Автор:
Гостренко Максим Володимирович,
студент 11 КНм групи
Науковий керівник:
Франчук Василь Михайлович,
доктор педагогічних наук, доцент,
завідувач кафедри комп'ютерної та програмної інженерії

СТВОРЕННЯ ЗАХИЩЕНОГО МЕРЕЖЕВОГО СХОВИЩА ДАНИХ В ОРГАНАХ ПРАВОСУДДЯ

Анотація. Метою роботи є проектування, та впровадження захищеного мережевого сховища для органів правосуддя. Завданнями роботи є аналіз сучасного стану мережевих сховищ в органах правосуддя в Україні, розгляд та порівняння технологій розробки мережевих сховищ, підбір технологій для розробки захищеного мережевого сховища, створення, впровадження та тестування захищеного мережевого сховища в органах правосуддя. Об'єктом роботи є захищені мережеві сховища. Предметом роботи є створення мережевого сховища для органів правосуддя та захист його даних. Результатом роботи є база знань про апаратне та програмне забезпечення мережевих сховищ, захист даних, а також розроблене на її основі захищене мережеве сховище даних для органів правосуддя.

Ключові слова: сервер, мережеве сховище, накопичувач даних, RAID, шифрування, система моніторингу мережі.

Вступ. В Україні на даний час мережеві сховища загалом працюють не дуже вдало, зокрема в органах правосуддя, де є дуже важливою безперервна робота мережі та серверу. Відключення світла та постійні атаки спричиняють збої у системі, затримки в отриманні даних, синхронізації з іншими організаціями та витік конфіденційних даних. Важливо розробити надійне захищене мережеве сховище, щоб уникнути проблемам захисту даних.

Проектування та створення захищеного мережевого сховища даних для органів правосуддя є важливим завданням сучасності для гарантування безпеки даних та надійного безперервного доступу до них.

Постановка задачі. Для створення захищеного мережевого сховища потрібні відповідні апаратні та програмні засоби, а саме сервер мережевого сховища, накопичувачі даних, технологія RAID, система шифрування даних та система моніторингу мережі.

Сервер – це певний виділений комп'ютер для обробки та зберігання даних мережі. У випадку, якщо це мережеве сховище, він більше спрямований саме на зберігання даних, а до обробки можна віднести шифрування.

Мережеве сховище, або ж NAS (Network Attached Storage – сховище, підключене до мережі, також зустрічається назва мережева СЗД – система зберігання даних) – це пристрій, який використовують для зберігання файлів і надання доступу до них. Мережевим сховищем є комп'ютер, де його компоненти – процесор, пам'ять, диски пристосовані саме для зберігання даних [1].

Накопичувачі даних – пристрої для зберігання даних, які використовуються комп'ютерами. У випадку з мережевим сховищем буде надаватись доступ до даних іншим користувачам мережі або за її межами.

Технологія RAID (Redundant Array of Independent Disks – надлишковий масив незалежних дисків) – спосіб зберігання одних і тих же даних на кількох накопичувачах, що запобігає втраті даних та зменшує або виключає зовсім простої під час їх відмови. Разом з цим загальна кількість збоїв може збільшуватись через збільшення кількості накопичувачів. Технологія RAID збільшує відмовостійкість шляхом надмірного зберігання однакових даних, але є і версії, які підвищують не відмовостійкість, а швидкість роботи з даними [3].

Шифрування – метод перетворення даних, під час якого відкриті дані перетворюються у зашифровані за допомогою криптографічного ключа, щоб переглянути їх могли лише ті особи, у яких є відповідний ключ. Шифрування забезпечує конфіденційність збережених даних, допомагає запобігти витоку. Навіть якщо дані потраплять у відкритий доступ, їх буде дуже складно або неможливо розшифрувати без ключа [5].

Система моніторингу мережі – це програмне забезпечення для перегляду стану комп'ютерної мережі та під'єднаних пристроїв. Система збирає дані про помилки в мережі, небезпеки, мережевий трафік та стан серверів для запобігання ризиків та збільшення надійності мережі [4].

Мета роботи. Метою роботи є дослідження важливих компонентів захищеного мережевого сховища для органів правосуддя.

Основна частина. Різних моделей мережевих сховищ існує багато, від звичайних невеликих домашніх пристроїв, до великих серверних рішень, які вставляються у серверну стійку. Зазвичай, в одне мережеве сховище можна встановити від 1 до 12 накопичувачів, але є рішення і під більшу кількість накопичувачів. На роботу мережевого сховища впливає процесор та оперативна пам'ять. Чим потужніше процесор, швидше та об'ємніше оперативна пам'ять, тим оперативніше мережеве сховище буде працювати. У сховищах використовується окрема операційна система від виробника, або ж стороння, яка базується на ОС Linux чи Windows, управління якою здійснюється через веб-інтерфейс з персонального комп'ютера. Також потрібно звернути увагу на сумісність з різними типами накопичувачів та режимами технології RAID [1].

Накопичувачі відрізняються за типом, формою та підключенням. У мережевих сховищах можуть використовуватись жорсткі або твердотільні накопичувачі, HDD та SSD відповідно.

Жорсткі диски можуть бути двох розмірів – 2,5 та 3,5 дюйми, які технічно на даний час можуть відрізнятись лише максимальним обсягом пам'яті. Переважна більшість сучасних жорстких дисків мають роз'єм підключення SATA [2].

Твердотільні накопичувачі, або ж SSD можуть мати форму, як у 2,5 дюймових жорстких дисків з роз'ємом SATA, а також форм-фактор M.2 роз'єму. Загалом вони швидші за жорсткі диски, не створюють шум під час роботи, менші, а також їм не потрібна дефрагментація, адже вони мають однаково швидкий доступ до будь-якої частини пам'яті. Але є і недоліки: SSD мають набагато менший ресурс, що робить їх не зовсім придатними для мережевих сховищ. До того ж, відновлення втрачених даних набагато складніше, ніж на HDD [2].

Технологія RAID має велике значення, коли дані повинні безвідмовно надаватись та зберігатись. У технології є кілька рівнів, основними є RAID 0, 1 та 5.

RAID 0 не є рівнем надлишкового зберігання даних, хоч це і суперечить назві технології. В цьому режимі блоки даних рівномірно розподіляються на два або більше накопичувачі, залишаючи об'єм пам'яті всіх накопичувачів, збільшуючи швидкість читання та запису, але не збільшуючи відмовостійкість, тому що при виході з ладу одного з накопичувачів, втрачаються всі дані [3].

Рівень RAID 1 дзеркально копіює дані на накопичувачах, збільшуючи відмовостійкість пропорційно до кількості накопичувачів, але об'єм пам'яті залишається як у одного накопичувача, через що кількість та вартість всіх накопичувачів можуть бути суттєво великими. Разом з цим швидкість запису може бути меншою за швидкість запису на один диск, а швидкість читання збільшується через можливість читання відразу з кількох дисків [3].

RAID 5 використовує принцип чергування на рівні блоків парності. Блоки парності відповідальні за перевірку цілісності накопичувачів та розташовані на різних накопичувачах, в кількості від трьох. Інші блоки, за які відповідає блок парності розташовані на інших накопичувачах, цим самим забезпечуючи відмовостійкість системи. Швидкість читання та запису будуть майже відповідні швидкості під час використання RAID 0. Об'єм пам'яті буде

повним, окрім одного накопичувача, а відмовостійкість майже на рівні RAID 1. Саме через цю збалансованість RAID 5 є досить популярним. З недоліків можна виділити сильне навантаження на накопичувачі під час інтенсивного запису та тривале відновлення при відмові [3].

Шифрування може бути як симетричне так і асиметричне. Під час симетричного шифрування використовується один ключ як для зашифровування, так і для розшифровування. Під час асиметричного шифрування використовується два різні ключі для цих дій, що збільшує надійність та захищеність, але займає більше часу та ресурсів [5].

Використання систем моніторингу мережі допомагають завчасно виявити несправності в мережі, такі як апаратні збої, проблеми програмного забезпечення або його налаштування. До цього ж, моніторинг мережі надає дані про продуктивність мережі, її пропускну здатність, споживання ресурсів мережі для їх правильного розподілу. За допомогою моніторингу можна також виявити спроби атаки на мережу та інші несанкціоновані дії. Системи моніторингу мережі збирають дані про використання пропускної здатності, трафік даних та стан пристроїв, таких як маршрутизатори, сервери та інші пристрої, під'єднані до мережі, виконують аналіз цих даних, виявляють відхилення від нормальної поведінки мережі та сповіщають про це адміністраторів, створюють детальні звіти про використання мережі [4].

Висновки. Для побудови якісного захищеного мережевого сховища важливо здійснити правильний вибір його моделі, а саме: використання накопичувачів, технології RAID, системи моніторингу мережі, системи захисту даних для надійної та ефективної роботи серверу. Під час створення мережевого сховища для державних установ потрібно приділити особливу увагу технологіям захисту даних та забезпеченню безперервної роботи системи.

Список використаних джерел

1. NAS-сховище – специфіка і 4 критерії вибору. URL: https://e-server.com.ua/uk/poradi/nas-shovishhe-specifika-i-4-kriterii-viboru.
2. SSD або HDD – що краще: відмінності 2 видів накопичувачів. URL: https://www.moyo.ua/ua/news/ssd-ili-hdd-chto-luchshe-otlichiya-2-vidov-nakopiteley.html.
3. Рівні RAID: 0, 1, 2, 3, 4, 5, 6, 7 … Що вони означають? URL: https://hetmanrecovery.com/uk/recovery_news/summary-concept-and-description-of-available-capabilities-of-a-redundant-array-of-independent-disks-raid.htm.
4. Що таке моніторинг мережі та чому він важливий? URL: https://techukraine.net/що-таке-моніторинг-мережі-та-чому-він-в.
5. Що таке шифрування та як воно працює? URL: https://www.kingston.com/ua/blog/data-security/what-is-encryption.
6. Франчук В.М. Резервне копіювання даних. Науковий часопис НПУ імені М.П. Драгоманова. Серія № 2. Комп'ютерно-орієнтовані системи навчання. 2018. №20 (27). С. 61-67. https://doi.org/10.31392/NPU-nc.series2.2018.20(27).10