в домені, що довіряється, можуть отримувати права і повноваження в домені, що довіряє, навіть якщо їх немає в його каталозі.

Кожен домен включає один або кілька контролерів, на яких зберігається повна репліка (копія) каталогу домену. Для спрощення адміністрування всі контролери домену рівноправні. Тому зміни, виконані на будь-якому контролері домену, можна реплікувати на інші контролери.

Хоча ОП дають змогу групувати ресурси і користувачів домену, що належать до того чи іншого структурного підрозділу підприємства, вони не здатні організувати мережу таким чином, щоб оптимізувати мережевий трафік. Річ у тім, що під час побудови мережі потрібно враховувати і той факт, що підмережі, які належать до одного домену, можуть розташовуватися в різних географічних точках

і при цьому бути з'єднаними повільними лініями зв'язку. У зв'язку з цим в AD, як зазначено вище, введено поняття сайту (site).

Планування сайту проводиться незалежно від логічної структури домену.

AD дає змогу створити безліч сайтів в одному домені або один сайт, що охоплює безліч доменів. Немає також зв'язку між діапазоном IP-адрес сайту і простором імені домену. Комп'ютери приписуються до сайтів залежно від місця розташування в підмережі або в наборі підмереж. Якщо комп'ютери в підмережах здатні взаємодіяти на досить високих швидкостях, їх називають добре пов'язаними. В ідеалі сайти складаються з добре пов'язаних підмереж і комп'ютерів. Якщо швидкість обміну між підмережами і комп'ютерами низька, може знадобитися створити кілька сайтів. Хороший зв'язок дає сайтам деякі переваги.

Коли клієнт входить у домен, у процесі автентифікації спочатку проводиться пошук локального контролера домену на сайті клієнта, тобто за можливості першими опитуються локальні контролери, що обмежує мережевий трафік і прискорює автентифікацію.

Інформація каталогу реплікується частіше всередині сайтів, ніж між сайтами. Це знижує міжмережевий трафік, викликаний реплікацією, і гарантує, що локальні контролери доменів швидко отримають оновлену інформацію. Є можливість налаштування порядку реплікації даних каталогу, використовуючи зв'язки сайтів. Наприклад, визначити сервер-плацдарм для реплікації між сайтами. Основна частина навантаження від реплікації між сайтами ляже на цей спеціалізований сервер, а не на будь-який доступний сервер сайту.

2.3. Дослідження можливостей використання Active Directory у організації

Основним методом управління ідентифікацією та доступом у Active Directory є групові політики. Групова політика - важливий елемент будь-якого середовища

Microsoft Active Directory (AD). Її основна мета - дати IT-адміністраторам можливість централізовано керувати користувачами та комп'ютерами в домені. Групова політика, зі свого боку, складається з набору політик, які називаються об'єктами групової політики (GPO). Під час створення домену AD автоматично створюються два об'єкти групової політики:

політика домену за замовчуванням встановлює базові параметри для всіх користувачів і комп'ютерів у домені в трьох площинах: політика паролів, політика блокування облікових записів і політика Kerberos;

політика контролерів домену за замовчуванням встановлює базові параметри безпеки та аудиту для всіх контролерів домену в межах домену.

Налаштування різних об'єктів групової політики можуть перекриватися або конфліктувати. За замовчуванням об'єкти групової політики обробляються в такому порядку (причому створені пізніше мають пріоритет над створеними раніше):

локальний (індивідуальний комп'ютер);

сайт;

домен;

організаційна одиниця.

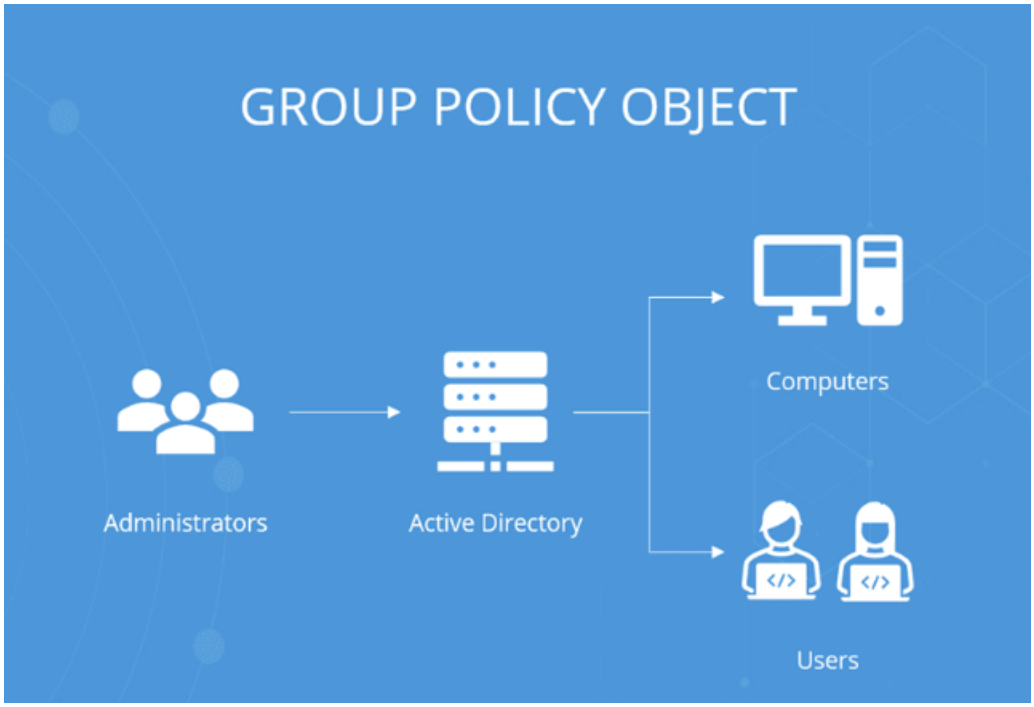


Рис.2.4. Об’єкти групових політик

Цінність групової політики полягає в її силі. Одним махом ви можете застосувати політики в домені або підрозділі, які значно зміцнять безпеку або поліпшать продуктивність бізнесу. Або навпаки.

Але цією владою також можна зловживати, навмисно чи випадково. Одна неправильна зміна об'єкта групової політики може призвести до порушення безпеки. Зломщик або зловмисний адміністратор можуть легко змінити об'єкти групової політики, щоб, наприклад:

дозволити необмежену кількість спроб вгадати пароль облікового запису;

увімкнути можливість підключення знімних носіїв для спрощення крадіжки даних;

розгорнути шкідливе ПЗ на всіх машинах у домені;

замінити сайти, збережені в закладках браузерів користувачів, шкідливими URL-адресами;

запустити шкідливий сценарій під час запуску або завершення роботи

комп'ютера.

Для управління груповими політиками Microsoft надає консоль управління груповими політиками (GPMC). Використовуючи цей безкоштовний редактор групової політики, IT-адміністратори можуть створювати, копіювати, імпортувати, створювати резервні копії та відновлювати об'єкти групової політики, а також складати звіти щодо них. Microsoft також пропонує цілий набір інтерфейсів GPMC, які можна використовувати для програмного доступу до багатьох операцій, підтримуваних консолю.

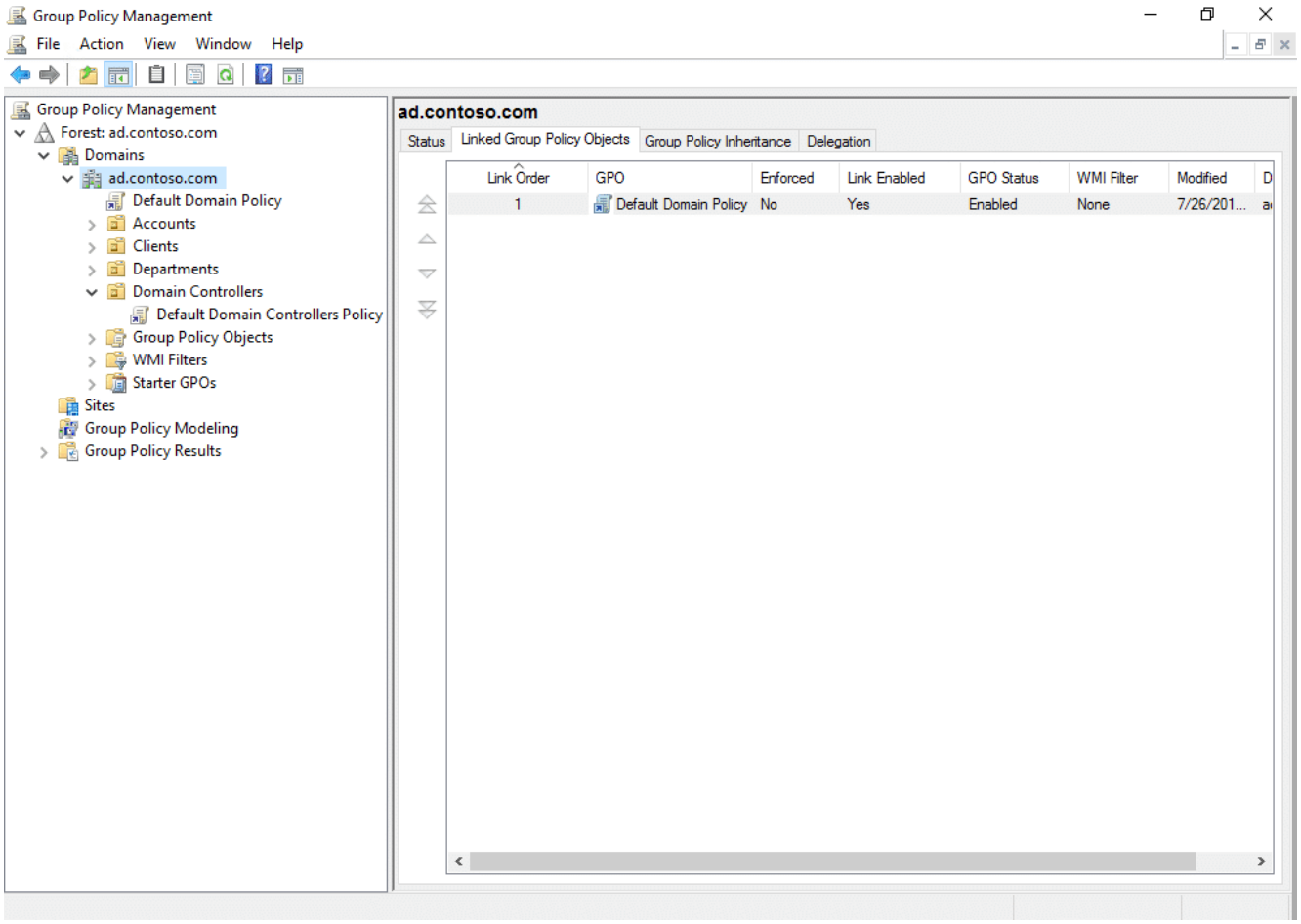


Рис.2.5. Вигляд консолі Group Policy Management

За допомогою групових політик ми можемо налаштовувати «майже все» в межах логічних або фізичних мереж у Active Directory. Групові політики є незамінними для підвищення безпеки підприємства, бо вони дозволяють налаштовувати й закривати шляхи можливого проникнення або зломів у

організації, декілька прикладів, яким чином правильне налаштування групових політик може підвищити безпеку.

Windows генерує та зберігає паролі облікових записів користувачів у "хешах". Windows генерує як хеш LAN Manager (LM хеш), так і хеш Windows NT (NT хеш) паролів. Вона зберігає їх у локальній базі даних диспетчера облікових записів безпеки (Security Accounts Manager, SAM) або в Active Directory. Групові політики дозволяють заборонити збереження LM хешу.

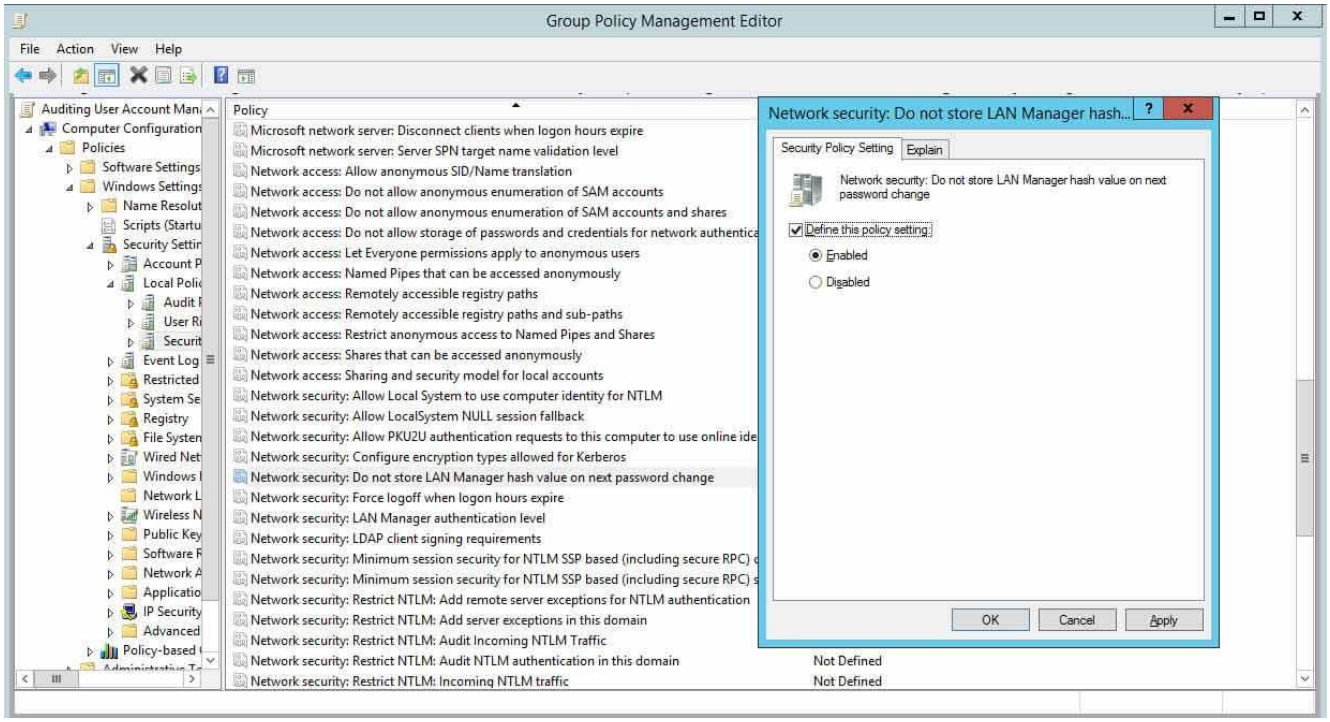


Рис.2.6. Заборона збереження хешу LM

LM хеш є слабким і схильним до злому. Тому слід заборонити Windows зберігати LM-хеш ваших паролів.

Командний рядок може використовуватися для запуску команд, які надають користувачам високорівневий доступ і дозволяють обійти інші обмеження в системі. Тому для забезпечення безпеки системних ресурсів доцільно відключити Командний рядок для співробітників, які не відносяться до IT, Software Engineering та Security підрозділів. До того ж, це може допомогти Security підрозділу у реагуванні на злом, тому що шкідливе ПЗ зможе отримати доступ до юзерського облікового запису, воно все одно не зможе використати командний рядок.

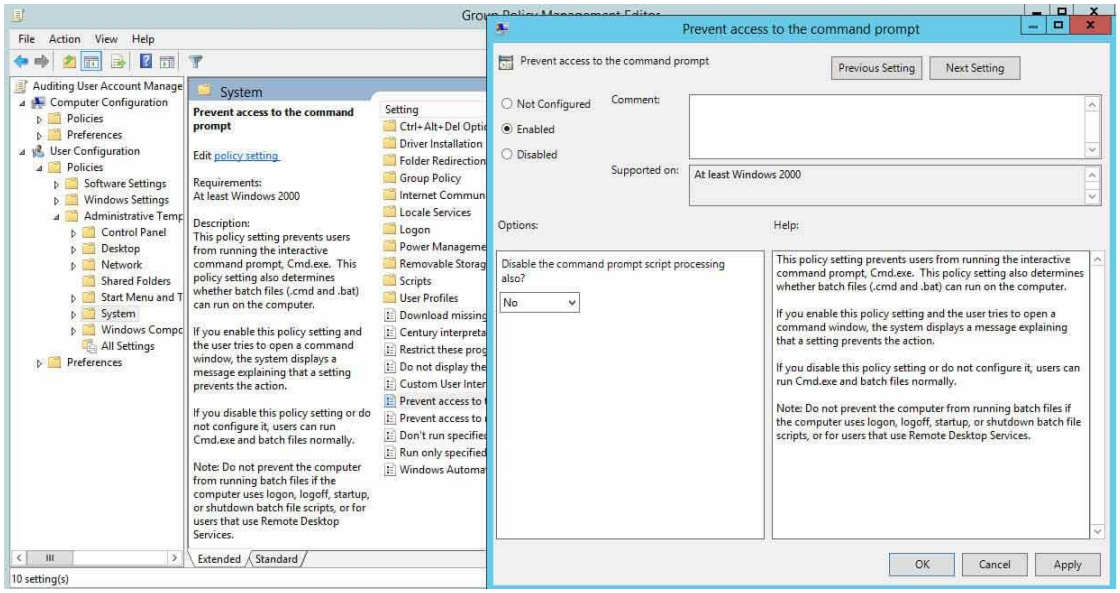


Рис.2.7. Вимкнення командного рядку у Group Policy Management Editor

Знімні носії інформації дуже схильні до зараження, і вони також можуть містити вірус або шкідливе програмне забезпечення. Якщо користувач підключить заражений диск до мережевого комп'ютера, це може вплинути на всю мережу. Аналогічно, DVD-диски, компакт-диски та дискети схильні до зараження. Групові політики надають можливість відключення підключення знімних носіїв інформації для того, щоб користувачі не приносили та не використовували будь-які некорпоративні носії інформації.

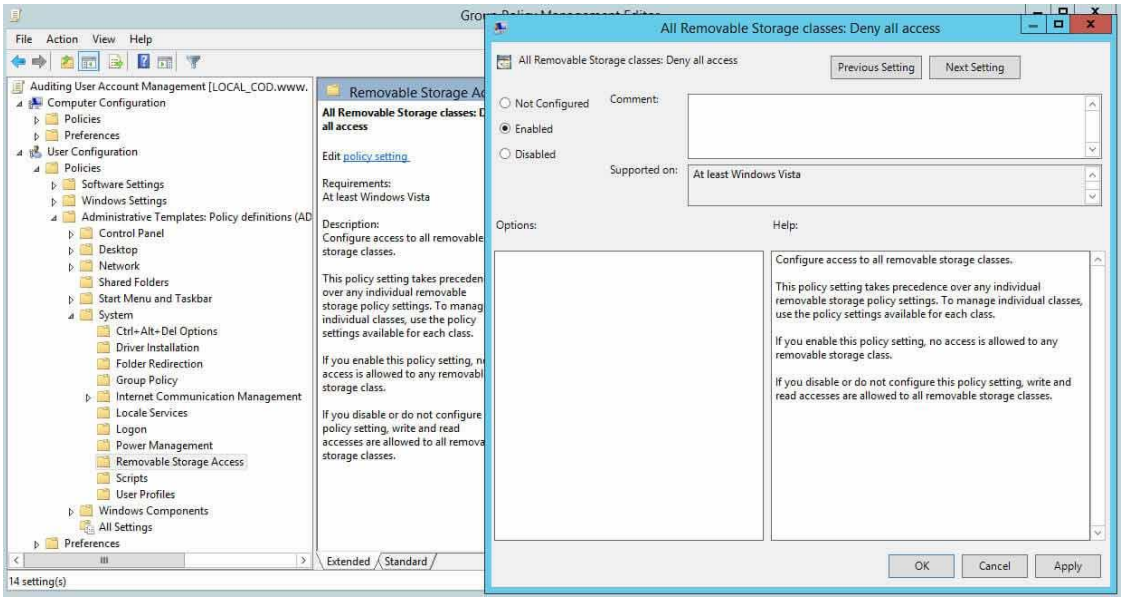


Рис.2.8. Заборона підключення знімних носіїв інформації

Групові політики надають можливість заборони підключення будь-яких знімних носіїв інформації до комп’ютерів користувачів. Але на цьому рівні це можна обійти за допомогою атаки Bad USB - коли пристрій, якій під’єднується через USB і містить в собі якісь дані(шкідливе або нешкідливе ПЗ) видає себе за периферію - клавіатури, мишки, навушники та інше.

Коли ви надаєте користувачам свободу у встановленні програмного забезпечення, вони можуть встановити небажані програми, які можуть скомпрометувати вашу систему. Системним адміністраторам зазвичай доводиться регулярно проводити технічне обслуговування та очищення таких систем. Щоб перестрахуватися, бажано запобігти встановленню програмного забезпечення за допомогою групової політики.

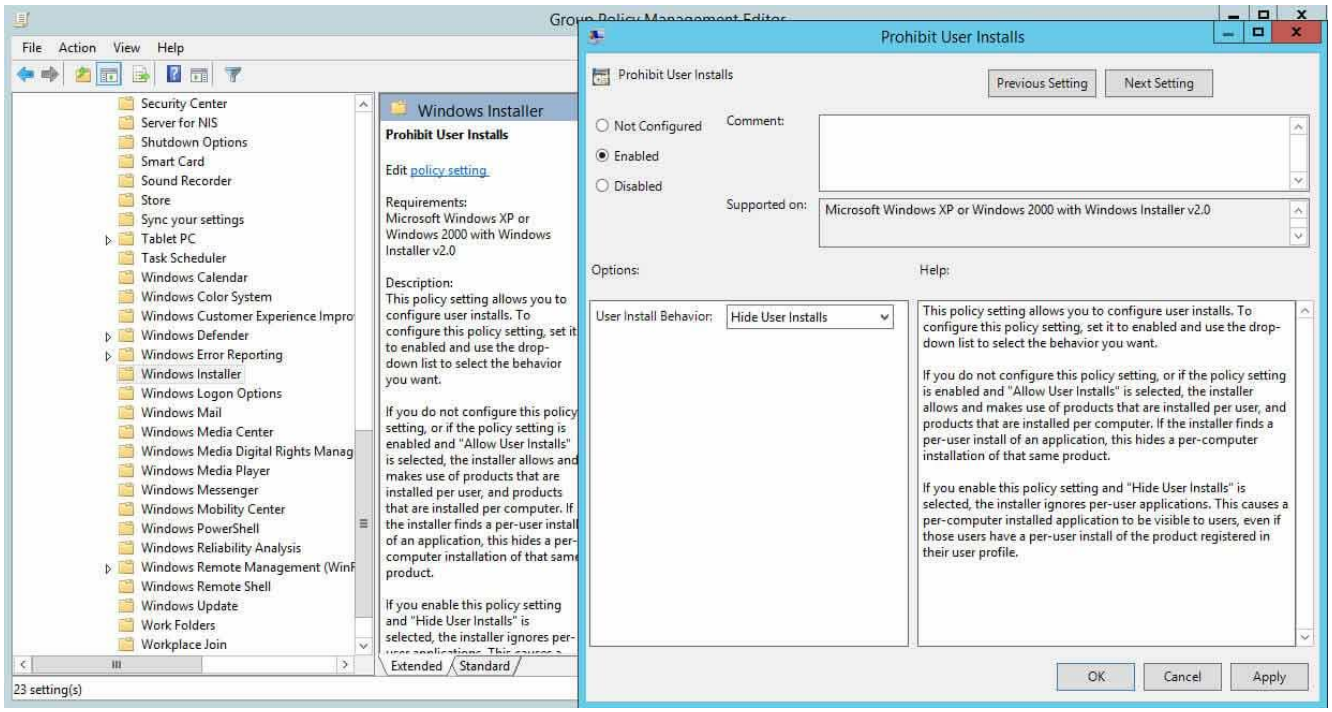


Рис.2.9. Заборона можливості встановлення програмного забезпечення користувачами

Через гостьовий обліковий запис користувачі можуть отримати доступ до конфіденційних даних. Такі облікові записи надають доступ до комп'ютера з ОС Windows і не вимагають введення пароля. Увімкнення такого облікового запису

означає, що будь-хто може зловживати доступом до ваших систем.

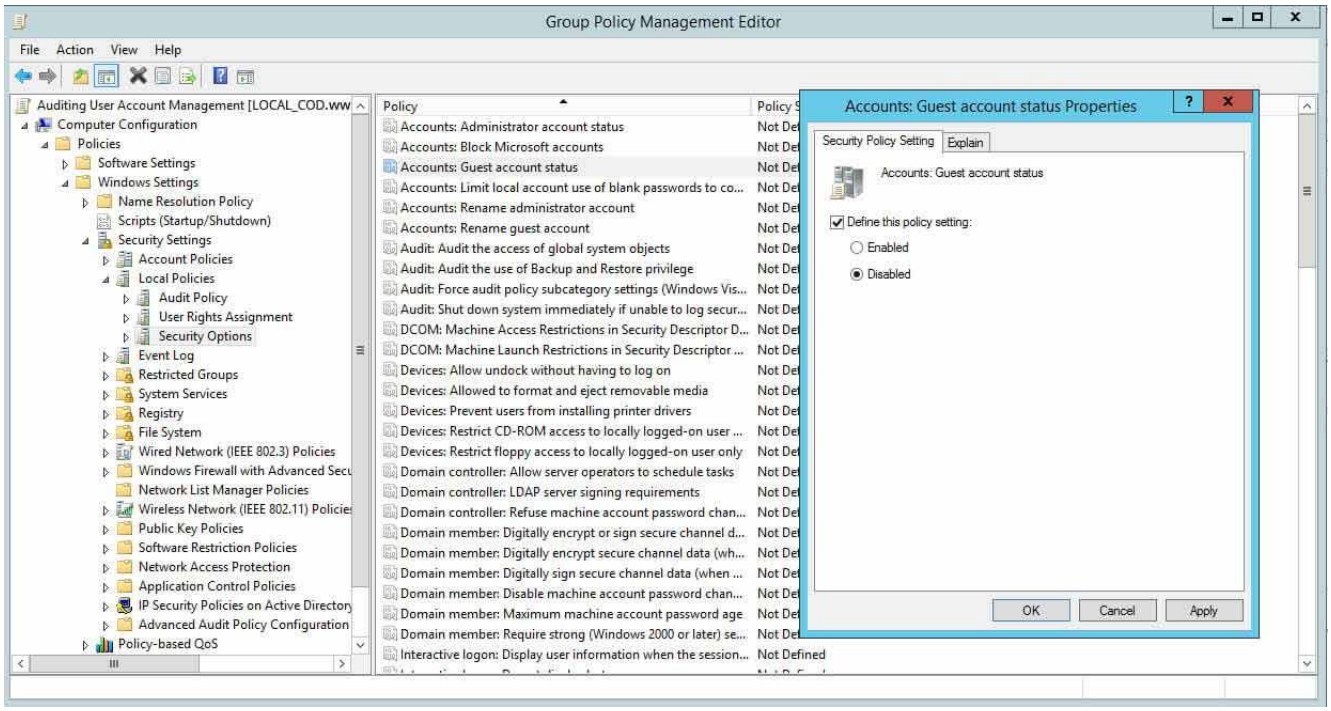


Рис.2.10. Вимкнення гостьового облікового запису

Встановити вищі ліміти мінімальної довжини пароля. Наприклад, для підвищених облікових записів паролі мають бути не менше 15 символів, а для звичайних облікових записів - не менше 12 символів. Встановлення меншого значення мінімальної довжини пароля створює невиправданий ризик.

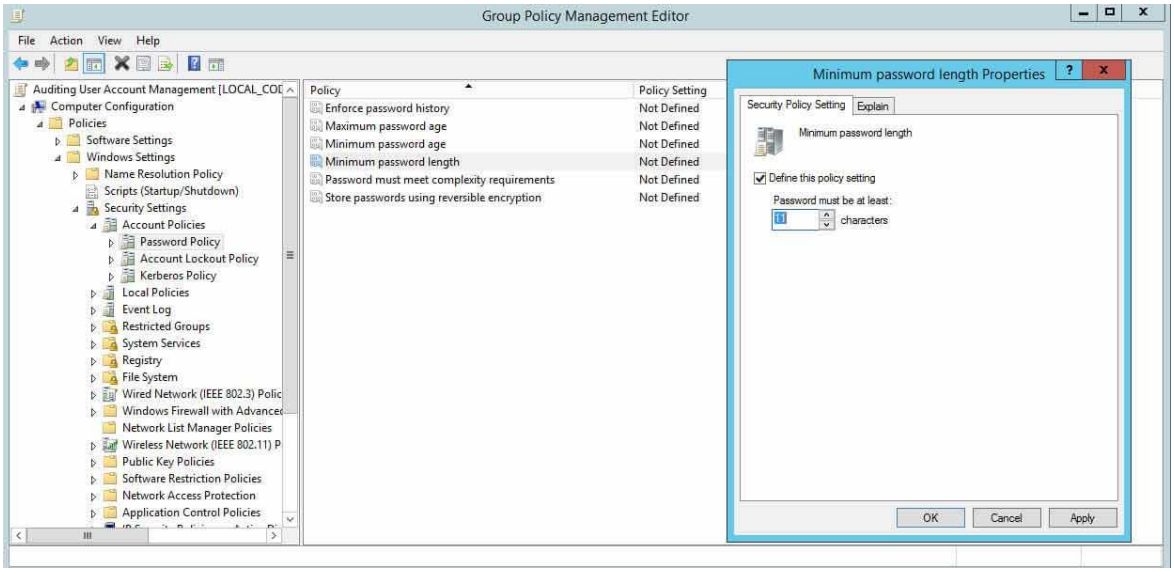


Рис.2.11. Встановлення мінімальної довжини пароля

Якщо ви встановите тривалий термін дії пароля, користувачам не доведеться змінювати його дуже часто, а це означає, що зростає ймовірність крадіжки пароля. Коротший термін дії пароля завжди є кращим.

За замовчуванням в Windows максимальний вік пароля встановлений на 42 дні. На наступному скріншоті показано налаштування політики, що використовується для налаштування "Максимального віку пароля".

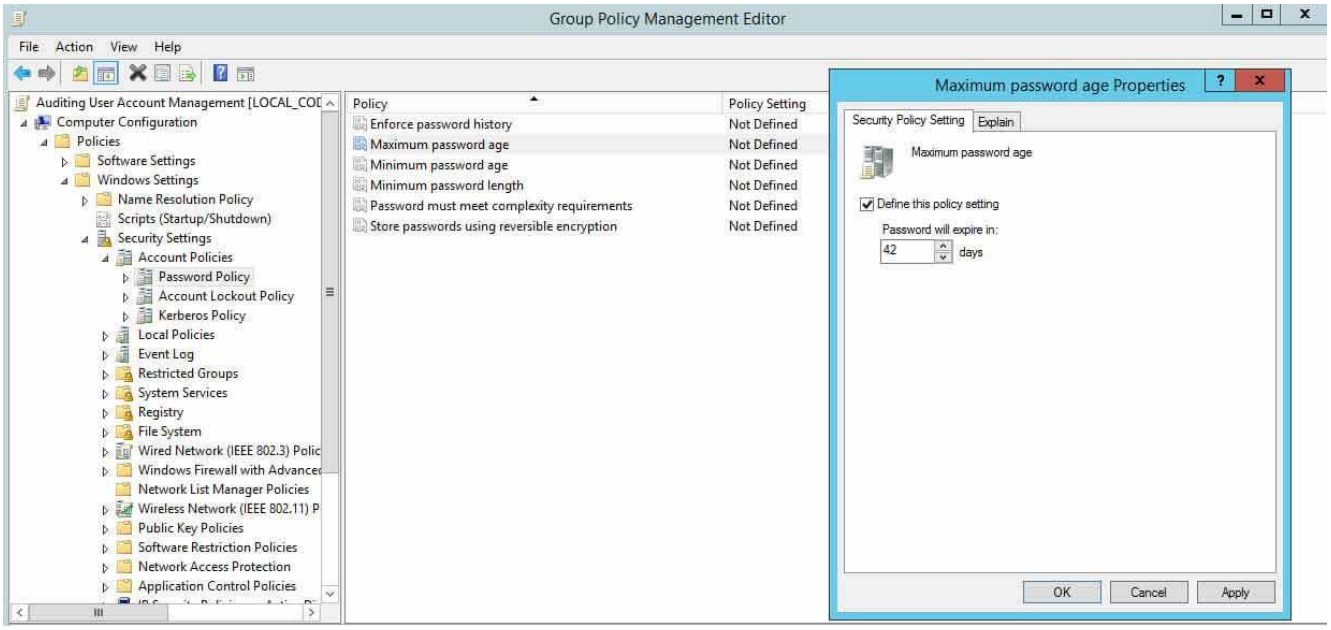


Рис.2.12. Встановлення максимального віку пароля

Active Directory присвоює унікальні номери всім об'єктам безпеки в Active Directory, включаючи користувачів, групи та інші, які називаються ідентифікаторами безпеки (SID). У старих версіях Windows користувачі могли запитувати SID для ідентифікації важливих користувачів і груп. Ця можливість може бути використана хакерами для отримання несанкціонованого доступу до даних.

Групова політика може вийти з-під контролю, якщо ви дозволите всім вашим адміністраторам вносити зміни так, як вони вважають за потрібне. Але відстежити зміни в груповій політиці може бути складно, оскільки журнали безпеки не можуть дати вам повну картину того, який саме параметр був змінений і як саме. Ви можете подивитися, як можна відстежувати зміни в груповій політиці в Короткому

довіднику з аудиту групової політики.

Найбільш важливі зміни GPO повинні бути обговорені з керівництвом і повністю задокументовані. Крім того, слід налаштувати оповіщення по електронній пошті про зміни в критично важливих об'єктах групової політики, оскільки вам потрібно знати про ці зміни якомога швидше, щоб уникнути простою системи.

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

3.1. Порядок розгортання рішення Active Directory

Розгортання рішення Active Directory проводиться на базі доменного контролеру Windows Server. Для початку встановлення потрібно назначити роль доменного контролера серверу.

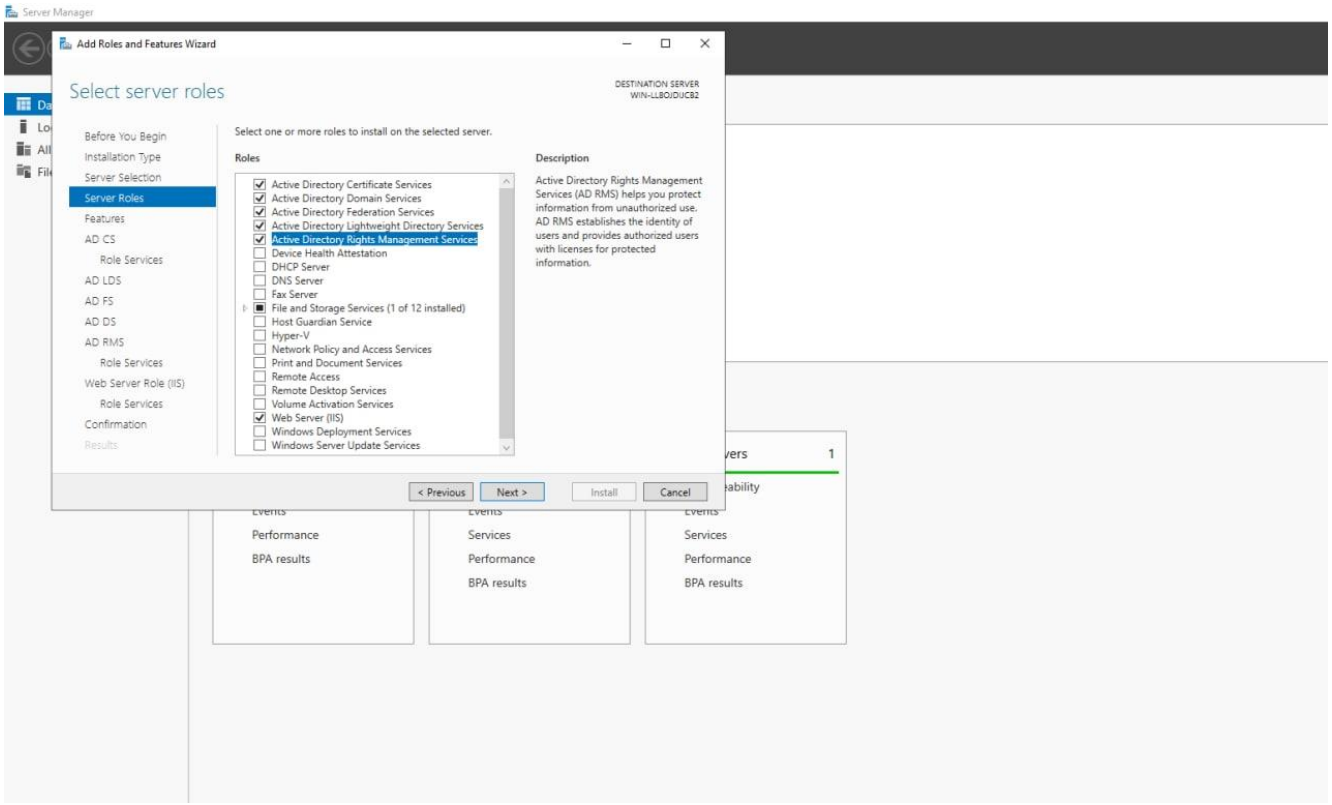


Рис.3.1. Процес встановлення ролі доменного контролеру для сервера

У даній роботі ми будемо створювати новий ліс і відповідно домен в ньому під назвою CONTOSO.

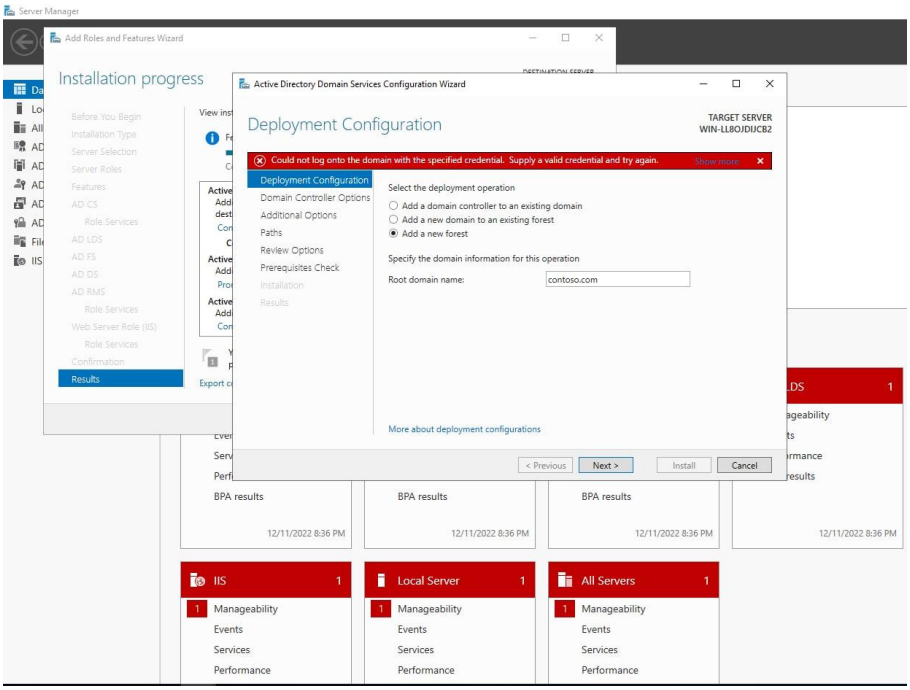


Рис.3.2. Створення нового лісу та домену

Також потрібно назначити цьому серверу роль DNS, оскільки в нашій інфраструктурі немає окремого dns серверу. У разі наявності такого у налаштуваннях можна делегувати ці повноваження іншому серверу.

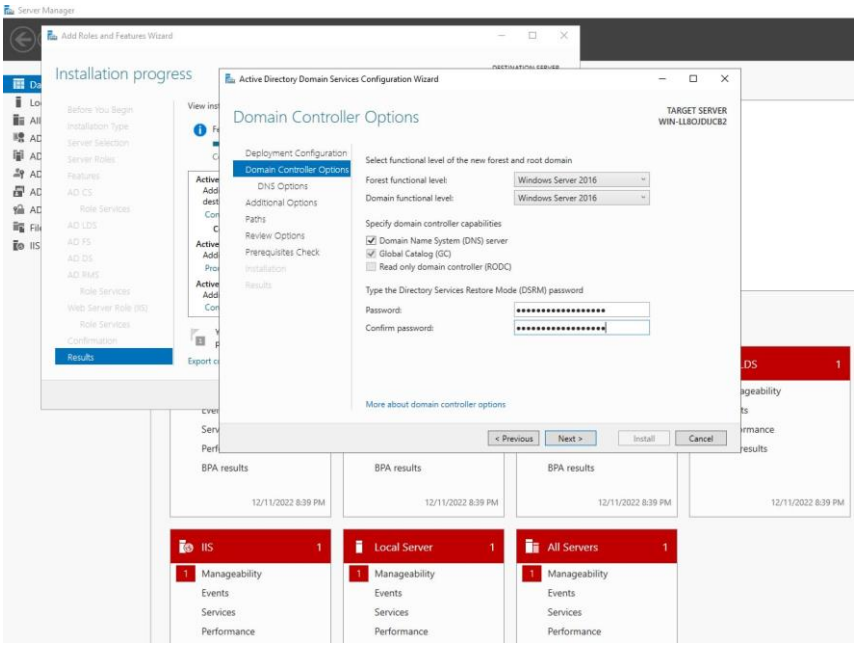


Рис.3.3. Встановлення ролі DNS серверу

Після встановлення ролі доменного контролеру для серверу, необхідно ввести будь-який хост Windows у домен, для подальших перевірок.

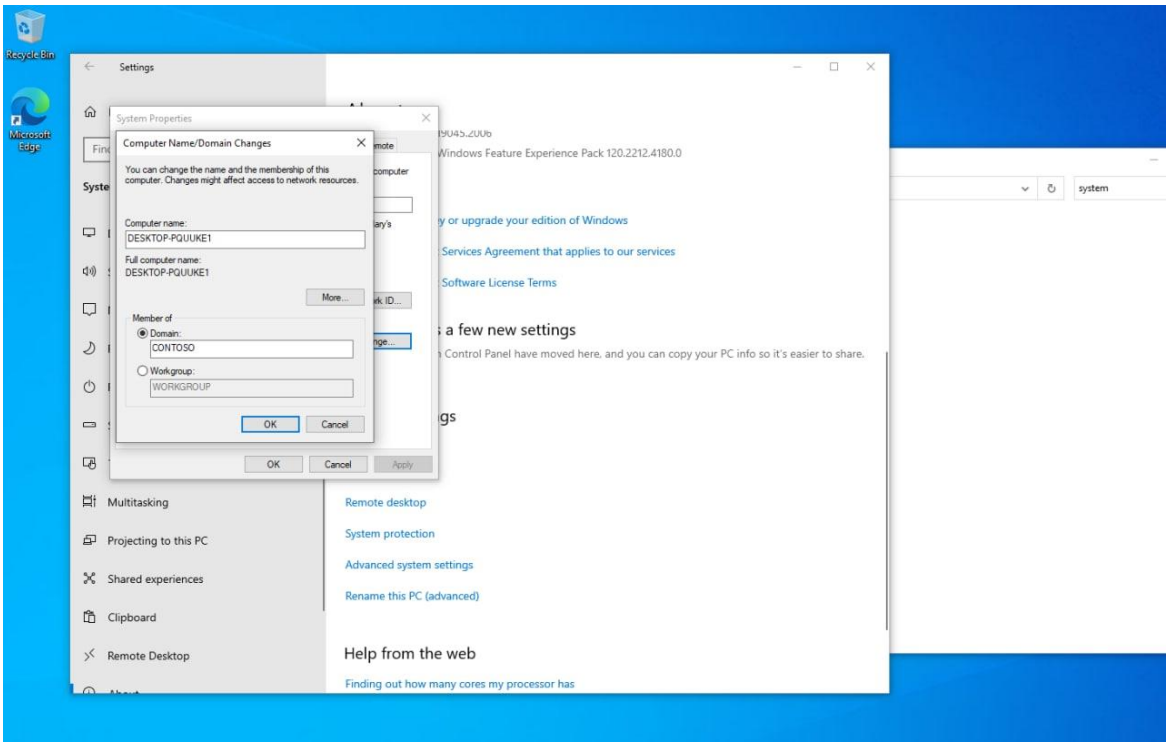


Рис.3.4. Введення хоста в домен

Для введення хоста в домен також необхідно створити для нього обліковий запис, під яким він зможе приєднатися до домену.

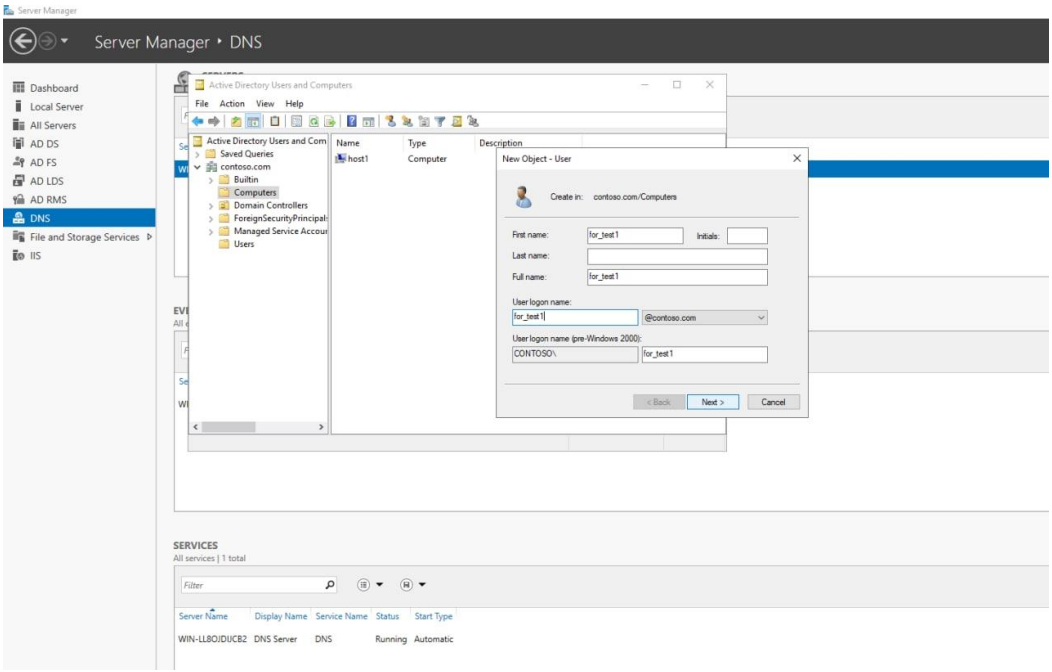


Рис.3.5. Створення облікового запису для хоста у Active Directory

Після введення облікових даних від спеціально створеного облікового запису робочий хост було успішно введено в домен

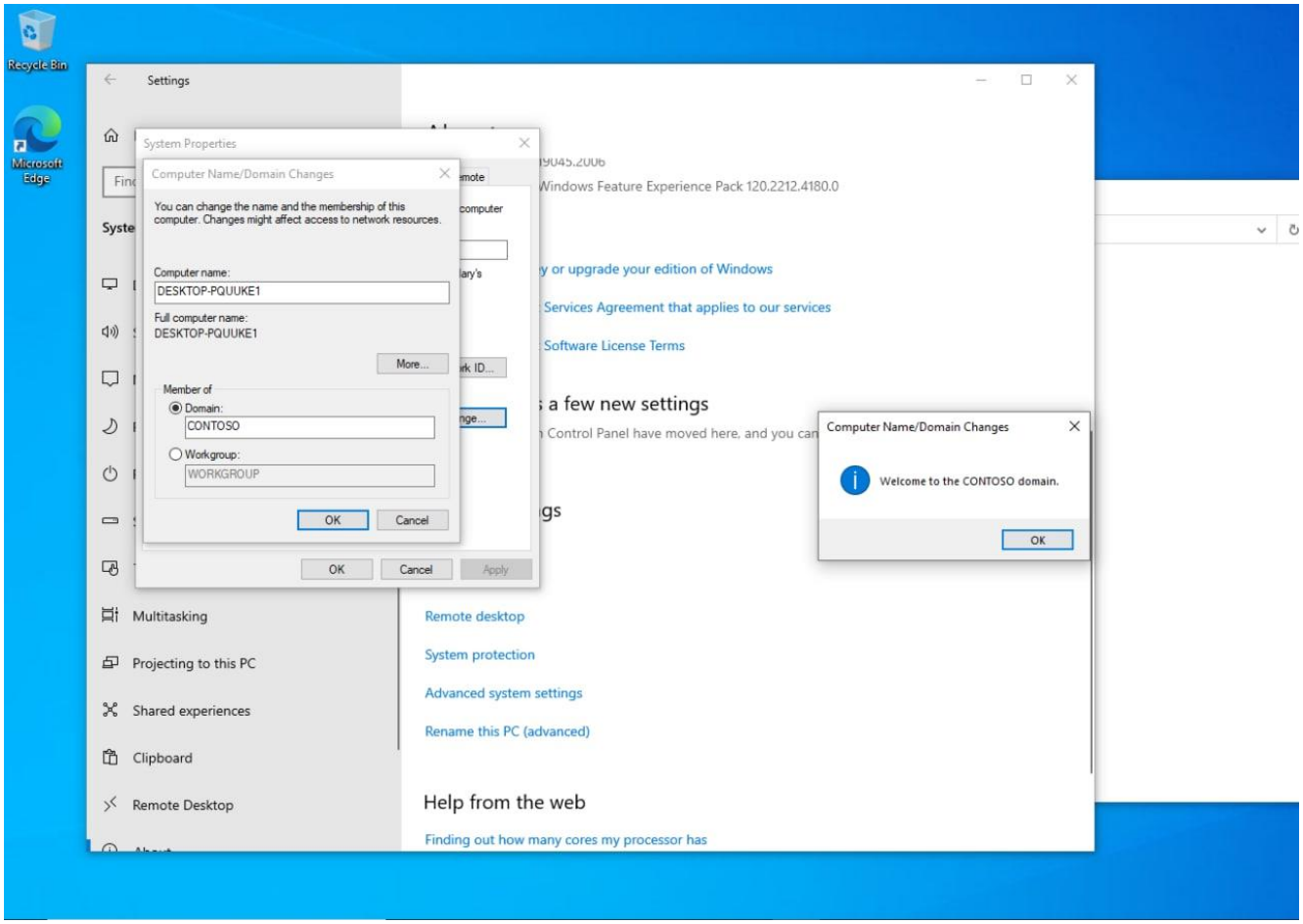


Рис.3.6. Введення хоста в домен

3.2. Технологія застосування рішення Active Directory

Основною технологією застосування рішення Active Directory тобто використання Active Directory для управління ідентифікацією та доступом користувачів до ресурсів є групові політики. Групові політики дають можливості налаштування великої кількості різних параметрів, в тому числі параметрів безпеки для об’єктів у Active Directory. Для початку роботи з груповими політиками, створимо тестову групову політику.

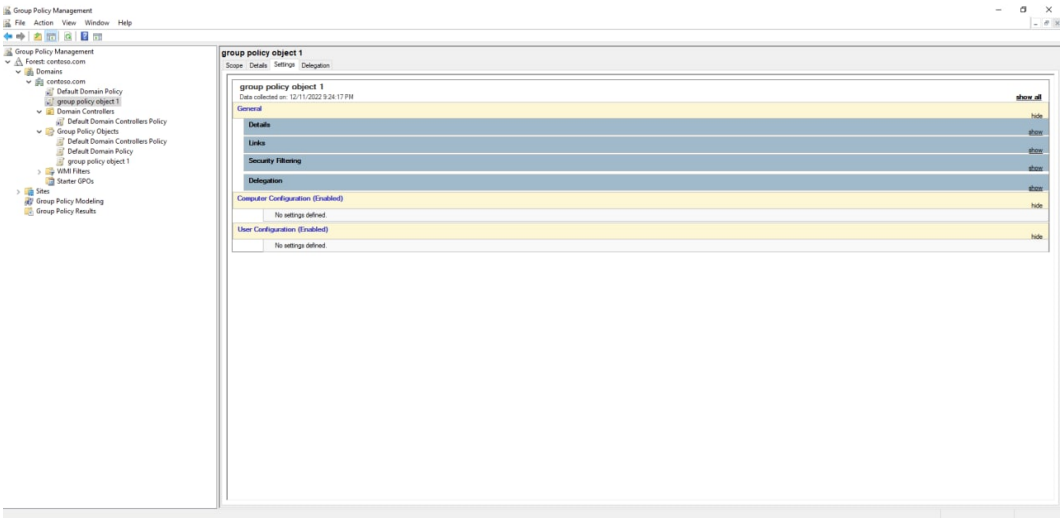


Рис.3.7. Тестова групова політика

Необхідно провести стандартні налаштування. До них входить вимкнення локальних адміністраторів на хостах у домені.

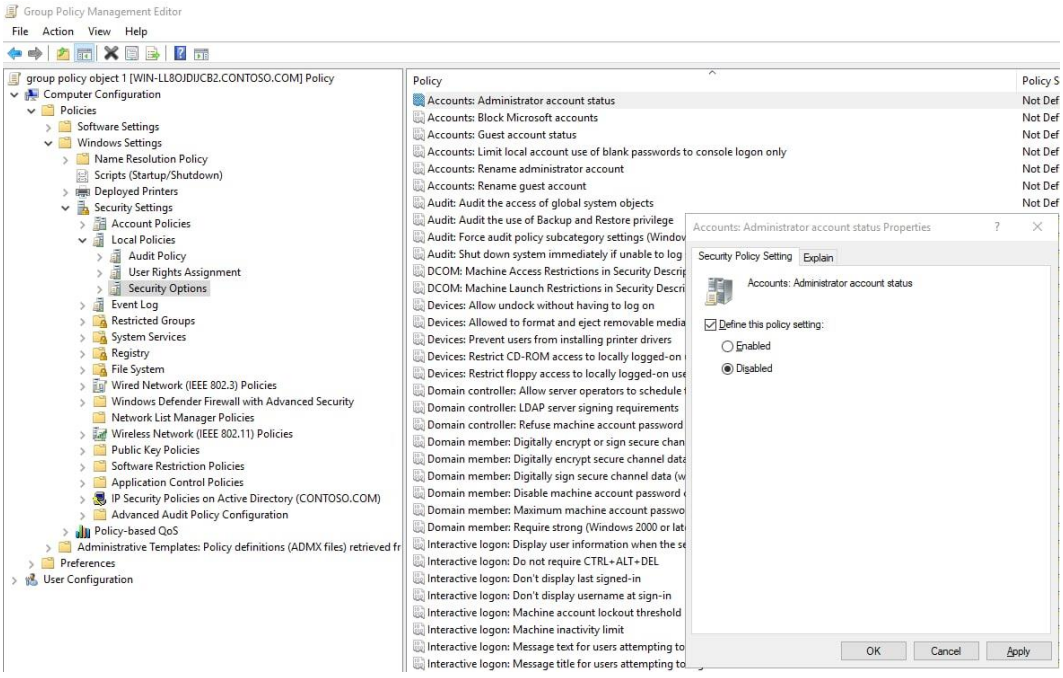


Рис.3.8. Вимкнення локальних адміністраторів на хостах у домені

Обліковий запис локального адміністратора, окрім того що був вимкнений, також був перейменований на qqqwwe.

Також необхідно налаштувати політику аудиту, яка містить параметри налаштувань аудиту подій у системі(події успішних та неуспішних входів, події доступів до об’єктів, події роботи з обліковими записами та їх зміни, системні події).

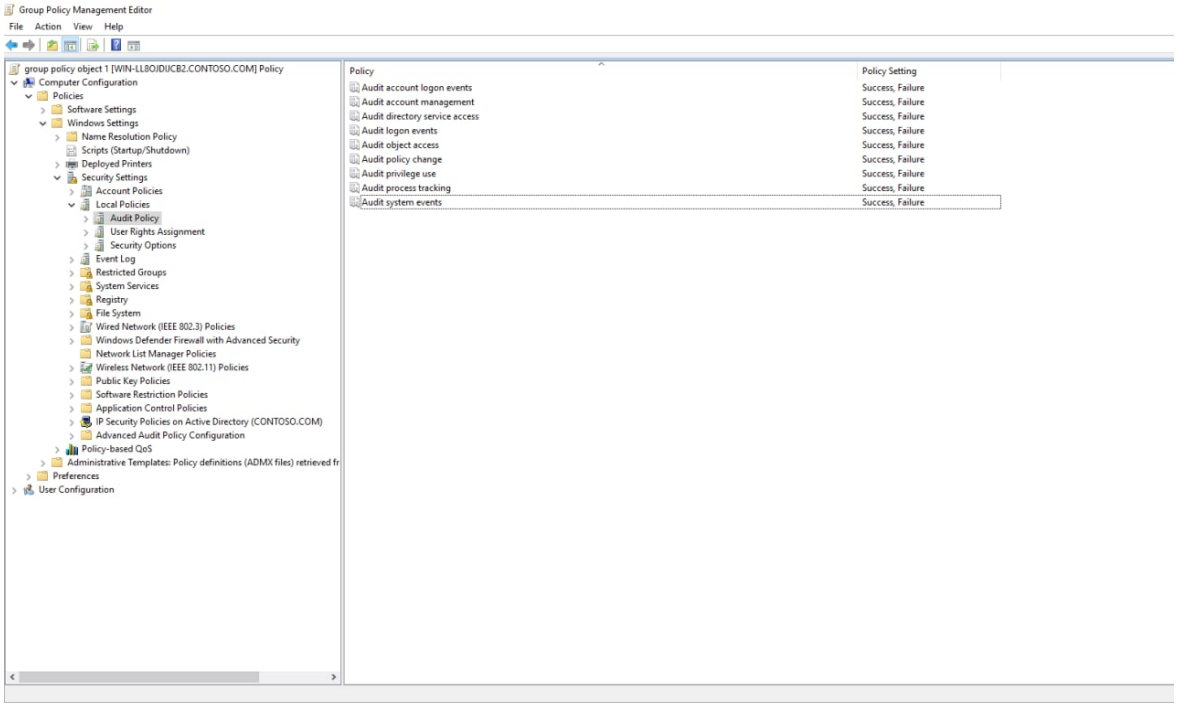


Рис.3.9. Політика аудиту

Після цього також потрібно налаштувати політики паролей, їх максимальний вік, мінімальну довжину, чи повинен пароль відповідати мінімальним параметрам складності.

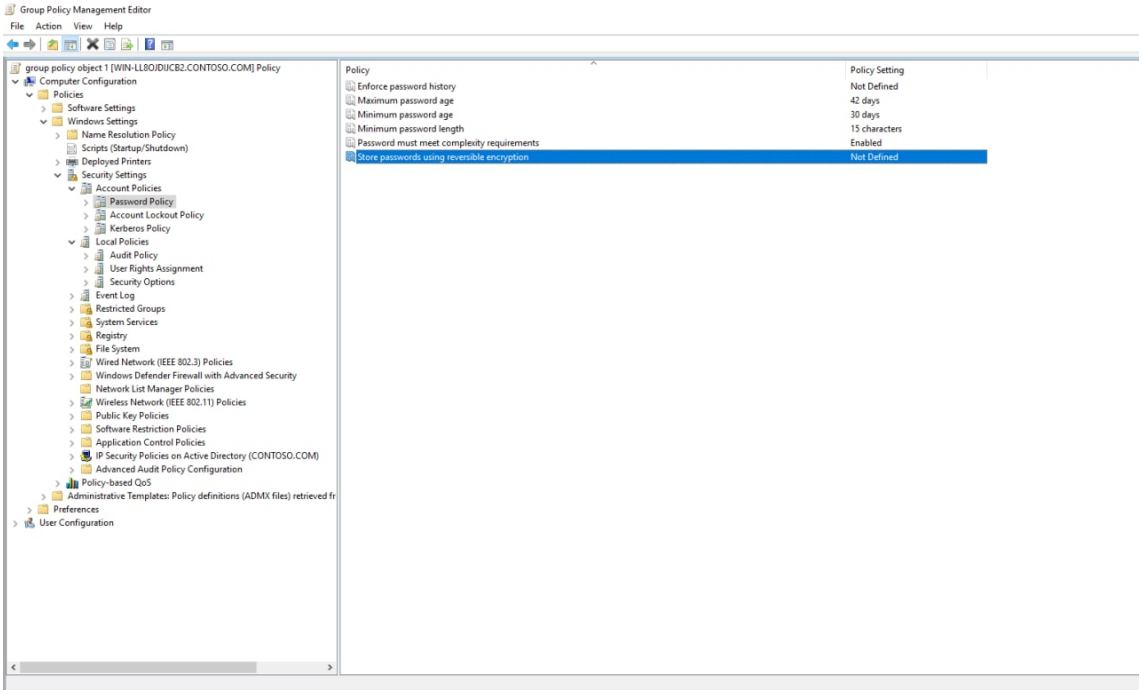


Рис.3.10. Політика паролей

Також необхідно налаштувати політику блокування акаунту при неуспішних спробах входу - через скільки спроб буде заблоковано аккаунт і на який час.

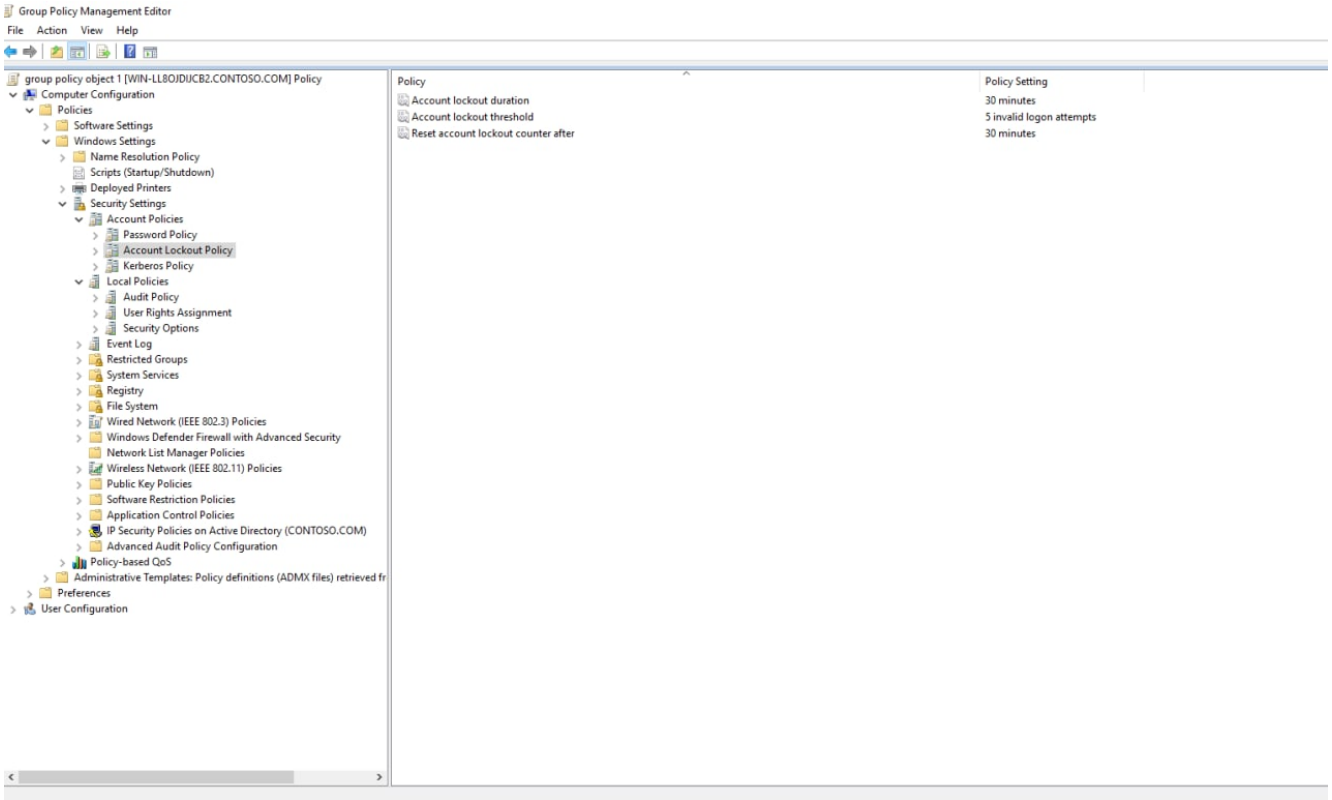


Рис. 3.11. Політика блокування акаунту

Перевіримо, чи спрацювали групові політики на робочій станції у домені. для цього виконаємо команду “gpupdate”, для оновлення групових політик на станції.

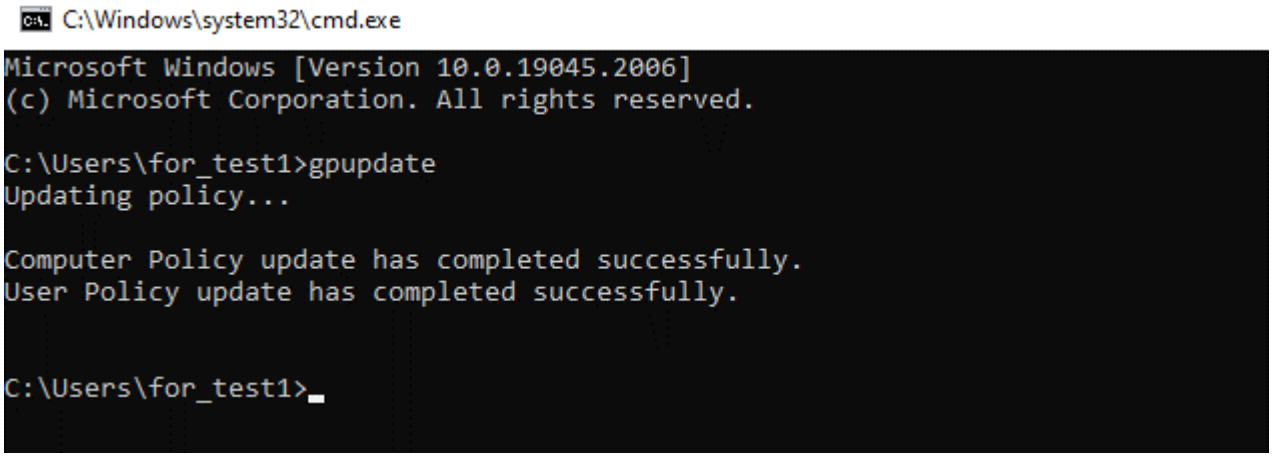


Рис.3.12. Оновлення групових політик на станції

Після цього, за допомогою команди “net user qqqwwe” перевіримо, чи застосувались зміни щодо локального адміністратора на робочій станції.

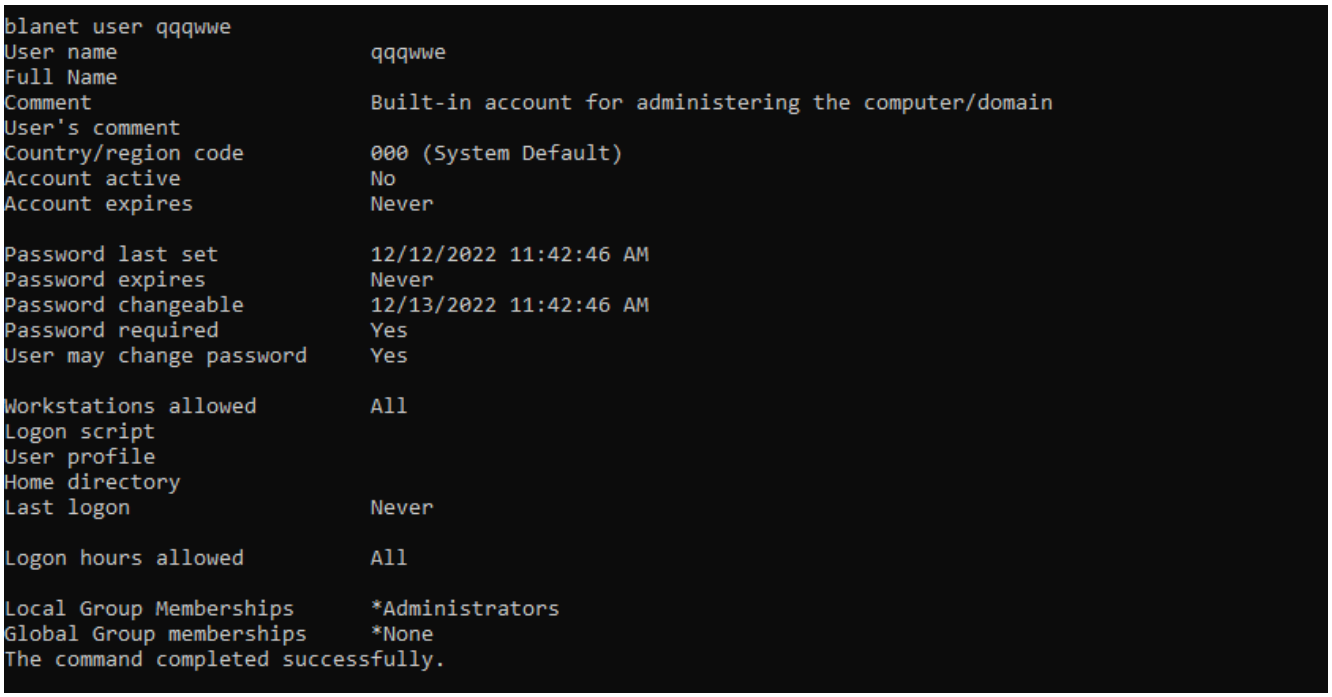


Рис.3.13. Інформація щодо акаунту qqqwwe

Як ми можемо побачити, акаунт не є активним та називається не як стандартний локальний адміністратор.

Також, для підвищення безпеки локальних акаунтів, є додаткове рішення під назвою LAPS (Local Administrator Password Solution) - "Рішення для паролів локальних адміністраторів" забезпечує управління паролями локальних облікових записів комп'ютерів, приєднаних до домену. Паролі зберігаються в Active Directory (AD) і захищені списками ACL, тому лише авторизовані користувачі можуть читати їх або вимагати їх скидання.

Переваги використання Windows LAPS:

захист від атак типу pass-the-hash і латерального обходу;

покращена безпека для сценаріїв віддаленої служби підтримки;

можливість входу і відновлення пристроїв, які в іншому випадку недоступні;

детальна модель безпеки (списки контролю доступу і додаткове шифрування паролів) для захисту паролів, які зберігаються в Windows Server Active Directory;

підтримка моделі управління доступом на основі ролей Azure для захисту паролів, що зберігаються в Azure Active Directory.

3.3. Рекомендації щодо застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи організації

Основною технологією застосування рішення Active Directory тобто використання Active Directory для управління ідентифікацією та доступом користувачів до ресурсів є групові політики. Групові політики дають можливості налаштування великої кількості різних параметрів, в тому числі параметрів безпеки для об’єктів у Active Directory. Для початку роботи з груповими політиками, створимо тестову групову політику.

Зважаючи на складність сучасних мереж, забезпечення належного нагляду за мережевою ідентифікацією та пов'язаними з нею активами має вирішальне

значення. Так само, як захист периметра та управління виправленнями є важливими компонентами програми безпеки, управління ідентифікацією та доступом також повинно бути освоєно.

Впровадження успішної програми IAM є складним завданням, оскільки кожна організація має унікальні потреби та толерантність до ризику. Однак існує кілька основних кроків, які команди безпеки можуть зробити для освоєння IAM в організаціях будь-якого розміру і галузей. Уникнути того, щоб нагляд за ідентифікацією та доступом не став ахіллесовою п'ятою мережі, можна за допомогою наступних чотирьох найкращих практик управління ідентифікацією та доступом.

Задокументуйте очікування та відповідальність за успіх IAM.

Успішна система IAM не є повною до тих пір, поки не будуть задокументовані правила взаємодії. Хоча документація - це ще не все - занадто багато організацій покладаються на неї занадто сильно - вона є необхідністю. Фахівці з інформаційної безпеки повинні уникати надмірної залежності від документації і замість цього розробляти - і повідомляти - стандарти і політики в збалансований спосіб.

Багато організацій впроваджують управління привілейованими обліковими записами, єдиний вхід і забезпечення користувачів, але ці засоби контролю IAM знову і знову виявляються неефективними. Це часто є результатом порушення комунікації між командами IT та безпеки, зацікавленими сторонами, системними аналітиками, керівниками бізнес-підрозділів та менеджерами по роботі з персоналом. Часто трапляється так, що кожен дивиться один на одного і вважає, що кожен виконує свою частину роботи. На жаль, в результаті стандарти, політики і процедури IAM висять на волосині. Важливо, щоб ця документація була зрозуміла і узгоджена всіма співробітниками організації для успішного впровадження кращих практик управління ідентифікацією та доступом.

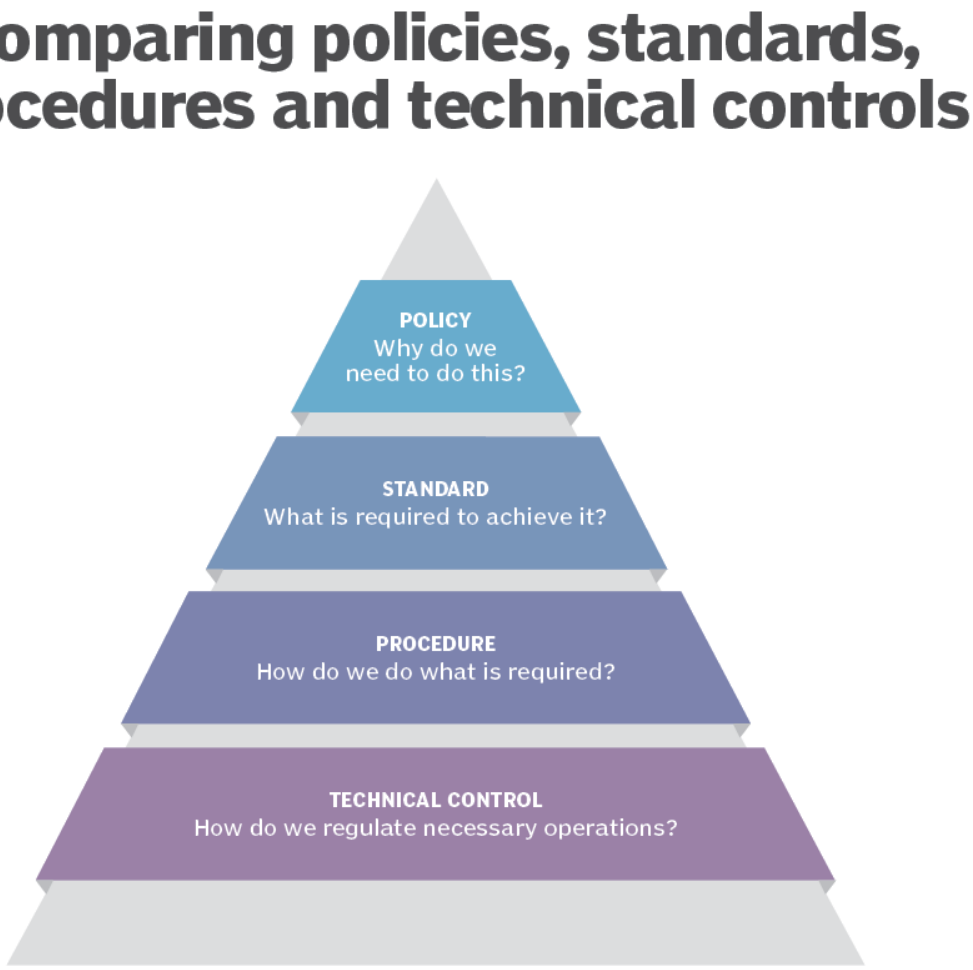


Рис.3.14. Відмінності між політиками, процедурами, стандарти та технічним контролем

Забезпечте успіх IAM, визначивши обов'язки та очікування в політиках, стандартах та процедурах.

Централізуйте безпеку та критичні системи навколо ідентичності

Багато організацій роблять помилку, впроваджуючи дорогі системи IAM в одній частині мережі - як правило, з Windows Active Directory - в той час як інші критичні системи виходять за рамки такої компетенції. Сюди входять ERP та інші веб-системи, мобільні і хмарні середовища, сховища вихідного коду і IoT. У цих випадках плутанина ще більше ускладнюється тим, що внутрішні ідентифікаційні дані співробітників регулюються, але зовнішні партнери, підрядники і клієнти часто не підлягають нагляду.

IAM є непростим завданням, і успішне впровадження системи IAM в масштабах всього підприємства може зайняти значну кількість часу. Найкращою практикою управління ідентифікацією та доступом є розгортання програми поетапно, щоб забезпечити безпечне прийняття політик та процедур. Переконайтеся, що короткострокові та довгострокові плани розширюють сферу застосування IAM у всіх критично важливих для бізнесу системах, де це можливо та доцільно.

Програми IAM повинні забезпечувати захист ідентифікаційних даних, систем та каналів.

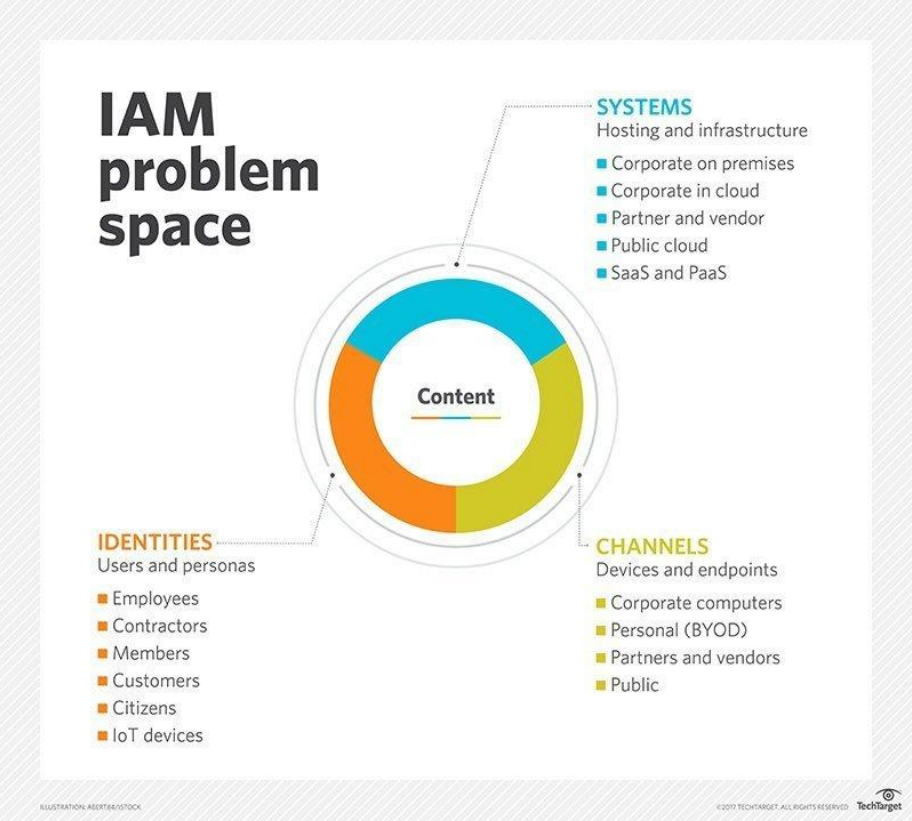


Рис.3.15. Системи IAM повинні забезпечувати захист корпоративних систем, сутностей та кінцевих точок

Кодифікація бізнес-процесів для мінімізації ризиків.

Часто повсякденні процеси управління ідентифікацією та доступом до облікових записів сприймаються як належне. Наприклад, необхідно враховувати загальні ролі, які потребують доступу, аномальні запити на доступ та фактичні

права доступу у порівнянні із запитуваними.

Неналежним чином захищені та керовані мережеві ідентифікаційні дані становлять відчутний ризик.

Не слід ігнорувати ці фундаментальні найкращі практики управління ідентифікацією та доступом. Якщо їх не контролювати, вони увічнюють недогляди, пов'язані з ідентифікацією та обліковими записами, а також те, що можна вважати непотрібними ризиками для безпеки. Наприклад, може статися "повзуче розмивання привілеїв" та неправильне управління життєвим циклом ідентичності, що може призвести до швидких та серйозних наслідків.

Оцініть ефективність поточних засобів контролю IAM

На жаль, впровадження засобів контролю безпеки в програму IAM може приспати в організаціях помилкове відчуття безпеки. Це явище сприйняття безпеки як належного може проявлятися в тому, що команди безпеки не вимірюють прогрес програми IAM з плином часу.

У деяких випадках підприємство інвестує кошти і впроваджує засоби контролю, але при цьому програма IAM не забезпечує ефективного впровадження або управління автентифікацією ідентичності та доступом в мережі. Найкращий спосіб уникнути недостатнього впровадження систем IAM таким чином - це постійно задавати питання: "Як ця програма працює для організації?" Визначте конкретні переваги та недоліки в контексті нагляду за безпекою та виміряйте ці показники. Використовуйте мислення, засноване на нульовій точці, щоб визначити, що організація повинна робити більше, а що менше, коли справа доходить до впровадження IAM. Ця вправа може суттєво допомогти у досягненні та підтримці дійсно ефективної системи управління інформаційною безпекою.

Дорогі інвестиції в новітні інструменти та технології кібербезпеки не можуть замінити захист, який можуть забезпечити кращі практики IAM. Також необхідно дотримуватись наступних правил:

зменшення складності мережі, де це можливо;

вдосконалення аудиторських процесів , щоб допомогти з наглядом та дотриманням вимог;

впровадження розподілу обов'язків та принципу найменших привілеїв;

забезпечення надання користувачам належних дозволів, необхідних для виконання їхньої роботи;

забезпечення належного управління привілейованими обліковими записами;

використання продуктів IAM для точного налаштування середовища;

мінімізація витрат і максимізація задоволеності користувачів, надаючи їм можливість керувати власними обліковими записами за допомогою налаштованих робочих процесів IAM;

зосередження на видимості та контролі.

Неправильно захищені і керовані мережеві ідентичності представляють відчутний ризик. Останнє, що повинна робити команда безпеки - це неправильно управляти цими активами.

ВИСНОВКИ

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

Active Directory - це вбудований у Windows продукт який має багато можливостей для вирішення цієї проблеми. Підтримка та побудова на основних поширених протоколах, водночас проста та дуже гнучка система налаштування та управління, можливість інтегрування хмарного варіанту з великою кількістю різних додатків та систем робить це рішення дуже вдалим для використання у організації.

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 Active Directory

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

Active Directory за замовчуванням має власну базу і підтримку протоколу LDAP, що надає змогу інтеграції з більшістю продуктів, через поширеність цього протоколу.

Для використання Azure Active Directory 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 Active Directory. Також розроблено рекомендації щодо застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи організації.

Технології IAM покликані спростити процес надання послуг користувачам та налаштування облікових записів. Ці системи повинні скоротити час, необхідний для завершення цих процесів, за допомогою контрольованого робочого процесу, який зменшує кількість помилок і потенціал для зловживань, дозволяючи автоматизувати виконання облікових записів. Система IAM також повинна дозволяти адміністраторам миттєво переглядати та змінювати ролі та права доступу.

Ці системи повинні забезпечувати баланс між швидкістю та автоматизацією процесів і контролем, необхідним адміністраторам для моніторингу та зміни прав доступу. Отже, для управління запитами на доступ центральному каталогу потрібна система прав доступу, яка автоматично співвідносить назви посад співробітників, ідентифікатори підрозділів та місцезнаходження з відповідними рівнями привілеїв.

Кілька рівнів перевірки можуть бути включені в робочі процеси, щоб забезпечити належну перевірку окремих запитів. Це спрощує налаштування відповідних процесів перевірки для доступу вищих рівнів, а також полегшує перевірку існуючих прав для запобігання "повзучості привілеїв", тобто поступового накопичення прав доступу, які виходять за рамки того, що потрібно користувачам для виконання їхніх робочих завдань.

Системи IAM повинні використовуватися для забезпечення гнучкості у створенні груп з конкретними привілеями для конкретних ролей, щоб права доступу, засновані на посадових функціях працівників, могли бути рівномірно розподілені. Система також повинна забезпечувати процеси запиту та затвердження для зміни привілеїв, оскільки працівники з однаковими посадами та місцем роботи можуть потребувати індивідуального або дещо відмінного доступу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Most Important Group Policy settings Режим доступу: World Wide Web - URL - https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/
2. Group Poicy Best Practices Режим доступу: World Wide Web - URL - https://www.netwrix.com/group_policy_best_practices.html
3. Group Policy Best Practices Режим доступу: World Wide Web - URL - https://www.manageengine.com/products/active-directory-audit/kb/best-practices/best-group-policy-settings.html
4. What is group policy Режим доступу: World Wide Web - URL - https://adamtheautomator.com/what-is-group-policy/
5. How to work with Group Policy objects Режим доступу: World Wide Web - URL - https://blog.quest.com/what-is-group-policy-and-how-do-gpos-work/
6. Microsoft Group Policy tutorials Режим доступу: World Wide Web - URL - https://www.techtarget.com/searchwindowsserver/tutorial/Microsoft-Group-Policy-Tutorial?_ga=2.16154166.1670747231.1670582474-1932888692.1670582474&_gl=1*gvnrda*_ga*MTkzMjg4ODY5Mi4xNjcwNTgyNDc0*_ga_TQKE4GS5P9*MTY3MDU4MjQ3My4xLjEuMTY3MDU4MjQ5My4wLjAuMA..
7. What is group policy and what role it is playing in security Режим доступу: World Wide Web - URL - https://www.lepide.com/blog/what-is-group-policy-gpo-and-what-role-does-it-play-in-data-security/
8. How to work with Group Policy Режим доступу: World Wide Web - URL - https://habr.com/ru/company/galssoftware/blog/543588/
9. Active Directory Режим доступу: World Wide Web - URL - https://learn.microsoft.com/ru-ru/windows/win32/ad/active-directory-domain-services
10. Architecture of Active Directory Режим доступу: World Wide Web - URL - https://studfile.net/preview/4603396/
11. Global Settings and synchronization with AD Режим доступу: World Wide Web - URL - https://mirobase.com/spravka/globalni-nalashtuvannja-sinkhronizacija-

z-active-directory/

12. Installing and using Active Directory Users and Computers Режим доступу: World Wide Web - URL - https://petri.com/install-active-directory-users-and-computers/#Why_you_should_install_Active_Directory_Users_and_Computers_on_a_management_workstation
13. Active Directory Users and Computers Режим доступу: World Wide Web - URL - https://petri.com/how-to-access-active-directory/#Active_Directory_Users_and_Computers
14. Active Directory Domain Services overview Режим доступу: World Wide Web - URL - https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
15. Active Directory Documentation Режим доступу: World Wide Web - URL - https://learn.microsoft.com/en-us/azure/active-directory/
16. Active Directory Режим доступу: World Wide Web – URL - https://en.wikipedia.org/wiki/Active_Directory

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 ACTIVE DIRECTORY»

Виконав: Гребенюк Владислав Олександрович

Керівник: Гахов Сергій Олександрович, д.в.н., доц

2

Об'єкт дослідження – управління ідентифікацією та доступом користувачів на базі рішення Active Directory

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;

Дослідження проблеми управління ідентифікацією та доступом користувачів до інформаційної системи організації

3

У сучасному світі технологій, системи управління ідентифікацією та доступом користувачів є невід'ємною частиною бізнес-процесів, тому що керівники підприємств та IT-відділи перебувають під посиленим регуляторним та організаційним тиском щодо захисту доступу до корпоративних ресурсів і з часом цей регуляторний тиск посилюється. Системи IAM - це системи політики технологій, що гарантують, що потрібні користувачі (які є частиною екосистеми, пов'язаної з підприємством або всередині нього) мають відповідний доступ до технологічних ресурсів

Система IAM дозволяє IT-спеціалістам контролювати доступ користувачів до критично важливої інформації в організаціях. Системи IAM повинні виконувати наступні функції: збирати та реєструвати реєстраційні дані користувачів, керувати корпоративною базою даних ідентифікаційних даних користувачів, а також організовувати призначення та скасування привілеїв доступу.

Аналіз основних засобів управління ідентифікацією та доступом користувачів до інформаційної системи організації

4

Основні інструменти управління ідентифікацією та доступом користувачів є широкоохоплюючими та взаємодоповнюючими. До них входить: налаштування користувачів, централізоване управління доступом, SSO (єдиний вхід), MFA, сервіс порталу доступу та інші. Два базових принципа, які мають бути імплементовані для безпечного доступу до цифрових активів:

- IAM підтверджує, що користувач, програмне або апаратне забезпечення є тим, за кого себе видає, шляхом перевірки його облікових даних у базі даних.
- Системи управління доступом на основі ідентифікаційних даних надають лише відповідний рівень доступу.

У організації має бути налаштований життєвий процес PAM (Privileged Access Management). У цей процес входять наступні кроки:

- визначення привілейованого доступу
- управління привілейованим доступом
- моніторинг використання привілейованих прав
- алерти на можливе перевищення прав доступу

Аналіз існуючих рішень щодо ідентифікації та управління доступом користувачів до інформаційної системи організації

5

Основними вендорами IAM системе:

- Microsoft AD та Azure AD
- IBM Cloud IAM
- Oracle Identity Cloud Service
- Ping Identity
- RSA SecurID Suite
- CyberArk Workforce Identity
- SailPoint tdentity IQ

Всі IAM системи мають відповідати регуляторним стандартам. IAM системи повинні забезпечувати наступні контролі у організації:

- механізми ідентифікації користувачів та систем, до яких вони мають доступ
- опис процесу авторизації та рівнів доступу, які були надані користувачу
- управління привілейованими обліковими записами
- опис процесів та критеріїв створення, модифікації та видалення акаунтів

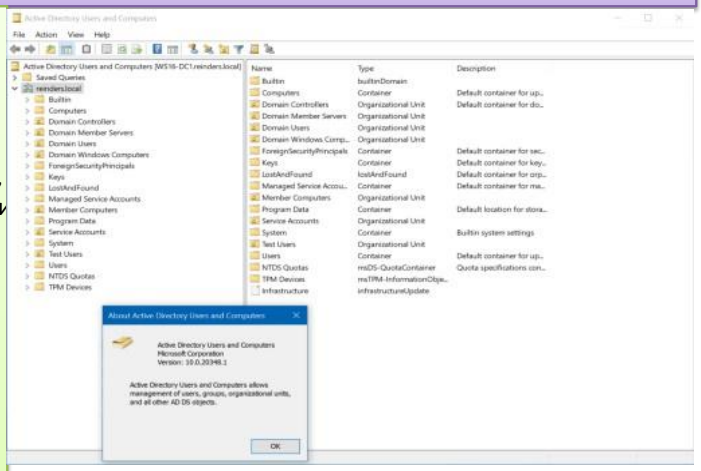
Призначення та основні функції рішення Active Directory

6

Active Directory - це ієрархічно організоване сховище даних про об'єкти мережі, що забезпечує зручні засоби для пошуку та використання цих даних. Active Directory - це ієрархічно організоване сховище даних про об'єкти мережі, що забезпечує зручні засоби для пошуку та використання цих даних.

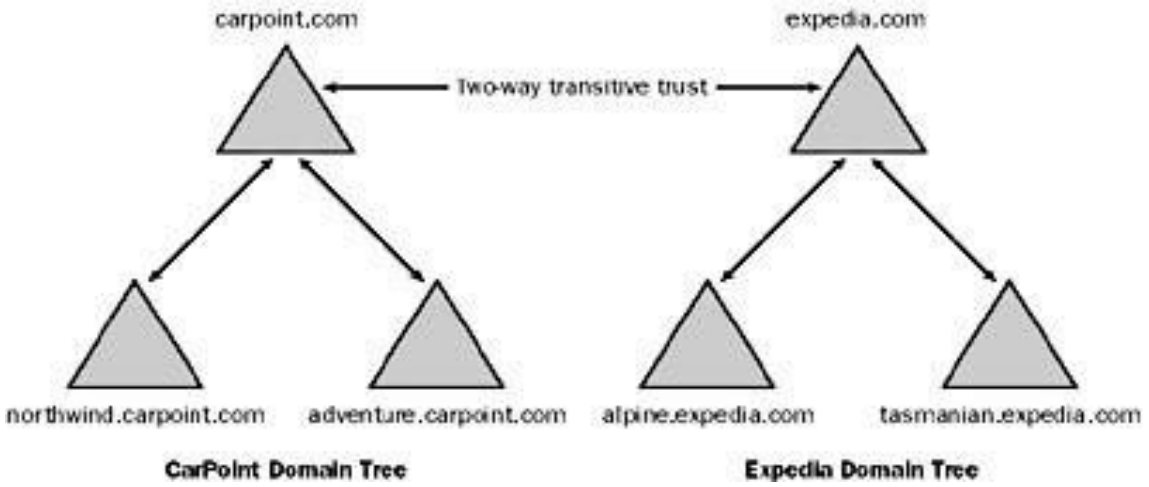
Для керування Active Directory призначені засоби адміністрування та підтримки

- *Active Directory - користувачі та комп'ютери (Active Directory Users and Computers)* - дозволяє керувати користувачами, групами, комп'ютерами та організаційними підрозділами (ОП);
- *Active Directory - домени та довіра (Active Directory Domains and Trusts)* - служить для роботи з доменами, деревами доменів та лісами доменів;
- *Active Directory - сайти та служби (Active Directory Sites and Services)* - дозволяє керувати сайтами та підмережами;
- *Результуюча політика (Resultant Set of Policy) - використовується для перегляду поточної політики користувача або системи та планування змін у політиці*



Архітектура рішення Active Directory

7



Основний вигляд структури Active Directory - верхнім рівнем структури є ліс - сукупність всіх об'єктів, атрибутів та правил в Active Directory. Ліс містить одне або кілька дерев, пов'язаних транзитивними стосунками довіри. Дерево містить один або декілька доменів, також пов'язаних в ієрархію транзитивними стосунками довіри. Домени ідентифікуються своїми структурами імен DNS — просторами імен.

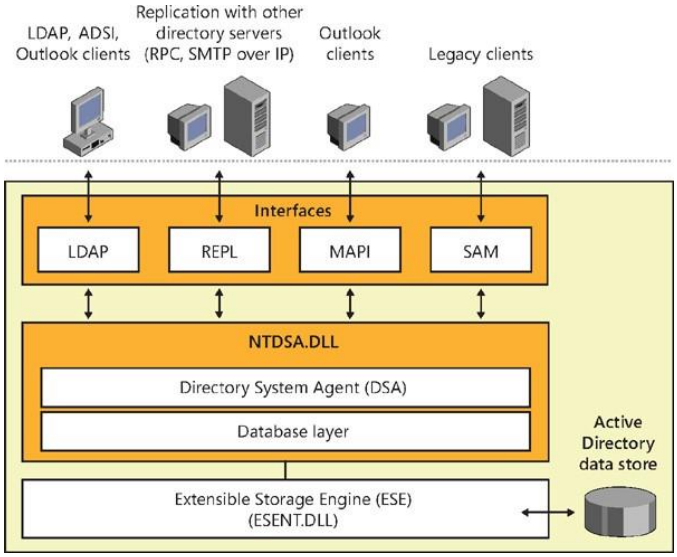
Архітектура Active Directory

8

В основі архітектури Active Directory лежать такі технології:

- Стандарти X.500 і X.509;
- Стандартний протокол доступу до каталогів LDAP (Lightweight Directory Access Protocol);
- Стек протоколів TCP/IP, що є основним при побудові мережі масштабу корпорації;
- Служба DNS (Domain Name Service), що використовується для дозволу доменних імен в IP-адреси;
- Протокол динамічної конфігурації клієнта DHCP Система Kerberos

Архітектура AD включає три рівні служб, кілька інтерфейсів і протоколів. Вищим рівнем AD є системний агент каталогу (Directory System Agent, DSA), що надає API-інтерфейси для доступу до каталогу. Нижній рівень архітектури AD представлений розширюваним ядром сховища

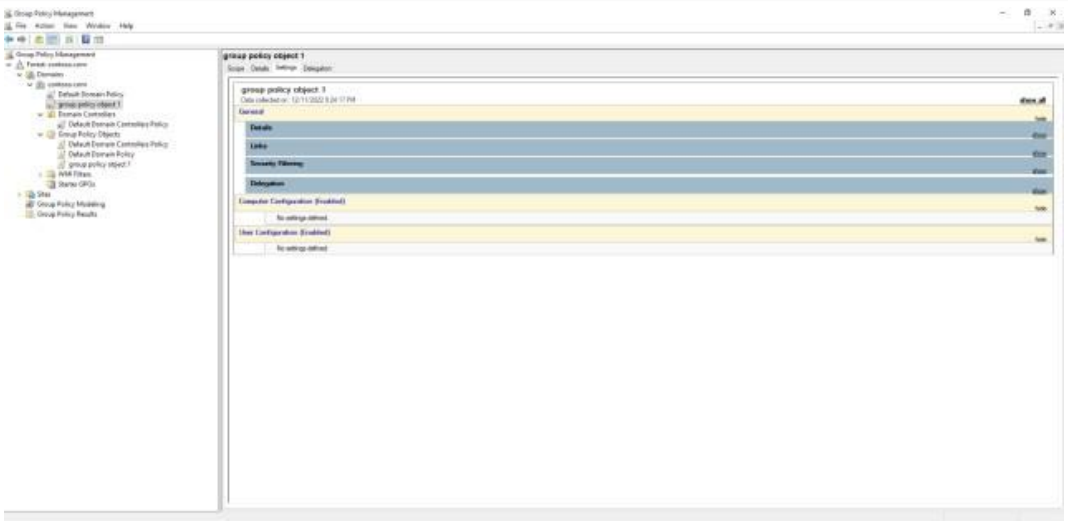


Технологія застосування рішення Active Directory

9

Основною технологією застосування рішення Active Directory тобто використання Active Directory для управління ідентифікацією та доступом користувачів до ресурсів є групові політики. Групові політики дають можливості налаштування великої кількості різних параметрів, в тому числі параметрів безпеки для об'єктів Active Directory.

Необхідно провести стандартні налаштування. До них входить вимкнення локальних адміністраторів та гостьових облікових записів на хостах у домені, налаштування політики аудиту, яка містить параметри налаштувань аудиту подій у системі, налаштування політики паролей та політики блокування облікових записів



Рекомендації щодо управління ідентифікацією та доступом користувачів до інформаційної системи організації

11

Основні рекомендації з ідентифікації та управління доступом користувачів до інформаційної системи організації

- документуванняочікуваньта відповідальностідля успішноговпровадженнята використанняIAM системи IAM - Успішна система IAM не є повною до тих пір, поки не будуть задокументовані правилавзаємодії;
- централізаціябезпеки та критичнихсистемнавколоідентичності– під наглядомIAM системповинні бути всі сегменти мережі, ERP, мобільні хмарнісередовища,сховищавихідногокодуі IoT, зовнішні партнериі підрядники,якщовони користуютьсясистемамиорганізації
- оцінка ефективності поточних засобів контролю IAM - впровадженнязасобівконтролюбезпеки в програмуIAM можеприспатив організаціяхпомилковевідчуттябезпеки;
- вдосконаленняаудиторськихпроцесів, щоб допомогтиз наглядомта дотриманнямвимог;
- впровадженнярозподілуобов'язківта принципунайменшихпривілеїв;
- забезпеченнянаданнякористувачаминалежнихдозволів,необхідних для виконанняїхньої роботи;
- забезпеченняналежногоуправлінняпривілейованимиобліковимизаписами;
- використанняпродуктівIAM для точногоналаштуваннясередовища;
- мінімізаціявитрат і максимізаціязадоволеності користувачів, надаючи їм можливість керувати власнимиобліковимизаписамиза допомогоюналаштованихробочихпроцесівIAM;
- зосередженняна видимостіта контролі

ВИСНОВКИ

12

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

- 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 Active Directory
- Active Directory - це вбудований у Windows продукт який має багато можливостей для вирішення цієї проблеми . Підтримка та побудова на основних поширених протоколах, водночас проста та дуже гнучка система налаштування та управління, можливість інтегрування хмарного варіанту з великою кількістю різних додатків та систем робить це рішення дуже вдалим для використання у організації
- У роботі запропоновано порядок розгортання та застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи на основі рішення Active Directory, встановлено основні функції та принципи роботи продукту Active Directory. Також розроблено рекомендації щодо застосування технології управління ідентифікацією та доступом користувачів до інформаційної системи організації .

Дякую за увагу!