УДК 004.056
DOI: 10.31673/2409-7292.2023.020008

Захаржевський А. Г., Даценко Ю. О., Куліш І. В.

ОСОБЛИВОСТІ ІДЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ КОРИСТУВАЧІВ В ХМАРНИХ ПРОВАЙДЕРАХ НА ОСНОВІ MICROSOFT AZURE CLOUD

В даній статті розглядається впровадження авторизації та аутентифікації на базі хмарних провайдерів, через зростання їх популярності серед використання бізнесом, компаніями. Проведено аналіз існуючих рішень на базі різних хмарних провайдерів. Виявлено наявні недоліки та переваги кожного з рішень та визначено найкраще рішення серед можливих існуючих. Досліджено процеси аутентифікації та авторизації в Amazon Web Services на основі Microsoft Azure Cloud.

Ключові слова: інформаційна система, кібербезпека, хмарні технології, загрози безпеки, крадіжки, ddos, безпека веб-додатків, авторизація, аутентифікація, управління ресурсами.

Вступ

Сьогодні, зі зростанням кількості різноманітних автоматизованих, інформаційних систем, безпека користування цими система стикається з багатьма проблемами. Серед найголовніших проблем, можна виділити безпечна авторизація та аутентифікація користувачів певними системами. Адже, що таке авторизація – це процес встановлення відповідних прав на якісь певні дії, для певних користувачів системи. В той час, як аутентифікація допомагає автоматизованим системам визначити, чи дійсно це саме цей користувач хоче отримати доступ до системи, чи виконати якісь певні дії, а не зловмисник.

Формулювання проблеми

Amazon Web Services (AWS) – платформа, хмарний провайдер, який є одним із найпопулярнішим у використанні бізнесом. AWS є дочірньою компанією Amazon.com, що надає платформу хмарних обчислень в оренду приватним особам, компаніям та урядам. Технологія дозволяє абонентам мати у своєму розпорядженні повноцінний віртуальний кластер комп’ютерів, який завжди доступний через Інтернет. Віртуальні комп’ютери AWS мають більшість атрибутів реального комп'ютера, включаючи апаратні пристрої (процесор, відеокарту, локальну та оперативну пам'ять, жорсткий диск або SSD-накопичувач); операційну систему на вибір; мережу; і попередньо встановлені прикладні програми, такі як вебсервер, база даних, CRM і т. д. Кожна система AWS також віртуалізує консольний ввід/вивід (клавіатура, дисплей і миша), що дозволяє користувачам AWS підключитися до своєї системи AWS за допомогою браузера. Браузер виступає як вікно у віртуальний комп’ютер, дозволяючи користувачу входити в систему, налаштовувати та використовувати свої віртуальні системи так само, як справжній, фізичний комп’ютер. Це дозволяє їм налаштувати систему так, щоб надавати інтернет-орієнтовані сервіси та послуги своїм клієнтам.

Сервіси AWS, які доступні для впровадження авторизації та аутентифікації користувачів та додатків: AWS Identity and Access Management; Amazon Cognito; AWS Amplify; AWS Directory Service; AWS Audit Manager.

Мета статті – дослідити технологію по впровадженню безпечної авторизації та аутентифікації користувачів або додатків на базі хмарного провайдера Microsoft Azure.

Виклад основного матеріалу

Відповідно до мети статті є необхідність більш детально дослідити рішення щодо авторизації та аутентифікації користувачів або додатків в AWS.

AWS Identity and Access Management (IAM) – це веб-служба, яка допомагає безпечно контролювати доступ до ресурсів AWS. Ви використовуєте IAM, щоб контролювати, хто аутентифікований (увійшов в систему) і авторизований (має дозволи) для використання ресурсів. При створенні облікового запису AWS, ви починаєте з одного облікового запису, який має повний доступ до всіх служб і ресурсів AWS в обліковому запису. Цей обліковий

запис називається кореневим користувачем облікового запису AWS, і доступ до неї здійснюється шляхом входу за допомогою адреси електронної пошти та пароля, які ви використовували при створенні облікового запису.

Як працює AWS Identity and Access Management (IAM).

IAM Resources. Об'єкти користувачів, груп, ролей, політик і постачальників ідентифікаційних даних, які зберігаються в IAM. Як і в інших службах AWS, ви можете додавати, редагувати і видаляти ресурси з IAM.

IAM Identities. Об'єкти ресурсів IAM, які використовуються для ідентифікації та групування. Ви можете прикріпити політику до IAM Identities. До них відносяться користувачі, групи і ролі.

IAM Entities. Об'єкти ресурсів IAM, які AWS використовує для аутентифікації. До них відносяться користувачі та ролі IAM.

Principals. Особа або програма, яка використовує кореневого користувача облікового запису AWS, користувача IAM або роль IAM для входу і виконання запитів до AWS.

Коли root-user намагається використовувати консоль управління AWS, AWS API або AWS CLI, цей root-user надсилає запит до AWS.

Запит включає наступну інформацію:

Дії або операції – дії або операції, які довіритель хоче виконати. Це може бути дія в консолі управління AWS або операція в AWS CLI або AWS API.

Ресурси – ресурсний об'єкт AWS, над яким виконуються дії або операції.

Root-user – особа або додаток, які використовували сутність (користувача або роль) для відправки запиту. Інформація про довірителя включає в себе політики, які пов'язані з сутністю, яку довіритель використовував для входу в систему.

Дані про середовище – інформація про IP-адресу, агента користувача, статус увімкненого SSL або час доби.

Дані про ресурс – дані, пов'язані з ресурсом, який запитується. Це може включати таку інформацію, як ім'я таблиці DynamoDB або тег на екземплярі Amazon EC2.

AWS збирає інформацію про запит в контекст запиту, який використовується для оцінки та авторизації запиту.

Аутентифікація. Для надсилання запиту до AWS root-user повинен пройти аутентифікацію (увійти до AWS), використовуючи свої облікові дані. Деякі сервіси, такі як Amazon S3 та AWS STS, допускають декілька запитів від анонімних користувачів. Однак вони є винятком з правил. Для аутентифікації з консолі в якості користувача root необхідно увійти за допомогою адреси електронної пошти та пароля. Як користувач IAM, вкажіть ідентифікатор облікового запису або псевдонім, а потім ім'я користувача та пароль. Для аутентифікації за допомогою API або AWS CLI необхідно вказати ключ доступу і секретний ключ. Вам також може знадобитися надати додаткову інформацію про безпеку. Наприклад, AWS рекомендує використовувати багатофакторну автентифікацію (MFA) для підвищення безпеки вашого облікового запису (рис. 1).

Авторизація. Ви також повинні бути авторизовані (допущені) до виконання запиту. Під час авторизації AWS використовує значення з контексту запиту, щоб перевірити наявність політик, які застосовуються до запиту. Потім він використовує політики, щоб визначити, дозволити або відхилити запит. Більшість політик зберігаються в AWS у вигляді JSON-документів і визначають дозволи для основних сутностей. Існує кілька типів політик, які можуть впливати на те, чи буде запит дозволений. Щоб надати своїм користувачам дозволи на доступ до ресурсів AWS в їх власному обліковому записі, вам потрібні тільки політики на основі ідентифікаційних даних. Політики на основі ресурсів популярні для надання доступу між обліковими записами. Інші типи політик є розширеними функціями і повинні використовуватися з обережністю.

AWS перевіряє кожну політику, яка застосовується до контексту вашого запиту. Якщо одна політика дозволів включає в себе заборонену дію, AWS відхиляє весь запит і припиняє оцінку. Це називається явною відмовою. Оскільки запити відхиляються за замовчуванням, AWS авторизує ваш запит тільки в тому випадку, якщо кожна частина вашого запиту дозволена відповідними політиками дозволів. Логіка оцінки запиту в межах одного облікового запису відповідає цим загальним правилам:

1. За замовчуванням всі запити відхиляються. (Як правило, запити, зроблені з використанням облікових даних кореневого користувача облікового запису AWS для ресурсів в облікового запису, завжди дозволяються).

2. Явний дозвіл в будь-якій політиці дозволів (на основі ідентифікаційних даних або на основі ресурсів) перевизначає це значення за замовчуванням.

3. Існування Organizations SCP, межі дозволів IAM або політики сеансу перевизначає дозвіл. Якщо існує один або декілька з цих типів політик, всі вони повинні дозволити запит. В іншому випадку, він неявно відхиляється.

Явна заборона в будь-якій політиці скасовує будь-які дозволи.

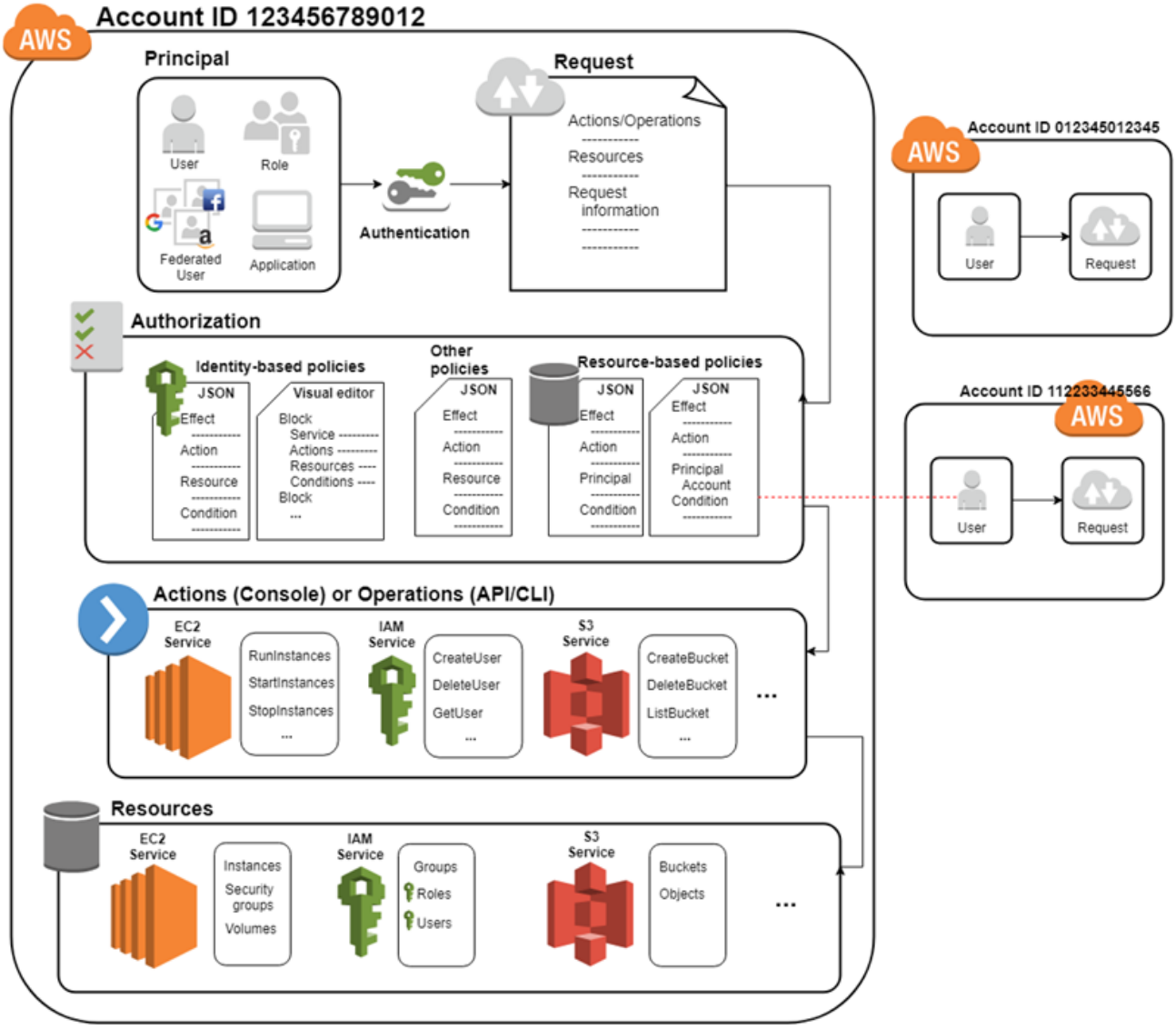

Рис. 1. Аутентифікація та авторизація в Amazon Web Services

Amazon Cognito

Amazon Cognito забезпечує аутентифікацію, авторизацію та управління користувачами для ваших веб- та мобільних додатків. Ваші користувачі можуть входити безпосередньо за допомогою імені користувача та пароля або через третю сторону, таку як Facebook, Amazon, Google або Apple.

Двома основними компонентами Amazon Cognito є пули користувачів та пули ідентичностей. Пули користувачів - це каталоги користувачів, які надають можливості реєстрації та входу для користувачів вашого додатку. Пули ідентичностей дозволяють надавати користувачам доступ до інших сервісів AWS. Ви можете використовувати пули ідентичностей і пули користувачів окремо або разом.

Пули користувачів. Пул користувачів - це каталог користувачів в Amazon Cognito. За допомогою пулу користувачів ваші користувачі можуть входити у ваш веб- або мобільний додаток через Amazon Cognito або об'єднуватися через стороннього постачальника ідентифікаційних даних (IdP). Незалежно від того, чи входять ваші користувачі безпосередньо або через третю сторону, всі члени пулу користувачів мають профіль каталогу, до якого ви можете отримати доступ через SDK.

Пули користувачів надають: послуги реєстрації та входу в систему; веб-інтерфейс для ходу користувачів; вхід через Facebook, Google, вхід через Amazon і вхід через Apple, а також через постачальників ідентифікаційних даних SAML і OIDC з вашого пулу користувачів; управління каталогами і профілями користувачів. Функції безпеки, такі як багатофакторна автентифікація (MFA), перевірка скомпрометованих облікових даних, захист від поглинання облікових записів, а також перевірка телефону та електронної пошти. Налаштовані робочі процеси і міграція користувачів за допомогою тригерів AWS Lambda (рис. 2).

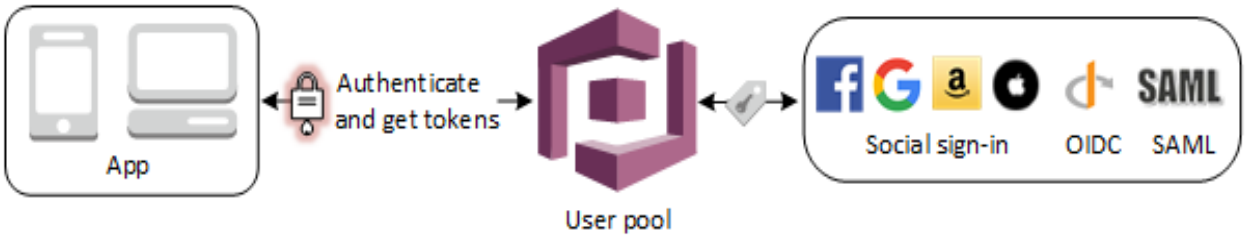

Рис. 2. Пули користувачів

Пули ідентичності. За допомогою пулу ідентичностей ваші користувачі можуть отримати тимчасові облікові дані AWS для доступу до служб AWS, таких як Amazon S3 і DynamoDB. Пули ідентичностей підтримують анонімних гостьових користувачів, а також наступних постачальників ідентичностей, які ви можете використовувати для аутентифікації користувачів для пулів ідентичностей: пули користувачів Amazon Cognito; вхід за допомогою Facebook, Google, Вхід за допомогою Amazon і Apple; постачальники OpenID Connect (OIDC); постачальники ідентичностей SAML; аутентифіковані ідентичності розробника. Щоб зберегти інформацію про профіль користувача, ваш пул ідентичностей повинен бути інтегрований з пулом користувачів.

Як працює Amazon Cognito.

Дивіться схему роботи Amazon Cognito. Тут метою є аутентифікація вашого користувача, а потім надання йому доступу до іншого сервісу AWS. На першому кроці користувач вашого додатку реєструється через пул користувачів і отримує токени пулу користувачів після успішної аутентифікації. Далі ваш додаток обмінює токени пулу користувачів на облікові дані AWS через пул ідентифікаторів. Нарешті, користувач вашого додатку може використовувати ці облікові дані AWS для доступу до інших служб AWS, таких як Amazon S3 або DynamoDB.

Amazon Directory Service

Служба каталогів AWS надає безліч способів використання Microsoft Active Directory (AD) з іншими службами AWS. Каталоги зберігають інформацію про користувачів, групи та пристрої, а адміністратори використовують їх для управління доступом до інформації та ресурсів. Служба каталогів AWS надає кілька варіантів каталогів для клієнтів, які хочуть використовувати існуючі додатки Microsoft AD або Lightweight Directory Access Protocol (LDAP) в хмарі. Вона також пропонує той же вибір для розробників, яким потрібен каталог для управління користувачами, групами, пристроями і доступом.

AWS Directory Service дозволяє легко налаштовувати і запускати каталоги в хмарі AWS Cloud або підключати ресурси AWS до існуючої локальної Microsoft Active Directory. Після створення каталогу ви можете використовувати його для різних завдань:

керування користувачами та групами;

забезпечення SSO в додатки і служби;

створення та застосування групової політики;

спростити розгортання і управління хмарними робочими навантаженнями Linux і Microsoft Windows.

Ви можете використовувати AWS Managed Microsoft AD для забезпечення багатофакторної автентифікації шляхом інтеграції з існуючою інфраструктурою MFA на основі RADIUS для забезпечення додаткового рівня безпеки при доступі користувачів до додатків AWS.

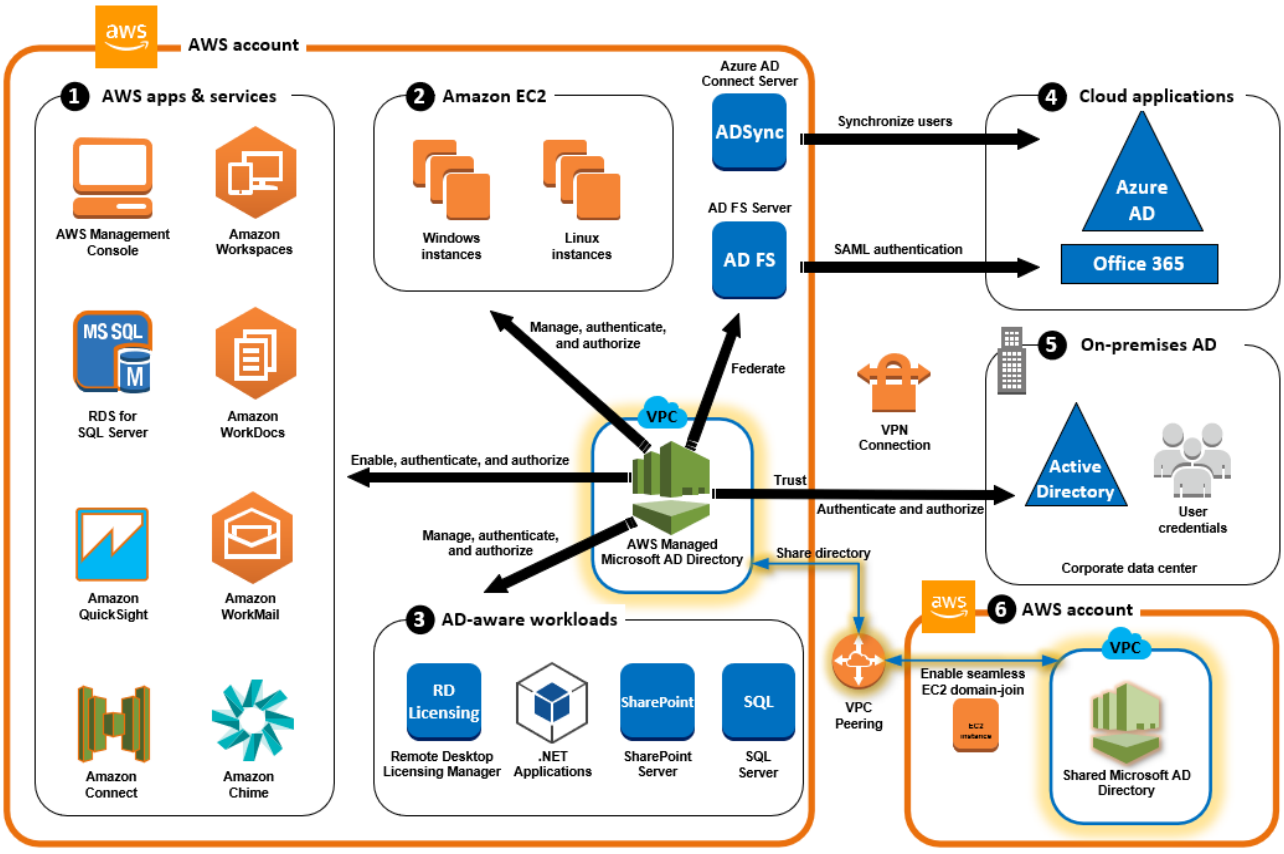

Рис. 3. Порядок використання AWS

Хмарна платформа Microsoft Azure

Microsoft Azure - це платформа хмарних обчислень, що експлуатується корпорацією Майкрософт для управління додатками через розподілені по всьому світу центри обробки

даних. Microsoft Azure має безліч можливостей, таких як програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) та інфраструктура як послуга (IaaS), і підтримує багато різних мов програмування, інструментів та фреймворків, включаючи як специфічне програмне забезпечення Microsoft, так і сторонні програмні продукти та системи.

Сервіси Microsoft Azure, які доступні для впровадження авторизації та аутентифікації користувачів та додатків:

Azure Active Directory;

Azure Active Directory Domain Services;

Azure information;

Azure Active Directory External.

Azure Active Directory

Azure Active Directory (Azure AD) - це хмарна служба управління ідентичностями та доступом. Ця служба допомагає вашим співробітникам отримувати доступ до зовнішніх ресурсів, таких як Microsoft 365, портал Azure і тисячі інших програм SaaS. Azure Active Directory також допомагає їм отримувати доступ до внутрішніх ресурсів, таких як програми в корпоративній інтрамережі, а також до будь-яких хмарних програм, розроблених для вашої організації.

Порівняння Azure Active Directory та Active Directory

Azure Active Directory - це наступна еволюція рішень для управління ідентифікацією та доступом у хмарі. Корпорація Майкрософт представила служби доменів Active Directory в Windows 2000, щоб дати організаціям можливість управляти декількома локальними компонентами інфраструктури і системами, використовуючи єдиний ідентифікатор для кожного користувача.

Azure AD виводить цей підхід на новий рівень, надаючи організаціям рішення Identity as a Service (IDaaS) для всіх своїх додатків в хмарних і локальних середовищах. Більшість IT-адміністраторів знайомі з концепціями доменних служб Active Directory. У наступній таблиці описані відмінності та подібності між концепціями Active Directory і Azure Active Directory (табл. 1).

Azure Active Directory Domain Services

Azure Active Directory Domain Services (Azure AD DS) надає керовані доменні служби, такі як приєднання до домену, групові політики, полегшений протокол доступу до каталогів (LDAP) і аутентифікація Kerberos/NTLM. Ви можете використовувати ці доменні служби без необхідності розгортати, керувати та виправляти контролери доменів (DC) у хмарі.

Керований домен Azure AD DS дозволяє запускати в хмарі застарілі програми, які не можуть використовувати сучасні методи автентифікації, або якщо ви не хочете, щоб пошук у каталогах завжди повертався в локальне середовище AD DS. Ви можете підняти і перемістити ці застарілі програми з локального середовища в керований домен, без необхідності керувати середовищем AD DS в хмарі. Azure AD DS інтегрується з існуючим орендарем Azure AD. Ця інтеграція дозволяє користувачам входити в служби і програми, підключені до керованого домену, використовуючи свої існуючі облікові дані. Ви також можете використовувати існуючі групи та облікові записи користувачів для захисту доступу до ресурсів. Ці функції забезпечують більш плавне перенесення локальних ресурсів в Azure.

Як працює Azure Active Directory Domain Services

Коли ви створюєте керований домен Azure AD DS, ви визначаєте унікальний простір імен. Цим простором імен є доменне ім'я, наприклад aaddscontoso.com. Потім у вибраному регіоні Azure розгортаються два контролери домену (DC) Windows Server. Таке розгортання контролерів доменів називається набором реплік. Вам не потрібно керувати, налаштовувати або оновлювати ці контролери домену. Платформа Azure обробляє DC як частину керованого домену, включно з резервним копіюванням і шифруванням у стані спокою за допомогою Azure Disk Encryption.

Таблиця 1

Порівняння Active Directory та Azure Active Directory

Концепція	**Active Directory (AD)**	**Azure Active Directory**
Створення користувачів	Організації створюють внутрішніх користувачів вручну	Підтримка автоматичного створення користувачів з хмарних HR-систем.
Зовнішні користувачі / додатки	Створення зовнішніх користувачів вручну як звичайних користувачів	Надає спеціальний клас ідентичностей для підтримки зовнішніх ідентичностей.
Управління правами та групами	Адміністратори роблять користувачів членами груп.	Вручну або використовуючи запит для динамічного включення користувачів.
Адміністрування	Використоання комбінації доменів, підрозділів і груп в AD для делегування прав.	Вбудовані ролі на основі Azure AD (Azure AD RBAC) з обмеженою підтримкою створення користувацьких ролей.
Управління обліковими даними	Облікові дані базуються на паролях, аутентифікації за допомогою сертифікатів та аутентифікації за допомогою смарт-карт.	Використовує інтелектуальний захист паролями для хмарних і локальних середовищ. Інтелектуальне блокування, а також блокування загальних і спеціальних фраз і замін паролів.
Інфраструктурні додатки	Є основою для багатьох локальних компонентів інфраструктури, наприклад, DNS, DHCP, IPSec, WiFi, NPS і VPN доступу	Conditional access (CA) контролює, які користувачі мають доступ до програм за певних умов.
Традиційні та застарілі програми	LDAP, інтегрована аутентифікація Windows (NTLM і Kerberos) або на основі заголовків.	Може надавати доступ до цих типів локальних програм за допомогою агентів проксі додатків Azure AD, що працюють локально.
SaaS-додатки	Не підтримує додатки SaaS і потребує системи федерації, наприклад, AD FS.	Програми SaaS, що підтримують аутентифікацію OAuth2, SAML і WS-*, можна інтегрувати для використання Azure AD для аутентифікації.
Мобільні телефони	Не підтримує мобільні пристрої за замовчуванням без сторонніх рішень.	Microsoft Intune надає інформацію про стан пристрою системі ідентифікації для оцінки під час автентифікації.
Настільні комп'ютери Windows	Надає можливість приєднання до домену пристроїв Windows для управління ними за допомогою групової політики.	Пристрої Windows можна приєднати до Azure AD. Умовний доступ може перевіряти, чи підключено пристрій до Azure AD, як частину процесу аутентифікації.
Сервери Windows	Надає потужні можливості управління локальними серверами Windows за допомогою групової політики.	Віртуальними машинами серверів Windows в Azure можна керувати за допомогою служб доменів Azure AD.
Linux/Unix машини	Не підтримує ОС, відмінні від Windows, без сторонніх рішень. Машини Linux можуть бути налаштовані на аутентифікацію в Active Directory як в області Kerberos.	Віртуальні машини Linux/Unix можуть використовувати керовані ідентичності для доступу до системи ідентифікації або ресурсів.

Керований домен налаштований на односторонню синхронізацію з Azure AD, щоб забезпечити доступ до центрального набору користувачів, груп і облікових даних. Можна створювати ресурси безпосередньо в керованому домені, але вони не синхронізуються з Azure AD. Додатки, служби і віртуальні машини в Azure, які підключаються до керованого домену, можуть використовувати загальні функції AD DS, такі як приєднання до домену, групова політика, LDAP і аутентифікація Kerberos/NTLM. У гібридному середовищі з локальним середовищем AD DS Azure AD Connect синхронізує інформацію про ідентичність з Azure AD, яка потім синхронізується з керованим доменом (рис. 4).

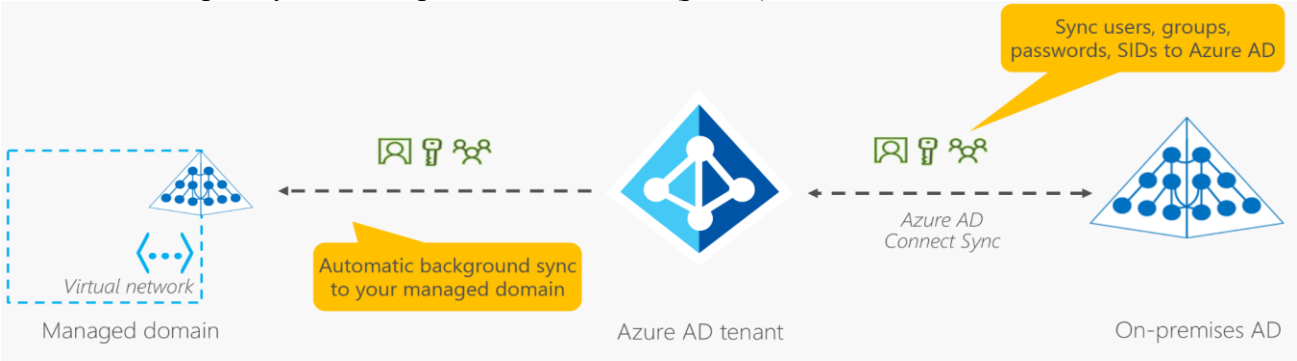

Рис. 4. Робота Azure Active Directory Domain Services

Для хмарних середовищ не потрібне традиційне локальне середовище AD DS, щоб використовувати централізовані служби ідентичностей Azure AD DS. Ви можете розширити керований домен, щоб мати більше одного набору реплік для кожного тенанта Azure AD. Набори реплік можна додавати в будь-яку віртуальну мережу в будь-якому регіоні Azure, що підтримує Azure AD DS. Додаткові набори реплік у різних регіонах Azure забезпечують географічне відновлення після аварій для застарілих програм, якщо регіон Azure переходить в автономний режим.

Висновки

Microsoft Azure Cloud надає різноманітні сервіси для аутентифікації та авторизації, що дозволяють забезпечити безпеку та контроль доступу до ресурсів. Для аутентифікації можна використовувати Azure Active Directory (Azure AD), який є хмарним сервісом ідентифікації та управління доступом до ресурсів. Azure AD може бути використаний як для внутрішньої аутентифікації користувачів компанії, так і для зовнішньої аутентифікації користувачів за допомогою соціальних мереж, таких як Facebook, Google або Microsoft. Для авторизації можна використовувати Azure Role-Based Access Control (RBAC), який дозволяє призначати ролі для користувачів та груп користувачів для доступу до ресурсів. Крім того, можна використовувати Azure Policy, щоб контролювати доступ до ресурсів та забезпечити відповідність до політики безпеки компанії.

Перелік посилань

1. Azure Services Platform. Windows Azure, Windows .Net Services (2016 p.) https://victana.lviv.ua/knyhy/konspekty-lektsii/133-kros-platformenne-prohramuvannia-ta-khmarni-servisy/552-lektsiia-4-azure-services-platform-windows-azure-windows-net-services-2016-r

2. Stephen J. Bigelow. Microsoft Azure. https://www.techtarget.com/searchcloudcomputing/definition/Windows-Azure

3. What Is Microsoft (MS) Azure Cloud? Cloud Compute 101. https://www.perforce.com/blog/vcs/what-microsoft-azure-cloud

4. Nicola Wright. Everything you ever wanted to know about Microsoft Azure. https://www.nigelfrank.com/insights/everything-you-ever-wanted-to-know-about-microsoft-azure

Надійшла: 12.03.2023 Рецензент: д.т.н., професор Кожухівський А.Д.