УДК 004

Д.Кашпуровський, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО МОНІТОРИНГУ ТА КОНТРОЛЮ СТАНУ ІТ

У статті розроблено програмне забезпечення, яке призначено для системи мережевого моніторингу та контролю стану ІТ. Метою розробки є дослідження та принципи побудови системи мережевого моніторингу та контролю стану ІТ. Об'єктом дослідження є процес мережевого моніторингу та контролю стану ІТ. Предметом дослідження є методи мережевого моніторингу та контролю стану ІТ. Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи мережевого моніторингу та контролю стану ІТ. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

мережевий моніторинг, контроль стану ІТ

Постановка проблеми. Інструменти моніторингу мережі – це програмні рішення для контролю, аналізу та управління продуктивністю та станом мережі. Ці інструменти постійно контролюють різні мережеві компоненти, такі як маршрутизатори, комутатори, сервери та програми, щоб забезпечити їх правильне функціонування.

Відстежуючи такі показники, як трафік, затримка та час безвідмовної роботи, вони допомагають ІТ-командам виявляти та вирішувати проблеми, перш ніж вони переростуть у серйозні проблеми. Основною метою інструментів моніторингу мережі є підтримка доступності, надійності та безпеки мережі. Вони забезпечують видимість мережевої активності, дозволяючи організаціям виявляти неефективність, збої або загрози безпеці.

Крім того, ці інструменти підтримують планування потужностей, оптимізацію продуктивності та дотримання угод про рівень обслуговування (SLA). Сучасні інструменти моніторингу мережі часто інтегрують такі функції, як аналітика в режимі реального часу, аналітика на основі штучного інтелекту та підтримка хмарної інфраструктури.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевого моніторингу та контролю стану ІТ.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевого моніторингу та контролю стану ІТ.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем мережевого моніторингу та контролю стану ІТ.
– Дослідження системи мережевого моніторингу та контролю стану ІТ.
– Програмна реалізація системи мережевого моніторингу та контролю стану ІТ.

Об'єктом дослідження є процес мережевого моніторингу та контролю стану ІТ.

Предметом дослідження є методи мережевого моніторингу та контролю стану ІТ.

Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Сформулюємо поради, які допоможуть вам вибрати, розгорнути та максимізувати цінність інструментів моніторингу мережі:

1. Пріоритет гібридної та багатохмарної сумісності: оскільки гібридні та багатохмарні середовища стають нормою, обирайте інструменти моніторингу, які пропонують безперешкодну інтеграцію з постачальниками публічних хмарних послуг (наприклад, AWS, Azure, Google Cloud) та інфраструктурою приватних хмар. Це забезпечує видимість на різних мережевих рівнях.

2. Впроваджуйте поетапний підхід до розгортання: уникайте розгортання інструментів моніторингу по всій мережі одночасно. Натомість розгортайте рішення поетапно, починаючи з критичної інфраструктури, щоб мінімізувати перебої та точно налаштувати конфігурації під час масштабування.

3. Інтеграція з платформами SIEM та SOAR: підключіть інструменти моніторингу до рішень SIEM або SOAR для централізації аналізу даних, покращення виявлення загроз та забезпечення автоматизованих робочих процесів реагування на інциденти. Така інтеграція допомагає створити єдину екосистему безпеки.

4. Використовуйте виявлення аномалій на основі штучного інтелекту: використовуйте інструменти, що включають штучний інтелект та машинне навчання, для виявлення незначних відхилень від нормальної поведінки мережі. Такий підхід зменшує залежність від статичних порогів та покращує виявлення загроз нульового дня або повільних атак.

5. Встановлення базового профілю продуктивності: Проведення комплексного базового дослідження показників продуктивності мережі (наприклад, затримки, пропускної здатності та пропускної здатності) під час нормальної роботи. Це допоможе швидко виявити аномалії та оцінити майбутні покращення продуктивності.

Як вибрати правильний інструмент для моніторингу мережі

Ось деякі основні фактори, які слід враховувати під час оцінки рішень для моніторингу мережі.

Міркування щодо масштабованості

Зі зростанням організацій їхні мережі стають складнішими, що вимагає інструментів, здатних обробляти збільшений обсяг даних та складність мережі. Масштабоване рішення для моніторингу може враховувати додаткові пристрої, користувачів та робочі навантаження без шкоди для продуктивності чи точності.

Вибір інструменту з опціями масштабованості дозволяє організаціям адаптуватися до змінних вимог мережі. Інструменти, що пропонують механізми горизонтального та вертикального масштабування, забезпечують безперебійний моніторинг під час зростання мережі.

Можливості інтеграції

Сучасні IT-середовища часто включають різноманітні технології та системи. Інструмент, який добре інтегрується з іншими програмами та платформами, може забезпечити комплексне уявлення про стан та продуктивність мережі. Така інтеграція дозволяє автоматизувати робочі процеси та обмін даними.

Обираючи інструменти моніторингу з потужними функціями інтеграції, організації можуть спростити IT-операції та зменшити ручну роботу. Інтегровані системи забезпечують централізований моніторинг та управління, пропонуючи єдину платформу для всіх мережевих дій.

Інтерфейс користувача та зручність використання

Інтерфейс користувача (UI) інструменту моніторингу мережі суттєво впливає на його зручність використання та ефективність. Добре розроблений інтерфейс дозволяє IT-фахівцям легко орієнтуватися в інструменті, налаштовувати конфігурації та інтерпретувати дані. Простота використання гарантує, що команди можуть швидко реагувати на проблеми та приймати обґрунтовані рішення на основі чіткої візуалізації продуктивності мережі.

Вибір інструменту з інтуїтивно зрозумілим інтерфейсом скорочує криву навчання та підвищує продуктивність. Зручні функції, такі як панелі інструментів з функцією перетягування елементів та автоматизована звітність, покращують впровадження та ефективність використання користувачами.

Моделі вартості та ліцензування

Організаціям необхідно враховувати початкові витрати, поточні платежі та потенційні приховані платежі. Моделі ліцензування різняться, включаючи варіанти на основі підписки, безстрокові або freemium, кожна з яких має свої власні витрати та переваги залежно від бюджету та потреб організації.

Оцінка загальної вартості володіння допомагає організаціям збалансувати бюджетні обмеження з вимогами до функціональності. Розуміння умов ліцензування та майбутніх витрат на масштабованість гарантує, що інвестиції задовольнять як поточні потреби, так і майбутнє зростання.

Інструменти моніторингу мережі є важливими для підтримки продуктивності, надійності та безпеки сучасних мереж. Вибираючи рішення, яке відповідає конкретним потребам організації, враховуючи такі фактори, як масштабованість, інтеграція, зручність використання та вартість, IT-команди можуть забезпечити оптимальну роботу мережі та проактивно вирішувати проблеми. Інвестування в правильний інструмент моніторингу не лише покращує стан мережі, але й підтримує безперервність бізнесу та операційну ефективність.

Моніторинг мережі включає спостереження та аналіз продуктивності та стану мережі за допомогою різних пристроїв та програмних інструментів. Цей процес спрямований на забезпечення безперебійної роботи мережевої інфраструктури шляхом відстеження потоків даних, станів пристроїв та потенційних несправностей, які можуть порушити роботу сервісу.

Мережеві адміністратори часто використовують ці дані для керування пропускною здатністю, виявлення аномалій та забезпечення проактивного обслуговування, зменшуючи час простою та пом'якшуючи ризики, пов'язані з проблемами мережі.

Інструменти моніторингу мережі збирають дані за допомогою таких протоколів, як SNMP (простий протокол керування мережею) та ICMP (протокол керування інтернет-повідомленнями), що дозволяє адміністраторам оцінювати стан мережі в режимі реального часу. Ці інструменти часто надають графічні інтерфейси, які відображають такі показники, як втрата пакетів, затримка та час безвідмовної роботи, що спрощує розуміння стану мережі.

Важливість моніторингу мережі

Існує кілька причин, чому організації повинні впроваджувати стратегії моніторингу мережі.

Раннє виявлення проблем з мережею

Раннє виявлення мережевих проблем передбачає постійне сканування мережевої активності для виявлення порушень. Ці порушення можуть включати незвичайні обсяги трафіку, неочікувані простої або несправності обладнання. Мережеві адміністратори можуть швидко втрутитися, виявивши ці проблеми на ранній стадії та усунувши першопричину, перш ніж вони порушать роботу мереж. Це заощаджує час і ресурси, необхідні для тривалого усунення несправностей.

Раннє виявлення може запобігти порушенням безпеки, виявляючи потенційні загрози в міру їх виникнення. Наприклад, раптові сплески передачі даних можуть свідчити про спроби несанкціонованого доступу або витоку даних. Завдяки сповіщенням та звітам у режимі реального часу системи моніторингу мережі можуть повідомляти адміністраторів про ці аномалії, що дозволяє швидко реагувати та негайно зменшувати ризики безпеки.

Забезпечення продуктивності та доступності мережі

Відстежуючи ключові показники продуктивності, такі як використання пропускної здатності та затримка, мережеві адміністратори можуть забезпечити ефективне використання ресурсів та уникнути потенційних вузьких місць. Постійний моніторинг надає уявлення про стан мережі, що дозволяє своєчасно оновлювати або перерозподіляти ресурси для підтримки зв'язку в організації.

Крім того, моніторинг мережі підтримує високу доступність, оперативно сповіщаючи команди про збої або погіршення стану мережевих компонентів. Ці сповіщення дозволяють швидко діяти, мінімізуючи час простою та підтримуючи доступність послуг.

Моніторинг відповідності та безпеки

Відповідність вимогам та безпека є важливими питаннями, на які звертають увагу системи моніторингу мережі. Ці системи відстежують журнали доступу, дії користувачів та передачу даних, забезпечуючи відповідність використання мережі нормативним стандартам та політикам організації. Моніторинг може допомогти виявити прогалини у відповідності, що дозволяє компаніям оперативно вживати коригувальних заходів, щоб уникнути штрафів.

Моніторинг безпеки зосереджений на виявленні та реагуванні на потенційні загрози, такі як несанкціонований доступ та проникнення шкідливого програмного забезпечення. Моніторинг мережі в режимі реального часу виявляє відхилення від встановлених норм безпеки, запускаючи сповіщення для негайного реагування. Це посилює захист організації від кіберзагроз, захищаючи конфіденційні дані.

Ключові компоненти систем мережевого моніторингу

Методи збору даних

Збір даних включає збір інформації про мережевий трафік, стан пристроїв та показники продуктивності. Традиційні методи включають SNMP, який збирає та впорядковує дані про мережеві пристрої, та ICMP-зонди, які вимірюють час підключення та відгуку. Ці інструменти працюють разом, щоб створити детальний огляд мережі, допомагаючи адміністраторам приймати обґрунтовані рішення щодо оптимізації продуктивності або усунення несправностей.

Методи збору даних також використовують технології на основі потоків, такі як NetFlow та sFlow, які пропонують детальну видимість моделей мережевого трафіку та використання пропускної здатності. Ці методи надають безцінну інформацію про продуктивність програм та поведінку користувачів, допомагаючи виявляти вузькі місця або несанкціоноване використання даних.

Топологія та відображення мережі

Топологія мережі та картографування є критично важливими компонентами мережевого моніторингу, що забезпечують візуальне уявлення про те, як пристрої та з'єднання організовані в мережі. Таке графічне зображення дозволяє мережевим адміністраторам краще зрозуміти, як трафік передається між пристроями, виявляти потенційні точки збою та оцінювати вплив перебоїв у роботі мережі.

Точне картографування топології допомагає ефективно виявляти несправності та оптимізувати мережеві шляхи. Інструменти картографування мережі автоматично виявляють та документують зміни в мережевому середовищі, підтримуючи актуальність топологічних представлень. У міру розвитку мереж з появою нових пристроїв та технологій динамічне картографування підтримує інтеграцію та прозорість.

Механізми оповіщення та звітності

Механізми сповіщень та звітності є незамінними для моніторингу мережі, надаючи сповіщення про аномалії або збої в режимі реального часу. Сповіщення налаштовуються на спрацьовування за певних порогових значень, таких як збільшення затримки або відключення пристроїв. Коли ці умови виконуються, сповіщення надсилаються адміністраторам мережі, що спонукає до негайного розслідування та вирішення проблеми.

Функції звітності доповнюють системи сповіщень, надаючи інформацію про довгострокові тенденції та показники ефективності. Регулярно генеровані звіти допомагають виявити закономірності, які можуть свідчити про основні проблеми або можливості для оптимізації. Вони також підтримують дотримання вимог, документуючи мережеву активність та демонструючи дотримання нормативних стандартів.

Сформулюємо поради, які допоможуть вам оптимізувати стратегії моніторингу мережі для підвищення продуктивності та безпеки:

1. Використовуйте штучний інтелект та машинне навчання для прогнозної аналітики: використовуйте інструменти моніторингу на базі штучного інтелекту для аналізу історичних даних та прогнозування потенційних збоїв або вузьких місць. Такий підхід допомагає вирішувати проблеми до того, як вони вплинуть на продуктивність мережі.

2. Сегментація мереж для покращення видимості: розділіть мережу на логічні сегменти (наприклад, за відділами чи програмами), щоб зосередити зусилля моніторингу та швидше виявляти проблеми. Сегментація також підвищує безпеку, обмежуючи обсяг потенційних загроз.

3. Використовуйте моніторинг на основі потоку разом із традиційними метриками: інтегруйте такі інструменти, як NetFlow або sFlow, для аналізу потоків трафіку для глибшого розуміння використання пропускної здатності, продуктивності програм та аномальної поведінки. Це доповнює моніторинг на основі SNMP для отримання більш повного уявлення.

4. Впроваджуйте порогові значення для сповіщень на основі часу: встановлюйте динамічні порогові значення для показників продуктивності на основі тенденцій часу доби. Наприклад, налаштуйте вищі порогові значення пропускної здатності в години пікової зайнятості, щоб зменшити кількість хибних спрацьовувань та зосередитися на справді аномальній активності.

5. Поєднання локальних та хмарних інструментів моніторингу: використовуйте гібридні рішення для отримання видимості в традиційних та хмарних інфраструктурах. Інструменти, що інтегруються в різних середовищах, є важливими для моніторингу гібридних або багатохмарних мереж.

Метрики та протоколи моніторингу мережі

Загальні показники, що відстежуються

Ефективний моніторинг мережі залежить від відстеження показників, які показують стан, продуктивність та надійність мережі. Зазвичай моніторингові показники включають:

1. Використання пропускної здатності: Цей показник показує, яка частина доступної пропускної здатності мережі використовується в певний момент часу. Високий рівень використання може свідчити про перевантаження мережі, що вимагає перерозподілу ресурсів або оновлення.

2. Затримка: Затримка вимірює час, необхідний для передачі даних від джерела до місця призначення і назад. Висока затримка впливає на програми реального часу, такі як VoIP та відеоконференції, що вимагає своєчасного втручання для покращення взаємодії з користувачем.

3. Втрата пакетів: Втрата пакетів – це відсоток пакетів даних, які не досягають місця призначення. Навіть невелика кількість втрачених пакетів може порушити роботу програм, чутливих до доставки даних, таких як потокове передавання або онлайн-ігри.

4. Час безперебійної роботи та простої: Моніторинг часу безперебійної роботи пристроїв та послуг дає уявлення про надійність мережевих компонентів. Часті або тривалі простої можуть сигналізувати про несправне обладнання, неправильні конфігурації програмного забезпечення або ширші проблеми з інфраструктурою.

5. Коефіцієнт помилок: Цей показник відстежує кількість помилок у переданих даних, таких як колізії, втрачені пакети або повторні передачі. Високий коефіцієнт помилок часто вказує на такі проблеми, як збій обладнання або погане кабельне з’єднання.

6. Пропускна здатність: Пропускна здатність вимірює фактичну швидкість передачі даних по мережі. Розбіжності між пропускною здатністю та використанням пропускної здатності можуть сигналізувати про проблеми з продуктивністю, такі як вузькі місця або перешкоди.

7. Джиттер: Джиттер стосується варіації часу доставки пакетів. Цей показник особливо важливий для програм реального часу, оскільки надмірний джиттер може призвести до погіршення якості голосового та відеозв'язку.

8. Використання процесора та пам'яті на пристроях: моніторинг використання ресурсів на мережевих пристроях, таких як маршрутизатори, комутатори та сервери, допомагає запобігти зниженню продуктивності через перевантажене обладнання.

9. Стан з’єднання: Регулярна перевірка стану з’єднань між пристроями забезпечує працездатність усіх компонентів. Швидке виявлення несправних з’єднань мінімізує перебої в обслуговуванні.

SNMP (Простий протокол керування мережею)

SNMP – це критично важливий протокол для моніторингу мережі, який дозволяє збирати та керувати мережевими даними на різних пристроях. Він працює шляхом запиту інформації до пристроїв, такої як показники продуктивності та сповіщення, що забезпечує централізоване управління мережею. Завдяки широкому розповсюдженню та сумісності з багатьма пристроями, SNMP допомагає в зусиллях з моніторингу.

Архітектура SNMP, що складається з агентів, менеджерів та баз управлінської інформації (MIB), формує структурований підхід до пошуку та управління даними. Агенти SNMP працюють на мережевих пристроях, звітуючи перед менеджерами SNMP, які обробляють та аналізують дані. MIB визначають структуру даних, забезпечуючи стандарти щодо того, яка інформація доступна та як до неї здійснюється доступ.

NetFlow та sFlow

NetFlow та sFlow – це технології, що використовуються для забезпечення видимості мережі та аналізу трафіку шляхом захоплення потоків пакетів. NetFlow, розроблений Cisco, збирає дані IP-трафіку та надає інформацію про джерело, пункт призначення, обсяг та шляхи, що проходять мережею. Така видимість дозволяє проводити поглиблений аналіз трафіку, виявляти тенденції, моделі використання та аномалії.

sFlow – це технологія вибірки пакетів, яка забезпечує статистичне представлення даних, що проходять мережею. Вона ефективна для моніторингу високошвидкісних мереж, де захоплення всіх пакетів може бути неможливим. sFlow пропонує аналітику трафіку як другого, так і третього рівня, що робить її універсальною для моніторингу мережі.

ICMP (Протокол керування інтернет-повідомленнями)

ICMP допомагає в діагностиці та моніторингу мережі, надаючи зворотний зв'язок про проблеми, пов'язані з підключенням. Він в основному використовується для звітування про помилки, що дозволяє обмінюватися повідомленнями між пристроями, щоб вказати на проблеми з підключенням до мережі, такі як недоступні пункти призначення. Утиліти, такі як «ping» та «traceroute», покладаються на ICMP для перевірки доступності хоста та трасування мережевих шляхів.

Незважаючи на свою корисність, ICMP також може становити ризики для безпеки, якщо його використовувати для атак типу «відмова в обслуговуванні» або мережевої розвідки. Тому, хоча ICMP є невід'ємною частиною моніторингу продуктивності, його використання в мережах має бути ретельно керованим та захищеним.

Типи мереж та пристроїв, що контролюються

Маршрутизатори, комутатори та концентратори

Маршрутизатори, комутатори та концентратори – це основні мережеві пристрої, що забезпечують передачу даних. Маршрутизатори керують трафіком між різними мережами, що необхідно для підключення локальних мереж до Інтернету. Моніторинг маршрутизаторів забезпечує усунення потенційних вузьких місць та оптимізацію шляхів маршрутизації для ефективного потоку трафіку. Це включає відстеження таких показників, як пропускна здатність, затримка та коефіцієнт помилок, для підтримки зв'язку та продуктивності.

Комутатори забезпечують зв'язок у мережі, спрямовуючи дані на певні пристрої, забезпечуючи ефективний розподіл даних. Моніторинг комутаторів допомагає визначити стан портів, використання пропускної здатності та рівень колізій, щоб запобігти зниженню продуктивності. Концентратори, хоча й простіші за функціями, діють як основні з'єднувачі в мережах. Їх моніторинг є важливим для виявлення потенційних несправностей, що впливають на сегменти мережі.

Брандмауери та пристрої безпеки

Пристрої мережевої безпеки, включаючи брандмауери, утворюють критично важливий захист від кіберзагроз та несанкціонованого доступу. Моніторинг цих пристроїв гарантує їх ефективне функціонування у забезпеченні дотримання політик та блокуванні шкідливого трафіку. Ключові показники, такі як спроби атак, порушення доступу та моделі трафіку, ретельно перевіряються для швидкого виявлення інцидентів безпеки та реагування на них.

Крім того, рішення для моніторингу забезпечують дотримання вимог, реєструючи спроби доступу та зміни конфігурації на пристроях безпеки. Такий рівень видимості допомагає проводити судово-медичний аналіз після порушення безпеки, швидко виявляючи скомпрометовані системи або порушення політик.

Сервери та віртуальні машини

Моніторинг серверів і віртуальних машин допомагає підтримувати безперервність та продуктивність обслуговування. На серверах розміщено програми та дані, життєво важливі для бізнес-функцій, що вимагає ретельного моніторингу використання процесора, споживання пам'яті та обсягу дискового вводу/виводу. Ці показники виявляють потенційне перевикористання або збої обладнання, що допомагає своєчасно вживати заходів з технічного обслуговування, щоб запобігти незапланованим простоям.

Віртуальні машини потребують особливого моніторингу через свою масштабованість та тимчасовість. Такі показники, як розподіл ресурсів, завантаження віртуального процесора та використання мережі, стають критично важливими для оптимізації віртуального середовища. Забезпечуючи ефективний моніторинг віртуальних активів, організації можуть динамічно адаптувати ресурси відповідно до потреб.

Хмарна інфраструктура та послуги

Завдяки своїй розподіленій та масштабованій інфраструктурі, хмарні сервіси потребують рішень для моніторингу, які забезпечують видимість розподілу ресурсів, доступності та продуктивності в кількох регіонах. Ключові показники, такі як час відгуку, час безвідмовної роботи сервісу та журнали доступу, є вирішальними для забезпечення надійної роботи та безпеки хмарного середовища.

Моніторинг хмарних сервісів також дозволяє проактивно керувати ресурсами, забезпечуючи масштабування віртуальних екземплярів під час пікових навантажень без погіршення продуктивності. Крім того, моніторинг підтримує управління витратами, виявляючи недостатньо використані ресурси або непотрібні витрати.

Дротові та бездротові мережі

Дротові мережі вимагають моніторингу таких компонентів, як комутатори Ethernet та кабелі, зосереджуючись на цілісності з'єднання та пропускній здатності для запобігання перебоям. Бездротові мережі пов'язані з унікальними проблемами, такими як перешкоди сигналу, перевантаження каналів та оцінка зони покриття. Моніторинг цих аспектів має вирішальне значення для підтримки продуктивності бездротового зв'язку.

Моніторинг бездротової мережі збирає дані про пристрої користувачів і точки доступу, допомагаючи виявляти проблеми з підключенням або спроби несанкціонованого доступу. Аналізуючи силу сигналу та швидкість передачі даних, адміністратори можуть оптимізувати конфігурації бездротової мережі для покращення покриття та зручності використання.

Проблеми моніторингу мережі

Організації повинні знати про фактори, що ускладнюють моніторинг мережі.

Моніторинг у гібридних та багатохмарних середовищах

Гібридні та мультихмарні середовища вносять багаторівневу складність у моніторинг мережі, вимагаючи рішень, що відповідають різноманітним проблемам інфраструктури та інтеграції. Ці середовища охоплюють приватні та публічні хмарні екземпляри, а також локальні системи, що вимагає інструментів, здатних забезпечувати узгоджені дані про продуктивність усіх компонентів.

Динамічна природа хмарних середовищ означає, що рішення для моніторингу повинні адаптуватися до швидкого масштабування та змін, не порушуючи видимість. Це вимагає гнучких архітектур та функцій автоматизованого виявлення, щоб йти в ногу з розвитком інфраструктури.

Обробка великих обсягів даних

Величезний обсяг даних, що генеруються в сучасних мережах, може бути приголомшливим, що створює значні труднощі для систем моніторингу, які відповідають за обробку та аналіз цієї інформації. Ефективне управління та фільтрація величезних потоків даних є важливими для отримання корисної інформації без перевантаження системних ресурсів.

Забезпечення цілісності та точності даних має вирішальне значення для надійних результатів моніторингу. Неточні або неповні дані перешкоджають прийняттю рішень, що призводить до неправильних діагнозів або пропущених сповіщень.

Забезпечення безпеки мережі та відповідності вимогам

Ефективний моніторинг вимагає стратегій впровадження, які забезпечують дотримання політик безпеки та захищають дані під час передачі та зберігання. Розширене шифрування та засоби контролю доступу необхідні для захисту процесів моніторингу та забезпечення дотримання таких норм, як GDPR та HIPAA.

Також важливо мати записи, які підтверджують дотримання стандартів безпеки та нормативних вимог, що підтримують процеси аудиту.

Практики для ефективного моніторингу мережі

Ось деякі способи, за допомогою яких організації можуть забезпечити ефективний моніторинг своїх мереж.

1. Визначте чіткі цілі моніторингу

Цілі можуть бути зосереджені на підтримці безперебійної роботи, своєчасному виявленні аномалій або оптимізації використання ресурсів. Встановлюючи точні цілі, організації можуть адаптувати свої стратегії моніторингу для отримання змістовної аналітики та підтримки прийняття стратегічних рішень.

Така чіткість також забезпечує ефективний розподіл ресурсів і допомагає встановити реалістичні показники та контрольні показники ефективності. Завдяки чітко визначеним цілям моніторингу команди можуть визначити пріоритети ключових видів діяльності та розробити цільові плани дій.

2. Регулярно оновлюйте мережеву документацію

Постійне оновлення мережевої документації гарантує точне відображення всіх змін в інфраструктурі, що сприяє ефективному моніторингу та втручанню. Документація повинна детально описувати топологію, конфігурації пристроїв та залежності, надаючи довідник адміністраторам, які керують мережею. Регулярні оновлення дозволяють точно відстежувати активи, зміни конфігурації та зростання мережі з часом.

Вичерпна документація допомагає у вирішенні проблем, швидко виявляючи уражені ділянки під час інцидентів. Вона також підтримує зусилля з дотримання вимог, підтверджуючи дотримання політик і процедур безпеки.

3. Впроваджуйте проактивне оповіщення та реагування на інциденти

Проактивне оповіщення та реагування на інциденти дозволяють швидко діяти, коли виникають проблеми з продуктивністю або загрози безпеці. Налаштування порогів оповіщень на основі тенденцій історичних даних дозволяє адміністраторам виявляти аномалії до того, як вони переростуть у серйозні проблеми. Ці оповіщення підтримують гнучке реагування на інциденти, надаючи практичну інформацію, яка спрямовує цілеспрямовані зусилля з усунення наслідків.

Протоколи реагування на інциденти доповнюють проактивне оповіщення, детально описуючи кроки для діагностики, ескалації та вирішення. Ці протоколи гарантують оперативне вирішення проблем, мінімізуючи час простою та вплив на операції.

4. Виконуйте планові оцінки та аудити мережі

Регулярні оцінки та аудити мережі надають уявлення про продуктивність мережі та стан безпеки. Ці оцінки визначають області для покращення, виявляючи вразливості або неефективність, які можуть перешкоджати роботі. Аудити систематично перевіряють конфігурації мережі, політики та процедури, забезпечуючи відповідність передовим практикам та нормативним вимогам.

Регулярні оцінювання також допомагають вимірювати успішність стратегій моніторингу, що дозволяє постійно вдосконалювати інструменти та процеси.

5. Навчіть персонал інструментам та процедурам моніторингу

Навчання персоналу використанню інструментів та процедур моніторингу мережі має вирішальне значення для максимального використання можливостей систем моніторингу. Добре навчені команди можуть точно інтерпретувати дані, розпізнавати аномалії та вживати обґрунтованих заходів для оперативного вирішення проблем. Регулярне навчання гарантує, що персонал завжди в курсі нових функцій та методологій моніторингу.

Навчання також заохочує спільну роботу між IT-командами, сприяючи спільному розумінню цілей та практик моніторингу. Це покращує комунікацію та координацію під час реагування на інциденти, сприяючи більш ефективним та результативним процесам вирішення проблем.

На рисунку 1 зображена структурна схема системи.

Рисунок 1 – Структурна схема системи

Зі структурної схеми видно, що система керування кодом підтримує програмні бібліотеки контролюючи доступ до елементів бібліотек, координує дії безлічі користувачів і допомагає в проведенні робочих процедур. Інші інструменти підтримують процес складання й випуску програмного забезпечення й документації на основі програмних елементів, що втримуються в бібліотеках. Інструменти для керування запитами на зміни програмного забезпечення використовуються для контрольованих системою конфігураційного керування програмних елементів. Інші інструменти можуть забезпечувати керування базою даних і необхідними менеджменту звітними засобами, а також діяльністю по розробці й забезпеченню якості.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого моніторингу та контролю стану IT.Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевого моніторингу та контролю стану ІТ.

– Досліджена система мережевого моніторингу та контролю стану ІТ.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевого моніторингу та контролю стану ІТ.Розроблені алгоритми дозволяють успішно вирішувати завдання мережевого моніторингу та контролю стану ІТ. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
2. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
3. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
4. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
5. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
6. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
7. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
8. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
9. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
10. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
11. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
12. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
13. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
14. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56
15. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
16. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
17. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks.

Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
18. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
19. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи hозвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
20. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
21. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
22. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.
23. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
24. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
25. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
26. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
27. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
28. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
29. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
30. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
31. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.
32. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58.