МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ, КОМП'ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри

_____ Ігор ЖУКОВ
(підпис) (ПІБ)

« ____ » _____ 2022 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ "МАГІСТР"
спеціальність 123 "Комп'ютерна інженерія"

Тема: "Комп'ютерна система моніторингу активності користувачів і стану апаратного забезпечення компанії"

Виконавець: студент групи КСМ-201Мз Старовєров Іван Олександрович

Керівник: кандидат технічних наук, доцент Дрововозов Володимир Іванович

Нормоконтролер: _____ Андрєєв Олександр Володимирович

Засвідчую, що у магістерській роботі немає
запозичень праць інших авторів
без відповідних посилань

Студент _____Старовєров І.О.

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії

Кафедра комп'ютерних систем та мереж

Спеціальність 123 «Комп'ютерна інженерія»

Форма навчання заочна

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____Ігор ЖУКОВ
(підпис) (ПІБ)

« ___ » _____ 2022 р.

З А В Д А Н Н Я
на виконання дипломної роботи

Старовєрова Івана Олександровича
(прізвище, ім'я, по батькові)

1. Тема роботи: " Комп'ютерна система моніторингу активності користувачів і стану апаратного забезпечення компанії"
затверджена наказом ректора від " 06 " вересня 2022 року № 1266 /ст
2.Термін виконання проекту (роботи):): з 05.09.2022 до 30.11.2022
3. Вихідні дані до роботи: розробити комп'ютерну систему моніторингу активності користувачів компанії і стану апаратного забезпечення компанії
4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
1) аналіз архітектури комп'ютерних систем моніторингу;
2) методи моніторингу активності користувачів і стану апаратного забезпечення;
3) описання розробленої комп'ютерної системи моніторингу активності користувачів і стану апаратного забезпечення компанії.

5. Перелік обов'язкового графічного матеріалу:
Презентація *Power Point*

6. Календарний план-графік

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1	Ознайомитись з постановкою задачі дипломної роботи	05.09.2022 – 06.09.2022	
2	Вивчити спеціальну літературу і технічну документацію	21.09.2022 – 22.09.2022	
3	Проаналізувати системи моніторингу	23.09.2022 – 29.09.2022	
4	Написати розділ 1.	30.09.2022 – 10.10.2022	
5	Проаналізувати принципи аналізу активності користувачів і стану обладнання	11.10.2022 – 21.10.2022	
6	Написати розділ 2.	22.10.2022 – 29.10.2022	
7	Провести опис роботи розробленої системи	30.10.2022 – 05.11.2022	
8	Написати розділ 3.	06.11.2022 – 09.11.2022	
9	Оформити пояснювальну записку та пройти нормоконтроль	10.11.2022 – 16.11.2022	
10	Підготувати презентаційний матеріал та захистити дипломну роботу	17.11.2022 – 30.11.2022	

7. Дата видачі завдання «05» вересня 2022 р.

Керівник дипломної роботи _____ Дрововозов В.І.
(підпис)

Завдання прийняв до виконання _____ Старовєров І.О.
(підпис студента)

РЕФЕРАТ

Пояснювальна записка до дипломної роботи “Комп'ютерна система моніторингу активності користувачів і стану апаратного забезпечення компанії”: 110 с., 22 рис., 27 літературних джерел.

АКТИВНІСТЬ КОРИСТУВАЧІВ, МОНІТОРИНГ СТАНУ, СЕРВЕР, АРХІТЕКТУРА СЕРВЕРІВ, ВІЗУАЛІЗАЦІЯ ДАНИХ, ГРАФІЧНИЙ ІНТЕРФЕЙС

Об’єкт дипломного дослідження – процес моніторингу активності користувачів і стану обладнання.

Предмет дипломного дослідження – комп'ютерна система моніторингу активності користувачів і стану апаратного забезпечення компанії.

Мета дипломного дослідження – розгляд основних методів моніторингу активності користувачів і стану апаратного забезпечення компанії.

Прогнози припущення щодо розвитку об’єкта дослідження – створення робочого зразка комп’ютерної системи та налаштування апаратного середовища на серверах компанії.

Результати дипломної роботи рекомендується використовувати при розробці нових програмних засобів та налаштуванні апаратного забезпечення, які надають можливість моніторингу активності користувачів і стану апаратного забезпечення компанії.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

API – *Application Programming Interface* (прикладний програмний інтерфейс)

CGI – *Common Gateway Interface* (загальний інтерфейс об’єднання)

CRM – *Customer Relationship Management*

DNS – *Domain Name Service* (сервер доменних імен)

FTP – *File Transfer Protocol* (протокол передачі файлів)

GUI – *Graphical User Interface* (графічний інтерфейс користувача)

LAN – *Local Area Network* (локальная мережа)

TCP/IP – *Transmission Control Protocol/Internet Protocol* (протокол управління передачею/міжмережевий протокол)

HCI – гіперконвергентна інфраструктура

ВСТУП

Актуальність теми.

Аналіз даних у режимі реального часу дозволяє оперативно визначати чинники, що впливають швидкість обробки транзакцій бізнес-додатків. Однією з ключових можливостей цього рішення є моніторинг стану та продуктивності трейдингових мереж. Контролюються показники щодо ринкових даних, потоків замовлень, шлюзів для передачі замовлень, затримки при обробці транзакцій.

Мережі стають масштабнішими і складнішими, що створює нові проблеми для IT-персоналу. Розширюється застосування мобільних пристроїв для доступу до зростаючих обсягів даних з дедалі більших джерел, багато з яких з'явилися завдяки віртуалізації. Завдання, що вирішуються IT-персоналом, ще більше ускладнюються через підвищення вимог користувачів до надійності мережевих підключень та швидкості роботи програм. Внаслідок складності мереж у них утворюються мертві зони (blind spots), де зароджуються мережеві проблеми та організуються атаки.

Сучасні технології дозволяють кардинально змінити підхід до моніторингу та контролю діяльності персоналу на виробництві. Можна виділити два основних класи систем [2]: - системи на основі засобів відеофіксації та технологій відеоаналітики; - системи на базі персональних пристроїв, що носяться.

Системи на базі засобів відеофіксації, що масово застосовуються в завданнях контролю доступу та охорони периметра об'єктів, у плані моніторингу виробничої діяльності персоналу мають обмеження як у частині функціональності, так і в частині роздільної здатності, площі покриття та допустимих місць встановлення.

Системи на базі персональних пристроїв, що носяться, мають ширші функціональні можливості, можуть використовуватися не тільки на промислових майданчиках, але і для контролю роботи виїзних бригад. Сьогодні

на ринку представлений широкий перелік персональних пристроїв, що носяться. Так, наприклад, доступні виконання у вигляді «розумних» касок, бейджів, ременів, промислових смартфонів, рацій та планшетів. Основне обмеження перелічених варіантів персональних пристроїв, що носяться, зводиться до неможливості вирішення широкого спектра завдань, що стоять перед підприємством (див. вище). Так, наприклад, рішення на базі «розумних» касок здатне вирішувати завдання позиціонування та одностороннього повідомлення співробітника, але не дозволяє забезпечувати контроль параметрів життєдіяльності (наприклад, значення пульсу) без додаткових пристроїв.

Мертві зони зазвичай утворюються з таких причин:

– Неправильне використання SPAN-портів та брак портів відгалужувачів, що перешкоджає організації доступу пристроїв моніторингу до контрольованих даних.

– Втрата або дуплікація пакетів, що зупиняє або затримує передачу інформації, яка має велике практичне значення.

– Застосування зашифрованого трафіку SSL, в якому може бути заховано зловмисне програмне забезпечення.

–Відставання планів моніторингу циклів міграції.

– Перевантаженість систем моніторингу ускладнює або унеможливлює відстеження трафіку та фільтрацію непотрібних даних на лінійних швидкостях.

– Поява мертвих зон стала серйозною проблемою, що загрожує фінансовими втратами та різними ризиками, для операторів мереж. Крім того, відсутність контролю трафіку, що передається між віртуальними машинами або блейд-серверами в ЦОДі, робить мережу ЦОДу вразливою для загроз інформаційній безпеці, не дозволяє гарантувати відповідність мережі нормативним вимогам, створює ризики зниження надійності мережі та її продуктивності. Сьогодні до 80% трафіку в ЦОД передається між серверами, що суттєво ускладнює його наскрізний (end-to-end) моніторинг.

Вирішенням проблеми контролю трафіку є використання масштабованої архітектури систем мережевого моніторингу, що дозволяє усунути мертві зони.

Архітектура заснована на повному асортименті продуктів, до якого входять мережеві відгалужувачі, обхідні комутатори, брокери мережевих пакетів (NPB), платформа моніторингу хмар та рішення для активного моніторингу мережі. Всі ці продукти та рішення дуже просто встановлювати (на мережі) та ними також просто керувати. Система моніторингу сприяє прискоренню доставки додатків, забезпечує ефективну діагностику та мережевий моніторинг, що здійснюється для контролю загроз безпеки мережі, продуктивності додатків та виконання вимог SLA. Крім того, ця архітектура допомагає IT-персоналу гарантувати виконання нормативних вимог.

Архітектура системи моніторингу дає можливість реалізувати out-of-band- та inline-моніторинг у мережах та хмарних середовищах. Підсистема безпеки (Security Fabric) – ключовий елемент системи моніторингу – забезпечує безаварійне підключення численних inline- та out-of-band-пристроїв інформаційної безпеки або моніторингу продуктивності, включаючи системи запобігання вторгненням (IPS), міжмережні екрани наступного покоління (NGFW). засоби для моніторингу продуктивності додатків та мереж (APM та NPM) та ін.

Система моніторингу дозволяє визначати продуктивність баз даних без втручання у їхню роботу. Існують функціональні розширення для наступних СУБД: MySQL, Sybase, PostgreSQL, MS SQL та Oracle. Аналітика забезпечує:

- виявлення затримок відгуків запити;
- аналіз транзакцій;
- виявлення причин виникнення помилок;
- декомпозицію запитів.

Продуктивність веб-додатків контролюється за допомогою функціонального розширення, що надає такі можливості:

- глибокий аналіз HTTP-транзакцій;
- визначення затримок у передачі запитів та відгуків;
- аналіз помилок;
- підтримку TLS (визначення типу шифрування, термінів дії сертифікатів, виявлення вразливостей та атак).

Спеціальне функціональне розширення автоматично визначає BGP-сесії та надає оперативну інформацію про зміни маршрутів, що впливають на мережеве оточення. Детальна аналітика з усіх змін маршрутів забезпечує швидкий пошук причин. BGP-аналітика реалізує:

- інформування про видалення маршрутів;
- виявлення нестабільних маршрутів;
- визначення затримок збіжності.

Функціональне розширення для VoIP є одним із ключових рішень для контролю якості голосового зв'язку в режимі реального часу. Підтримуються протоколи SIP, H.323, RTP та RTCP. Функціональне розширення для VoIP дозволяє здійснювати:

- контроль показника якості передачі голосу (MOS);
- аналіз метрик продуктивності SIP;
- аналіз помилок SIP;
- отримання сумарної статистики за дзвінками;
- запис трафіку RTP.

РОЗДІЛ 1.
АНАЛІЗ АРХІТЕКТУРИ СИСТЕМ МОНІТОРИНГУ

Сучасні серверні платформи пропонують багато варіантів для малого та середнього бізнесу та корпоративних IT-покупців; які дозволяють моніторити практично все,що відбувається в мережі компанії і на підключених до неї пристроях.

1.1. Аналіз принципів побудови систем моніторингу

Одним із найважливіших компонентів найкращого інструменту моніторингу мережі є можливість моніторингу та оптимізації доступності мережі. Зрештою, якщо мережа не працює, більшість повсякденних операцій, особливо для корпоративних мереж, зупиняються. Однак, оскільки в більшості мереж кілька процесів і програм працюють одночасно, досягнення оптимальної доступності, яка відповідає вимогам угоди про рівень обслуговування (SLA), може бути складним завданням.

Інструменти моніторингу доступності мережі надають IT-фахівцям миттєвий аналіз даних з усіх мережевих пристроїв за допомогою прикладного рівня під назвою простий протокол керування мережею (SNMP), який також допомагає адміністраторам знаходити потенційні вузькі місця та больові точки для усунення проблем мережі до їх виникнення. . Провідні рішення для мережевого моніторингу сповіщають адміністраторів щоразу, коли виникає проблема, від несправності пристрою до несправного рівня пропускної здатності, DoS-атак та інших потенційних мережевих проблем.

Крім того, програмне забезпечення для моніторингу мережі також має мати захист від можливого збою або тимчасової недоступності сервера, на якому працює інструмент моніторингу мережі. Організації повинні прийняти рішення для моніторингу мережі, які автоматично вирішують проблему, покладаючись на резервну подвійну програму моніторингу мережі. Ці функції перемикання

та відновлення після збоїв забезпечують постійну безпеку важливих баз даних і цілодобову доступність мереж.

Іншим важливим аспектом моніторингу мережі є чітке розуміння вхідного та вихідного трафіку мережі. Більшість мережевих пристроїв підтримують стандарт SNMP, який дозволяє повідомляти про працездатність і продуктивність усього мережевого обладнання через адресу Інтернет-протоколу (IP). IP-адреса надає показники продуктивності окремих мережевих пристроїв, що дозволяє мережевим адміністраторам збирати показники за допомогою інструментів моніторингу мережі, щоб уникнути вузьких місць і оцінити загальну продуктивність окремих пристроїв і мережі в цілому. Ось список цих показників:

Використання пропускної здатності: цей термін стосується обсягу трафіку, що надсилається з мережі, і відсотка загальної пропускної здатності, яку використовує мережа в будь-який момент часу. Пропускна здатність вимірюється кількістю даних (у байтах), отриманих і надісланих конкретними мережевими інтерфейсами.

Завантаження ЦП: яка частина обчислювальної потужності мережевого пристрою наразі використовується для обробки вхідних даних, зберігання даних і створення вихідних даних.

Помилки/відкидання інтерфейсу: ці умови враховують помилки на приймаючих пристроях, через які мережеві інтерфейси можуть відкидати пакети даних. Ці помилки та відхилення можуть мати багато причин, зокрема помилки конфігурації або проблеми з пропускною здатністю.

IP-метрики: IP-метрики – це інші показники, які використовуються для вимірювання швидкості та ефективності з’єднань між мережевими пристроями, наприклад затримка часу та кількість переходів.

Пропускна здатність: це швидкість трафіку, виміряна байтами за секунду, яка проходить через інтерфейс пристрою протягом певного періоду часу.

Час роботи: термін, який використовується для опису часу, протягом якого мережевий пристрій успішно отримує та надсилає дані.

Моніторинг мережі проти керування мережею

Хоча терміни моніторинг мережі та керування мережею іноді помилково використовуються як синоніми, моніторинг мережі є попередником процесу керування мережею. Однак гарний план керування мережею також передбачає чудовий моніторинг мережі, а застосування належних інструментів моніторингу мережі є життєво важливим для оптимізації мережі та забезпечення безперервної нормальної роботи.

Простіше кажучи, керування мережею — це з'єднання. План керування мережею — це система, за допомогою якої організація налаштовує, контролює та підтримує надійну мережу, постійно гарантуючи, що пристрої підтримують підключення до програмних програм і що користувачі можуть використовувати їх безперешкодно та безпечно. Ефективне керування мережею включає надання, конфігурацію, безпеку та моніторинг кожного елемента мережі, створюючи стійку систему, яка забезпечує зростання та ефективність. Отже, легко зрозуміти, як правильні рішення для моніторингу мережі можуть допомогти підвищити ефективність керування мережею.

Окрім надання легкодоступних звітів про всі основні показники IP для оцінки швидкості та працездатності мережі, рішення для моніторингу мережі мають пропонувати варіанти як для вирішення проблем у міру їх виникнення, так і для передбачення проблем, перш ніж вони виникнуть, для вжиття запобіжних заходів. Ось кілька основних способів, якими інструменти моніторингу мережі повинні дозволити IT-адміністраторам виявляти, планувати та швидко вирішувати щоденні проблеми з мережею.

Сповіщення: автоматизовані рішення для моніторингу мережі повинні дозволити IT-фахівцям швидко й ефективно вирішувати проблеми з мережею, щойно вони виникають, пропонуючи варіанти для створення налаштованого арсеналу спеціальних попереджень, тривог і сповіщень щодо багатьох проблем, які можуть впливати на мережу. Ці сповіщення також мають бути налаштовані пристроєм і членом команди, щоб гарантувати, що правильний адміністратор буде сповіщений про проблему, як тільки вона виникне.

Вузькі місця: іноді на продуктивність мережі може вплинути недостатня пропускна здатність, через що пакети даних у мережі не можуть досягти місця призначення протягом прийнятного періоду часу. Хороше рішення для моніторингу мережі забезпечить оперативну інформаційну панель для моніторингу продуктивності мережі, дозволяючи адміністраторам швидко та легко визначати збої, які спричиняють або можуть спричинити вузькі місця.

Ідентифікація несправностей: як і сповіщення, системи ідентифікації несправностей сповіщають команди про проблеми в мережі незалежно від того, де вони знаходяться. Функції ідентифікації несправностей можуть сповіщати команди про проблеми з мережею через електронну пошту, SMS, модем і мобільний додаток.

Усунення несправностей: найкраще програмне забезпечення для моніторингу мережі допомагає IT-фахівцям зрозуміти нормальну поведінку мережі, щоб визначити потенційні проблеми в майбутньому, допомагаючи командам зрозуміти базову поведінку широкого спектру елементів, які можуть впливати на мережу, включаючи використання ЦП і використання пропускної здатності. Розуміння та документування цих порогових значень за допомогою рішень моніторингу мережі може допомогти адміністраторам установити відповідні сповіщення та нагадування.

Інструменти моніторингу мережі також можуть допомогти у вирішенні проблем, тримаючи всіх інженерів і адміністраторів на сторінці щодоінфраструктури, додатків та інших показників, що допомагає швидше й ефективніше діагностувати, усувати неполадки та вирішувати проблеми. Розширена здатність консолідувати дані моніторингу дозволяє командам швидко визначати, чи є затримка чи помилки спричиненими кодом мережі, проблемою на рівні хоста чи іншим джерелом.

Використання програмного забезпечення моніторингу мережі для відображення мережі, сканування та виявлення

Інше важливе використання рішень для мережевого моніторингу – сканування мережі, відображення та виявлення. Величезний обсяг даних, які

генерує мережа, іноді може бути величезним і без інструментівмережеве скануванняі картографування, критичні проблеми можуть залишитися непоміченими. Інструменти моніторингу мережі можуть допомогти командам виявити всі мережеві пристрої, підключені до мережі, і дозволити IT-фахівцям створювати карти топології та створювати звіти на основі цих карт. Ці скани та карти є життєво важливими ресурсами для розуміння компонентів кожної мережі та проведення регулярної інвентаризації цих компонентів.

Сканування мережі – це термін, який використовується для ідентифікації пристроїв у мережі шляхом надсилання сигналу та очікування відповіді. Відображення мережі стосується створення графічного представлення мережевих вузлів та їхніх зв'язків. Вузли мережі можуть включати маршрутизатори, комутатори, брандмауери та інші пристрої, підключені до мережі.Відображення мережіможна автоматизувати та використовувати для створення огляду мережі або зосередження на вибраній частині. Але, як правило, відображення мережі використовується для відображення поточного стану та іншої важливої інформації для всіх пристроїв, підключених до мережі. Відображення мережі може включати як фізичні, так і логічні зв'язки між мережами.

Мережні карти спираються на візуальне представлення топології мережі. В управлінні мережею топологія — це термін, який використовується для опису організації мережі. Топологія служить картою мережі. Він містить список пристроїв, підключених до мережі або пов'язаних з нею, разом із детальною інформацією про те, де ці пристрої розташовані один з одним. Для ефективного керування мережею адміністраторам потрібна чітка топологічна карта, щоб визначити структуру, компонування та з'єднання, пов'язані з мережею. Ось кілька поширених мережевих топологій.

Зіркоподібна конфігурація: найпоширеніша топологія мережі, кожен вузол у зіркоподібній мережі підключений до одного центрального концентратора через коаксіальний кабель, виту пару або оптоволоконний кабель. Цей хаб діє як сервер.

Топологія шини: ця конфігурація з’єднує всі пристрої в мережі центральним кабелем. Дані переміщуються в одному напрямку по цій центральній лінії.

Кільцева топологія: у цій топології вузли з’єднані у вигляді кола. Дані переміщуються в одному або обох напрямках.

Мережі відображення забезпечують видимість, але ці карти вимагають розуміння того, як з’єднані вузли. Інструменти моніторингу мережі можуть автоматично надавати повну картину, використовуючи візуальні дані навколо цих з’єднань, а також можуть автоматично оновлювати ці карти мережі для швидкого використання в разі виникнення проблем.

Організації повинні знати, що не кожен інструмент моніторингу мережі матиме всі перелічені вище функції. Необхідно приділяти особливу увагу під час вибору рішень, які відповідають розміру організації, потенційним проблемам і потребам у безпеці, залишаючи при цьому достатньо місця для зростання мережі.

Багато інструментів моніторингу мережі пропонують можливості «віддаленого моніторингу мережі». Термін віддалений мережевий моніторинг стосується процесу моніторингу, керування та регулювання пристроїв у мережі, які можуть бути поза приміщенням. Використовують великі та корпоративні мережі та постачальники керованих послуг (які часто контролюють декілька мереж).програмне забезпечення для віддаленого моніторингу мережідля збору даних і відстеження тенденцій для оцінки продуктивності мережі. Маючи ці дані та нагляд, вони можуть вирішувати проблеми, які виникають за межами підприємства.

Оскільки програмне забезпечення для віддаленого моніторингу мережі дає змогу мережевим пристроям отримувати доступ із будь-якого місця, воно ідеально підходить для усунення несправностей, а це означає, що пристрої починають працювати швидше. Кінцеві користувачі мережі можуть краще підключатися, підвищуючи загальну ефективність організації та одночасно знижуючи витрати. Віддалений моніторинг мережі також є ефективним способом підвищення безпеки, оскільки багато найкращих рішень для

віддаленого моніторингу мережі пропонують важливу опцію спостереження в режимі реального часу, що має вирішальне значення для того, щоб усі команди були в курсі обох протоколів безпеки та були в курсі потенційної безпеки. порушення. Крім того, автоматично оновлювані карти та показники у віддалених мережах можуть надати універсальні дані про загальний стан системи та безпеку для всієї мережі одночасно в розгалуженій мережі, незалежно від розташування частин мережі.

Віддалений моніторинг мережі чудово допомагає виявляти такі проблеми, як перевантаження мережевого трафіку, конфлікти та викинуті пакети, а також досліджувати проблеми, збираючи всі дані, щоб допомогти вирішити та задокументувати проблему. Озброївшись цією інформацією, мережеві адміністратори підприємств і MSP можуть краще керувати великими мережевими роботами, включаючи локальні, хмарні або гібридні пристрої, одночасно зменшуючи час простою та покращуючи безпеку мережі.

Успішний моніторинг мережі — це більше, ніж просто застосування правильних інструментів. Хороша стратегія моніторингу мережі має подвійний характер: по-перше, організація повинна провести ретельну оцінку вищезазначених функцій, щоб переконатися, що інструменти моніторингу мережі, які вона прийняла, дозволяють командам швидко та легко отримувати доступ до інформації про стан мережі, дозволяючи IT-фахівцям працювати на випередження, щоб вирішити проблеми до їх виникнення. Другим компонентом ефективного моніторингу мережі є процес, за допомогою якого команди складають карту мереж, документують ці висновки та встановлюють протоколи для підтримки працездатності мережі. Ось деякі вказівки щодо найкращих практик моніторингу мережі.

Розуміння тонкощів мережі є проблемою, особливо для корпоративних мереж. Але для вирішення майбутніх проблем у міру їх виникнення інженери та адміністратори повинні мати повне уявлення про те, як функціонує мережа, коли все йде правильно. Використовуйте інструменти моніторингу мережі, щоб установити базові показники для ініціювання сповіщень, коли в мережі

виникають порушення. Ці базові показники дозволяють командам вирішувати проблеми, коли вони виникають швидко або до того, як проблеми переростуть у проблеми.

Інструменти моніторингу мережі ідеально запропонують детальний аналіз і усунення несправностей для кожного рівня мережі, від фізичних пристроїв до проблем з IP-адресами, серверами тощо. Ці вичерпні звіти та інструменти для візуалізації цієї інформації мають вирішальне значення для швидкого вирішення проблем у вашій мережі.

Одним із важливих застосувань рішень мережевого моніторингу є розвиток здатностіусунути проблеми з мережеюдо того, як вони виникнуть. Важливою частиною побудови функціональної мережі є використання інструментів мережевого моніторингу для створення документації щодо базових операцій та історії відомих проблем і рішень, застосованих для вирішення цих проблем у минулому. І після закладення цього фундаменту команди повинні розробити протоколи для вирішення цих проблем, щоб заощадити час і зусилля та мінімізувати час простою. Сповіщення та виявлення несправностей, які дозволяють правильному члену команди бути попередженим про проблеми, як тільки вони виникають, є життєво важливим компонентом ефективної системи протоколів. Тому обов’язково шукайте надійну та зручну систему для встановлення сповіщень у ваших інструментах моніторингу мережі.

Хоча інструменти моніторингу мережі існують для захисту організацій від проблем із безпекою та технічних проблем, ті самі проблеми, які можуть спричинити збої в мережах, також можуть призвести до збою інструментів моніторингу мережі. Переконайтеся, що ваші рішення для моніторингу мережі також містять плани на випадок непередбачених ситуацій, щоб гарантувати, що системи резервного копіювання ввімкнено, а інструменти моніторингу мережі все ще доступні, якщо сервери чи інші частини мережі вийдуть з ладу.

Оскільки потреби кожної організації в моніторингу мережі відрізняються, настроювані параметри для полегшення використання рішень моніторингу мережі є важливою функцією, про яку часто не звертають уваги. Найпопулярніші

інструменти моніторингу мережі включають інформаційні панелі з настроюваними ключовими показниками ефективності. Ваші IT-фахівці можуть отримати доступ до показників, які є найбільш важливими для вашої організації, тож команди не витрачають дорогоцінний час на пошук важливої інформації.

Організаціям також потрібні інструменти для сповіщення конкретних членів команди про певні проблеми. Не всі в організації здатні впоратися з кожною потенційною проблемою в мережі, і попередження потрібного професіонала про проблеми в секунду, коли вони виникають, також економить критичний час, витрачений на пошук потрібної людини для вирішення проблеми. Найкращі інструменти мережевого моніторингу дозволяють фільтрувати сповіщення до правильного одержувача та пропонують кілька каналів для доставки цих сповіщень, включаючи SMS, електронну пошту та інші канали. Інструменти мережевого моніторингу також повинні дозволяти встановлювати пріоритетність сповіщень відповідно до серйозності проблеми та містити інформацію про місцезнаходження.

Правильна ідентифікація кожного пристрою та з’єднання з мережею є основою створення надійних і безпечних мереж. Однак ручне сканування мереж у пошуках нових мережевих пристроїв і з’єднань займає багато часу, є неефективним і застарілим. Системи моніторингу мережі повинні включатиавтоматичне виявлення пристроюфункції, призначені для сканування та відображення існуючих вузлів і автоматичного виявлення нових пристроїв після додавання в мережу.

Оскільки засоби моніторингу мережі мають зображення кожного підключеного пристрою, вони можуть намалювати візуальне представлення мережі. Ці карти мережі дозволяють адміністраторам дивитися на абстракцію своєї мережі, що важливо для підприємств із розгалуженими складними мережами. Найкращі карти мережі містять візуальну інформацію про вузли та пристрої, що дозволяє користувачам одразу побачити проблеми з продуктивністю.

Проблеми з мережею, наприклад простої, можуть бути спричинені багатьма різними проблемами. Без відповідних інструментів моніторингу доступності мережі пошук першопричин проблеми в мережі може бути схожим на пошук голки в стозі сіна.

Найкращі інструменти моніторингу мережі нададуть можливості для усунення несправностей, наприклад інструмент мережевої діагностики, створений для постійного моніторингу продуктивності та доступності мережевих пристроїв, щоб інженери та адміністратори могли отримати допомогу з усунення несправностей, коли виникають проблеми. У поєднанні з інтелектуальним мережевим оповіщенням можливості аналізу першопричини допомагають тримати команди в курсі того моменту, коли ключові показники ефективності перевищують критичні пороги, і краще підготуватися до швидкого вирішення цих проблем.

1.2. Огляд методів аналізу та моніторингу мережного трафіку

Оскільки продовжують зростати приватні внутрішні мережі компаній, надзвичайно важливо, щоб мережеві адміністратори знали та вміли керувати вручну різними типами трафіку, що подорожує їхньою мережею. Моніторинг та аналіз трафіку необхідні для того, щоб більш ефективно діагностувати та вирішувати проблеми, коли вони відбуваються, таким чином не доводячи мережеві сервіси до простою протягом тривалого часу. Доступно багато різних інструментів, які дозволяють допомогти адміністраторам з моніторингом та аналізом мережного трафіку. Ця стаття обговорює методи моніторингу орієнтовані маршрутизатори і методи моніторингу не орієнтовані маршрутизатори (активні і пасивні методи). Стаття дає огляд трьох доступних та найбільш широко використовуваних методів моніторингу мережі, вбудованих у маршрутизатори (SNMP,

Мережевий моніторинг (моніторинг мережі) — це складне завдання, яке потребує великих витрат сил, що є життєво важливою частиною роботи

мережевих адміністраторів. Адміністратори постійно прагнуть підтримати безперебійну роботу своєї мережі. Якщо мережа «впаде» хоча б на невеликий період часу, продуктивність у компанії скоротиться і (у разі організацій, що надають державні послуги), сама можливість надання основних послуг буде поставлена під загрозу. У зв'язку з цим адміністраторам необхідно стежити за рухом мережевого трафіку та продуктивністю по всій мережі та перевіряти, чи з'явилися в ній проломи в безпеці.

"Аналіз мережі - це процес захоплення мережевого трафіку та його швидкого перегляду для визначення того, що сталося з мережею" - Анжелла Оребаух. У наступних розділах обговорюються два способи моніторингу мережі: перший маршрутизаторо-орієнтований, другий не орієнтований на маршрутизатори. Функціональність моніторингу, який вбудований у самі маршрутизатори і не вимагає додаткової установки програмного чи апаратного забезпечення, називають методами, що базуються на маршрутизаторі. Не засновані на маршрутизаторах методи вимагають встановлення апаратного та програмного забезпечення та надають більшу гнучкість. Обидві техніки обговорюються нижче у відповідних розділах.

Методи моніторингу засновані на маршрутизаторі – жорстко задані (вшити) у маршрутизаторах і, отже, мають низьку гнучкість. Короткий опис методів такого моніторингу, що найчастіше використовуються, наведені нижче. Кожен метод розвивався багато років, перш ніж стати стандартизованим способом моніторингу.

1.2.1. Протокол простого мережевого моніторингу (SNMP)

SNMP – протокол прикладного рівня, який є частиною протоколу TCP/IP. Він дозволяє адміністраторам керувати продуктивністю мережі, знаходити та усувати мережеві проблеми, планувати зростання мережі. Він збирає статистику з трафіку до кінцевого хоста через пасивні датчики, які реалізуються разом із маршрутизатором. У той час, як існують дві версії (SNMPv1 та SNMPv2), цей

розділ описує лише SNMPv1. SNMPv2 побудований на SNMPv1 і пропонує ряд удосконалень, таких як додавання операцій із протоколами. Стандартизується ще один варіант версії SNMP. Версія 3 (SNMPv3) перебуває у стадії розгляду.

Для протоколу SNMP притаманні три ключові компоненти: керовані пристрої (Managed Devices), агенти (Agents) та системи управління мережею (Network Management Systems – NMSs). Вони показані на рис. 1.

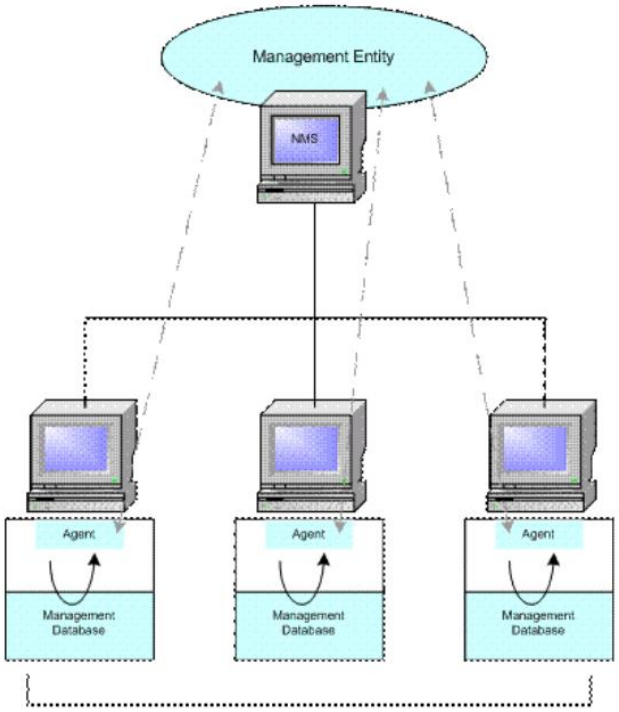

Рис. 1.1. Компоненти SNMP

Керовані пристрої включають SNMP-агента і можуть складатися з маршрутизаторів, перемикачів, комутаторів, концентраторів, персональних комп'ютерів, принтерів та інших елементів, подібних цим. Вони несуть відповідальність за збирання інформації та роблять її доступною для системи управління мережею (NMS).

Агенти включають програмне забезпечення, яке володіє інформацією з управління, і переводять цю інформацію у форму, сумісну з SNMP. Вони закриті для керування.

Системи керування мережею (NMS) виконують програми, які займаються моніторингом та контролем пристроїв керування. Ресурси процесора та пам'яті, необхідні для керування мережею, надаються NMS. Для будь-якої керованої

мережі має бути створена хоча б одна система керування. SNMP може діяти виключно як NMS або агент, або може виконувати свої обов'язки або ін.

Існує 4 основні команди, що використовуються SNMP NMS для моніторингу та контролю керованих пристроїв: читання, запис, переривання та операції перетину. Операція читання розглядає змінні, що зберігаються керованими пристроями. Команда запису змінює значення змінних, які зберігаються керованими пристроями. Операції перетину володіють інформацією про те, які змінні керованих пристроїв підтримують, і збирають інформацію з таблиць змінних, що підтримуються. Операція переривання використовується керованими пристроями для того, щоб повідомити NMS про настання певних подій.

SNMP використовує 4 протокольні операції у порядку дії: Get, GetNext, Set та Trap. Команда Get використовується, коли NMS видає запит на інформацію для керованих пристроїв. SNMPv1-запит складається з заголовка повідомлення та одиниці даних протоколу (PDU). PDU-повідомлення містить інформацію, яка необхідна для вдалого виконання запиту, який або отримуватиме інформацію від агента, або задавати значення в агенті. Керований пристрій використовує SNMP агентів, розташованих у ньому, для отримання необхідної інформації і потім надсилає повідомлення NMS'у, з відповіддю на запит. Якщо агент не має будь-якої інформації стосовно запиту, він нічого не повертає. Команда GetNext отримуватиме значення наступного екземпляра об'єкта. Для NMS також можна надсилати запит (операція Set), коли встановлюється значення елементів без агентів Коли агент повинен повідомити NMS-події, він використовуватиме операцію Trap.

Як говорилося раніше, SNMP – протокол рівня додатків, який використовує пасивні сенсори, щоб допомогти адміністратору простежити за мережевим трафіком та продуктивністю мережі. Хоча, SNMP може бути корисним інструментом для адміністратора мережі, він створює можливість для загрози безпеці, тому що він позбавлений можливості аутентифікації. Він відрізняється від віддаленого моніторингу (RMON), який обговорюється в

наступному розділі, тим, що RMON працює на мережному рівні та нижче, а не на прикладному.

1.2.2. Віддалений моніторинг (RMON)

RMON включає різні мережеві монітори та консольні системи для зміни даних, отриманих в ході моніторингу мережі. Це розширення для SNMP інформаційної бази даних управління (MIB). На відміну від SNMP , який має надсилати запити про надання інформації, RMON може налаштовувати сигнали, які «моніторити» мережу, засновану на певному критерії. RMON надає адміністраторам можливості керувати локальними мережами так само добре, як віддаленими від однієї певної локації/точки. Його монітори для мережного рівня наведені нижче. RMON має дві версії RMON та RMON2. Однак у цій статті йдеться лише про RMON. RMON2 дозволяє проводити моніторинг на всіх мережевих рівнях. Він фокусується на IP-трафіку та трафіку прикладного рівня.

Хоча існує 3 ключові компоненти моніторингового середовища RMON, тут наводяться тільки два з них. Вони показані на рис. 2 нижче.

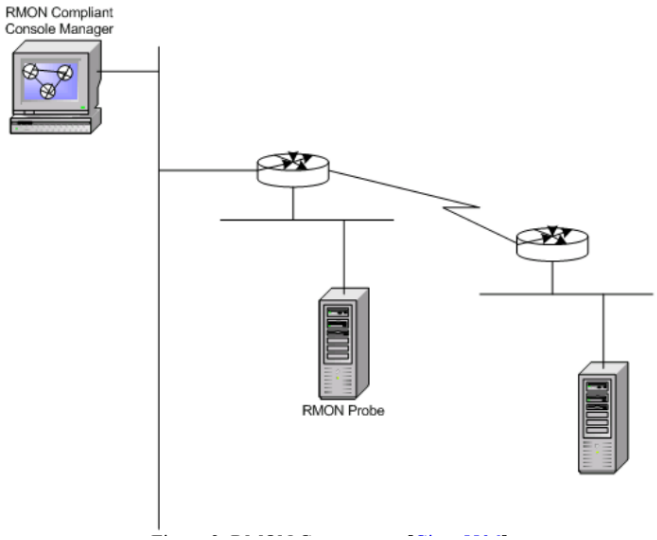

Рис. 1.2. Компоненти RMON

Два компоненти RMON це датчик, також відомий як агент або монітор, і клієнт, також відомий як станція управління (станція управління). На відміну від SNMP датчик або агент RMON збирає та зберігає мережну інформацію. Датчик

— це вбудоване в мережевий пристрій (наприклад, маршрутизатор або перемикач) програмне забезпечення. Датчик може запускатися на персональному комп'ютері. Датчик повинен розміщуватися для кожного різного сегмента локальної або глобальної мережі, тому що вони здатні бачити трафік, який проходить тільки через їх канали, але вони не знають про трафік за їхніми межами. Клієнт - це зазвичай керуюча станція, яка пов'язана з датчиком, що використовує SNMP для отримання та корекції даних RMON.

RMON використовує 9 різних груп моніторингу для отримання інформації про мережу.

- Statistics — статистика вимірювана датчиком кожного інтерфейсу моніторингу даного пристрою.
- History — облік періодичних статистичних вибірок із мережі та зберігання їх для пошуку.
- Alarm – періодично бере статистичні зразки та порівнює їх із набором порогових значень для генерації події.
- Host містить статистичні дані, пов'язані з кожним хостом, виявленим у мережі.
- HostTopN - готує таблиці, що описують вершину хостів (головний хост).
- Filters — включає фільтрацію пакетів, ґрунтуючись на фільтровому рівнянні для захоплення подій.
- Packet capture – захоплення пакетів після їх проходження через канал.
- Events – контроль генерації та реєстрація подій від пристрою.
- Token ring – підтримка кільцевих лексем.

Як встановлено вище, RMON будується на протоколі SNMP. Хоча моніторинг трафіку може бути виконаний за допомогою цього методу, аналітичні дані інформації, отримані SNMP і RMON мають низьку продуктивність. Утиліта Netflow, яка обговорюється в наступному розділі,

успішно працює з багатьма пакетами аналітичного програмного забезпечення, щоб зробити роботу адміністратора набагато простіше.

1.2.3. Розширення Netflow

Netflow – це розширення, яке було представлене у маршрутизаторах Cisco, які надають можливість збирати IP мережевий трафік, якщо це встановлено в інтерфейсі. Аналізуючи дані, які надаються Netflow, мережевий адміністратор може визначити такі речі як: джерело та приймач трафіку, клас сервісу, причини переповненості. Netflow включає 3 компоненти: FlowCaching (кешуючий потік), FlowCollector (збирач інформації про потоки) і Data Analyzer (аналізатор даних). Рис. 3 показує інфраструктуру Netflow. Кожен компонент, показаний малюнку, пояснюється нижче.

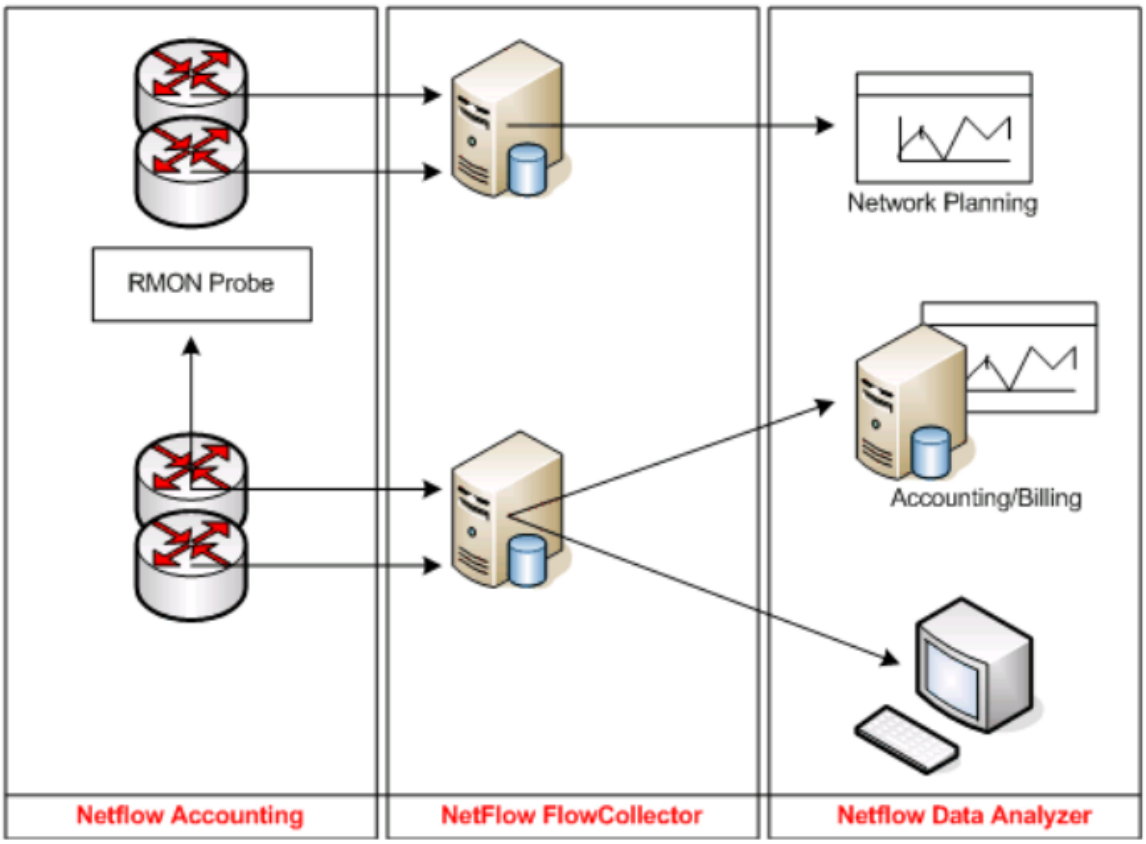

Рис. 1.3. Інфраструктура NetFlow

FlowCaching аналізує та збирає дані про IP потоки, які входять до інтерфейсу, і перетворює дані для експорту.

З Netflow-пакетів може бути отримана така інформація:

- Адреса джерела та одержувача.
- Номер вхідного та вихідного пристрою.
- Номер порту джерела та приймача.
- Протокол 4 рівня.
- Кількість пакетів у потоці.
- Кількість байтів у потоці.
- Тимчасовий штамп у потоці.
- Номер автономної системи (AS) джерела та приймача.
- Тип сервісу (ToS) та прапор TCP.

Перший пакет потоку, що проходить через стандартний шлях перемикання, обробляється створення кешу. Пакети з подібними характеристиками потоку використовуються для створення запису про потік, який міститься в кеш для всіх активних потоків. Цей запис відзначає кількість пакетів та кількість байт у кожному потоці. Потім інформація, що кешується, потім періодично експортується в Flow Collector (складальник потоків).

Flow Collector - відповідальний за збирання, фільтрування та зберігання даних. Він включає історію про інформацію про потоки, які були підключені за допомогою інтерфейсу. Зниження обсягу даних також відбувається за допомогою Flow Collector'a за допомогою вибраних фільтрів та агрегації.

Data Analyzer (аналізатор даних) необхідний, коли потрібно подати дані. Як показано на малюнку, зібрані дані можуть використовуватися для різних цілей, навіть відмінних від моніторингу мережі, таких як планування, облік та побудова мережі.

Перевага Netflow над іншими способами моніторингу, такими як SNMP і RMON, у тому, що в ній існує програмні пакети, призначені для різного аналізу трафіку, які існують для отримання даних від Netflow-пакетів та представлення їх у більш дружньому для користувача вигляді.

При використанні інструментів, таких як Netflow Analyzer (це тільки один інструмент, який доступний для аналізу Netflow-пакетів), інформація, наведена

вище, може бути отримана від Netflow-пакетів для створення діаграм та звичайних графіків, які адміністратор може вивчити для більшого розуміння про його мережі. Найбільша перевага використання Netflow на відміну від доступних аналітичних пакетів у тому, що в даному випадку можуть бути побудовані численні графіки, що описують активність мережі будь-якої миті часу.

1.2.4. Технології не засновані на маршрутизаторах

Хоча технології, не вбудовані в маршрутизатор все ж таки обмежені у своїх можливостях, вони пропонують більшу гнучкість, ніж технології вбудовані в маршрутизатори. Ці методи класифікуються як активні та пасивні.

Активний моніторинг повідомляє проблеми у мережі, збираючи вимірювання між двома кінцевими точками. Система активного вимірювання має справу з такими метриками, як корисність, маршрутизатори/маршрути, затримка пакетів, повтор пакетів, втрати пакетів, нестійка синхронізація між прибуттям, вимірювання пропускної здатності.

Головним чином використання інструментів, такі як команда ping, яка вимірює затримку та втрати пакетів, та traceroute, яка допомагає визначити топологію мережі, є прикладом основних активних інструментів вимірювання. Обидва ці інструменти посилають пробні ICMP-пакети до точки призначення та чекають, коли ця точка відповість відправнику.

Даний метод може не тільки збирати поодинокі метрики про активний вимір, але й визначатиме топологію мережі. Ще один важливий приклад активного виміру - утиліта iperf. Iperf – це утиліта, яка вимірює якість пропускної спроможності TCP та UDP протоколів. Вона повідомляє пропускну здатність каналу, існуючу затримку та втрати пакетів.

Проблема, яка існує з активним моніторингом - це те, що представлені проби в мережі можуть втручатися в нормальний трафік. Часто час активних проб обробляється інакше, ніж нормальний трафік, що ставить під сумнів важливість наданої інформації від цих проб.

Згідно з загальною інформацією, описаною вище, активний моніторинг – це надзвичайно рідкісний метод моніторингу, взятий окремо. Пасивний моніторинг навпаки вимагає великих мережевих витрат.

Пасивний моніторинг на відміну від активного не додає трафік до мережі та не змінює трафік, який вже існує у мережі. Також на відміну від активного моніторингу, пасивний збирає інформацію лише про одну точку в мережі. Вимірювання відбуваються набагато краще, ніж між двома точками при активному моніторингу.

Пасивні вимірювання мають справу з такою інформацією, як: трафік та суміш протоколів, кількість бітів (бітрейт), синхронізація пакетів та час між прибуттям. Пасивний моніторинг може бути здійснений за допомогою будь-якої програми, що витягує пакети.

Хоча пасивний моніторинг немає витрат, які має активний моніторинг, він має недоліки. З пасивним моніторингом, вимірювання можуть бути проаналізовані лише оф-лайн і вони не представляють колекції. Це створює проблему, пов'язану з обробкою великих наборів даних, зібраних під час вимірювання.

Пасивний моніторинг може бути кращим за активний у тому, що дані службових сигналів не додаються до мережі, але пост-обробка може викликати велику кількість тимчасових витрат. Саме тому існує комбінація цих двох методів моніторингу.

Після прочитання розділів вище, можна благополучно переходити до висновку про те, що комбінування активного та пасивного моніторингу є кращим способом, ніж використання першого чи другого окремо. Комбіновані технології використовують найкращі сторони і пасивного, і активного моніторингу середовищ. Дві нові технології, що становлять комбіновані технології моніторингу, описуються нижче. Це "Перегляд ресурсів на кінцях мережі" (WREN) та "Монітор мережі з власною конфігурацією" (SCNM).

WREN використовує комбінацію технік активного та пасивного моніторингу, активно обробляючи дані, коли трафік малий, та пасивно

обробляючи дані протягом великого трафіку. Він дивиться трафік і від джерела, і від одержувача, що уможливлює більш акуратні виміри. WREN використовує трасування пакетів від створеного додатком трафіку для вимірювання корисної пропускної спроможності. WREN розбитий на два рівні: основний рівень швидкої обробки пакетів та аналізатор трасувань користувача рівня.

Основний рівень швидкої обробки пакетів відповідає за отримання інформації, пов'язаної з вхідними та вихідними пакетами. Рис. 6 показує список інформації, що збирається кожному пакету. До Web100 додається буфер для збору цих параметрів. Доступ до буфера здійснюється за допомогою двох системних дзвінків. Один виклик починає трасування і надає необхідну інформацію для її збору, поки другий виклик повертає трасування з ядра.

Об'єкт трасування пакетів – здатний координувати обчислення між різними машинами. Одна машина активуватиме роботу іншої машини, задаючи прапор у заголовку пакета, що йде, для початку обробки деякого діапазону пакетів, які вона трасує. Інша машина у свою чергу трасуватиме всі пакети, для яких вона бачить, що в заголовку встановлено схожий прапор. Така координація забезпечує те, що інформація про схожі пакети зберігається в кожній кінцевій точці незалежно від зв'язку та того, що відбувається між ними.

Аналізатор трасувань рівня користувача — інший рівень у середовищі WREN. Це компонент, який починає трасування будь-якого пакета, збирає та обробляє повернені дані на рівні ядра оператора. Згідно з проектуванням, компоненти рівня користувача не потребують читання інформації від об'єкта трасування пакетів весь час. Вони можуть бути проаналізовані негайно після того, як трасування буде завершено, щоб зробити висновок у реальному часі, або дані можуть бути збережені для подальшого аналізу.

Коли трафік малий, WREN активно вводитиме трафік у мережу, зберігаючи порядок проходження потоків вимірювання. Після численних досліджень, знайдено, що WREN представляє схожі вимірювання в перенасичених і ненасичених середовищах.

У поточній реалізації WREN користувачі не примушуються тільки до захоплення трасування, які були ініційовані ними. Хоча будь-який користувач може стежити за трафіком додатків інших користувачів, вони обмежені в інформації, яка може бути отримана від трасування інших користувачів. Вони можуть лише отримати послідовність та підтвердження чисел, але не можуть отримати актуальні сегменти даних із пакетів.

Загалом WREN - це дуже корисна установка, яка використовує переваги і активного, і пасивного моніторингу. Хоча ця технологія знаходиться на ранньому етапі розвитку, WREN може надати адміністраторам корисні ресурси у моніторингу та аналізі їх мереж. Монітор Власного конфігурування мережі (SCNM) - інший інструментарій, який використовує технології як активного, так і пасивного моніторингу.

SCNM - це інструмент моніторингу, який використовує зв'язок пасивних та активних вимірювань для збору інформації на 3 рівні проникнення, маршрутизаторів, що виходять, та інших важливих точок моніторингу мережі. Середовище SCNM включає і апаратний, і програмний компонент.

Апаратний засіб встановлюється у критичних точках мережі. Воно відповідає за пасивний збір заголовків пакетів. Програмне забезпечення запускається на кінцевій точці мережі. Рис. 1.4, наведений нижче, показує програмний компонент SCNM середовища.

Програмне забезпечення відповідає за створення та надсилання активованих пакетів, які використовуються для старту моніторингу мережі. Користувачі будуть надсилати до мережі пакети активації, що містять деталі про пакети, які вони хочуть отримати для моніторингу та збору. Користувачі не потребують знання розташування SCNM-хоста, приймаючи за істину те, що всі хости відкриті для прослуховування пакетів. На основі інформації, яка існує в рамках активаційного пакета, фільтр міститься в потік збору даних, який також працює в кінцевій точці.

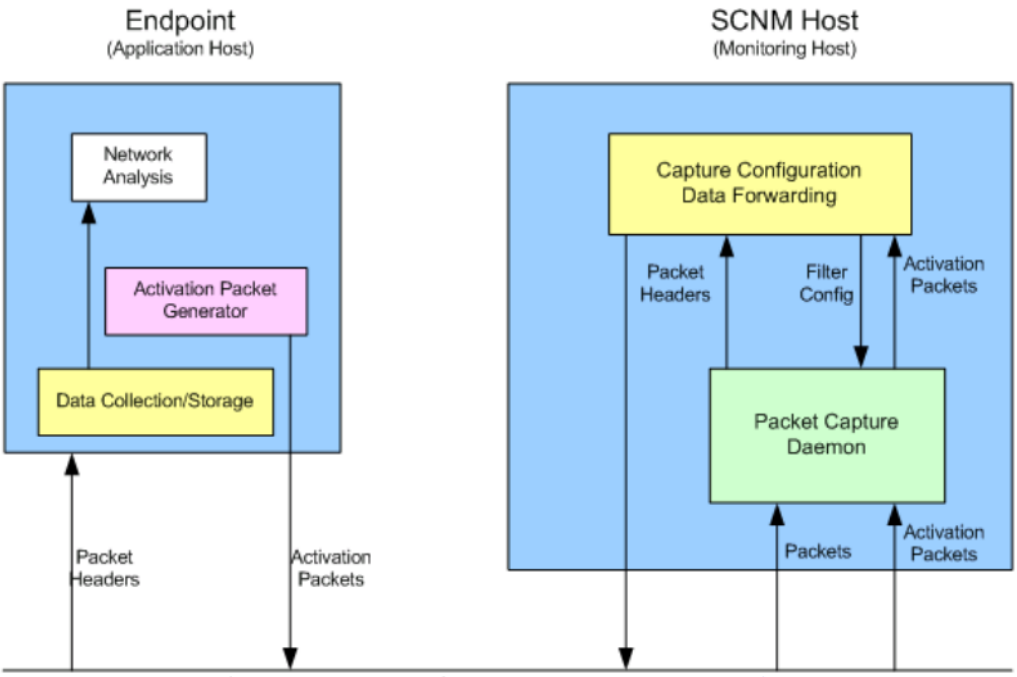

Рис. 1.4. Програмний компонент SCNM

Збираються заголовки пакетів мережного та транспортного рівня, які відповідають фільтру. Фільтр буде автоматично введений у тайм аут після точно заданого часу, якщо він отримує інші пакети програми. Служба вибірки пакетів, яка запускається на SCNM-хості,

Коли інструментами пасивного моніторингу визначається проблема, трафік може бути згенерування за допомогою інструментів активного моніторингу, дозволяючи збирати дані для більш детального вивчення проблеми. При розгортанні цього монітора в мережі на кожному маршрутизаторі протягом шляху ми можемо вивчати тільки секції мережі, які мають проблеми.

SCNM призначений для встановлення та використання, головним чином, адміністраторами. Тим не менш, звичайні користувачі можуть використовувати деяку частину цієї функціональності. Хоча звичайні користувачі здатні використовувати частини середовища SCNM моніторингу, їм дозволено дивитися лише власні дані.

Насамкінець скажемо, що SCNM — це ще один спосіб комбінованого моніторингу, який використовує і активний, і пасивний методи, щоб допомогти адміністраторам моніторити та аналізувати їх мережі.

Висновки за розділом

Оскільки більшість організацій постійно додають пристрої, програми та інші компоненти до своїх мереж, не кажучи вже про постійно зростаючі занепокоєння щодо безпеки, постійним для більшості мереж є те, що вони постійно розширюються. Вибираючи нові рішення для моніторингу мережі, важливо пам’ятати, що мережі майже напевно зростатимуть. Застосування інструментів мережевого моніторингу, які не залишають місця для зростання, означає, що команди майже напевно шукатимуть нові рішення протягом кількох років, постійно стикаючись із перешкодами. Вибирайте програмне забезпечення для моніторингу мережі, яке працює в межах можливостей, але переконайтеся, що ці рішення пропонують простір для зростання.

Підбираючи приватні інструменти для використання їх у моніторингу мережі, адміністратор повинен спочатку вирішити, чи хоче він використовувати системи, що добре зарекомендували себе, які вже використовувалися багато років, або нові. Якщо існуючі системи більш підходяще рішення, тоді NetFlow - найбільш корисний інструмент для використання, так як у зв'язки з цією утилітою можуть використовуватися пакети даних, що аналізуються, для подання даних у більш дружелюбному користувачеві вигляді.

Спостереження та аналіз мережі - життєво необхідні в роботі системного адміністратора. Адміністратори повинні намагатися утримувати свою мережу в порядку як для нерозрізненої продуктивності всередині компанії, так і для зв'язку з будь-якими існуючими публічними сервісами. Згідно з вищеописаною інформацією, кілька маршрутизаторо-орієнтованих технологій і не засновані на маршрутизаторах, придатні для допомоги мережевим адміністраторам у щоденному моніторингу та аналізі їх мереж.

РОЗДІЛ 2
МЕТОДИ МОНІТОРИНГУ АКТИВНОСТІ КОРИСТУВАЧІВ І СТАНУ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ

Сьогодні адміністратори можуть вибирати програмне забезпечення для моніторингу активності користувачів і стану апаратного забезпечення, яке призначене для будь-яких завдань: від простого відстеження часу роботи та простою до отримання інформації про користувачів і пристрої у мережі в режимі реального часу.

2.1. Аналіз роботи популярних інструментів моніторингу активності користувачів

Сніфінг пакетівце розмовний термін, який стосується мистецтва аналізу мережевого трафіку.

Існує багато потужних інструментів, які збирають активність мережевого трафіку, і більшість із них використовують pcap (системи, схожі на Unix) або libcap (системи Windows) для фактичного збору даних.

Програмне забезпечення аналізу пакетів розроблено, щоб допомогти проаналізувати ці зібрані пакети, оскільки навіть невелика кількість даних може призвести до тисяч пакетів, у яких може бути важко орієнтуватися.

Було проведено класифікацію аналізаторів пакетів відповідно до таких загальних міркувань: корисні функції, надійність, простота встановлення, інтеграція, використання, обсяг пропонованої допомоги та підтримки, наскільки добре оновлюється та підтримується програмне забезпечення та наскільки авторитетними є розробники в промисловість.

Ось наш список найкращих сніферів пакетів:

Інструмент глибокої перевірки та аналізу пакетів SolarWinds Дає детальну інформацію про те, що спричиняє повільність мережі, і використовує глибоку перевірку пакетів, щоб дозволити вам вирішити основні причини. Ви можете

ідентифікувати трафік за програмою, категорією та рівнем ризику, щоб усунути та відфільтрувати проблемний трафік. Завдяки чудовому інтерфейсу користувача, це чудове програмне забезпечення для аналізу пакетів ідеально підходить для аналізу мережі. Завантажити а30-денна безкоштовна пробна версія.

ManageEngine NetFlow Analyzer Інструмент аналізу трафіку, який працює з NetFlow, J-Flow, sFlow Netstream, IPFIX і AppFlow

Інструмент захоплення пакетів PaesslerСніффер пакетів, датчик NetFlow, датчик sFlow і датчик J-Flow, вбудовані в Paessler PRTG.

Omnipeek Network Protocol Analyzer Мережевий монітор, який можна розширити для захоплення пакетів.

tcpdumpОсновний безкоштовний інструмент захоплення пакетів, який потрібен кожному мережевому менеджеру.

WindumpБезкоштовний клон tcpdump, написаний для систем Windows.

WiresharkДобре відомий безкоштовний інструмент захоплення пакетів і аналізу даних.

tsharkЛегка відповідь для тих, хто хоче функціональність Wireshark, але тонкий профіль tcpdump.

NetworkMinerАналізатор мережі на базі Windows із простою безкоштовною версією.

СкрипальІнструмент захоплення пакетів, який зосереджується на трафіку HTTP.

КапсаБезкоштовний інструмент захоплення пакетів, написаний для Windows, можна оновити за плату, щоб додати аналітичні функції.

Переваги перехоплення пакетів

Сніффер пакетів є корисним інструментом, який дозволяє реалізувати політику пропускної здатності мережі вашої компанії. Основні переваги полягають у тому, що вони:

Визначте перевантажені посилання

Визначте програми, які генерують найбільше трафіку

Збирайте дані для прогнозного аналізу

Виділіть піки та спади мережевого попиту

Дії, які ви вживаєте, залежать від вашого доступного бюджету. Якщо у вас є ресурси для розширення пропускної здатності мережі, сніффер пакетів дозволить вам ефективніше орієнтуватися на нові ресурси. Якщо у вас немає бюджету, аналіз пакетів допоможе сформувати трафік за допомогою пріоритезації трафіку програм, зміни розміру підмереж, перепланування подій інтенсивного трафіку, обмеження пропускної здатності для певних програм або заміни програм більш ефективними альтернативами.

Безладний режим

Важливо розуміти, як працює мережева карта на вашому комп'ютері, коли ви встановлюєте програмне забезпечення аналізу пакетів. Інтерфейс від комп'ютера до мережі називається «контролером мережевого інтерфейсу» або NIC. Ваш мережевий адаптер отримуватиме лише інтернет-трафік, який адресовано на його MAC-адресу.

Щоб захопити загальний трафік, вам потрібно перевести мережевий адаптер у «безладний режим». Це знімає обмеження на прослуховування на мережевій карті. У безладному режимі ваш мережевий адаптер перейматиме весь мережевий трафік. Більшість аналізаторів пакетів мають утиліту в інтерфейсі користувача, яка керує перемиканням режимів за вас.

Типи мережевого трафіку

Аналіз мережевого трафіку вимагає розуміння того, як працює мережа. Немає інструменту, який магічним чином усуне вимогу до аналітика розуміти основи роботи в мережі, наприклад, тристороннє рукостискання TCP, яке використовується для встановлення з'єднання між двома пристроями. Аналітики також повинні мати певне уявлення про типи мережевого трафіку, які існують у нормально функціонуючій мережі, наприклад трафік ARP і DHCP. Ці знання є важливими, тому що інструменти аналізу просто покажуть вам, що ви просите – ви самі визначаєте, що просити. Якщо ви не впевнені, як зазвичай виглядає ваша

мережа, може бути важко переконатися, що ви шукаєте правильну річ у масі пакетів, які ви зібрали.

Інструменти підприємства

Давайте почнемо з самого верху, а потім перейдемо вниз до найдрібніших основ. Якщо ви маєте справу з мережею корпоративного рівня, вам знадобиться велика зброя. Хоча майже все використовує tcpdump у своїй основі (докладніше про це пізніше), інструменти корпоративного рівня можуть надавати інші аналітичні функції, такі як кореляція трафіку з багатьох серверів, надання інтелектуальних інструментів запитів для виявлення проблем, попередження про виняткові випадки та створення гарних графіків, які вимоги керівництва.

Інструменти корпоративного рівня зазвичай зосереджені на потоці мережевого трафіку, а не на оцінці вмісту пакетів. Під цим я маю на увазі, що більшість системних адміністраторів на підприємстві зосереджені на підтримці мережі без перешкод у продуктивності. Коли виникають вузькі місця, метою зазвичай є визначення проблеми в мережі чи в програмі в мережі. З іншого боку медалі, ці інструменти корпоративного рівня зазвичай здатні бачити стільки трафіку, що вони можуть допомогти передбачити, коли сегмент мережі насититься, що є критичним елементом управління потужністю.

Хакерські інструменти

Сніфери пакетів також використовуються хакерами. Майте на увазі, що ці інструменти можна використовувати для атаки на вашу мережу, а також для вирішення проблем. Сніфери пакетів можна використовувати як перехоплювачі, щоб допомогти викрасти дані під час передавання, а також вони можуть сприяти атакам «людина посередині», які змінюють дані під час передавання та перенаправляють трафік, щоб ошукати користувача в мережі. Інвестувати ввиявлення вторгненьсистеми для захисту вашої мережі від цих форм несанкціонованого доступу

Як працюють пакетні аналізатори та мережеві аналізатори?

Ключовою особливістю сніфера пакетів є те, що він копіює дані під час переміщення по мережі та робить їх доступними для перегляду. Пристрій для аналізу просто копіює всі дані, які він бачить у мережі. Якщо реалізовано на комутаторі, налаштування пристрою дозволяють надсилати прохідний пакет на другий порт, а також на призначений пункт призначення, таким чином дублюючи трафік. Зазвичай пакети даних, отримані з мережі, копіюються у файл. Деякі інструменти також відображатимуть ці дані на інформаційній панелі. Однак сніфери пакетів можуть збирати багато даних, зокрема закодовану інформацію адміністратора. Вам потрібно буде знайти інструмент аналізу, який може допомогти вам розіменувати інформацію про шлях пакетів у витягу та іншу інформацію, таку як релевантність номерів портів, між якими переміщуються пакети.

Простий аналізатор пакетів скопіює всі пакети, що переміщуються в мережі. Це може бути проблемою. У t випадках вміст пакета не потрібен для аналізу продуктивності мережі. Якщо ви хочете відстежувати використання мережі протягом 24 годин або протягом кількох днів, то збереження кожного пакета займе дуже великий обсяг дискового простору — навіть якщо ви берете лише заголовки пакетів. У цих сценаріях доцільно робити вибірку пакетів, що означає копіювання кожного 10-го або 20-го пакета, а не кожного окремого.

Найкращі сніфери пакетів

Інструменти, які я перерахував у цій статті, можуть використовувати досвідчені мережеві адміністратори, які вже знають, що вони шукають, але не впевнені, які інструменти найкращі. Вони також можуть використовуватися більш молодшими системними адміністраторами, щоб отримати досвід того, як виглядають сучасні мережі під час повсякденних операцій, що допоможе виявити проблеми з мережею пізніше.

Наша методологія вибору сніфера пакетів

Ми розглянули ринок сніферів пакетів і проаналізували варіанти на основі таких критеріїв:

Можливість читати заголовки пакетів і ідентифікувати адреси джерела та призначення

Аналізатор протоколів, який може класифікувати трафік за програмою

Опція захоплення всіх пакетів або вибірки кожного n-го пакета

Можливість спілкуватися з комутаторами та маршрутизаторами через NetFlow та інші мови протоколу аналізу трафіку

Інструменти планування ємності та формування трафіку

Безкоштовний пробний період або гарантія повернення грошей для оцінки без ризику

Безкоштовний інструмент, який варто встановити, або платний інструмент, який вартий своєї ціни

Майже всі ці інструменти збираються однаково; це аналіз, який їх відрізняє.

1. Інструмент SolarWinds Deep Packet Inspection and Analysis.

SolarWindsце комплексний набір інструментів управління IT. Інструмент, який більше стосується цієї статті, цеІнструмент глибокої перевірки та аналізу пакетів.

Ключові риси:

Класифікує мережевий трафік

Аналізатор стека протоколу

Живий моніторинг

Підтримує формування трафіку

30-денна безкоштовна пробна версія

Збір даних про активність мережевого трафіку є відносно простим. Використовуючи такі інструменти, як WireShark, базовий аналіз рівня також не завадить. Але не всі ситуації є такими чіткими. У жвавій мережі може бути важко визначити навіть деякі фундаментальні речі, такі як:

Яка програма в локальній мережі створює цей трафік?

Якщо програма відома (скажімо, веб-браузер), де люди проводять більшу частину свого часу?

Які з’єднання займають найдовше та забивають мережу?

Більшість мережевих пристроїв просто використовують метадані кожного пакета, щоб гарантувати, що пакет потрапляє туди, куди він прямує. Вміст пакета невідомий мережевому пристрою. Глибока перевірка пакетів відрізняється; це означає, що фактичний вміст пакета перевіряється, щоб дізнатися про нього більше.

У такий спосіб можна виявити важливу мережеву інформацію, яку неможливо отримати з метаданих. Інструменти, подібні до тих, які надає SolarWinds, можуть надати більш значущі дані, ніж просто рух транспорту.

Інші методи керування мережами великого обсягу включають NetFlow і sFlow. Кожен має свої сильні та слабкі сторони, про які ви можете прочитати більшеТехніки NetFlow і sFlow тут.

Загалом аналіз мережі — це складна тема, яка складається наполовину з досвіду й наполовину з навчання. Можна навчити когось розуміти кожну деталь мережевих пакетів. Тим не менш, якщо ця особа також не має знань про цільову мережу та певного досвіду виявлення аномалій, вона не зайде дуже далеко.

Плюси:

Пропонує поєднання DPI і функцій аналізу, що робить це чудовим універсальним варіантом для детального усунення несправностей і перевірки безпеки

Створений для підприємства, пакет пропонує надійний збір даних і різноманітні варіанти візуалізації та пошуку зібраних даних

Підтримує збір NetFlow і sFlow, надаючи йому більше гнучкості для мереж з великим об’ємом

Кольорове кодування та інші візуальні підказки допомагають адміністраторам швидко знаходити проблеми перед поглибленим аналізом

Мінуси:

Дуже просунутий інструмент, розроблений для мережевих професіоналів, не ідеальний для домашніх користувачів або любителів

2.2. Аналіз роботи популярних систем моніторингу стану обладнання

Мережі складні. Додавання віртуальних середовищ покращує ефективність, але також ускладнює завдання адміністрування мережі. Ми покажемо вам, як спростити роботу за допомогою найкращих інструментів моніторингу віртуальних машин.

Віртуальне середовище пропонує спосіб розширити використання локальних ресурсів. Це поширене рішення в більшості бізнес-мереж завдяки простоті використання VMWare та програмного забезпечення віртуальної машини (VM) Hyper-V від Microsoft. Однак, коли справа доходить до моніторингу ресурсів, додатковий рівень трафіку, який неминучий при налаштуваннях віртуальної машини, може ускладнити відображення ресурсів. Коли ваш бізнес розвивається, відстеження цього рішення віртуальної машини може швидко вийти з-під контролю.

Моніторинг віртуальної машини допомагає вам бути в курсі проблем із ресурсами під час розподілу ресурсів від однієї віртуальної машини до іншої. Проблеми з мережевим трафіком неминучі, коли віддалені ресурси стають доступними миттєво та локально. Вам потрібно відстежувати попит і адаптувати ресурси, щоб користувачі мережі були задоволені. Планування потужностей є ключовою частиною керування віртуальною машиною, а моніторинг використання допомагає вам випереджати попит і скорочує час відповіді.

Ось наш список найкращих інструментів моніторингу ВМ:

Менеджер віртуалізації SolarWindsВИБІР РЕДАКТОРАЦей локальний пакет моніторингу здатний відстежувати продуктивність хмарних віртуальних серверів, а також гіпервізорів, розташованих у мережі. Відстежуйте діяльність Amazon EC2 і Azure, а також продуктивність віртуалізацій Hyper-V і VMWare.

Цей пакет працює на Windows Server, і ви можете отримати його на30-денна безкоштовна пробна версія.

eG Enterprise VM Monitoring. Система моніторингу для віртуалізацій VMware vSphere, Citrix XenServer, Microsoft Hyper-V, Oracle VM Server, Red Hat Enterprise Virtualization, AIX LPAR, Solaris Container. Доступ а30-денна безкоштовна пробна версія.

AppOptics APM. Хмарний монітор продуктивності додатків із доданим моніторингом інфраструктури, який є чудовим монітором віртуалізації.

Моніторинг віртуалізації Site24x7. Хмарний сервіс, який дає змогу відстежувати продуктивність віртуалізації Hyper-V і VMWare, а також впровадження AWS і хмарних віртуальних машин Azure.

Моніторинг інфраструктури Sematext. Ця хмарна платформа здатна відстежувати продуктивність JVM, контейнерів та інших служб, а також фізичних серверів.

ManageEngine OpManager. Пакет інструментів моніторингу для мереж і серверів, який включає служби відстеження для гіпервізорів VMWare, Hyper-V, Nutanix і Citrix. Доступно для Windows Server і Linux.

SentryOne SQL Sentry. Цей монітор SQL Server також відстежує продуктивність ваших віртуальних машин, якщо база даних працює поверх гіпервізора. Доступно для Windows Server або як служба Azure.

Мережевий монітор Paessler PRTG. Розширений пакет моніторингу мережі, серверів і додатків, який включає спеціалізовані функції моніторингу для Citrix Xen, Microsoft Hyper-V, VMWare, Parallels Virtuozzo Containers і Amazon EC2.

LogicMonitorХмарна служба моніторингу мережі, яка включає покриття для VMware vCenter, ESXi, Microsoft Hyper-V і Citrix XenServer.

Veeam OneІнструмент моніторингу ресурсів, який відстежує все обладнання, програмне забезпечення та служби, які сприяють віртуалізації VMWare vSphere і Hyper-V.

Квест ПротитуманкаМонітор віртуалізації для Citrix Xen, VMWare та Hyper-V, який працює на Windows, Linux і Solaris.

Менеджер віртуалізації AptareЦей інструмент відстежує VMWare, Amazon Web Services, Microsoft Azure і OpenStack.

Надбудова моніторингу віртуалізації Progress WhatsUp GoldДоповнення до основної системи моніторингу мережі WhatsUp Gold.

Вбудований хост-клієнт ESXiБезкоштовний клієнтський монітор ESXi від VMWare.

ТурбономічнийЦей інструмент відстежує локальну реалізацію VMware, Hyper-V і XenServer і зовнішні хмарні ресурси.

5Дев'ять МенеджерЦей інструмент зосереджений на моніторингу віртуальних машин Microsoft, створених за допомогою Azure та Hyper-V.

Інтеграція хмарних ресурсів є стандартною функцією сучасних бізнес-систем. Традиційні методи віртуалізації лягли в основу зв’язку між локальними терміналами та зовнішніми додатками та файловими серверами. Отже, отримання інструменту моніторингу віртуальної машини, який розпізнає ваші сервери, незалежно від того, знаходяться вони на місці чи в хмарі, є важливою вимогою для будь-якого системного інструменту.

Найкращі інструменти та програмне забезпечення для моніторингу віртуальних машин

Ми зібрали аналіз найкращих рішень для моніторингу віртуальних машин і склали список утиліт, які слід враховувати, купуючи програмне забезпечення.

Наша методологія вибору програмного забезпечення для моніторингу віртуальних машин

Ми розглянули ринок програмного забезпечення для моніторингу віртуальних машин і проаналізували варіанти на основі таких критеріїв:

Система, яка може аналізувати використання фізичних ресурсів сервера, а також діяльність віртуального середовища

Живий монітор із графічною інтерпретацією даних для миттєвого розуміння продуктивності

Інструменти аналізу для оцінки продуктивності на основі збереженої статистики

Порогові значення продуктивності, які викликають попередження, коли продуктивність падає або ресурси вичерпуються

Підтримка переналаштування віртуальних машин на сервери та коригування розподілу ресурсів

Безкоштовний пробний період для безкоштовної оцінки або безкоштовний інструмент

Система, яка економить час і гроші на моніторинг віртуальної машини, окупаючи вартість її покупки

Ці інструменти моніторингу віртуальних машин є лідерами галузі та заощадять ваш час під час відстеження середовища вашого віртуального пристрою. У наступному розділі наведено інформацію про кожен із цих інструментів моніторингу віртуальної машини.

1. Менеджер віртуалізації SolarWinds.

Якщо ваша система віртуальної машини трохи складніша, ніж один сервер, вам, ймовірно, доведеться перейти доМенеджер віртуалізації SolarWinds. Цей інструмент не тільки охоплює більше ніж один сервер, він пропонує набагато більш глибокий моніторинг умов у середовищі віртуального пристрою. З цим пакетом ви не обмежені локальними серверами віртуальних машин, оскільки він також може інтегрувати віртуальні сервери Amazon EC2 і Azure у середовище моніторингу.

Ключові риси:

Відстежує хмарні та локальні системи

Hyper-V і VMWare

Amazon EC2 і Azure

Ступінь сповіщень

Управління розростанням

Інформаційна панель програмного забезпечення Virtualization Manager показує детальні показники продуктивності та містить елементи візуалізації

даних, такі як циферблати та лінійні графіки продуктивності. Система відображатиме середовища VMWare та Hyper-V, зберігаючи окремі списки показників для кожного типу ОС, якщо у вашій мережі працює суміш обох систем. Сповіщення позначено кольором: жовтий колір позначає попередження, а червоний — критичні умови. На окремій панелі приладової панелі готовий список потенційних ситуацій тривоги. Ця утиліта стежить за умовами обслуговування, які досягли точки погіршення продуктивності та наближаються до стану попередження.

Основні оновлення, які цей інструмент має над VM Monitor, включають допомогу в плануванні потужності та «керування розповзанням». Поєднання цих двох інструментів дає прогнозні рекомендації. Завдяки цій функції планування ви краще озброєні, щоб запобігти надлишковій потужності в одній частині середовища та перерозподілити недостатньо використані ресурси в інших областях системи.

Модуль моделювання дозволяє перевірити наслідки додавання нових користувачів або програм до мережі. Це моделює використання ЦП, доступність пам’яті, ємність пам’яті та вимоги до мережі для певного сценарію. Функція розповсюдження показує, де віртуальні машини неактивні, і дозволяє вимкнути їх і перерозподілити призначені їм ресурси.

Це зручна функція, яка допомагає отримати максимальну віддачу від вашого бюджету та запобігає сплутанню мертвих процесів із попитом на ресурси. На іншому кінці спектру монітор розповсюдження показує, які віртуальні машини поглинають усі ваші ресурси. Це дозволяє обмежити виділення для цих вузлів, а також забезпечує відправну точку для розслідування неефективного програмного забезпечення або зловживання системою.

Інформаційна панель містить стек додатків, який просто показує рівні ресурсів і умови стану, наявні на кожному з них. Стек представлено рядками умовних символів попереджень для груп користувачів, програм, баз даних, транзакцій, серверів і хостів. Це дає змогу швидко побачити, де проблеми з

пропускною здатністю впливають на продуктивність програми та якість обслуговування.

Функція Perf Stack менеджера віртуалізації — це утиліта, доступна в ряді інструментів керування інфраструктурою SolarWinds. Отже, якщо ви вже користувалися іншим продуктом SolarWinds, можливо, ви знайомі з PerfStack. Це графічний еквівалент стеку додатків. Він показує поточні дані на лінійному графіку для кожного ресурсу у віртуальному середовищі. Ви вибираєте кожен із графіків, які вас цікавлять, і перетягуєте їх на дошку. Це дає вам змогу створити власний стек, який показує, як піки та спади попиту на один ресурс, наприклад базу даних чи мережу, впливають на продуктивність інших ресурсів, наприклад час відповіді програми або використання ЦП.

Програмне забезпечення Virtualization Manager містить багато інформації, а перегляди підсумків стають у нагоді, щоб уникнути перевантаження даними. Незабаром ви звикнете до формату презентації панелі моніторингу віртуальної машини та створите власні методи роботи. Завдяки цьому ви зможете перемикатися між зведеннями та деталями та переходити до інструментів планування, щоб віртуальне середовище працювало.

Плюси:

Чудова інформаційна панель, яку можна масштабувати для комфортного моніторингу кількох хостів і віртуальних машин у корпоративному середовищі

Підтримує моніторинг окремих ресурсів ВМ

Може інтегруватися з хмарними продуктами, такими як Azure і Amazon EC2

Містить рекомендації щодо покращення разом із кольоровими показниками здоров’я

Пропонує можливості планування потужностей і докладних звітів

Мінуси:

Розроблений спеціально для підприємств, домашні користувачі та малі підприємства, ймовірно, віддадуть перевагу SolarWinds VM Monitor

SolarWinds Virtualization Manager коштує недешево — ціни починаються від 2995 доларів США. Однак ви можетевипробувати систему протягом 30 днів безкоштовно.

ВИБІР РЕДАКТОРА

Менеджер віртуалізації SolarWindsє нашим найкращим вибором для інструменту моніторингу віртуальних машин, оскільки ця система пропонує глибоке занурення в локальні гіпервізори та хмарні віртуальні служби. SolarWinds включає моніторинг віртуалізації за допомогою Network Performance Monitor, але компаніям, які потребують детального керування віртуалізацією, слід вибрати цей пакет. Використовуйте цю систему для відстеження керування пам’яттю та відображення віртуальної машини для розміщення, а також використання ресурсів і доступність допоміжних фізичних серверів.

2. eG Enterprise VM Monitoring.

TheeG Enterprisecистема моніторингу від eG Innovations охоплює VMware vSphere, Citrix XenServer, Microsoft Hyper-V, Oracle VM Server, Red Hat Enterprise Virtualization, AIX LPAR, віртуалізацію Solaris Container та їхню допоміжну інфраструктуру. Головною перевагою моніторингу віртуальних машин eG Enterprise є те, що перевірка використання пам’яті сервера та ЦП не дає повної картини працездатності віртуалізації. Вам також потрібно бачити проблеми, які виникають у мережі, на сервері зберігання, у базі даних або в програмному забезпеченні платформи віртуалізації.

Ключові риси:

Віртуалізації Hyper-V, VMWare, Citrix, Oracle і Red Hat

Моніторинг контейнерів

Виявляє та відображає віртуалізацію

Стежить за наявністю ресурсу

Інтерфейс системи є браузерним. Він містить графічні дисплеї, списки поточних даних і попереджень, а також розділи для допомоги в плануванні потужності. Зв’язки між ресурсами відображаються на інформаційній панелі під час інсталяції системи. eG Enterprise особливо сильний у визначенні

взаємозалежності ресурсів. Приклади цих зв’язків включають взаємодію додатків і платформи віртуальної машини, а також основні потреби фізичної інфраструктури програмного забезпечення віртуальної машини. Ця базова лінія інформує базу правил eG Enterprise про умови тривоги, які погіршують продуктивність середовища.

Ви не тільки отримуватимете сповіщення, наприклад, що час відповіді певної віртуальної машини повільний; ви отримаєте сповіщення, якщо база даних перевантажена та чи це спричиняє низьку продуктивність конкретної віртуальної машини.

Здатність визначати першопричину проблем із продуктивністю на найнижчих рівнях надає eG Enterprise всю силу. Це означає, що вам не потрібно витрачати час на зворотне зв’язування шарів стека, щоб зрозуміти, що йде не так. Середовище багатьох постачальників є поширеним явищем, і eG Enterprise уніфікує моніторинг стека забезпечення для широкого діапазону можливих комбінацій систем віртуалізації. Отже, ви побачите кожну з платформ окремо, але базові ресурси, які підтримують кілька середовищ, відстежуються на загальний попит, а не на основі кожної платформи.

Перевага підходу з уніфікованим стеком полягає в тому, що він дає змогу бачити, яка віртуальна машина використовує ресурси, і ускладнює роботу решти мережі. Інформаційна панель містить чудову кольорову стекову діаграму, яка показує співіснування платформ на підтримуваних рівнях. EG називає це своїм моніторингом входу-виходу. Зовнішній вигляд показує всі віртуальні машини в групах, розмір яких пропорційно використанню ресурсів кожної служби. У поданні зсередини показано кожен шар стеку з використанням кожної віртуальної машини на цьому рівні поруч, знову ж таки, пропорційно.

Ще одна приємна функція візуалізації eG Enterprise — це діаграма в стилі робочого процесу, яка відстежує всі ресурси, необхідні віртуальній машині, і, у свою чергу, ресурси, необхідні для кожної функції підтримки. Кожен елемент ланцюжка показує свій статус. Отже, якщо один із цих вузлів показує

сповіщення, ви точно знаєте, куди звернутися, щоб повернути цю віртуальну машину в належний стан.

Плюси:

Може контролювати широкий діапазон віртуальних хост-середовищ, що робить його справді придатним для великих підприємств або MSP

Зміна на основі порогового значення може сповіщати, коли віртуальні машини виходять з мережі або стають повільними через проблеми, пов’язані з ресурсами

Пропонує аналіз першопричин, щоб допомогти технічним спеціалістам швидше вирішувати проблеми, що призводить до збільшення часу безвідмовної роботи

Мінуси:

Немає безкоштовної версії

Інтерфейс можна оновити, щоб він став більш сучасним

Конфігурація може бути заплутаною та важкою для вивчення

Ринок моніторингу віртуальних машин переповнений кількома дуже потужними інструментами, які надають величезні компанії програмного забезпечення. Пакет eG Enterprise має деякі зручні функції, яких бракує багатьом його конкурентам. Великою перевагою послуги моніторингу eG Enterprise є те, що вона оплачується за фізичний сервер, тому ви можете контролювати скільки завгодно віртуалізацій, не турбуючись про вартість. Безкоштовної версії eG Enterprise немає, але ви можете отримати доступ до а30-денна безкоштовна пробна версіящоб оцінити ваші вимоги до мережі.

3. AppOptics APM.

AppOptics APMце монітор продуктивності програми. Таким чином, він здатний відстежувати віртуалізацію, яка формується програмами. Послуга APM також включає моніторинг інфраструктури, оскільки в багатьох випадках погіршення продуктивності програми спричинене певною основною допоміжною службою, а не самою програмою.

Ключові риси:

Hyper-V, Azure і Docker

Моніторинг використання ресурсів

Відстеження залежностей програми

AppOptics APM спеціально має можливості для моніторингу операцій віртуалізації Hyper-V, Azure та Docker. У кожному разі служба відстежує продуктивність сервера, на якому розміщено реалізацію віртуалізації, перевіряючи доступність ЦП і пам’яті та гарантуючи наявність достатнього дискового простору для роботи віртуальної машини.

Система AppOptics базується на хмарі, і для неї потрібно, щоб програмне забезпечення агента було інстальовано в системі, яку потрібно контролювати. Інформаційна панель і вся обчислювальна потужність системи розміщені в хмарі та включені у вартість програмного забезпечення. Користувачі отримують доступ до консолі AppOptics через будь-який стандартний веб-браузер.

Плюси:

Пропонує чудові візуалізації, що відображають реальні та історичні показники здоров’я та споживання ресурсів

Легко масштабується, побудований як хмарний сервіс

Відстежує всі основні ресурси, такі як ЦП, пам’ять і використання мережі

Може контролювати платформи Docker, Azure і Hyper-V, пропонуючи більшу гнучкість, ніж конкуруючі варіанти

Мінуси:

Хотілося б побачити довший випробувальний період

Плата за AppOptics стягується за передплатою за рік. Немає обмежень щодо кількості технічних спеціалістів, яким компанія-клієнт може надати доступ до системи AppOptics, а також немає обмежень на моніторинг або обробку послуги. Ви можете отримати14-денна безкоштовна пробна версіяAppOptics, щоб перевірити систему.

4. Моніторинг віртуалізації Site24x7.

Моніторинг віртуалізації Site24x7пропонується онлайн за моделлю програмного забезпечення як послуги. Немає локальної версії. Інструмент є продуктом Zoho Group, яка також володіє ManageEngine.

Ключові риси:

Hyper-V, VMWare, AWS, Azure і Nutanix

Платформа SaaS

Docker і Kubernetes

Ця система моніторингу пропонується в кількох спеціалізованих випусках, які призначені для звичайних компаній, MSP та веб-підприємств. Його компетенція охоплює сервери, мережі та програми – комбінація, яка ідеально підходить для моніторингу віртуалізації. Система здатна відстежувати віртуалізацію Microsoft Hyper-V і VMWare на місці, а також хмарні сервери на базі AWS і Microsoft Azure.

Окрім віртуалізації, пакет моніторингу Site24x7 охоплює нагляд за контейнерами, керованими Docker або Kubernetes. Він також може контролювати систему гіперконвергентної інфраструктури Nutanix.

Доступ до консолі сервісу здійснюється через браузер, і ви також можете встановити програму на мобільних зануреннях, щоб отримати доступ. Той факт, що система заснована на віддалених серверах, звільняє її можливості, щоб вона могла контролювати мережі в будь-якій точці світу. Інструменти служби включають моніторинг стану в реальному часі та аналіз продуктивності на основі історичних даних.

Система починає свою роботу з виявлення та реєстрації всієї вашої інфраструктури. Він виявить ваші віртуалізації та відобразить усі ресурси, що вносять внесок. Після завершення початкової фази виявлення система продовжує перевіряти топологію вашої мережі та віртуалізації, автоматично коригуючи свої записи, якщо ви змінюєте будь-який аспект своєї реалізації.

Екрани візуалізації представлені дуже чітко. Простота кожного монітора для віртуальної машини є корисною, оскільки вона дає чудову видимість того, що інколи може здатися надзвичайно складною технологією.

Перегляд системи розгортається на кількох екранах, і ви можете детально переглянути зіставлення віртуальних машин із хостами, продуктивність кожного сервера та активність у мережі, яка забезпечує ваші віртуалізації. Статуси позначено кольором для миттєвого виявлення проблеми, а сповіщення про ресурси надають вам постійне оновлення стану кожного елемента, який сприяє реалізації віртуалізації.

Ви можете налаштувати рівні сповіщень і запобігти будь-якій потенційній загрозі середовищу віртуальної машини до того, як виникне дефіцит ресурсів. Звіти в пакеті містять звіти про керування SLA та журнали використання ресурсів.

Функції аналізу допомагають переналаштувати віртуальні машини на хости, якщо один сервер виглядає перевантаженим. Ви можете використовувати звіти в пакеті, щоб продемонструвати зацікавленим сторонам вимоги до ресурсів.

Це чудовий інструмент для групового моніторингу віртуальних машин. Плата стягується на основі передплати, і ви платите за кількість серверів, які вам потрібні для моніторингу, а не за кількість технічних спеціалістів, яким ви хочете мати доступ до монітора. Цінові плани для моніторингу інфраструктури дуже масштабовані. Ви берете початковий план, який охоплює до 10 серверів і додаткову ємність, якщо вам потрібно спостерігати за більшою кількістю серверів.

Плюси:

Високомасштабований продукт SaaS

Платформа дозволяє легко переходити до інших областей моніторингу, таких як моніторинг мережі, програми або реального користувача

Простий і зручний інтерфейс

Підтримує безкоштовну версію, чудово підходить для домашніх лабораторій і тестування

Мінуси:

Site24x7 дуже детальний і може знадобитися час, щоб повністю вивчити всі параметри та функції

Можливості моніторингу віртуалізації пропонуються як частина пакета Site24x7 Infrastructure. Це дуже комплексна система, яка підходить для великих корпорацій. Однак невеликі підприємства також можуть використовувати його. Більше того, Site24x7 можна використовувати безкоштовно, якщо вам потрібно лише контролювати до п’яти серверів. Таким чином, Site24x7 є хорошим вибором для бізнесу будь-якого розміру. Ви можете отримати30-денна безкоштовна пробна версіясистеми. Після закінчення пробного періоду ваша підписка автоматично перейде на безкоштовну версію, якщо ви вирішите не платити. Цю послугу можна будь-коли оновити до ширшої платної послуги.

Моніторинг віртуалізації Site24x7Почніть 30-денну БЕЗКОШТОВНУ пробну версію

5. Моніторинг інфраструктури сематексту.

Моніторинг інфраструктури Sematextце хмарний монітор серверів і служб, який шукає інформацію про продуктивність системи в журналах. Цей інструмент відстежує потужність і використання ресурсів сервера, а також діяльність віртуальної машини Java і контейнера.

Ключові риси:

Моніторинг JVM

Docker і Kubernetes

Переглядає всередині та під віртуальними машинами

Оскільки Sematext базується на хмарі, він не обмежується моніторингом серверів лише на одному сайті. Ви можете включити будь-який сервер будь-де в програму моніторингу. Це включає хмарні сервіси. Щоб підключити сервер до системи моніторингу Sematext, необхідно встановити на нього програму-агент. Після реєстрації сервера всі служби, що працюють на ньому, відстежуються. Це включає екземпляри JVM і контейнери.

Частина моніторингу контейнерів Sematext Infrastructure Monitoring зосереджена на Docker і Kubernetes. Він може відстежувати діяльність кожного

контейнера та реєструвати використання його ресурсів. Така продуктивність може бути пов’язана з використанням ресурсів допоміжного сервера.

Моніторинг JVM стежить за діяльністю Java та контролює її ресурси. Це включає в себе дії зі збирання сміття та використання пам'яті. Показники пам’яті, які відстежуються в службі моніторингу інфраструктури Sematext, включають розмір купи та використання для кожного пулу пам’яті. Ви також можете використовувати систему Sematext для налаштування розподілу пам’яті, тому це не просто служба моніторингу. Система підраховує потоки JVM і записує взаємодію з файлами.

Служба моніторингу інфраструктури Sematext надає огляди діяльності сервера та служби, які консолідують дані про продуктивність. Отже, ви починаєте з загального перегляду продуктивності сервера або JVM, а потім переходите до окремих екземплярів. Система надає дані про ефективність у реальному часі, а також дозволяє фільтрувати та сортувати звіти про ефективність для аналізу. Ви також можете викликати історичні дані для аналізу діяльності.

Інші функції платформи моніторингу інфраструктури Sematext включають відстеження транзакцій для API, які відстежують через Інтернет хости служб, які лежать за цими інтерфейсами API. Він також може контролювати бази даних.

Плюси:

Моніторинг використання пам'яті JVM і активності керування

Агреговані перегляди та фокус на окремих примірниках

Кореляція між діяльністю ресурсів JVM і фізичного сервера

Моніторинг активності контейнера Docker

Механізми налаштування ресурсів Docker

Мінуси:

У цьому пакеті немає моніторингу Hyper-V або VMWare

Ви можете отримати Sematext Infrastructure Monitoring безкоштовно, отримавши доступ до пакета Basic, який обмежується моніторингом трьох серверів. Є два платних плани: Standard і Pro. Кожен платний план є

тарифікованою послугою з оплатою за хост за годину. Ви можете отримати а14-денна безкоштовна пробна версіямоніторингу інфраструктури сематексту.

Моніторинг інфраструктури SematextПочніть 14-денну БЕЗКОШТОВНУ пробну версію

6. ManageEngine OpManager.

ManageEngine OpManagerвідстежує мережі та сервери, що є чудовою комбінацією послуг, якщо ви хочете відстежувати віртуалізацію. Система здатна відстежувати віртуалізації, створені за допомогою:

VMWare vSphere і ESXi

Microsoft Hyper-V

Citrix XenServer

Nutanix HCI

Послуга включає системи моніторингу для спостереження за продуктивністю операційних систем, мережевих інтерфейсів і ресурсів сервера, таких як доступність ЦП, пам'ять і дисковий простір. Таким чином, він має всю допоміжну інфраструктуру для гіпервізорів.

Ключові риси:

Моніторинг мережі та серверів

VMWare, Hyper-V, Citrix і Nutanix

Сповіщення про проблеми з продуктивністю

Система OpManager містить службу виявлення системи. Це поширюється на всю мережу, ідентифікуючи всі мережеві пристрої та кінцеві точки та реєструючи їх у списку. Сервіс виконує те саме завдання для віртуальної інфраструктури.

Система відстеження віртуальної машини в OpManager визначає всі ваші віртуальні сервери та виявляє всі зв’язки через віртуальні комутатори з залежними віртуальними машинами. Служби виявлення як фізичної, так і віртуальної мережі є постійними, тому якщо ви внесете будь-які зміни у свою інфраструктуру, OpManager миттєво виявить їх і налаштує свої системні карти.

Постійний моніторинг віртуальної машини за допомогою OpManager визначає використання ресурсів кожної віртуальної машини на віртуальному сервері, зокрема цей важливий показник використання пам’яті. Ви можете побачити, яка віртуальна машина споживає найбільше доступної пам’яті в системі, і спостерігати за продуктивністю кожної віртуальної машини зі статистикою використання в реальному часі. Це дає змогу запобігти катастрофі, змінивши розподіл або перевіривши, чому певна віртуальна машина використовує так багато пам’яті.

Відстеження фізичних ресурсів сервера, виділених гіпервізору, також відбувається одночасно з моніторингом активності віртуальної системи. Таким чином, ви можете побачити, чи один конкретний віртуальний сервер споживає багато пам’яті або ЦП. Служба OpManager відстежує всю активність на кожному сервері, щоб ви могли помітити, чи зовсім непов’язаний процес може загрожувати успішній роботі вашої віртуалізації, споживаючи всі доступні ресурси сервера.

Система OpManager відстежуватиме кожен рівень вашої віртуалізації – як у гіпервізорі, так і під ним, а також спостерігатиме за всіма службами, які працюють поверх них. Ці завдання створюють багато живої інформації, яка відображається на різних екранах системної панелі, яку неможливо переглянути вручну.

На щастя, OpManager містить систему порогових значень продуктивності, і кожен з них ініціює попередження, якщо ресурсу не вистачає або продуктивність елемента падає. Ці сповіщення можна пересилати технікам у вигляді електронних листів або SMS-повідомлень. Отже, нікому не потрібно сидіти й дивитися на екрани, оскільки OpManager подбає про регулярний моніторинг продуктивності вашої фізичної та віртуальної інфраструктури.

Плюси:

Розроблений для негайної роботи, містить понад 200 настроюваних віджетів для створення унікальних інформаційних панелей і звітів

Використовує функцію автоматичного виявлення для пошуку, інвентаризації та картографування нових пристроїв

Використовує інтелектуальне сповіщення для зменшення помилкових спрацьовувань і усунення втоми сповіщень у великих мережах

Підтримує електронну пошту, SMS і вебхук для багатьох каналів оповіщення

Добре інтегрується в екосистему ManageEngine з іншими їхніми продуктами

Мінуси:

Це багатофункціональний інструмент, для належного навчання якого знадобляться витрати часу

OpManager поставляється як локальне програмне забезпечення, доступне для Windows Server і Linux. ManageEngine пропонує систему на а30-денна безкоштовна пробна версія.

ManageEngine OpManagerЗавантажте 30-денну БЕЗКОШТОВНУ пробну версію

7. SentryOne SQL Sentry.

SentryOne SQL Sentryце інструмент моніторингу, який відстежує продуктивність SQL Server. Якщо ви запускаєте свою реалізацію SQL Server через гіпервізор, ви можете використовувати цю систему моніторингу для спостереження за обома технологіями. Система SQL Sentry здатна контролювати віртуалізацію Hyper-V і VMWare, а також віртуальні сервери Amazon і Azure.

Ключові риси:

Відстежує віртуалізацію, що підтримує SQL Server

Hyper-V, VMWare, Azure та AWS

Спостерігає за активністю пам'яті

Частина моніторингу віртуальної машини служби SQL Sentry має власний екран на панелі інструментів системи. На екрані показано серію графіків, кожен з яких відстежує певний показник продуктивності віртуальної машини. Вони показують дані в реальному часі, які можна порівняти, щоб зробити висновки

про кореляцію активності. Послуга особливо зосереджена на продуктивності vCPU та віртуальних комутаторів.

Монітор відстежує низку статистичних даних про використання ЦП, а також активність введення/виведення пам’яті та диска для кожної віртуальної машини. Він також записує час очікування доступу до ЦП кожної віртуальної машини. Служба SQL Sentry може стежити за продуктивністю баз даних SQL Server, базових віртуальних машин і фізичних серверів, які їх підтримують.

Усі графіки продуктивності для віртуальної машини відображаються разом на одному екрані. Якщо навести курсор на точку на одному з графіків, відкриється накладена панель статистики, яка показує статистичні дані, які створили цю точку на діаграмі.

Служби моніторингу віртуалізації в SQL Sentry також відстежують діяльність віртуальних серверів і взаємодію між хостами та віртуальними машинами. Він також переглядає діяльність операційної системи, щоб перевірити, чи вся система віртуалізації підтримується без проблем.

Окрім показу поточних статусів, SQL Sentry представляє минулі дані для аналізу. Це доступно в двох режимах: режим зразка та режим історії. Режим вибірки дає змогу переглядати інформацію про продуктивність віртуальної машини в певний момент часу, тоді як режим історії представляє ті самі графіки часових рядів, що й у режимі live view, але зміщені назад у часі.

Плюси:

Пропонує єдиний інтерфейс для моніторингу баз даних SQL-сервера, віртуальних машин, віртуальних серверів, операційних систем і фізичних серверів

Показує реальну статистику продуктивності для кожної віртуальної машини

Визначає продуктивність зіставлення між віртуальними машинами та хостами

Пропонує функції історичного аналізу

Відстежує продуктивність пам'яті, процесора та дискового вводу-виводу

Мінуси:

Не буде цікавим для підприємств, які не використовують SQL Server

Програмний пакет SentryOne SQL Sentry встановлюється на Windows Server. Він також доступний на платформі Azure. Ви можете отримати а14-денна безкоштовна пробна версіялокальної версії.

SentryOne SQL SentryПочніть 14-денну БЕЗКОШТОВНУ пробну версію

8. Мережевий монітор Paessler PRTG.

Песслерстворює чудове рішення для моніторингу мережі, яке охоплює як моніторинг мережевих пристроїв, так і аналіз трафіку. Ця служба об'єднує функції для відстеження продуктивності віртуальної машини. ХочаМережевий монітор Paessler PRTGце мережевий монітор із повним набором послуг, він доступний у безкоштовній версії. Paessler встановлює ціни на кількість датчиків, які контролює система. «Сенсор» — це аспект служби, як-от швидкість мережі, або точка моніторингу, як-от порт. PRTG орієнтований на великі мережі, але безкоштовна версія підійде малому бізнесу.

Ключові риси:

Hyper-V, VMWare та Citrix

Моніторинг контейнерів

Віртуальні сервери AWS

Можливості моніторингу додатків віртуальної машини Paessler PRTG поширюються на такі платформи:

Citrix Xen

Microsoft Hyper-V

VMWare

Контейнери Parallels Virtuozzo

Amazon EC2

Можливості монітора дають вам можливість контролювати всю мережу за допомогою цього інструменту, а не лише віртуальне середовище. Базовий аналіз мережевого трафіку працює на типових системах обміну повідомленнями, які є частиною мікропрограми основних виробників мережевого обладнання. Фізичні

мережеві пристрої контролюються через систему SNMP. PRTG розширює моніторинг мережі на сайтах і в хмарі.

Моніторинг продуктивності сервера зосереджується на завантаженні процесора, використанні диска та швидкості передачі даних по мережі. Фізичні аспекти хост-машин, які відстежує PRTG, включають температуру сервера, поточне енергоспоживання, напругу акумулятора та швидкість вентилятора.

Ці метрики сервера призводять до виділення служби, яка попередить вас про перевантаження серверів. Маючи ці знання, ви можете перерозподіляти віртуальні машини між серверами, щоб отримати більш справедливе навантаження та кращу продуктивність. Ви можете встановити рівні попередження про продуктивність для різних атрибутів сервера. Ці спеціальні сповіщення дають вам змогу побачити, які сервери перевантажені. Попередження відображаються на інформаційній панелі, але ви також можете надіслати їх за допомогою SMS, електронної пошти або через API.

Інформаційну панель і сповіщення можна відфільтрувати для створення користувацьких переглядів із обмеженим контролем для різних членів команди. Ви можете надсилати сповіщення різним одержувачам відповідно до джерела попередження або ступеня серйозності.

Плюси:

Використовує комбінацію аналізу пакетів, WMI та SNMP для звітування про продуктивність мережі

Повністю настроювана інформаційна панель чудово підходить як для самотніх адміністраторів, так і для команд NOC

Редактор перетягування спрощує створення власних переглядів і звітів

Підтримує широкий спектр засобів сповіщення, таких як SMS, електронна пошта та сторонні інтеграції в такі платформи, як Slack

Кожен датчик спеціально розроблено для моніторингу кожної програми, наприклад, існують попередньо вбудовані датчики, конкретна мета яких — фіксувати та контролювати діяльність VoIP

Підтримує безкоштовну версію

Мінуси:

Це дуже комплексна платформа з багатьма функціями та рухомими частинами, для вивчення яких потрібен час

Безкоштовний PRTG обмежений 100 датчиками. Ви також можете отримати30-денна безкоштовна пробна версіяповної системи, який не має обмежень щодо кількості датчиків, які ви можете контролювати.

Мережевий монітор Paessler PRTGЗавантажте 30-денну БЕЗКОШТОВНУ пробну версію

9. LogicMonitor

LogicMonitor — це система керування продуктивністю мережі, але вона інтегрує моніторинг віртуальних серверних середовищ. Отже, ви можете використовувати його як загальносистемний монітор або просто обмежити його моніторингом реалізацій віртуальної машини. Система LogicMonitor пропонує моніторинг VMware vCenter, моніторинг хостів ESXi, а також охоплює окремі віртуальні машини, включаючи ESX і ESXi.

Ключові риси:

Платформа SaaS

Hyper-V, VMWare, Citrix, AWS і Amazon

Відображення віртуалізації та моніторинг ресурсів

LogicMonitor виконує відстеження продуктивності Microsoft Hyper-V як на рівні гіпервізора, так і на рівні окремої віртуальної машини. Ця система також може взаємодіяти з технологією Citrix XenServer.

Програмне забезпечення для цього монітора доступне в хмарі. Він не залежить від платформи та може контролювати хмарні послуги віртуальних машин, а також локальні системи. Однак це не зовсім зовнішня реалізація, оскільки вам потрібно встановити колектори на ваших серверах і мережевих пристроях. Ці колектори направляють через ваш шлюз до центрального сервера LogicMonitor. Усі комунікації через Інтернет зашифровані, як і дані, що зберігаються на сервері LogicMonitor. Інформація розшифровується в режимі

реального часу за умови доступу через дійсний обліковий запис користувача, для якого потрібні облікові дані.

Монітор запускається з процесу автоматичного виявлення, який відображає всю вашу мережу, включаючи реалізації XenServer, VMWare та Hyper-V. Система поширюється на хмарні сервери Amazon і Microsoft Azure.

Технологія, що лежить в основі систем віртуальних машин, породжує широкий спектр тем моніторингу. Насправді, щоб підтримувати роботу системи віртуальної машини, вам потрібно стежити за обладнанням, операційними системами, продуктивністю мережі, виконанням додатків і служб і, перш за все, за використанням ресурсів. У вас є віртуальні комутатори, з якими вам потрібно боротися, і вам потрібно переконатися, що сервери зберігання та додатків не перевантажуються та доступні з прийнятною швидкістю доставки. Інформаційна панель LogicMonitor охоплює всі ці питання.

Атрибути продуктивності обладнання, які відстежує монітор віртуальної машини, включають загальний стан ваших серверів. Вони зосереджуються на використанні пам’яті, завантаженні процесора, затримці диска, швидкості передачі даних диска, частоті вводу/с диска та частоті підкачки VMkernel, щоб підтримувати рівень обслуговування на належному рівні.

Системні сповіщення можна надсилати електронною поштою, SMS або сповіщеннями Slack. Ви можете вказати, які члени команди отримують сповіщення за класифікацією та джерелом. Якщо частину вашого віртуального середовища ви передаєте на аутсорсинг, команда підтримки постачальника може бути повідомлена автоматично. Інформаційну панель також можна налаштувати відповідно до ролі, тож ви можете безпечно використовувати консолі для всіх членів команди, навіть молодшого персоналу. Можна створити режим перегляду лише даних, щоб дозволити членам відділу фінансів і C-Suite переглядати події в системі віртуальної машини.

Плюси:

Дуже візуальний інтерфейс – чудовий для НОК і моніторингу на великому екрані

Підтримує кілька хост-середовищ, таких як ESX, ESXi та vCenter

Ціноутворення є гнучким і доступне в трьох варіантах

Мінуси:

Хотілося б побачити довший 30-денний пробний період

LogicMonitor не є безкоштовним, але ви можете отримати14-денна безкоштовна пробна версіящоб дати йому оберт. Пакет доступний у трьох версіях: Starter, Pro та Enterprise. Така масштабованість означає, що LogicMonitor підходить для підприємств будь-якого розміру.

10. Veeam One

Veeam One відстежує мережеві ресурси та аналізує використання системи реалізаціями віртуалізації VMWare vSphere та Hyper-V. Моніторинговий інструмент поширюється на хмарні служби. Veeam особливо сильний у резервному копіюванні та відновленні системи. Сервіс Veeam One був розроблений для інтеграції з диспетчером резервного копіювання та реплікації компанії.

Ключові риси:

Hyper-V і VMWare

Інтегрується з системою резервного копіювання

Безкоштовна версія

Система Veeam One використовує цілодобовий моніторинг у реальному часі. Ці монітори перевіряють 200 попередньо встановлених датчиків, і ви можете додати свої власні умови моніторингу та правила сповіщень. Модуль потужностей дає вам уявлення про постійне використання ресурсів, а також аналіз тенденцій на основі історичних даних. Компоненти збору даних охоплюють всю фізичну інфраструктуру, яка підтримує віртуалізацію та перевіряє попередження про обмеження ємності.

Вам не потрібно покладатися на інтерпретації візуалізацій інформаційної панелі та звітів, які надає Veeam One, оскільки ви також отримуєте доступ до необроблених даних. Це дає змогу створювати власні налаштовані звіти, програми та правила сповіщень.

Veeam One є платним продуктом. Однак є безкоштовна версія. Veeam One Free включає всі можливості моніторингу віртуальних машин платної системи. У безкоштовній версії системи немає обмежень щодо ємності, що рідко зустрічається в галузі. Veeam One Free у будь-якому випадку не має функцій об'єму, включених у Veeam One. У безкоштовній версії також відсутні функції відстеження плати та виставлення рахунків.

І безкоштовна, і платна версії відображають сповіщення на екрані. Їх також можна надіслати електронною поштою, але лише платні користувачі можуть налаштувати умови сповіщень.

Плюси:

Пропонує понад 200 попередньо налаштованих датчиків на додаток до настроюваних опцій

Можна створювати власні сповіщення та звіти через модульний інтерфейс

Попередження підтримуються в безкоштовній версії

Мінуси:

Інтерфейс здається застарілим – може бути незграбним під час керування великою кількістю віртуальних машин

Veeam One особливо ефективний для клієнтів резервного серверного програмного забезпечення компанії. Відстеження орендарів також робить це чудовим вибором для постачальників послуг як для надання хмарних сховищ, так і для програмного забезпечення як послуги. Якщо ви вважаєте, що повноцінна платна служба Veeam One вам буде краще обслуговуватися, ви можете протестувати її на30-денна безкоштовна пробна версія.

11. Квест Протитуманка

Foglight — це система моніторингу системи, яка має версії для хмарного моніторингу та керування середовищем віртуальної машини. Система працює з VMWare та Hyper-V, зосереджуючись на інформації, зібраній на vSwitch, у поєднанні з даними про фізичну продуктивність із сервера.

Ключові риси:

Hyper-V, VMWare та Citrix

Аналіз продуктивності на основі сканування пакетів

Може керувати розміщенням віртуальної машини на хості

Система налаштовується за допомогою функції автовиявлення. Він ідентифікує сервери та їхні клієнтські віртуальні машини та перевіряє трафік, який проходить між ними, щоб підкреслити продуктивність мережі. Розділ збору даних аналізу трафіку цього інструменту перевіряє дані на рівні пакетів, щоб визначити, які віртуальні машини та програми генерують найбільше трафіку.

Система Foglight також може контролювати середовища Citrix XenApp і XenDesktop. Інформаційна панель моніторингу додатків надає вам відображення всіх елементів у стеку Citrix VDI, підкреслюючи напружену інфраструктуру, яка може вплинути на продуктивність. Система вміло відображає топологію вашого віртуального середовища, щоб допомогти візуалізувати розташування кожної віртуальної машини та відстежувати фізичні потоки трафіку між серверами та віртуальними машинами.

Монітор також має функції керування. Ви можете налаштувати його на динамічне коригування ресурсів, виділених кожній програмі або віртуальній машині, щоб врахувати недостатнє використання або надмірну ємність у різних областях мережі. Інформаційна панель монітора надає широкий спектр переглядів активності сеансу користувача Citrix, від загальної кількості віртуальних машин до активності програм.

Система моніторингу Foglight ретельно відстежує продуктивність NetScaler і затримку мережі. Іншими міркуваннями є навантаження на фізичні пристрої та віртуальні комутатори. Монітор Foglight визначає неактивні віртуальні машини та дозволяє видаляти зомбі-процеси, щоб звільнити ресурси. Це чудова функція, оскільки, на жаль, середовище віртуальної машини схильне до зависання процесів і припинених сеансів, які залишають за собою блокування розподілу ресурсів.

Система Foglight досліджує та зберігає дані для створення випробувального стенду. Інформаційна панель показуватиме тенденції та варіанти продуктивності та виділить дані для кожного апаратного елемента

вашої системи. Це допомагає виявити вузькі місця та неправильний розподіл ресурсів.

Шаблони даних і регулярна статистика використання дають вам функцію планування потужності. За допомогою цього інструменту ви можете визначити, де відкоригувати розподіл ресурсів, щоб покращити продуктивність і опрацювати наслідки збільшення попиту. Монітор Foglight включає можливості прогнозування, які пропонують дії для вирішення умов тривоги. Це також працюватиме з реальними даними, щоб допомогти регулювати використання мережі на льоту.

Якщо ви працюєте в середовищі багатьох постачальників із програмним забезпеченням VMWare і Hyper-V, що працює на місці, ви можете об’єднати свої завдання моніторингу та керування в одному місці за допомогою системи Foglight. Монітор розширюється до хмарного сховища, тож ви можете змінювати ємність, регулюючи додаткові параметри за межами сайту, наприклад додаткове сховище.

Плюси:

Може контролювати хмарні та фізичні хост-середовища

Використовує автовиявлення для пошуку та моніторингу нових віртуальних машин у міру їх створення

Хороший варіант для тих, хто хоче спеціально контролювати кілька середовищ Citrix

Мінуси:

Інтерфейс здається застарілим – може бути незграбним під час керування великою кількістю віртуальних машин

Звітування є дещо консервованим, можна було б отримати користь від додаткових параметрів налаштування

Квест Foglight не безкоштовний. Однак ви можете скористатися безкоштовною пробною версією, щоб відчути систему. Foglight працює в операційних системах Windows, Linux і Solaris.

12. Aptare Virtualization Manager

Aptare Virtualization Manager зосереджується на серверах зберігання, які працюють у віртуалізованих середовищах. Цей інструмент відстежуватиме використання сховища у вашій віртуальній мережі та повідомлятиме, які віртуальні машини використовують ємність.

Ключові риси:

Планувальник віртуалізації

Легко читається

Відображення ресурсів

Інтерфейс для Aptare Virtualization Manager містить інструмент планування. Цей інструмент може прогнозувати потреби в ємності на основі історичних даних. Монітор також відстежує доступ віртуальної машини до сховища та визначає потенційні вузькі місця та конфлікти доступу.

Функції керування поширюються на виявлення шахрайських процесів, які блокують розподіл сховища. Ви можете використовувати цей інструмент керування продуктивністю, щоб звільнити простір, виділений для завислих процесів, зробивши його доступним для інших віртуальних машин у середовищі.

Плюси:

Простий інтерфейс добре поєднує поточні підсумки та візуалізацію на головній інформаційній панелі

Включає інструмент планування, чудовий для MSP або підготовки до планування потужностей

Може автоматично визначити першопричину проблем

Висвітлює проблемні процеси, які можуть споживати безмежні ресурси (наприклад, Chrome)

Мінуси:

Має більш обмежену функціональність і звітність порівняно з аналогічними інструментами

Відсутність функцій планування потужності

Aptare Virtualization Manager доступний для використання з продуктами VMWare: ESX, ESXi, vSphere та vCenter; Веб-сервіси Amazon: Amazon Elastic

Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Billing Records; Microsoft Azure: віртуальна машина, сховище на дисках, таблицях і чергах, сховище blob; і сервери, сумісні з OpenStack. Хоча цей інструмент має обмежену функціональність, він стане в нагоді, якщо ви вважаєте, що поточна утиліта моніторингу віртуальної машини не надає достатньо деталей щодо керування сховищем.

13. Надбудова моніторингу віртуалізації WhatsUp Gold

Моніторинг середовищ віртуальних машин складний. Вам потрібно перевіряти як інфраструктуру, так і програмне забезпечення та постійно контролювати кожен елемент, щоб запобігти погіршенню продуктивності. Progress WhatsUp Gold охоплює всі ракурси, які вам потрібно спостерігати, щоб успішно підтримувати віртуалізацію.

Ключові риси:

Додає на мережевий монітор

Відстеження продуктивності в реальному часі

Історичний аналіз

Основне програмне забезпечення WhatsUp Gold реалізує моніторинг продуктивності мережі, стежачи за пристроями, які з’єднують ваші мережеві канали. Однак є ще багато чого, що потрібно відстежувати, щоб ваша система віртуальної машини працювала. Надбудова Virtualization Monitoring покриває ці додаткові завдання.

Важливою особливістю доповнення є розширення функції виявлення мережі WhatsUp Gold. Це застосує до всіх компонентів віртуальної машини процеси зіставлення підключень і залежностей, які основний пакет застосовує до мережевих пристроїв. Перевірка системи дає WhatsUp Gold базовий рівень, і на основі цього надбудова створює карту, яка показує стек програм, який підтримує кожну віртуальну машину. Ви зможете побачити, які сервери підтримують які віртуальні машини, а також статус атрибутів сервера та серверного програмного забезпечення віртуалізації.

Коли ваша система віртуальної машини переходить у звичайний режим роботи, надбудова продовжуватиме відстежувати продуктивність, виявляючи можливі збої в програмному забезпеченні, серверах і мережі. Дані, зібрані WhatsUp Gold, відображаються в режимі реального часу на інформаційній панелі, а також зберігаються як вихідна інформація для функцій аналізу. За допомогою цих інструментів планування ви можете визначити, чи є якісь із ваших серверів перевантаженими, і вжити відповідних заходів.

Плюси:

Інтерфейс користувача простий у навігації, а також настроюється

Може відображати та відстежувати залежності між хостами та віртуальними машинами

Може зберігати показники та інформацію про ресурси для довгострокового аналізу

Мінуси:

Звітність можна покращити

Конфігурація може бути надто складною, особливо на початку

Не є автономним рішенням, вимагає WhatsUp Gold

WhatsUp Gold і надбудову моніторингу віртуалізації можна придбати разом із надбудовою моніторингу продуктивності програми Progress у пакеті системного адміністратора. Пакет WhatsUp Gold Total Plus надає вам основну програму разом із усіма її доповненнями. Який би спосіб придбання WhatsUp Gold і надбудови моніторингу віртуалізації ви не вибрали, ви можете отримати їх на30-денна безкоштовна пробна версіяперш ніж взяти на себе зобов'язання купити.

14. Вбудований хост-клієнт ESXi

VMWare створює безкоштовне середовище для своїх систем ESXi, яким є вбудований хост-клієнт ESXi. Інтерфейс клієнта базується на браузері, тому він не залежить від операційної системи. Крім того, щоб використовувати цей інструмент моніторингу, у вас повинно бути встановлене та запущене програмне забезпечення VMWare. Він не працюватиме з системами Citrix або Hyper-V. Ця

утиліта не багата функціями, і вона не надасть вам повних можливостей моніторингу системи, ніж інші параметри в цьому списку. Однак він підійде для впровадження віртуалізації в малому бізнесі та лабораторних сценаріїв.

Ключові риси:

Безкоштовне використання

Виробник VMWare

Просте зчитування показників

Інструмент пропонує розширений інтерфейс для ваших клієнтів ESXi. Ви можете налаштувати нові віртуальні машини за допомогою цієї утиліти та налаштувати хостинг для кожної. Моніторинговий аспект інструменту дає вам уявлення про статуси хостів. Він також перераховує поточні дані про події, що відбуваються в середовищі віртуальної машини.

Плюси:

100% безкоштовне рішення для моніторингу

Добре підходить для домашніх лабораторій і невеликих середовищ віртуалізації

Простий макет, легко почати

Мінуси:

Потрібне встановлення програмного забезпечення VMWare

Лише для хостів ESXi

Не вистачає багатьох функцій, таких як звітування та планування потужностей, які є в інших інструментах

Це простий інструмент, але той факт, що він безкоштовний і походить безпосередньо від VMWare, спокусить вас встановити його.

15. Турбономічний

Зростання хмари у наданні віртуальних середовищ можна побачити в презентації продукту Turbonomic. До недавнього часу продукти віртуальних машин надавали пріоритет ресурсам на місці, а потім, можливо, мали справу з хмарними службами. У випадку Tubonomic цей інструмент називається утилітою

для моніторингу хмарних ресурсів. О, і, до речі, він також може спостерігати за будь-якими локальними серверами віртуальних машин, які у вас можуть бути.

Ключові риси:

Карти віртуальних структур

Добре підходить для гібридних середовищ

Прогнози потреб у ресурсах на основі AI

Turbonomic не економить на локальному моніторингу віртуальних машин, і система може дуже добре впоратися з гібридними впровадженнями. Цей дуже комплексний інструмент моніторингу продуктивності віртуальної машини для віртуальних середовищ поставляється в трьох пакетах: Essentials, Advance і Premier.

Хоча це програмне забезпечення для моніторингу не є безкоштовним, ви можете отримати 30-денну безкоштовну пробну версію пакета Premier. Ціна базується на кількості робочих навантажень, які покриває монітор. Пакет Essentials має обмеження в 750 робочих навантажень, але інші два випуски мають необмежену кількість. Монітор інтегрує механізми керування та інтегрує штучний інтелект у свої процеси рекомендацій щодо дій. Ви отримуєте більше автоматизації з вищими планами, але всі випуски містять можливості планування потужності.

Простий модуль моніторингу Turbonomic включає такі чудові функції візуалізації, як діаграми та графіки. Інструмент може взаємодіяти з середовищами VMware, Hyper-V і XenServer. Процес налаштування автоматизований і завершується перевіркою стану системи. Це сканування за допомогою механізму Turbonomic відображає все ваше віртуальне середовище. Він завершує свою адаптацію списком рекомендацій щодо проблем вашої системи та способів їх вирішення. Після завершення цього початкового етапу Turbonomic постійно стежить за навколишнім середовищем, створюючи сповіщення на панелі приладів, підкріплюючи їх рекомендаціями щодо дій.

Ви можете встановити базу правил дій у вищих версіях Turbonomic, щоб автоматично виконувати вирішення, коли виникають певні сповіщення. Ця

автоматизація необов’язкова, і ви можете запускати рекомендовані дії вручну або ігнорувати їх, якщо хочете.

Це хороший інструмент для відділів або служб, які дотримуються угод про рівень обслуговування. Ці SLA можна перевести безпосередньо в систему моніторингу як вимоги до якості обслуговування. Ви можете встановити рівні сповіщень для аспектів обслуговування, включаючи час відповіді для доставки та пропускну здатність транзакцій для виставлення рахунків.

Монітор дозволяє перерозподіляти ресурси між різними програмами або групами користувачів і виділяє області, де розширення хмарних ресурсів неминуче. З іншого боку, рушій Turbonomic AI покаже вам, де ви перевантажили, дозволяючи вам скоротити онлайн-сервіси та скоротити витрати. Ця візуалізація потужностей також поширюється на функції планування. Інтерфейс містить розділ тестування ємності, де можна попередньо переглянути вплив розширень на базу користувачів або включення нових програм і послуг. Це чудовий інструмент планування для обробки ставок, оскільки він дозволить вам ефективніше планувати додаткові послуги.

Плюси:

Підтримує як хмарні віртуальні машини, так і локальні хости

Користувальницький інтерфейс є гладким і добре використовує колір, щоб підкреслити важливі показники/функції

Візуальне відображення допомагає системним адміністраторам бачити залежності

Гнучка цінова політика

Мінуси:

Може отримати вигоду від автоматичного виявлення

Коштує дорожче аналогічних засобів

Інформаційну панель для монітора можна налаштувати, і ви можете призначити різні види та елементи керування членам вашої команди. Можливість створити інтерфейс користувача, який взагалі не містить жодних елементів керування, дає вам можливість дозволити клієнтам або директорам

отримати доступ до системи, не ризикуючи пошкодити налаштування вашої віртуальної машини.

16. 5Nine Manager

5Nine націлений на впровадження центрів обробки даних на хмарній платформі Microsoft. Отже, якщо ви хочете використовувати VMWare, то цей продукт, ймовірно, не буде для вас. Якщо ваше віртуальне середовище — це Hyper-V, читайте далі. 5Nine легко інтегрує хмарні сервери Azure у вашу інфраструктуру віртуальних машин. Це гарне рішення, якщо ви керуєте даними для інших компаній, оскільки ви можете визначити попит аж до орендаря, перевірити продуктивність кожного хоста та відстежувати дії користувачів.

Ключові риси:

Підходить для ЦОД

Hyper-V і Azure

Інформаційні панелі на основі ролей

Інформаційна панель цього сервісу має широкі можливості налаштування, що дозволяє створювати різні облікові записи користувачів з різними правами доступу. Це ще одна функція, яка приваблює компанії, які надають послуги. Ви можете надати клієнтам обмежену інформаційну панель і дозволити їм керувати власним розподілом віртуальних машин. Інші перегляди можна надати членам команди з різними рівнями старшинства у вашій власній групі, і це дає змогу директорам та іншим зацікавленим сторонам у вашій компанії переглядати дані про продуктивність у реальному часі. Настроювані звіти покращують функції обміну даними цього пакета.

5Nine адаптував свій продукт таким чином, щоб він спеціально перевіряв усі поля, необхідні постачальнику послуг. Однак, якщо ви керуєте власним підприємством, функції моніторингу розподілу ресурсів точно не зашкодять жодній угоді про рівень обслуговування та політиці центрів витрат, якими керує ваша компанія.

Плюси:

Звичний інтерфейс, схожий на багато продуктів Office

Добре підтримує командні середовища з керуванням дозволами на рівні облікового запису користувача

Може підтримувати середовища з кількома клієнтами, хороший вибір для MSP

Мінуси:

Незважаючи на звичний вигляд інтерфейсу, він може швидко стати захаращеним під час керування масштабними віртуальними машинами

Бракує детальної візуалізації

Немає безкоштовної версії

Підтримує лише Hyper-V

5Nine Manager є платною послугою, але ви можете отримати безкоштовну пробну версію.

Висновки за розділом

Проведений у розділі аналіз роботи систем дав широкий вибір інструментів моніторингу активності користувачів та стану обладнання. Деякі інструменти моніторингу віртуальних машин насправді є загальносистемними системами керування інфраструктурою, які мають чудові функції віртуалізації. Інші інструменти в списку – це лише невеликі утиліти, які покращують ваш погляд на дані віртуальної машини або покращують лише один аспект продуктивності віртуальної машини.

Надання інструментів віртуальної машини – це дуже широке поле. SolarWinds охоплює обидва кінці спектру, надаючи невеликий безкоштовний інструмент і «навороти» системи моніторингу. Paessler і ManageEngine також намагаються задовольнити всі точки ринку. Деякі дрібні гравці пропонують фантастичні продукти, які обов’язково сподобаються малим і середнім підприємствам, але також пропонують можливості, які можуть допомогти підприємствам із великими та складними віртуалізованими мережами.

Щоб відстежувати мережевий трафік у VMWare, спочатку потрібно ввімкнути безладний режим на vSwitch, який працює в середовищі. Функцію для активації безладного режиму на vSwitch можна знайти на інформаційній панелі vCenter Server у vSphere.

Коли vSwitch зможе прослуховувати весь мережевий трафік, ви можете встановити безкоштовну систему захоплення пакетів, щоб направляти мережевий трафік для аналізу. Для цього спробуйте Wireshark.

Віртуалізації типу 1 і типу 2 покладаються на гіпервізори типу 1 і типу 2. Гіпервізор також відомий як монітор віртуальної машини (VMM). Віртуалізація 1-го типу використовує гіпервізор 1-го типу, який працює на «голому металевому» сервері. Це тому, що Type 1 містить власну операційну систему. Віртуалізацію типу 2 із гіпервізором типу 2 слід інсталювати на сервері, на якому вже встановлено операційну систему.

Заміна сторінок є основною причиною уповільнення часу відповіді віртуальної машини. У цьому сценарії ваша віртуальна машина дуже повільна, тому що гіпервізор зайнятий переміщенням даних у файли на диску та з них, оскільки в пам’яті недостатньо місця. Перевірте використання пам’яті віртуальної машини та подивіться, чи досягає вона ліміту. З іншого боку, можна виділити занадто багато пам’яті для віртуальної машини та залишити в операційній системі хоста недостатньо місця. Отже, перевірте це також.

Щоб відстежувати активність користувачів потрібно налаштувати монітор підключення. Термінологія та метод створення моніторів підключення відрізняються від марки віртуалізації до марки віртуалізації. Однак монітор підключення має бути опцією, яку ви можете налаштувати в системі створення служб вашого диспетчера віртуальної машини.

РОЗДІЛ 3
ОПИСАННЯ РОЗРОБЛЕНОЇ КОМП'ЮТЕРНОЇ СИСТЕМИ МОНІТОРИНГУ АКТИВНОСТІ КОРИСТУВАЧІВ І СТАНУ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ КОМПАНІЇ

3.1. Вибір компонентів комп'ютерної системи моніторингу активності користувачів і стану апаратного забезпечення компанії

Моніторинг діяльності працівників, дотримання вимог охорони праці та техніки безпеки є невід'ємними складовими забезпечення ефективної та безперебійної роботи промислових підприємств та інфраструктурних об'єктів. Незважаючи на зміну ролі та завдань людини на виробництві та очевидну тенденцію до підвищення ступеня автоматизації виробничих процесів, людина залишається їх безпосереднім учасником, при цьому вимоги до забезпечення безпеки неухильно посилюються.

Сучасний підхід до вирішення цього завдання полягає у створенні комплексних систем, що дозволяють здійснювати повноцінну інформаційну інтеграцію діяльності персоналу з роботою виробничого обладнання та інфраструктури в рамках єдиного інформаційного простору підприємства. Це дає можливість не лише контролювати місцезнаходження співробітників та статус виконання ними окремих операцій, а й цілеспрямовано керувати процесами забезпечення безпеки та ефективності загалом.

Незважаючи на те, що підходи до забезпечення безпеки та ефективності, засновані на регламентуванні процесів, контрольних заходах та інших організаційних заходах, давно відомі і широко застосовуються, сучасні російські підприємства гостро потребують підвищення продуктивності праці при зниженні травматизму.

Причинами недостатньої продуктивності праці, пов'язаними з роботою виробничого персоналу, як правило, є [2]: - недотримання працівниками правил технологічного процесу, передбачених інструкціями, технологічними картами

тощо (у тому числі відхилення від режимів, послідовності дій, невиконання окремих операцій) або завдань в цілому); - відсутність можливості контролювати правильність виконання операцій та виробничих завдань співробітниками в режимі реального часу і, як наслідок, неможливість оперативно вживати коригуючих заходів у разі необхідності; - у ряді випадків - відсутність інформаційної поінформованості у співробітника при виконанні цільової операції про стан пов'язаних процесів і систем – тієї поінформованості,яка повинна бути для коректного виконання завдання (особливо на географічно розподілених та віддалених об'єктах).

Причини можливого травматизму та зниження безпеки також значною мірою пов'язані з відсутністю у співробітника інтерактивної інформації про завдання, що потребує виконання, та неможливістю оперативно контролювати фактично виконані дії. Зазначені обставини можуть призводити до наступних наслідків [2]: - помилок співробітників, що створюють загрозу заподіяння шкоди життю та здоров'ю людей, навколишньому середовищу; картини події попередження нещасних випадків надалі.

З урахуванням зазначених обмежень та вимог найперспективнішою апаратною платформою для об'єктивного моніторингу персоналу є «розумний» годинник зі спеціалізованим програмним забезпеченням.

Розглянуте рішення побудовано на базі платформи для створення комплексних систем моніторингу, аналізу та контролю ефективності роботи обладнання, оперативного управління та диспетчеризації виробничих процесів SIMATIC WinCC Open Architecture (WinCC OA) та програмно-апаратного комплексу SiWatch. Комплекс SiWatch у складі рішення забезпечує реалізацію функцій моніторингу стану, пересування та діяльності співробітників, а також передачі повідомлень чи іншої інформації. Система WinCC OA використовується у своїй традиційній ролі – як інтеграційна платформа та основа для реалізації комплексної системи збирання та обробки промислових даних та диспетчерського управління виробничими процесами [3]. Подібна інтеграція

дозволяє здійснювати єдине ефективне автоматизоване керування як обладнання,

З точки зору структури ПЗ комплекс SiWatch включає серверний компонент SiWatch Base для збору та аналізу інформації про стан і пересування персоналу, драйвер SiWatch Driver для інтеграції з WinCC OA і програмне забезпечення для пристроїв SiWatch firmware – «прошивку», що забезпечує збір телеметрії та передачу повідомлень. Логіка управління та моніторингу персоналу в залежності від стану виробничого процесу може бути описана стандартною для WinCC OA вбудованою скриптовою мовою CONTROL (CTRL), яка використовується також для реалізації прикладної бізнес-логіки диспетчеризації обладнання та технологічних процесів.

В якості апаратної частини комплексу SiWatch використовуються персональні пристрої типу «розумний годинник», якими екіпіруються співробітники підприємства, а також маяки Bluetooth Low Energy (BLE) для забезпечення позиціонування всередині приміщення/цеху, ідентифікації обладнання та технологічних вузлів підприємства. Позиціонування на відкритій місцевості здійснюється за допомогою GPS/GLONASS. Апаратна частина, що забезпечує керування обладнанням та техпроцесом, представлена відповідними засобами автоматизації – сполученими АСУ ТП, локальними САУ, окремими ПЛК та КВП, що взаємодіють з WinCC OA.

Описане вище рішення може забезпечувати реалізацію як базових, так і розширених та спеціалізованих сценаріїв моніторингу та забезпечення безпеки в промисловості.

До базових сценаріїв можна віднести: - контроль розташування зовні і всередині приміщень/цехів; - збір даних про активність співробітника та контроль значень пульсу; - контроль доступу в зони підвищеної небезпеки; - повідомлення співробітників; - запис та відправлення голосових повідомлень

Зазначені сценарії дозволяють вирішувати більшість завдань з моніторингу та забезпечення безпеки, які стоять перед промисловим підприємством. Однак найчастіше розробка нетривіальних сценаріїв роботи

рішення дозволяє привносити додаткову цінність та ефект за рахунок реалізованої інтеграції з платформою WinCC OA. Про це йтиметься нижче.

Розширені сценарії передбачають комплексний контроль виробничого обладнання та персоналу в рамках єдиного додатку. Розглянемо приклади таких сценаріїв.

Сценарій реагування на відмову виробничого обладнаннявключає наступні кроки (рис. 3): (1) на обладнанні (установці, виробничій лінії тощо) відбувається відмова одного з елементів; (2) на рівні системи WinCC OA за даними від відповідної системи автоматизації / системи управління генерується подія про несправність. Система WinCC OA робить запит у SiWatch; (3) SiWatch знаходить найближчого відповідального співробітника, перевіряє кваліфікацію, зайнятість; (4) SiWatch відправляє на пристрій співробітника (групи співробітників) повідомлення з необхідною інформацією для ідентифікації обладнання і даними для первинної діагностики несправності; 5) співробітник, отримавши інформацію, виконує роботи з обслуговування обладнання (виробничої лінії); (6) співробітник відзначає виконання завдання на персональному пристрої, що носиться; дані про це передаються SiWatch і WinCC OA; (7) далі опціонально система управління технологічним процесом здійснює валідацію виконання, отримує підтвердження про те, що обладнання справно і не генерує помилок; після цього в автоматичному режимі вводить обладнання технологічний процес.

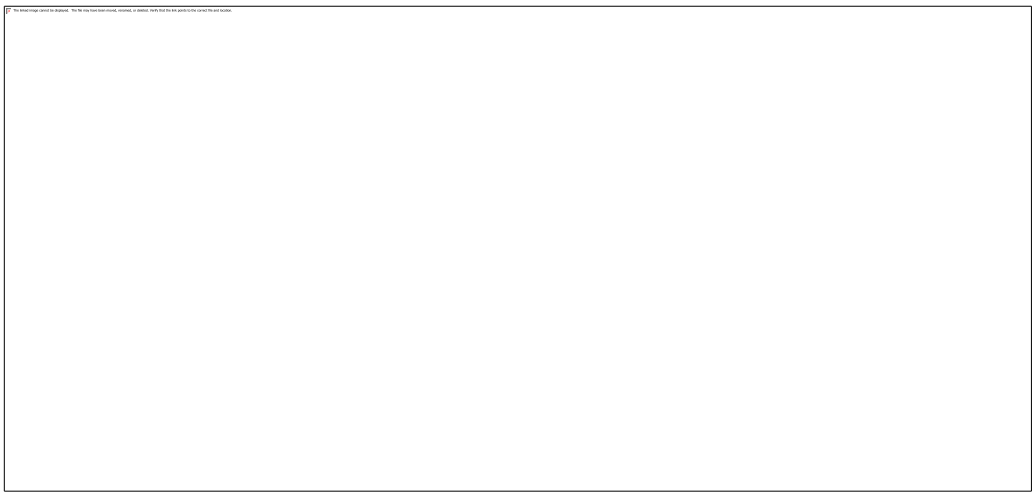

Рис. 3.1. Сценарій реагування на відмову виробничого обладнання

Досвід впровадження подібного сценарію компанією «Сіменс» в умовах реального підприємства машинобудівної галузі демонструє зниження середнього часу відновлення технологічного процесу (MTTR).

Сценарій контролю технологічних операцій. Під технологічними операціями розуміється жорстко регламентований порядок дій співробітників та бригад з обслуговування обладнання чи управління технологічним процесом. У цьому випадку інструкції та регламенти завантажуються в систему SiWatch, яка транслює їх у вигляді завдань на пристрої (рис. 4).

Рис. 3.2. Сценарій контролю технологічних операцій (збільшити зображення)

У ході виконання технологічних операцій пристроями автоматично та автономно контролюється: - місце проведення операції; - необхідні кроки та порядок виконання; - час виконання технологічної операції; - склад бригади та кваліфікація співробітників.

Результатом є автоматично сформований звіт про виконання технологічних операцій, де зазначено пропущені кроки та інші відхилення від регламенту виконання робіт. Подібний сценарій успішно апробовано на підприємстві нафтогазової галузі.

Спеціалізовані сценарії, що відповідають індивідуальним вимогам замовників та адаптовані до особливостей техпроцесів та характеристик об'єктів, можуть бути реалізовані засобами комплексу шляхом конфігурування базовими

інструментами, так і шляхом інжинірингу з використанням інструментів WinCC OA.

До планів щодо подальшого розвитку рішення можна віднести: - вдосконалення алгоритмів і підвищення точності позиціонування; - реалізацію механізмів прискореного розгортання (за технологією plug and play); - розширення засобів адміністрування пристроїв, що носяться безпосередньо у WinCC OA.

Оповіщення визначаються у конфігураційному файлі і задають набір правил для метрик. Якщо у часових рядах виникає відповідність правилу, оповіщення ініціюється та надсилається заданим одержувачам.

Як і в *Grafana*, як одержувач можна вказати електронну адресу, вебхук *Slack, PagerDuty* і кастомні *HTTP*-об'єкти.

Крім *Prometheus, Grafana* може вимагати і обробляти дані з багатьох інших систем (рис. 3.3).

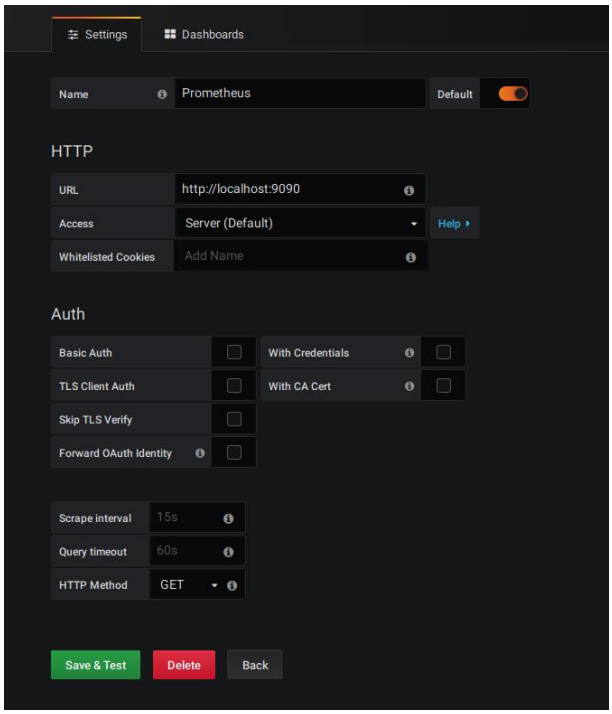

Рис. 3.8. Вікно налаштування системи *Grafana*

Після налаштування *Datasource* можемо створити дашборд. Дашборд це просто набір панелей, розташованих на одній сторінці. Панелі бувають різні: від

звичайного тексту до кругових діаграм. Кожну панель можна налаштувати для відображення різних метриків.

Можна оновити сторінку – панель із круговою діаграмою має відображатися правильно (рис. 3.10).

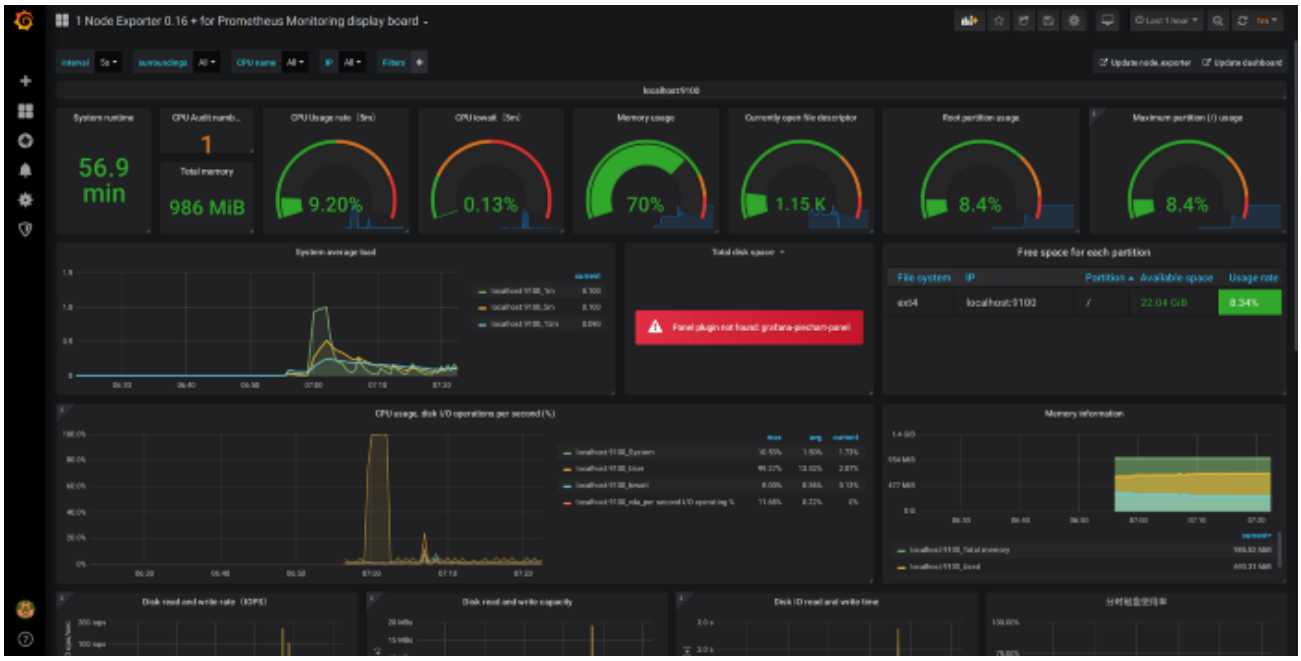

Рис. 3.10. Вікно імпортуваного плагіну дашборду

Поглянувши на цю сторінку, можете отримати інформацію про стан сервера: починаючи з того, як довго він працює, закінчуючи завантаження процесора і використанням пам'яті.

З розглянутими інструментами можна зробити набагато більше, включаючи налаштування автоматичних алертів при досягненні певних метриками порогових значень.

3.2. Розгортання розроблених компонентів

Багатофункціональні портативні прилади моніторингу

Останнім часом почали випускатися багатофункціональні портативні прилади, які об'єднують можливості кабельних сканерів, аналізаторів протоколів і навіть деякі функції систем управління, зберігаючи в той же час таку важливу

властивість, як портативність. Багатофункціональні прилади моніторингу мають спеціалізований фізичний інтерфейс, що дозволяє виявляти проблеми та тестувати кабелі на фізичному рівні, який доповнюється мікропроцесором із програмним забезпеченням для виконання високорівневих функцій.

Функції перевірки апаратури та кабелів

багатофункціональні прилади поєднують функції кабельних сканерів, що найбільш часто використовуються на практиці, з рядом нових можливостей тестування.

● Сканування кабелю

Функція дозволяє вимірювати довжину кабелю, відстань до найсерйознішого дефекту та розподіл імпедансу по довжині кабелю. При перевірці неекранованої кручений пари можуть бути виявлені такі помилки: розщеплена пара, обриви, коротке замикання та інші види порушення з'єднання. Для мереж Ethernet на коаксіальному кабелі ці перевірки можуть бути здійснені на працюючій мережі.

● Функція визначення розподілу кабельних жил

Здійснює перевірку правильності приєднання жил, наявність проміжних розривів та перемичок на кручених парах. На дисплеї відображається перелік зв'язаних між собою контактних груп.

● Функція визначення карти кабелів

Використовується для складання карти основних кабелів та кабелів, що відгалужуються від центрального приміщення.

● Автоматична перевірка кабелю

Залежно від конфігурації можна визначити довжину, імпеданс, схему підключення жил, згасання та параметр NEXT на частоті до 100 МГц. Автоматична перевірка виконується для коаксіальних кабелів, екранованої кручений пари з імпедансом 150 Ом, неекранованої кручений пари з опором 100 ОМ.

● Цілісність ланцюга під час перевірки постійним струмом

Ця функція використовується при перевірці коаксіальних кабелів для верифікації правильності термінаторів та їх установки.

● Визначення номінальної швидкості розповсюдження

Функція обчислює номінальну швидкість розповсюдження (Nominal Velocity of Propagation, NVP) по кабелю відомої довжини і додатково зберігає отримані результати у файлі для типу типу кабелю (User Defined Cable Type) або стандартного кабелю, що визначається користувачем.

● Комплексна автоматична перевірка пари "мережевий адаптер-концентратор"

Цей комплексний тест дозволяє послідовно підключити прилад між кінцевим вузлом мережі та концентратором. Тест дозволяє автоматично визначити місцезнаходження джерела несправності - кабель, концентратор, мережевий адаптер або програмне забезпечення станції.

● Автоматична перевірка мережних адаптерів

Перевіряє правильність функціонування нововстановлених або "підозрілих" мережевих адаптерів. Для мереж Ethernet за підсумками перевірки повідомляються: MAC-адреса, рівень напруги сигналів (а також присутність та полярність імпульсів Link Test для 10Base-T). Якщо сигнал не виявлено на мережному адаптері, тест автоматично сканує з'єднувальний роз'єм і кабель для їх діагностики.

Функції збору статистики

Ці функції дозволяють у реальному масштабі часу простежити за зміною найважливіших параметрів, що характеризують "здоров'я" сегментів мережі. Статистика зазвичай збирається з різним ступенем деталізації з різних груп.

● Мережева статистика

У цій групі зібрані найважливіші статистичні показники - коефіцієнт використання сегмента (utilization), рівень колізій, рівень помилок та рівень широкомовного трафіку. Перевищення цими показниками певних порогів насамперед говорять про проблеми у тому сегменті мережі, якого підключено багатофункціональний прилад.

● Статистика помилкових кадрів

Ця функція дозволяє відстежувати всі типи хибних кадрів для певної технології. Наприклад, для технології Ethernet характерні такі типи помилкових кадрів.

• Укорочені кадри (Short Frames). Це кадри, мають довжину, менше допустимої, тобто. менше 64 байт. Іноді цей тип кадрів диференціюють на два класи - просто короткі кадри (short), які мають коректну контрольну суму, і "коротушки" (runts), які мають коректної контрольної суми. Найімовірнішими причинами появи укорочених кадрів є несправні мережеві адаптери та його драйвери.

Подовжені кадри (Jabbers). Це кадри, що мають довжину, що перевищує допустиме значення 1518 байт з гарною або поганою контрольною сумою. Подовжені кадри є наслідком тривалої передачі, яка виникає через несправності мережевих адаптерів.

• Кадри нормальних розмірів, але з поганою контрольною сумою (Bad FCS) та кадри з помилками вирівнювання на межі байта. Кадри з невірною контрольною сумою є наслідком безлічі причин - поганих адаптерів, перешкод на кабелях, поганих контактів, портів повторювачів, мостів, комутаторів і маршрутизаторів, що некоректно працюють. Помилка вирівнювання завжди супроводжується помилкою контрольної суми, тому деякі засоби аналізу трафіку не роблять між ними відмінностей. Помилка вирівнювання може бути наслідком припинення передачі кадру при розпізнаванні колізії адаптером, що передає.

Кадри-привиди є результатом електромагнітних наведень на кабелі. Вони сприймаються мережевими адаптерами як кадри, які мають нормальної ознаки початку кадру - 10101011. Кадри-примари мають довжину понад 72 байт, інакше вони класифікуються як видалені колізії. Кількість виявлених кадрів-примар великою мірою залежить від точки підключення мережевого аналізатора. Причинами виникнення є петлі заземлення та інші проблеми з кабельною системою.

Знання відсоткового розподілу загальної кількості помилкових кадрів за їх типами може багато підказати адміністратору про можливі причини неполадок в мережі. Навіть невеликий відсоток помилкових кадрів може призвести до значного зниження корисної пропускної спроможності мережі, якщо протоколи, що відновлюють перекручені кадри, працюють з великими тайм-аутами очікування квитанцій. Вважається, що у нормально працюючої мережі відсоток помилкових кадрів нічого не винні перевищувати 0,01% , тобто. не більше 1 помилкового кадру із 10000.

● Статистика з колізій

Ця група характеристик дає інформацію про кількість та види колізій, зазначених на сегменті мережі, дозволяє визначити наявність та місцезнаходження проблеми. Аналізатори протоколів зазвичай не можуть дати диференційованої картини розподілу загальної кількості колізій за їх окремими типами, водночас знання переважаючого типу колізій може допомогти зрозуміти причину поганої роботи мережі. Нижче наведено основні типи колізій мережі Ethernet.

• Локальна колізія (Local Collision). Є результатом одночасної передачі двох або більше вузлів, що належать до того сегменту, в якому вимірюються. Якщо багатофункціональний прилад не генерує кадри, то в мережі на кручений парі або волоконно-оптичному кабелі локальні колізії не фіксуються. Занадто високий рівень локальних колізій є наслідком проблем із кабельною системою.

• Віддалена колізія (Remote Collision). Ці колізії відбуваються з іншого боку повторювача (стосовно тому сегменту, у якому встановлено вимірювальний прилад). У мережах, побудованих на багатопортових повторювачах (10Base-T, 10Base-FL/FB, 100Base-TX/FX/T4, Gigabit Ethernet), всі колізії, що вимірюються, є віддаленими (крім тих випадків, коли аналізатор сам генерує кадри і може бути винуватцем колізії). Не всі аналізатори протоколів та засоби моніторингу однаково фіксують видалені колізії. Це відбувається через те, що деякі вимірювальні засоби та системи не фіксують колізії, що відбуваються під час передачі преамбули.

• Пізня колізія (Late Collision). Це колізія, яка відбувається після передачі перших 64 байт кадру (за протоколом Ethernet колізія повинна виявлятися під час передачі перших 64 байт кадру). Результатом пізньої колізії буде кадр, який має довжину понад 64 байт та містить неправильне значення контрольної суми. Найчастіше це вказує на те, що мережевий адаптер, що є джерелом конфлікту, не може правильно прослуховувати лінію і тому не може вчасно зупинити передачу. Іншою причиною пізньої колізії є занадто велика довжина кабельної системи або занадто велика кількість проміжних повторювачів, що призводить до перевищення максимального часу подвійного обороту сигналу.

Середня інтенсивність колізій у нормально працюючій мережі має бути меншою за 5%. Великі сплески (понад 20%) можуть бути індикатором кабельних проблем.

● Розподіл використовуваних мережевих протоколів

Ця статистична група належить до протоколів мережного рівня. На дисплеї відображається список основних протоколів у спадному порядку щодо відсоткового співвідношення кадрів, що містять пакети даного протоколу до загальної кількості кадрів у мережі.

● Основні відправники (Top Sendes)

Функція дозволяє відстежувати найбільш активні передавальні вузли локальної мережі. Прилад можна налаштувати на фільтрацію за єдиною адресою та виявити список основних відправників кадрів для цієї станції. Дані відображаються на дисплеї у вигляді діаграми разом із переліком основних відправників кадрів.

● Основні одержувачі (Top Receivers)

Функція дозволяє стежити за найактивнішими вузлами-одержувачами мережі. Інформація відображається у вигляді, аналогічному наведеному вище.

● Основні генератори широкомовного трафіку (Top Broadcasters)

Функція виявляє станції мережі, які найбільше генерують кадри з широкомовними і груповими адресами.

● Генерування трафіку (Traffic Generation)

Прилад може генерувати трафік для перевірки роботи мережі за підвищеного навантаження. Трафік може генеруватися паралельно з активізованими функціями Мережева статистика, Статистика помилкових кадрів та Статистика колізій.

Користувач може встановити параметри генерованого трафіку, такі як інтенсивність і розмір кадрів. Для тестування мостів і маршрутизаторів прилад може автоматично створювати заголовки IP-і IPX-пакетів, і все, що потрібно від оператора, - це внести адреси джерела та призначення.

В ході випробувань користувач може збільшити на ходу розмір і частоту проходження кадрів за допомогою клавіш керування курсором. Це особливо цінно під час пошуку джерела проблем продуктивності мережі та умов виникнення відмов.

Функції аналізу протоколів

Зазвичай портативні багатофункціональні прилади підтримують декодування та аналіз лише основних протоколів локальних мереж, таких як протоколи стеків TCP/IP, Novell NetWare, NetBIOS та Banyan VINES.

У деяких багатофункціональних приладах відсутня можливість декодування захоплених пакетів, як у аналізаторах протоколів, а натомість збирається статистика про найбільш важливі пакети, що свідчать про наявність проблем у мережах. Наприклад, при аналізі протоколів стека TCP/IP збирається статистика пакетів протоколу ICMP, з допомогою якого маршрутизатори повідомляють кінцевим вузлам про виникнення різноманітних помилок. Для ручної перевірки досяжності вузлів мережі в прилади включається підтримка утиліти IP Ping, а також аналогічних утиліт NetWare Ping і NetBIOS Ping.

Так як перевантаження процесорів портів та інших обробних елементів комутатора можуть призводити до втрат кадрів, то функція спостереження за розподілом трафіку в мережі, побудованої на основі комутаторів, є дуже важливою.

Однак якщо сам комутатор не забезпечений вбудованим агентом SNMP для кожного свого порту, то завдання стеження за трафіком, що традиційно вирішується в мережах з середовищами, що розділяються за допомогою установки в мережу зовнішнього аналізатора протоколів, дуже ускладнюється.

Зазвичай у традиційних мережах аналізатор протоколів або багатофункціональний прилад підключався до вільного порту концентратора, що дозволяло йому спостерігати за трафіком, що передається між будь-якими вузлами мережі.

Якщо ж аналізатор протоколу підключити до вільного порту комутатора, він не зафіксує майже нічого, т.к. кадри йому передавати ніхто не буде, а чужі кадри до його порту також прямувати не будуть. Єдиний вид трафіку, який фіксуватиме аналізатор, - це трафік широкомовних пакетів, які передаватимуться всім вузлам мережі, а також трафік кадрів з невідомими комутатору адресами призначення. У випадку коли мережа розділена на віртуальні мережі, аналізатор протоколів фіксуватиме лише широкомовний трафік своєї віртуальної мережі, щоб аналізаторами протоколів можна було як і раніше користуватися і в мережах, що комутуються, виробники комутаторів забезпечують свої пристрої функцією дзеркального відображення трафіку будь-якого порту на спеціальний. До спеціального порту підключається аналізатор протоколів,

Наявність функції дзеркалізації портів частково знімає проблему, але залишає деякі питання. Наприклад, як переглядати одночасно трафік двох портів або трафік порту, що працює у повнодуплексному режимі.

Більш надійним способом стеження трафіком, що проходить через порти комутатора, є заміна аналізатора протоколу на агенти RMON MIB для кожного порту комутатора.

Агент RMON виконує всі функції хорошого аналізатора протоколу для протоколів Ethernet і Token Ring, збираючи детальну інформацію про інтенсивність трафіку, різні типи поганих кадрів, про втрачені кадри, причому самостійно будуючи часові ряди для кожного параметра, що фіксується. Крім

того, агент RMON може самостійно будувати матриці перехресного трафіку між вузлами мережі, які потрібні для аналізу ефективності застосування комутатора.

Так як агент RMON, що реалізує всі 9 груп об'єктів Ethernet, коштує дуже дорого, то виробники зниження вартості комутатора часто реалізують тільки перші кілька груп об'єктів RMON MIB. Іншим прийомом зниження вартості комутатора є використання одного агента RMON для кількох портів. Такий агент по черзі підключається до потрібного порту, дозволяючи зняти необхідні статистичні дані.

Управління віртуальними мережами

Віртуальні локальні мережі VLAN породжують проблеми для традиційних систем керування на платформі SNMP як під час їх створення, і під час спостереження над їх роботою.

Як правило, для створення віртуальних мереж потрібне спеціальне програмне забезпечення компанії-виробника, яке працює на платформі системи управління, наприклад HP Open View. Самі платформи систем управління цей процес підтримати що неспроможні переважно через тривалої відсутності стандарту на віртуальні мережі. Можна сподіватися, що поява стандарту 802.1Q змінить ситуацію у цій галузі.

Спостереження за роботою віртуальних мереж створює проблеми для традиційних систем управління. Під час створення карти мережі, що включає віртуальні мережі, необхідно відображати як фізичну структуру мережі, так і її логічну структуру, що відповідає зв'язкам окремих вузлів віртуальної мережі. При цьому за бажанням адміністратора система управління повинна вміти відображати відповідність логічних та фізичних зв'язків у мережі, тобто. на одному фізичному каналі повинні відображатися всі або окремі шляхи віртуальних мереж.

На жаль, багато систем управління або взагалі не відображають віртуальні мережі, або роблять це дуже незручним для користувача способом, що змушує звертатися до менеджерів компаній-виробників для вирішення цього завдання.

Діапазонний вектор (*range vector*) – це вектор, який зберігає діапазон значень метрики за певний час.Він потрібний, коли цього вимагає арифметика запиту. Найпростіше пояснити на графіку функції *avg_over_time*від чогось. У кожний момент часу система (рис. 3.11) обчислюватиме усереднене значення метрики за попередні *X* хвилин (секунд, годин).

Рис. 3.11. Вікно відображення результатів опитування стану сервера розробленим модулем

3.3. Реалізація модулів збору метрик

Комплексна система моніторингу та контролю обладнання, техпроцесів та персоналу закриває наявну прогалину в системах, здатних забезпечити ефективність роботи промислових об'єктів та безпеку задіяного на них виробничого персоналу в рамках єдиного рішення.

Використовуваний у системі принцип інтерактивної взаємодії зі співробітником під час виконання ним виробничих завдань та операцій забезпечує повноцінну інформаційну інтеграцію діяльності персоналу з роботою виробничого устаткування й інфраструктури у межах єдиного інформаційного простору – невід'ємною складовою цифрового підприємства.

Практика застосування рішення в реальних умовах показує підвищення продуктивності, зниження середнього часу відновлення при порушеннях технологічного процесу, а також створення умов для запобігання аваріям, інцидентам, виробничому травматизму.

Рішення затребуване як у промисловості, так і на об'єктах інфраструктури, сільському господарстві, будівництві, логістиці, медицині та інших галузях.

Відстеживши сумарний час виконання кожного завдання та частоту, з якою змінюється метрика, ми дізнаємося, скільки витрачено робочого часу. Якщо за відрізок 15 сек. цифра зросла на 15, це має на увазі 1 зайнятий обробник (по секунді на кожну минулу секунду), тоді як збільшення на 30 має на увазі 2 обробники і т.д.

Графік робочої активності під час інциденту покаже, з чим ми зіткнулися. Результати невтішні; час інциденту (16:02–16:04) відзначений лінією тривожного (в масть) червоного кольору:

Рис. 3.12. Активність оброблювача під час інциденту

Крива активності опинилася в самому низу якраз під час інциденту. Це час роботи з веб-хуками, на якій у нас зайнято 20 виділених обробників. З логів, що всі вони були при ділі, і я чекав, що крива буде приблизно на рівні 0 сек. Судячи з графіка, 20 однопотокових обробників витратило 45 сек. на кожну секунду діяльності, але це неможливо?

Графік інциденту приховує робочу активність і водночас показує зайве - дивлячись. Щоб з'ясувати, чому так відбувається, потрібно взяти до уваги

реалізацію відстеження метриків і як вона взаємодіє з *Prometheus*, що збирає метрики.

На рис. 3.13 відображено графіки, що відображають робочу активність; протяжністю до 0,1 с, на рис. 3.15 – протяжністю до 15 с, на рис. 3.16 – протяжністю до 30 с.

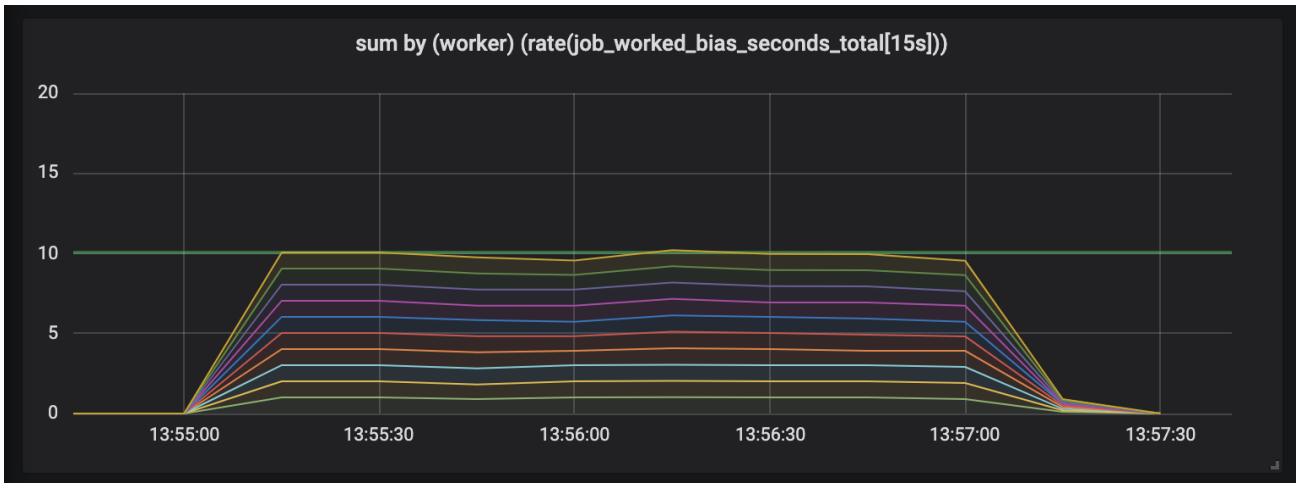

Рис. 3.14. Результати експерименту, що відображають робочу активність протяжністю до 0,1 с

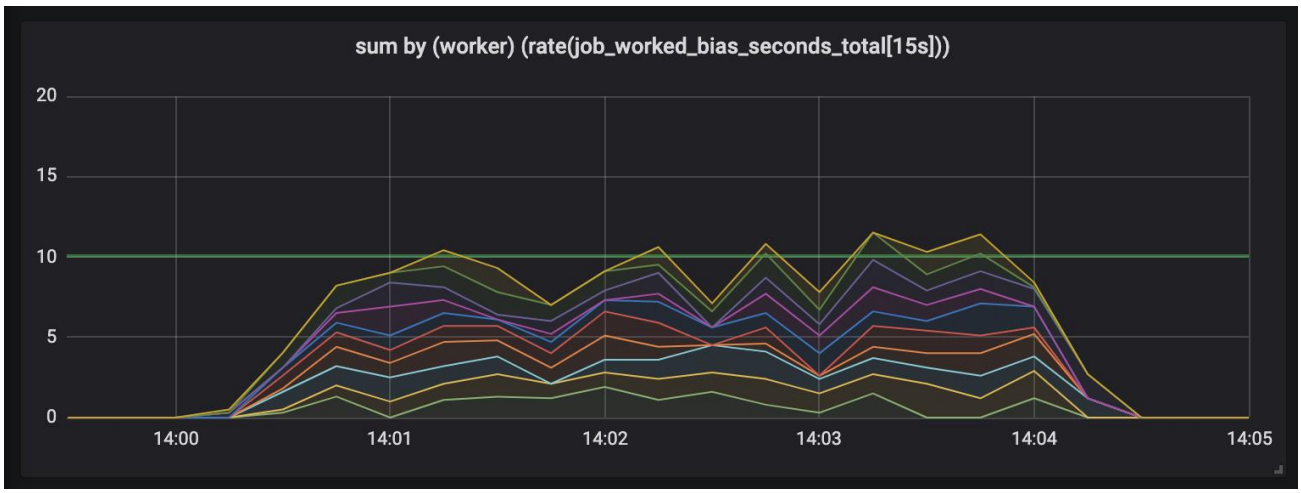

Рис. 3.15. Результати експерименту, що відображають робочу активність протяжністю до 15 с

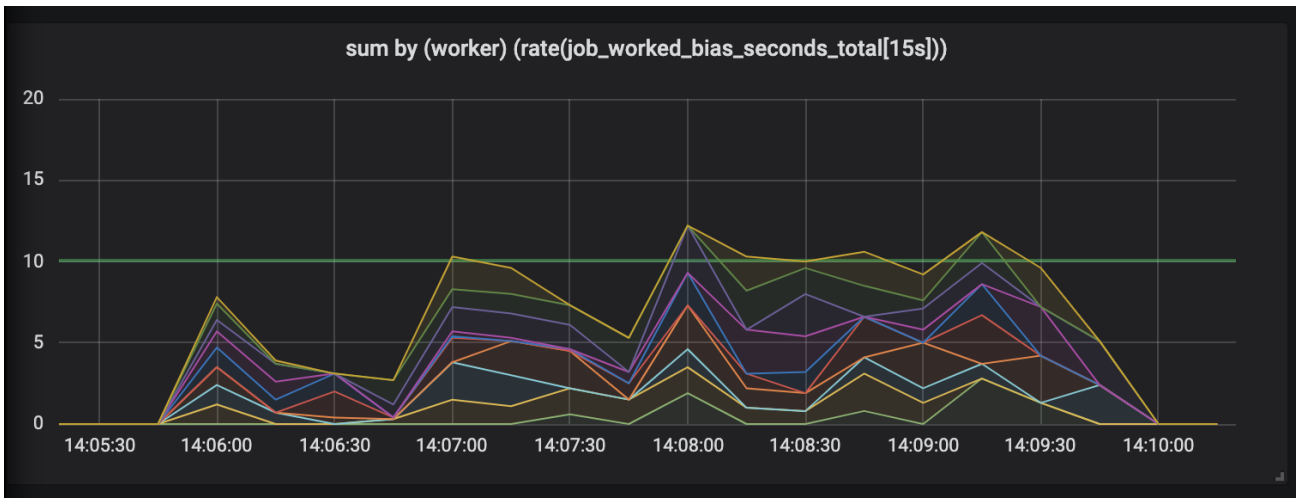

Рис. 3.16. Результати експерименту, що відображають робочу активність протяжністю до 30 с

Безперервно зростає кількість пристроїв, що підключаються до різних джерел інформації. Оскільки користувачі вкрай зацікавлені в постійній доступності мережевих додатків та їх високій продуктивності, IT-організації повинні розгортати масштабовані системи мережевого моніторингу, що дозволяють усувати безконтрольні (мертві) зони в мережі, де потай зароджуються мережеві проблеми, що загрожують зменшенням доходу підприємства та зниженням.

Існує чимало критично важливих сервісів та додатків, які, працюючи в режимі реального часу, потребують своєчасної доставки пакетів даних по мережі. До них відносяться:

- інтерактивні комунікаційні послуги, включаючи послуги Voice over IP (VoIP), Voice over LTE (VoLTE), відеоконференцзв'язку, відеочату та віртуальних нарад;
- мережеві фінансові послуги (для надання брокерських та банківських послуг);
- послуги з урахуванням технології Audio/Video Bridging (AVB);
- системи промислової автоматизації та Smart Grid;
- послуги синхронізації з урахуванням протоколу Precision Time Protocol (PTP).

Тимчасові мітки можуть бути додані при інкапсуляції пакету, як це передбачено у поширеному форматі PCAP, який використовується для захоплення мережевого трафіку. У цьому випадку тимчасова мітка є частиною зовнішнього заголовка, що інкапсулює пакет, і показує момент часу, в який пакет надійшов в інтерфейс, що інкапсулює. Зазвичай цей тип міток має формат часу ери Unix, який є числом секунд, що минули з моменту початку ери Unix, — з 1 січня 1970 року.

Тимчасові мітки протоколів

Тимчасові мітки можуть вставлятися в незмінну структуру пакета, наприклад, у зарезервовані поля пакетів таких протоколів, як Precision Time Protocol (PTP) і Network Time Protocol (NTP). У цьому випадку мітка зазвичай показує час, коли пакет був відправлений.

Дані тимчасові мітки зазвичай містять поля секунд і часток секунд, підрахованих, як і попередньому випадку, від початку ери Unix.

Фірмові тимчасові мітки

Існують і інші методи додавання та генерації тимчасових міток, що виконуються різними типами обладнання, включаючи комутатори та NPB. Реалізації міток можуть бути різними і, враховуючи, що вони фірмові, важливо розуміти суть методу додавання міток, що використовується, і можливі побічні ефекти його застосування.

Ключовий кадр та лічильник

Існує ряд фірмових тимчасових міток, яких приєднують до кінця пакета, утворюючи його трейлер (кінцевик). Ці мітки містять чисельні значення синхронізованого лічильника. Тактова частота лічильника залежить від його реалізації і може становити, наприклад, 200 МГц, що відповідає 5 нс кожного відліку. Періодично лічильник переповнюється, і тоді генерується ключовий кадр, що містить тимчасову мітку реального часу, яка може використовуватися спільно зі значенням лічильника в кінці кожного чергового пакета для визначення його реального часу.

При такому методі генерації та додавання тимчасових міток, як правило, тимчасова мітка приєднується до пакета в момент виходу з комутатора або NPB, а не в момент його входу в цей пристрій. З цієї причини ця тимчасова мітка не може позначати точний час надходження пакета в відгалужувач, який використовується для доступу до контрольованого мережного трафіку. Для визначення цього часу має бути зроблено певну поправку на затримку проходження пакета через комутатор. У деяких випадках можуть використовуватися комутатори без буферизації пакетів (cut-through), що забезпечують відносно постійну затримку, яка може бути врахована у тимчасовій мітці для позначення часу надходження пакета у відгалужувач.

Достоїнство методу, що передбачає використання ключового кадру, полягає в тому, що розмір тимчасової мітки (кінцевика) може бути дуже маленьким, оскільки ця мітка є результатом відліку часу від моменту створення останнього ключового кадру. При використанні згаданого вище 5-наносекундного лічильника чотирибайтовий кінцевик переповнюватиметься кожні 24,5 с і з такою ж періодичністю створюватимуться ключові кадри. Оскільки тимчасові мітки невеликі, з їхньої генерацію витрачається набагато менше процесорних ресурсів, ніж генерацію повних тимчасових міток форматі часу ери Unix. Ще одна перевага даного методу полягає в тому, що при невеликих тимчасових мітках створюються невеликі накладні витрати на передачу потоку даних.

Кінцевик у вигляді повної тимчасової мітки

У деяких методах до кінця кожного пакета приєднується тимчасова мітка, що показує реальний час даного пакета по відношенню до деякого фіксованого моменту часу, яким може бути початок ери Unix (1 січня 1970). У цих кінцевиках зазвичай міститься інформація про кількість секунд і часток секунди, наприклад наносекунд. Для секунд і числа наносекунд потрібні два поля даних довжиною 32 біта кожне. Великою перевагою даного підходу є те, що кожен пакет має власну унікальну повну тимчасову мітку, що спрощує використання тимчасових міток.

Оскільки (порівняно з методом, у якому використовуються ключові кадри) для кожного пакета потрібно підраховувати значно більші числа, для забезпечення кожного пакета міткою у форматі часу ери Unix на повній лінійній швидкості може знадобитися потужніший центральний процесор і в цілому більш високопродуктивний NPB.

В окремих методах, що передбачають використання кінцевиків у вигляді повної тимчасової мітки, забезпечується найвища точність цих міток шляхом їх генерації при надходженні пакетів NPB. У цьому випадку будь-яка тимчасова затримка, пов'язана з обробкою пакета та його пересиланням між мережевим портом NPB та портом засобу моніторингу, не внесе помилку у тимчасову мітку. Це найточніший варіант додавання тимчасових міток, що реалізується у високопродуктивних NPB.

Термінологія

Деякі терміни, що використовуються для передачі інформації про час пакетних мереж, мають специфічні значення, які можуть сильно відрізнятися від загальновживаних значень даних слів. Це може створювати плутанину під час обговорення технологій та пристроїв, що створюють тимчасові позначки.

У звичайних розмовах терміни accuracy (точність), precision (розкид) і resolution (дозвіл) можуть використовуватися один замість іншого (як синоніми), але в області передачі інформації про час через мережу вони мають різні значення. Вкрай важливо прояснити значення цих термінів, оскільки вони безпосередньо впливають можливості застосування будь-яких рішень, здійснюють контроль тимчасових параметрів передачі пакетів.

Поняття точності та розкиду тимчасових міток

Точність

Під точністю тимчасових міток, що генеруються NPB, розуміється максимальна розбіжність між будь-якою тимчасовою міткою і стандартним часом, наприклад всесвітнім координованим часом (Universal Time Coordinated, UTC). Вимірювати точність тимчасових міток, що генеруються NPB, може бути

дуже непросто, оскільки для цього потрібно знати час передачі пакетів, точність міток яких вимірюється за шкалою часу UTC. Не існує практичних способів оцінки точності тимчасових міток у розгорнутій інфраструктурі моніторингу, тому доводиться довіряти точнісним параметрам, зазначеним у специфікаціях на засоби контролю трафіку.

Розкид

Під розкидом тимчасових міток, що генеруються NPB, розуміється максимальна відмінність їх точності. Наприклад, якщо жодна тимчасова мітка, що генерується NPB, не відрізняється від часу UTC більш ніж на 1 мкс, їх точність становить 1 мкс. Але якщо точності всіх тимчасових міток знаходяться в межах 200 нс одна від одної, їх розкид становить 200 нс. Для вимірювання розкиду міток, що генеруються NPB, потрібні такі ж складні тестові процедури та спеціалізовані пристрої, які використовуються для вимірювання точності.

Роздільна здатність — це мінімальний часовий інтервал між пакетами, який NPB може виміряти. Зазвичай в NPB для постачання пакетів тимчасовими мітками використовується який-небудь генератор або лічильник, що задає, а дозвіл залежить від цього генератора або лічильника. Наприклад, якщо використовується генератор частотою 200 МГц, він видає тактовий імпульс кожні 5 нс. Отже, мінімальна роздільна здатність становить 5 нс. Однак генератор інтерфейсу 10GE, що задає, працює на частоті 156,25 МГц. Це означає, що початок кожного пакету знаходиться на межі часового інтервалу тривалістю 6,4 нс. NPB з 5-наносекундним лічильником при отриманні пакета повинен округлити цикл тривалістю 6,4 нс до наступного 5-наносекундного відліку.

Під час синхронізації часу в мережевому устаткуванні мається на увазі прив'язка внутрішньої шкали часу пристрою до стандартної шкали, наприклад до UTC. Така синхронізація забезпечується протоколами NTP і PTP, а система GPS є глобальним джерелом синхросигналів. Існує і таке поняття, як синтонізація (частотна синхронізація), що означає процес точного підстроювання частоти одного генератора до частоти іншого (наприклад, опорного) генератора. Синтонізація необхідна для порівняння тимчасових міток,

отриманих з різних джерел, або при вимірюванні відносного часу, наприклад, часу затримки передачі пакетів. Щоб гарантувати високу точність і малий розкид тимчасових міток, потрібно забезпечувати як синхронізацію, так і синтонізацію.

Існує безліч джерел часу, які можуть бути підключені до NPB для створення часових міток.

Локальний годинник реального часу та генератор

У більшості сучасних мережевих пристроїв є апаратний годинник реального часу, що встановлюється або на заводі, або користувачем вручну, після чого відлік часу здійснюється за допомогою локального генератора. Якість тимчасової синхронізації залежить від використовуваного методу встановлення локального годинника, а точність синтонізації - від типу і якості локального генератора.

Наприклад, деякий пристрій може бути оснащений годинником реального часу, встановленим на заводі з використанням протоколу NTP з точністю до 10 мс щодо UTC, і генератором Stratum 3 з точністю 4,6 ppm, що означає додавання помилки в 4,6 мкс на кожній секунді. . Тимчасові мітки, що генеруються з використанням такого обладнання, матимуть малий розкид, але нестабільну точність, яка погіршуватиметься приблизно на 3 с на тиждень.

Один імпульс на секунду (1PPS)

Одним із методів синхронізації часу в мережевому обладнанні є використання опорного сигналу 1PPS, що являє собою послідовність імпульсів, що передаються з періодом 1 с і прив'язаних до шкали часу UTC. Якщо годинник реального часу встановити з точністю ±0,5 з відносно UTC, а потім синхронізувати його за допомогою сигналу 1PPS, може бути досягнуто дуже хороша часова синхронізація, потрібна для забезпечення високої точності часових міток. У періоди між імпульсами 1PPS субсекундні значення часу будуть відраховуватись за допомогою високочастотного генератора, що визначає розкид тимчасових міток. Таким чином, сигнал 1PPS слід використовувати разом із високостабільним генератором.

Глобальна навігаційна супутникова система GPS

Будучи оснащеним атомним годинником, супутники системи GPS передають дуже точний час. Сигнали цих супутників можуть прийматися приймачами GPS, вбудованими в мережеве обладнання. При роботі з відповідним генератором та оптимальною конструкцією мережевого пристрою приймач GPS, виступаючи в ролі джерела часу, може забезпечити точність 100-200 нс щодо UTC.

Протокол Precision Time Protocol (PTP)

Протокол PTP, також званий протоколом IEEE1588 (або просто 1588), спеціально розроблений для синхронізації мережних пристроїв пакетної мережі. Цей протокол все ширше застосовується в центрах обробки даних, оскільки порівняно з протоколом NTP забезпечує більш високу точність тимчасової синхронізації. До того ж, для використання PTP не потрібні ніякі антени або спеціальні кабелі, які потрібні для синхронізації від приймача GPS або сигналу 1PPS. Протокол PTP може працювати за звичайною мережевою інфраструктурою. Досяжна точність тимчасової синхронізації за протоколом PTP майже повністю залежить від архітектури мережі, за якою працює цей протокол, та інтенсивності мережного трафіку. За певних умов PTP може забезпечити точність синхронізації ±1 мкс щодо UTC (приблизно у 10 разів гірше, ніж при синхронізації від приймача GPS).

Протокол Network Time Protocol (NTP)

Використання протоколу NTP — це класичний спосіб синхронізації часу на мережевих комп'ютерних пристроях. Він широко застосовується у всьому Інтернеті. Протокол NTP забезпечує точність тимчасової синхронізації десятків мілісекунд, чого може цілком вистачити, наприклад, для реєстрації системних подій. Але зазвичай такої точності мало для моніторингу чутливих до тимчасових затримок мережевих послуг і додатків.

Це класичний показник роботи мережі, для визначення якого (за базовою методикою) використовують дві тимчасові мітки, приєднані до того самого переданого пакету в двох різних точках мережі. Зіставляючи ці мітки, можна контролювати тимчасову затримку на маршруті проходження пакета.

Для нормальної роботи багатьох мережевих сервісів та програм потрібна низька тимчасова затримка передачі їх трафіку. Моніторинг тимчасової затримки передачі трафіку цих сервісів та додатків має велике значення для забезпечення необхідних рівнів QoE та виконання SLA, а також для виявлення тенденцій, які можуть призвести до погіршення роботи мережі або виходу її з ладу.

Приклад контрольованої мережної інфраструктури

Оскільки для вимірювання тимчасової затримки потрібно контролювати щонайменше дві точки мережі, слід використовувати більше одного NPB для генерації тимчасових міток у кожній із контрольованих точок. Щоб виконувати ці вимірювання, необхідно забезпечити тимчасову синхронізацію. Також велике значення має висока точність тимчасових міток щодо UTC. Для моніторингу тимчасової затримки найкращим методом постачання пакетів тимчасовими мітками є приєднання повної тимчасової мітки до кінця кожного пакета. Тобто тимчасова мітка в кожному пакеті повинна містити всю інформацію, необхідну визначення тимчасової затримки, щоб не потрібно було використовувати ключовий кадр.

Точність і розкид тимчасових міток, необхідні моніторингу тимчасової затримки у мережі, залежить від вимог додатків і засобів моніторингу.

- VoIP та VoLTE. Для забезпечення якісного двостороннього голосового зв'язку, голосові програми потребують невеликої тимчасової затримки передачі їх трафіку. Наприклад, у рекомендації MCE-T G.114 говориться, що прийнятною (для голосового зв'язку) є тимчасова затримка трохи більше 150 мс у кожному напрямі. Можливо, потрібно буде проводити моніторинг різних мережевих сегментів з метою визначення вкладу кожного з них у загальну тимчасову затримку. Справа в тому, що зазначене вище граничне значення тимчасової затримки стосується всього маршруту передачі голосового трафіку, куди можуть входити канали Інтернету та мобільної мережі.

• відео-конференц-зв'язок, відеочат та віртуальні наради. Оскільки державні організації та приватні компанії продовжують розвивати взаємодію між своїми територіально розподіленими підрозділами, а індивідуальні користувачі все ширше застосовують послуги відеоконференцзв'язку та відеочату для особистого спілкування, обсяги мережевого трафіку, для передачі якого потрібна невелика тимчасова затримка, зростатимуть. Для підтримки високої ефективності цих сервісів потрібно контролювати наскрізну затримку передачі їх трафіку, яка не повинна перевищувати 300 мс. Моніторинг мережевих сегментів з метою контролю затримки передачі відеотрафіку, що вноситься ними, дозволить виявляти перші ознаки можливих мережевих проблем.

• Передача ринкових даних як реального часу. Багато автоматизованих банківських і фінансових систем потребують своєчасної доставки ринкових даних та іншої інформації, здатної вплинути на ситуацію на ринку. У роботі таких систем важлива кожна мікросекунда. Існують спеціальні засоби контролю всіх аспектів впливу тимчасових затримок працювати мережевих трейдингових систем. Для максимальної ефективності цих коштів дуже важливо передавати їм пакети даних, забезпечені тимчасовими мітками з точністю до часток мікросекунди.

• Високочастотна торгівля. За останні кілька років високочастотна торгівля стала однією з найгарячіших тем у сфері чутливих до тимчасової затримки додатків. Для систем високочастотної торгівлі час затримки та забезпечення тимчасової синхронізації мають однаково велике значення. Тому для постійного контролю затримки передачі трейдингових даних та тимчасової синхронізації необхідні NPB, що забезпечують субмікросекундну точність тимчасових міток.

Пакети, кадри, бітова швидкість

Для нормальної роботи певних програм потрібно сталість бітової швидкості чи швидкості передачі пакетів. Постачальники мережевих послуг та контент-провайдери все більше зацікавлені у забезпеченні високої якості своїх

потокових сервісів, включаючи «відео на вимогу», для утримання наявних користувачів та збереження доходів. Моніторинг бітової швидкості або швидкості передачі пакетів реалізується шляхом додавання до них точних тимчасових міток апаратурі системи моніторингу, включаючи NPB.

Тимчасова синхронізація дуже важлива для нормальної роботи певних мереж та додатків. Для моніторингу тимчасової синхронізації потрібно, щоб NPB додавали до контрольованих даних високоточні тимчасові мітки.

- Мережі мобільного зв'язку потребують тимчасової синхронізації (це особливо вірно щодо TDM-мереж та рішень VoLTE) для виконання операцій хендовера, забезпечення ефективного використання спектра та підвищення пропускної спроможності. Все це сприяє утриманню користувачів та наданню якісних послуг. Для забезпечення належного рівня якості послуг мобільного зв'язку велике значення має контроль тимчасових міток (у трафіку), що згенеровані з наносекундною точністю.
- Системи промислової автоматизації також потребують тимчасової синхронізації, яка зазвичай забезпечується за допомогою технологій GPS, PTP та IRIG-B. Моніторинг тимчасової синхронізації на мікросекундному рівні необхідний для забезпечення надійної роботи синхронізованих мереж Ethernet автоматизації.
- Технології Smart Grid та Power Delivery є рішеннями наступного покоління з управління мережами електропостачання та електроенергетичними системами. Оператори енергосистем використовують пристрої GPS і PTP для точної синхронізації засобів виробництва електроенергії та навантажень користувача з метою ефективного застосування наявних енергоресурсів там, де вони потрібні найбільше. Для моніторингу синхронізації мереж електропостачання контрольовані пакети мають бути забезпечені субмікросекундними часовими мітками.
- У рішеннях на базі технології AVB для синхронізації аудіо- та відеопристроїв через мережу використовується протокол PTP. Щоб

контролювати ефективність синхронізації пристроїв AVB, брокери мережних пакетів повинні постачати їх субмікросекундними мітками.

• Концепція Інтернету речей передбачає мережне підключення різноманітних пристроїв, багатьом із яких потрібна синхронізація у реальному масштабі часу. У світі підключених пристроїв контроль тимчасової синхронізації в рамках Інтернету речей стане важливою складовою мережевого моніторингу. Для реалізації такого контролю будуть потрібні субмікросекундні тимчасові мітки, що генеруються NPB.

Багато сучасних систем мережевого моніторингу надають статистичні дані щодо пропускної спроможності мережі, але без тимчасової синхронізації та постачання пакетів точними тимчасовими мітками при розрахунках пропускної здатності може накопичуватися похибка. При необхідності точного виділення пропускної спроможності, що характерно для мереж мобільного зв'язку та програмно-визначуваних мереж (SDN), ця обчислювальна похибка може знизити ефективність розподілу мережевих ресурсів. Субмікросекундні часові мітки, що генеруються NPB, забезпечать необхідну точність розрахунків споживання пропускної спроможності мережі.

Події

Значення багатьох подій, що відбуваються в мережі, залежить від часу, тому моніторингове обладнання повинно мати можливість точно інформувати про час подій. Ця можливість дозволяє встановити кореляцію між підлягаючими контролю захопленими пакетами та накопиченими в syslog повідомленнями про події. Як правило, моніторинг подій здійснюється з мілісекундною роздільною здатністю в реальному масштабі часу, для синхронізації з UTC використовується протокол NTP. Тому тимчасові мітки, які NPB додає до пакетів, що відносяться до подій, що цікавлять, повинні мати мілісекундну точність при субмілісекундному розкиді.

Деяким програмам необхідно, щоб пакети приймалися правильно. Тому рекомендується проводити моніторинг або захоплення мережевого трафіку для аналізу порядку проходження пакетів.

У системах моніторингу, де має місце перепідписування портів засобів моніторингу, або відбувається агрегація потоків трафіку за схемою N:M, можуть бути сплески трафіку (bursts), що не ідентифікуються засобами моніторингу через агрегацію потоків трафіку. Субмікросекундні тимчасові мітки, що генеруються NPB на вхідних портах, дозволять контролювати сплески трафіку, проводити детальний аналіз порядку проходження пакетів у захопленому трафіку та аналізувати завантаження портів.

Висновки до розділу

В ефективних інфраструктурах моніторингу можуть використовуватися різні пристрої доступу до контрольованого трафіку, включаючи фізичні та віртуальні відгалужувачі, агрегатори трафіку та брокери мережевих пакетів (Network Packet Brokers, NPB), що направляють дані контролю, що підлягають контролю моніторингу.

Перед аналізом засобів та методів моніторингу мережевих ресурсів, чутливих до тимчасових затримок, важливо розглянути основні положення та концепції, що стосуються передачі інформації про час пакетної мережі.

Загальне правило таке: будь-якому аналізу тимчасових співвідношень лише на рівні пакетів має передувати додавання до них тимчасових міток. Існує безліч методів генерації цих міток. Також тимчасові мітки можуть пересилатися у різних форматах.

Розроблена система надає широкий спектр функціоналу для моніторингових пристроїв та систем, що забезпечують мережеві пакети точними тимчасовими мітками. Характерна для високопродуктивних моделей NPB можливість прикріплення до відстежуваних пакетів точних тимчасових міток потрібна для виконання ряду важливих контрольних функцій, включаючи моніторинг затримки передачі трафіку, швидкості передачі пакетів та тимчасової синхронізації обладнання.

ВИСНОВКИ

В даній дипломній роботі було досліджено актуальність розробки комп’ютерних систем для моніторингу для комерційних компаній.

Архітектура розробленої системи моніторингу сприяє покращенню функціонування мереж, забезпечуючи:

Повний контроль мережевого трафіку - брокери мережевих пакетів компанії Ixia постійно направляють всі дані, що цікавлять потрібним засобам моніторингу, перевіряючи трафік на відповідність відразу декільком критеріям фільтрації, що дозволяє уникнути непотрібного відкидання пакетів через конфлікт з накладенням фільтрів.

Автоматизоване реагування - моментальне перемикання трафіку на пристрій моніторингу при виявленні підозрілих дій у мережі, що дозволяє заощадити витрати часу та грошей, пов'язані із залученням людини до процесів усунення мережевих проблем.

Балансування навантаження — розподіл контрольованого трафіку по кількох аналізаторах для повного використання мережевої смуги пропускання та підвищення ефективності застосування пристроїв моніторингу навіть у тих випадках, коли їхня продуктивність нижча за пропускну здатність мережевих каналів.

Гнучкі фільтрації та дедуплікації, які покращують функціонування пристроїв моніторингу, позбавляючи їх від аналізу непотрібних даних.

Простоту використання - брокери мережевих пакетів компанії Ixia мають дружній до користувача інтерфейс з функцією перетягування екранних об'єктів, що дозволяє легко підключати пристрої моніторингу до потрібних SPAN-портів та портів відгалужувачів за допомогою миші.

Завдання мережевих з'єднань і фільтрів за допомогою інтуїтивно зрозумілого графічного інтерфейсу користувача, що дозволяє організовувати агрегування, фільтрацію і розподіл мережевого трафіку по пристроях моніторингу лише кількома клацаннями мишею і майже повністю усунути фізичну перекомутацію портів обладнання.

Обмеження доступу до певних фільтрів, портів або пристроїв моніторингу (для виконання регуляторних вимог) за допомогою покращених функцій контролю доступу.

Можливість контролю важливої SNMP-статистики, що збирається у всіх брокерах Vision, за допомогою будь-якої системи управління мережею, яка може надавати інформацію, наприклад, про обсяги трафіку, отриманого кожним пристроєм моніторингу, та негайно сповіщати про перевантажені пристрої моніторингу.

Простий доступ до всіх брокерів Vision з використанням адрес IPv4 або IPv6, що допомагає відповідати зростаючим потребам організацій в IP-адресах.

Технологічні переваги розробленої система моніторингу

- Автоматичне визначення, декодування та аналіз трафіку у високонавантажених мережах.
- Автоматична індексація зібраних даних, що забезпечує швидкий пошук за ключовими метриками.
- Моніторинг продуктивності бізнес-транзакцій по всій мережі на основі аналізу трафіку.
- Автоматична кореляція подій у мережі з часом відгуку програм.
- Швидка локалізація проблем у роботі розподілених програм.
- Відсутність додаткових затримок у контрольованих каналах.
- Видача звітів та оповіщень про швидкість виконання бізнес-транзакцій у режимі реального часу.

У відповідь на потреби у контролі функціонування сервісів та додатків, чутливих до тимчасових затримок, інноваційні компанії випускають спеціалізовані засоби для моніторингу трафіку цих сервісів та додатків. Багато з таких засобів можуть бути задіяні в системі мережевого моніторингу, але успішність їх роботи залежить від точності тимчасових міток, що додаються до контрольованих пакетів даних. В ефективних інфраструктурах моніторингу можуть використовуватися різні пристрої доступу до контрольованого трафіку, включаючи фізичні та віртуальні відгалужувачі, агрегатори трафіку та брокери мережевих пакетів (Network Packet Brokers, NPB), що направляють дані контролю, що підлягають контролю моніторингу.

Перед аналізом засобів та методів моніторингу мережевих ресурсів, чутливих до тимчасових затримок, важливо розглянути основні положення та концепції, що стосуються передачі інформації про час пакетної мережі.

Загальне правило таке: будь-якому аналізу тимчасових співвідношень лише на рівні пакетів має передувати додавання до них тимчасових міток. Існує безліч методів генерації цих міток. Також тимчасові мітки можуть пересилатися у різних форматах.

Розроблена система надає широкий спектр функціоналу для моніторингових пристроїв та систем, що забезпечують мережеві пакети точними тимчасовими мітками. Характерна для високопродуктивних моделей NPB можливість прикріплення до відстежуваних пакетів точних тимчасових міток потрібна для виконання ряду важливих контрольних функцій, включаючи моніторинг затримки передачі трафіку, швидкості передачі пакетів та тимчасової синхронізації обладнання.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Zambonelli, F., Jennings, N., Wooldridge, M.*: *Developing multiagent systems*: *the Gaia methodology*. *ACM Transactions on Software Engineering and Methodology* 12(3) (2013) 317–370.

2. *Loash, S.A. Engineering organization-based multi-agent systems*. *SELMAS*. *Volume* 3914 *of Lecture Notes in Computer Science*., *Springer* (2015) 109–125.

3. *Bresciani, P., Giorgini, P., Giunchiglia, F., Mylopoulos, J., Perini, A.*: *Tropos*: *An agentoriented software development methodology*. *Journal of Autonomous Agents and MultiAgent Systems* 8 (2014) 203–236.

4. *Padgham, L., Winikoff, M.*: *Developing Intelligent Agent Systems*: *A Practical Guide*. *John Wiley and Sons, Chichester, UK* (2014) *ISBN* 0-470-86120-7. 5. *Cossentino, M.*: *From requirements to code with the PASSI methodology*. *In HendersonSellers, B., Giorgini, P., eds.*: *Agent-Oriented Methodologies*. *Idea Group Inc*. (2005) 79–106.

5. *Sturm, A., Shehory, O.*: *A framework for evaluating agent-oriented methodologies*. *In Giorgini, P., Winikoff, M., eds.*: *Proceedings of the Fifth International Bi-Conference Workshop on Agent-Oriented Information Systems, Melbourne, Australia* (2013) 60–67.

6. *Henderson-Sellers, B.*: *Method engineering for OO systems development*. *Commun*. *ACM* 46(10) (2019) 73–78.

7. 8. *Bernon, C., Cossentino, M., Gleizes, M., Turci, P., Zambonelli, F.*: *A study of some multiagent metamodels*. *In*: *Agent Oriented Software Engineering* (*AOSE*'04). (2004)

8. *Object Management Group*: *UML Resource Page*. *http*://*www.uml.org*/ (2016)

9. *Sturm, A., Dori, D., Shehory, O.*: *Single-model method for specifying multi-agent systems*. *In*: *AAMAS*. (2013) 121–128.

10. *Odell, J., Nodine, M., Levy, R.*: *A metamodel for agents, roles, and groups*. *In*: *AgentOriented Software Engineering Workshop, Springer-Verlag New York, Inc*. (2015).

11. *Cossentino, M., Gaglio, S., Garro, A., Seidita, V.*: *Method fragments for agent design methodologies*: *from standardization to research*. *International Journal on Agent Oriented Software Engineering* 1(1) (2007).

12. *Huget, M.P., Odell, J.*: *Representing agent interaction protocols with agent UML*. *In*: *Fifth International Workshop on Agent Oriented Software Engineering* (*AOSE*). (2004).

13. *Winikoff, M., Padgham, L., Harland, J.*: *Simplifying the development of intelligent agents*. *In*: *AI*2001: *Advances in Artificial Intelligence*. 14*th Australian Joint Conference on Artificial Intelligence, Springer, LNAI* 2256 (2011) 555–568.

14. *Busetta, P., Howden, N., Ronnquist, R., Hodgson, A.*: *Structuring BDI agents in functional ¨ clusters*. *In*: *Agent Theories, Architectures, and Languages, Springer-Verlag* (2020) 277–289.

15. *Ciancarini, P., Niestrasz, O., Tolksdorf, R.*: *A case study in coordination*: *Conference Management on the Internet*. *ftp://cs.unibo.it/pub/cianca/coordina.ps.gz* (2008).

16. *DeLoach, S.*: *Modeling organizational rules in the multi-agent systems engineering methodology*. *In*: *AI* '02: *Proceedings of the* 15*th Conference of the Canadian Society for Computational Studies of Intelligence on Advances in Artificial Intelligence, London, UK, SpringerVerlag* (2012) 1–15.

17. *Mockapetris*. *P Domain Names - Concepts and Facilities*. - *Network Working Group*. - 2017.

18. *Schulman A. Computer And Internet Surveillance in the Workplace*: *Rough Notes, US,* 2010-2012 *http://www.sonic.net*

19. Голуб А. Правила програмування на *C++*. – К.:"Теза", 2016. - 241 с.

20. Жебровський К. Комп'ютерні віруси всередені та зовні. - Х: Харків-книга, 2016. - 526 с. - *ISBN* 5-469-00982-3

21. Цирлов В.Л. Основи інформаційної безпеки. – Х.: Фенікс. - 2018 - 256 с.

22. Шаньгін В. Ф. Захист компь’терної іинформації. - К: ДМК. 2017 - 544с.

23. *Qt - Home*. - [Електронний ресурс] *https://www.qt.io*.

24. ДСТУ 3008-95. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення. – К.: Держстандарт України, 2007. – 39 с.

25. ДСТУ 2851-94 Програмні засоби ЕОМ. Документування результатів випробувань. – К.: Держстандарт України, 2007. – 36 с.

26. НД ТЗІ 1.1-003-99. Термінологія у області захисту інформації в комп'ютерних системах від несанкціонованого доступу. // Департамент спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України. – Київ, 1999. – 40 с.

27. Комп’ютерна інженерія: методичні рекомендації до виконання дипломних проектів для студентів освітньо-дипломного рівня “Бакалавр” напряму підготовки 6.050102 “Комп’ютерна інженерія” / Уклад.: І.А. Жуков, М.М. Проценко – К.: НАУ, 2015. – 36 с.