Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

Кафедра мережних технологій факультету інформатики

СИСТЕМА МОНІТОРИНГУ ДЛЯ МЕРЕЖІ ПІДПРИЄМСТВА

Текстова частина до курсової роботи за спеціальністю «Прикладна математика» 113

Керівник курсової роботи
к.т.н., доц. Черкасов Д.І.

_____

(підпис)

“____”_____2021 р.

Виконав студент
Король Є.В.
“____”_____2021 р.

Календарний план виконання роботи:

№ п/п	Назва етапу курсової роботи	Термін виконанняетапу	Примітка
1.	Отримання теми курсової роботи.	1.11.2020	
2.	Огляд наявних рішень для системи моніторингу підприємства.	15.01.2021	
3.	Аналіз особливостей наявних рішень.	14.02.2021	
4.	Написання першого розділу	21.03.2021	
5.	Написання другого розділу.	26.03.2021	
6.	Написання третього розділу.	27.04.2021	
7.	Створення презентації та написання доповіді для захисту роботи.	14.05.2021	

ЗМІСТ

ВСТУП

Комп'ютерна мережа сьогодні є практично в кожній успішній компанії. Мережа вже не вважається чимось розкішним, а є прекрасною можливістю ефективно оптимізувати роботу, виробництво, об'єднавши усі комп'ютери в єдину систему. Стежити за роботою усієї мережі, вчасно реагувати на проблеми допомагає програма моніторингу. З її допомогою керівництво стежить за тим, що відбувається в службових комп'ютерах, як функціонує виробництво, налагоджуються і підтримуються контакти. Крім цього, програма блокує спам, попереджає вірусні атаки, робить перевірку контенту і файлів, що поступають. Моніторинг мережі підприємства - це реальна можливість контролювати і убезпечити робочий процес, який пов'язаний з інтернетом і комп'ютерами.

Вже доведено, що несправності в комп'ютерній мережі легше попередити, чим потім вирішувати проблеми. Регулярний моніторинг локальної мережі, сервера, мережевих пристроїв дозволяє заздалегідь дізнаватися про можливі неполадки і запобігати їх появі. Крім того, відстежуючи історію, адміністратор може дати зведення про частоту появи різних несправностей, що теж є запорукою роботи без проблем.

Сьогодні можна виділити два різновиди моніторингу мережі підприємства:

- оперативний;
- моніторинг безпеки.

На великих підприємствах ці різновиди можуть бути поділені на два процеси, які виконуються окремими фахівцями. У малих же і середніх фірмах моніторинг зазвичай буває загальним. Це правильно, оскільки невелика комп'ютерна мережа не потребує скрупульозної оперативної перевірки, вона завантажена не так серйозно і обслуговується простіше. У

них немає потреби в детальному аналізі звітів, завдань і тенденцій, які потрібні на великих підприємствах.

Для того, щоб гарантувати безпеку важливо піддавати контролю усі наявні мережеві пристрої. До них відносять безпровідні точки доступу, різні шлюзи, VPN- пристрої, брандмауери різних конфігурацій і сервери, на яких розміщені конфіденційні дані і цілісні процеси. Для Windows проводиться перевірка ОС (операційна система) і ключових додатків різного типу. Контролю повинні піддаватися і високорівневі застосування, щоб відразу виявити дії, які безпосередньо відносяться до збереження безпеки життєдіяльності підприємства і проведення виробничих процесів.

Моніторинговій перевірці повинні піддаватися як об'єкти продуктивності, так і стан безпечної роботи сервера. Відмінність між перевіркою конкретного об'єкту і журналу подій, що відбуваються, полягає в тому, що з журналу беруть дані про проблеми у будь-якій системній частині, тоді як об'єкт продуктивності показує, що певні параметри мають допустимі межі. Так, завдяки об'єктам продуктивності, можна контролювати простір жорсткого диска, а журнал лише видасть попередження, коли він заповниться до критичного стану.

Моніторинг міри використання ЦП (центральний процесор) - це ще одне корисне дослідження із застосуванням об'єкту продуктивності. Відстежувати доведеться досить довгий час. Проте такий моніторинг вимагає обережності, розуміння суті процесів і уваги, оскільки досить легко можна переплутати корисне навантаження з певним не керованим процесом.

Головними індикаторами коректної роботи системи є відсутність в журналі відомостей про помилки і безперебійні показники продуктивності. Але варто знати, що є проблеми, які не відображаються в індикаторах. І тут потрібна перевірка серверного стану, як відповідний спосіб упевнитися в

тому, що додатки, сервери функціонують правильно і обробляють усі запити.

Для цієї мети варто проводити іноді транзакції-тести з сервером через певні тимчасові інтервали. Для веб-сервера можна час від часу просити певну веб-сторінку і контролювати, як вона передається. Для SQL (Structured query language в перекл. «мова структурованих даних») сервера виконуються запити і перевіряються результати.

Зверніть увагу, що всі проблеми навіть після перевірки стану можуть бути не виявлені. Так, звичайний пінг-сигнал, що передається регулярно через п'ять хвилин, дозволяє упевнитися, що протоколи ОС активні, але він не скаже нічого про стан певного застосування. Буває і так, що на пінг-сигнал відповідають сервера, які знаходяться в стані зависання. Так само, запит з сервера конкретної HTML (Hypertext markup language в перекл. «мова гіпертекстової розмітки») - сторінки ще не гарантує, що додаток електронної комерції на базі ASP (технологія створення веб-застосунків і веб-сервісів від компанії Майкрософт) працює коректно.

Саме тому, важливо досягнути максимальної функціональності перевірки стану. Якщо є можливість, варто зробити обліковий запис-тест для додатка на базі ASP.

Ще одна деталь: розміщувати цю програму потрібно поза зоною, яка буде під контролем. Якщо так не зробити і розташувати її прямо на контрольованому сервері, то складно буде визначити відсутність з'єднання, серверну відмову. В цьому випадку додаток не зможе передати системному адміністраторові необхідне повідомлення.

Якщо ж розмістити на окремому сервері додаток перевірки, то воно працюватиме завжди, за винятком моменту, коли одночасно відмовляють середовища контролю і виробництва.

РОЗДІЛ 1. Огляд автоматизованої системи моніторингу використання ресурсів комп'ютерної мережі підприємства

Сучасна система моніторингу устаткування робить спостереження за серверами і хостингом, контролює файли, теки, бази даних, а також здійснює контроль над процесами і службами на комп'ютерах користувачів.

Моніторингу підлягає:

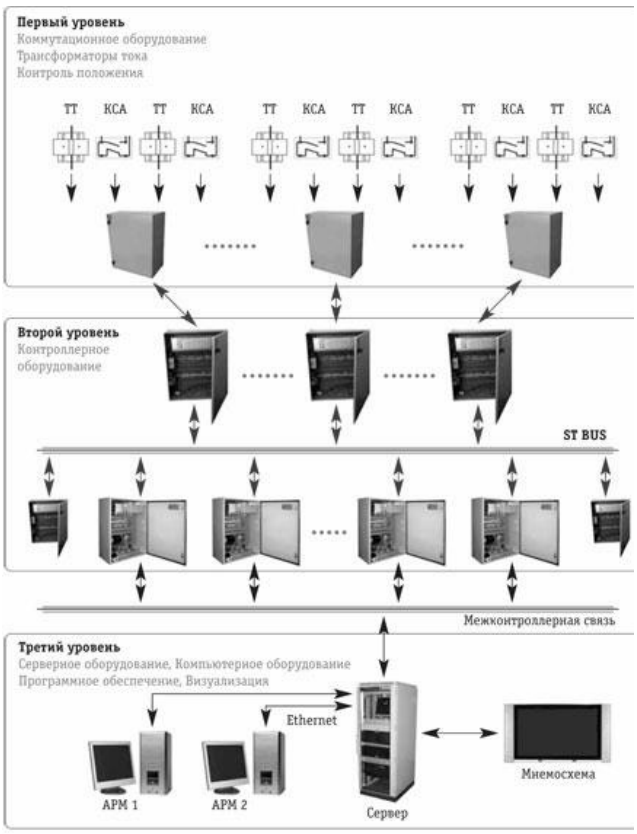
1) підключення до TCP- порту;
2) DNS- сервери;
3) ICMP (Internet control message protocol в перекл. «міжмережевий протокол керуючих повідомлень»);
4) порт на світчі;
5) протоколи ARP (Address resolution protocol в перекл. «протокол визначення адреси»);
6) комутатори протоколу SNMP (Simple network management protocol в перекл. «простий протокол керування мережею»);
7) HTTP (Hypertext transfer protocol в перекл. «протокол передачі даних») веб-сервер;
8) MAC-адреси по NetBIOS (Network basic input/output system в перекл. «базова мережа введення/виводу мережі») і ARP протоколам;
9) журнал подій Windows;
10) WMI-параметри (Windows management instrumentation в перекл. «засоби управління windows»);
11) виконання javascript і Visual Basic script та ін.

Для моніторингу устаткування нині існує багато різноманітних програм. Ці застосування потрібні для своєчасного сповіщення власника або обслуговуючого персоналу про тих, що виникли на сервері і з устаткуванням неполадок. Ще вони можуть знадобитися для того, аби заздалегідь попередити стосовно можливого їх прояву у системі.

Взагалі існує два види мережевого устаткування, активний та пасивний. До нього можна віднести пристрої, що можуть допомогти при роботі комп'ютерних мереж.

До активного виду мережевого устаткування відносяться:

- мережевий адаптер;
- репітер;
- концентратор;
- міст;
- комутатор (світч);
- маршрутизатор;
- медіаконвертер;
- мережевий трансивер.



(Рис. 1.1— зображення автоматизованої системи диспетчерського управління)

Пасивне мережеве устаткування - це устаткування, яке живиться безпосередньо від електромережі і передає сигнал без його посилення.

Основні проблеми, які можуть виникнути з сервером і супутнім устаткуванням:

1) розриви зв'язку;
2) збій в роботі баз даних;
3) зупинка використовуваних служб;
4) критично мала кількість вільного місця на диску та ін.

Аби не було зламу яких небудь бізнес-процесів даної компанії або пошкодження важливих даних, потрібно використовувати правильну систему моніторингу, що заздалегідь надішле вам повідомлення стосовно проблеми та неполадок, що виникли. Таким чином вона допоможе уникнути втрати великої кількості часу та доведення її до стану повної зупинки роботи через несправності.

Перед роботою з самою системою моніторингу, потрібно з’ясувати, чи зможе адміністратор мережі при необхідності використати власні скрипти, мавши на увазі перевірку служб та пристроїв, підтримку контролю різних змінних у керованих серверах або комутаторах. Програми сучасного життя надають дозвіл на перегляд графіків від отриманих змінних у реальному часі та накопичення статистичних даних. Це все робиться для того, аби була можливість аналізу заради своєчасного прояву та виведення теоретично можливих проблем. До комплексного моніторингу IT інфраструктури входить моніторинг мережевого устаткування, також він є важливою складовою цієї системи. Від того, наскільки якісно буде виконана дана робота, залежить надійне функціонування всієї в цілому системи.

Моніторинг мережі - дія спеціалізованого програмного застосування. Він постійно спостерігає за самою мережею, поставивши за мету своєчасне знаходження неполадок та більш повільну роботу мережі.

Коли проблема знайдена, система у свою чергу, оперативно надсилає повідомлення мережевому адміністратору через e-mail (електронну пошту). Взагалі, є ще багато різних варіантів надсилання подібних повідомлень, наприклад: по телефону, за допомогою будь-якого мессенджера і так далі.

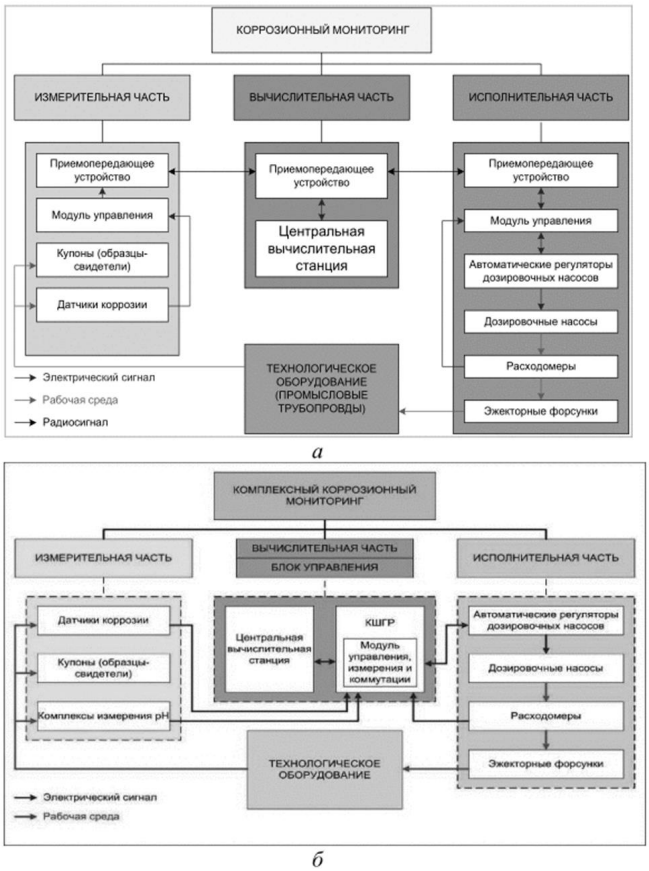
В процесі ведення спостереження ПЗ (програмне забезпечення) моніторингу мереж періодично виконує тест, наприклад, намагається відправити тестове повідомлення з метою перевірки роботи корпоративного поштового сервера або запросити певну сторінку на сервері. Якщо система не отримає відповіді, то відреагує за допомогою відправки сигналу адміністраторові, що відповідає за роботу мережі, або автоматично активує систему захисту від збоїв або здійснить будь-яку іншу, заздалегідь заплановану дію.

Моніторинг мережевого устаткування, часто у рамках IT аутсорсинга, разом з штатними системними адміністраторами проводять організації, що спеціалізуються в цьому виді діяльності. При обслуговуванні клієнтської компанії має бути здійснене впровадження системи моніторингу мережевого устаткування. Доручати таке складне і відповідальне завдання слід профільним фірмам, що мають достатній досвід побудови систем моніторингу різного масштабу, починаючи від спостереження за устаткуванням невеликих підприємств, яким необхідно бути впевненими в працездатності внутрішніх сервісів, і закінчуючи побудовою комплексних систем для контролю над корпоративною інфраструктурою.

Від безперебійної роботи серверів і супутнього устаткування часто залежить і безперервна робота усього підприємства в цілому. Тому обслуговування IT інфраструктури можна доручати тим, хто добре зарекомендував себе в цій сфері компаніям. Застосування спеціалізованого програмного забезпечення допоможе організувати складський і торговий облік, проводити маркетинговий аналіз доходу, створити високоякісне сервісне обслуговування.

Якісне обслуговування мережевої інфраструктури на великому підприємстві потребує більшого штату професіоналів. До їх обов'язків належить:

- постійний зв'язок з мережевими сервісами;
- ремонт та оновлення мережевого програмного, апаратного забезпечення;
- оптимізована робота усієї мережі;
- виявлення та усунення несправностей;
- підтримка працездатності устаткування;
- можливість виконання інших завдань.



(Рис. 1.2— зображення автоматизованого корозійного моніторингу)

Коли ми намагаємося вирішити їх власними силами, організація стикається з такими проблемами, як:

- співробітники повинні мати навички роботи з великою кількістю мережевих пристроїв і бути ознайомленими з новітніми технологіями, що підвищує вимоги до рівня їх кваліфікації;
- складне залучення досвідчених фахівців на роботу в непрофільних організаціях та висока заробітна плата;
- у держструктурах існують певні бюджетні і нормативні обмеження, із-за яких чисельність найманого персоналу не може перевищувати встановлені значення.

Через те, що для обслуговування користувачів використовується стандартний, традиційний підхід, це спричиняє збільшення кількості навантажених сервісних служб та підприємств. Коли мережі обслуговуються за допомогою сил внутрішнього IT-підрозділу, дії з усунення проблем чи виявлення маленьких проблем, заздалегідь здійснюються після виникнення негативних наслідків.

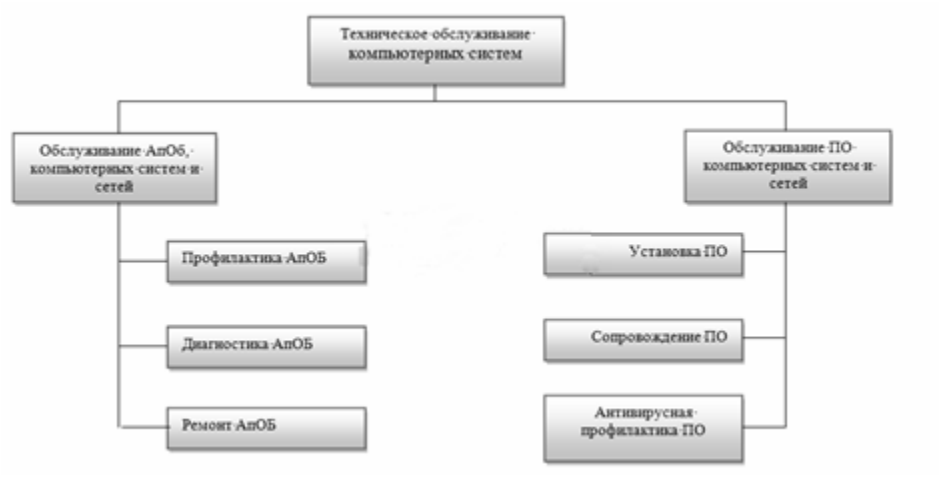
Заради того, аби уникнути усіх проблем, що можуть стосуватися користувача, потрібно звернутися до професіонала, фахівця, що здатен забезпечити вищий рівень обслуговування мережевого устаткування. Більшість завдань зараз можна виконувати у віддаленому режимі. При виникненні неполадок, з якими неможливо впоратися віддалено, в офіс замовника приїжджає співробітник, команда співробітників аутсорсингової фірми, і проблема усувається на місці її виникнення. Укладення договору на абонентське обслуговування обходиться клієнтській організації набагато дешевше, ніж наповнення штату внутрішнього IT підрозділу. У абсолютній більшості випадків, стан підтримки, істотно підвищується.

Вимоги до моніторингу мережевого устаткування:

1) можливість ведення спостереження на платформах Unix, Linux, Windows, BSD, Solaris;
2) функція моніторингу SNMP v1, v2, v3 - пристроїв;

3) рішення має бути готове до збільшення масштабу IT інфраструктури і числа перевірок;
4) робота в режимі реального часу - постійна перевірка продуктивності і доступності IT сервісів;
5) повідомлення системного адміністратора і при необхідності користувачів різними способами;
6) виконання визначених заздалегідь дій при виникненні інцидентів;
7) побудова звітів, діаграм і графіків, створення карти мережі;
8) можливість ведення розподіленого моніторингу, що включає перевірку серверів, мереж, комп'ютерів на доступ до усієї інформації з однієї точки;
9) контроль над тим, щоб робота IT сервісів відповідала заданому рівню;
10) підтримка інформаційної безпеки компанії;
11) гнучке налаштування прав доступу користувачів відповідно до їх статусу;
12) можливість аутентифікації по IP адресі;
13) захист від зовнішніх загроз і атак;
14) шаблони моніторингу мережевого устаткування і серверів, що настроюються;
15) можливість простого імпорту і експорту шаблонів. ергономічний веб-інтерфейс, що дозволяє управляти системою моніторингу, у тому числі віддалено;
16) функція автоматичного виявлення в мережі робочих станцій, мережевих облаштувань та ін.;
17) оптимальний розподіл і зниження навантаження і трафіку шляхом агрегації даних;

18) підтримка інтерфейсом системи моніторингу мережевого устаткування різних мов.



(Рис. 1.3 — зображення локальної вирахувальної мережі)

Роботи, що входять в налаштування сервера :

- інсталяція операційної системи;
- проведення встановлення необхідних програм і драйверів;
- здійснення тонкого налаштування ролі сервера;
- установка і налаштування антивірусних застосувань;
- налаштування резервного копіювання.

Жодним з перерахованих пунктів не можна нехтувати, оскільки від кожного з них безпосередньо залежить стійкість роботи сервера і усього підприємства, яке він обслуговує. Технічна підтримка сервера повинна здійснюватися на постійній основі силами кваліфікованих IT фахівців.

До техобслуговування сервера можна віднести:

- технічна підтримка вже встановлених додатків або пристроїв;
- захист від великої кількості вірогідних загроз, які можуть зустрітися на шляху користувача;

- надання доступу до управління ресурсами компанії, включаючи електронну пошту, файли, принтери і так далі;
- встановлення та дотримання правил безпеки;
- загальна організація резервного копіювання всіх файлів та зберігання даних користувача.

Адміністрування сервера поділяється на два види робіт впровадження нових сервісів: заплановані і разові.

У відповідних розділах «Угоди про рівень сервісу», які зазвичай проводяться щомісячно, закріплюються заздалегідь заплановані роботи, умови і графік проведення яких узгоджуються між замовником і виконавцем. Одноразові роботи можуть проводитися у зручний час на території клієнтського підприємства або віддалено. Рішення стосовно цього питання приймається на основі клієнтської зручності в першу чергу.

Для впровадження моніторингу у мережевого устаткування потрібно:

- скласти список пристроїв та фіксації параметрів їх роботи;
- зробити аналіз отриманих даних з пристроїв;
- скласти технічне завдання;
- узгодити його зі стороною замовника;
- детально визначити потрібне устаткування та бюджет;
- підготувати пристрої;
- підготувати IT-інфраструктури усієї компанії;
- інсталювати сервер моніторингу;
- провести налаштування системи моніторингу комп’ютера;
- провести тест роботи самої системи;
- усунути виявлені помилки;
- здати, за потреби, до промислової експлуатації.

Реалізацію проекту впровадження моніторингу потрібно доручати спеціалізованій компанії, яка позитивно зарекомендувала себе при

виконанні подібних проєктів для високопоставлених підприємців. Саме спостереження за працездатністю IT-інфраструктури повинні вести професіонали, здатні правильно налаштувати і ефективно використовувати сучасне програмне забезпечення для моніторингу мережевого устаткування.

РОЗДІЛ 2. Загальний огляд центрів обробки даних та систем моніторингу

2.1. Загальні відомості, склад, топологія та недоліки центрів обробки даних

Центр обробки даних (ЦОД), або дата-центр - єдина відмовостійка багатокомпонентна система, що забезпечує безперебійну автоматизовану роботу бізнес-процесів і виконує функції обробки, зберігання і поширення інформації.

Система електропостачання

Одною з основних потреб активного устаткування, що розміщується в ЦОД, являється потреба в якісному і безперебійному електроживленні. До складу інженерних систем ЦОД входить комплекс систем електропостачання, що складається з системи гарантованого електропостачання (СГЕ), безперебійного електропостачання (СБЕ) і розподілу живлення (СРЖ).

Живлення електроспоживачів ЦОД забезпечується системою гарантованого електропостачання, яка дозволяє підключити ЦОД до декількох незалежних джерел електроенергії, перемикання між якими відбувається в автоматичному режимі. До складу системи також можуть входити зовнішні дизельні генераторні установки, автоматичний запуск яких робиться при пропажі живлення від зовнішніх електричних мереж.

Для живлення найбільш відповідальних електроспоживачів, таких як IT-устаткування, в ЦОД використовується система безперебійного електропостачання. У її основі лежать джерела безперебійного живлення (ДБЖ) з комплектом акумуляторних батарей (АКБ), завдяки заряду яких система здатна забезпечувати харчуванням споживачі навіть при повній відсутності напруги на зовнішніх введеннях.

Система контролю мікроклімату

Для стабільної і ефективної роботи IT-устаткування усередині ЦОД вимагається постійно підтримувати строго певні параметри мікроклімату. Відхилення температури і вологості від необхідних значень може призвести до таких наслідків, як перегрівання устаткування, випадання конденсату, створення статичного заряду на робочих поверхнях і тому подібне. Для вирішення цього завдання при будівництві ЦОД застосовуються спеціалізовані комплексні системи контролю мікроклімату, до складу яких можуть входити підсистеми кондиціонування повітря, припливно-витяжної вентиляції, опалення, парозволоження та інші допоміжні підсистеми. Від аналогічних систем з інших сфер застосування систему контролю мікроклімату ЦОД відрізняють підвищені вимоги до точності підтримуваних параметрів, безперервний режим роботи (24x365), а також висока надійність і застосування різних схем резервування.

(Рис. 2.1 — центр обробки даних)

Структурована кабельна система

Структурована кабельна система (СКС) представляє з себе розподільчу систему, що складається з кабелів, сполучного і кросового устаткування. Основне завдання СКС - надати фізичне середовище для ефективної передачі даних між пристроями, розміщеними усередині центру обробки даних. СКС ЦОД зазвичай складається з мідного і оптичного сегментів. Залежно від місткості СКС і архітектура мережі передачі даних, всередині монтажних шаф в різній кількості розміщуються мідні і оптичні патч-панелі для підключення кінцевих активних пристроїв. Для обміну даними між облаштуваннями інженерних систем ЦОД організовується окремий мідний сегмент технологічної СКС (ТСКС).

Монтажні конструкції

Для захисту устаткування ЦОД від зовнішніх протікань, пилу і інших несприятливих фізичних дій, в приміщенні ЦОД зводиться внутрішній герметичний контур (гермозона). Для розміщення обчислювальної інфраструктури усередині ЦОД застосовуються спеціалізовані монтажні шафи, розраховані на високе навантаження і експлуатації як IT-устаткування, так і допоміжних пристроїв, що забезпечують зручність. Для організації кабельної інфраструктури ЦОД за межами монтажних шаф використовуються спеціалізовані кабельні лотки.

Системи безпеки

Фізична безпека ЦОД забезпечується комплексом систем, до складу якого зазвичай входить система контролю і управління доступом (СКУД), система охоронного телебачення (СТІЛЬНИК), система об'єктової і периметральної охоронної сигналізації (ООС і ПОС). Ці системи орієнтовані на захист устаткування і інформації від загроз, що виникають

при проникненні в ЦОД неуповноваженої на це особи. Системи безпеки ЦОД можуть мати різну архітектуру і міру інтеграції один з одним. Можлива реалізація архітектури, яка дозволяє контролювати доступ як до об'єкту в цілому, так і розділяти його на різні зони і рівні доступу.

Автоматична система усунення вогню

Центр обробки даних є об'єктом підвищеної пожежної небезпеки, оскільки в ньому розміщується велика кількість потужних електричних приладів. Висока щільність розміщення устаткування, а також наявність постійних інтенсивних повітряних потоків, значно збільшує як ризик виникнення пожежі, так і швидкість його поширення усередині ЦОД. Для захисту ЦОД від пожежі потрібно застосування автоматичних засобів пожежогасіння, які не лише ефективно ліквідують займання, але і не завдають шкоди дорогому устаткуванню, розміщеному в ньому.

Для вирішення цього завдання до складу інженерних систем при будівництві ЦОД зазвичай входить автоматична установка газового пожежогасіння (АУГП), ґрунтовна на застосуванні різних сертифікованих газових вогнегасних речовин, - різновиди "Хладонів", "Інерген", "Novec 1230" і так далі. На відміну від засобів пожежогасіння, ґрунтованих на воді або порошку, АУГП не представляють загрози для IT-устаткування і не накладають обмежень на його роботу. Така особливість дозволяє ліквідовувати виникле вогнище займання без зупинки роботи ЦОД.

(Рис. 2.2 — мережні архітектури)

Автоматична система моніторингу і управління

Автоматична система моніторингу і управління (АСМУ) призначена для дистанційного контролю параметрів роботи інженерних систем ЦОД, а також для автоматичного відробітку протиаварійних алгоритмів. АСМУ представляє з себе програмно-апаратний комплекс, що здійснює збір, зберігання, обробку, передачу і представлення інформації про параметри середовища і інженерні системи ЦОД в зручному для користувача виді. Зазвичай АСМУ дозволяє контролювати такі параметри, як параметри мікроклімату на рівні приміщень ЦОД і окремих монтажних шаф, параметри електричної мережі і стан автоматичних вимикачів системи електропостачання, стан інженерних систем ЦОД (кондиціонери, АУГП, система вентиляції і так далі).

Аудит і модернізація

Проведення аудиту дозволяє:

- отримати об'єктивну оцінку поточного стану інженерної інфраструктури ЦОД;
- виявити існуючі і потенційні точки відмови інженерних систем;
- завчасно розробити і реалізувати заходи для підвищення відмовостійкості систем і запобігання аварійних ситуацій.

За результатами обстеження створюється розгорнутий звіт, в якому фіксується:

- поточний стан інженерних систем ЦОД;
- рекомендації по підвищенню рівня надійності інженерної інфраструктури ЦОД, реалізації схем резервування, розробці регламентів, а також про необхідність проведення глибокого аналізу тих систем, в роботі яких були виявлені відхилення;
- рекомендації з підвищення енергоефективності і модернізації інженерної інфраструктури ЦОД з урахуванням планів по зростанню обчислювальних потужностей;
- оптимальні підходи, методи і шляхи усунення недоліків і несправностей, виявлених в ході проведення аудиту.

Модернізація ЦОД має на увазі проектування і внесення змін до існуючої інженерної інфраструктури. Метою модернізації може бути:

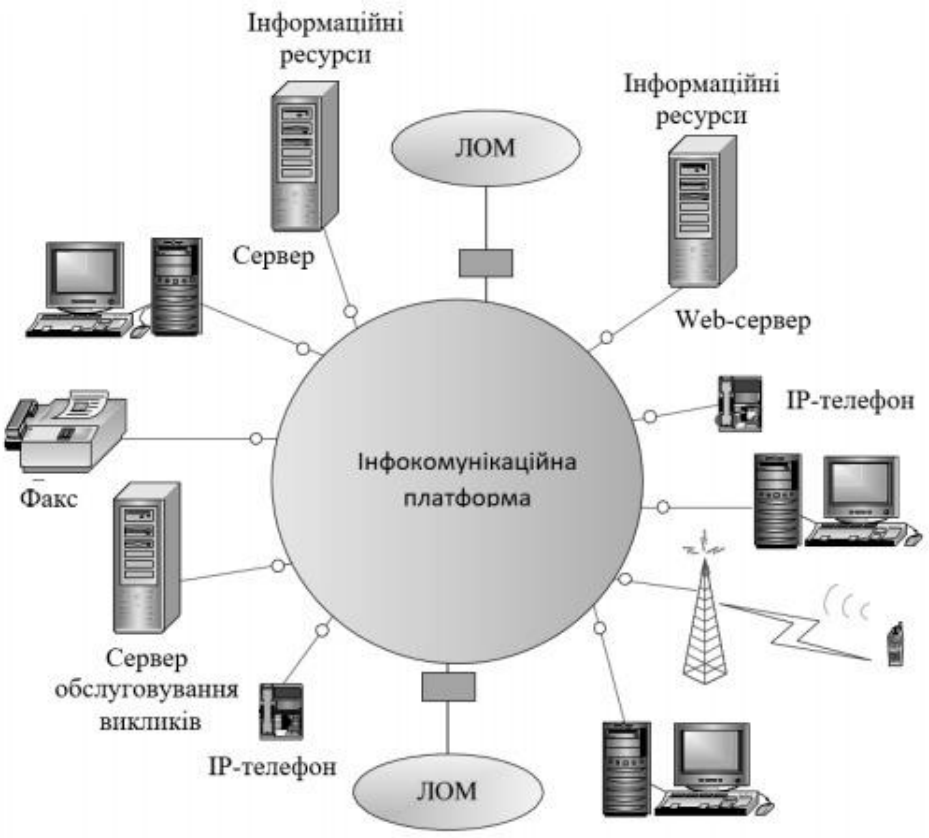
- усунення наявних недоліків, що ускладнюють експлуатацію ЦОД в його поточному стані;

- підвищення відмовостійкості окремих систем і інженерної інфраструктури ЦОД в цілому;

- розширення інженерної системи у зв'язку з плановим збільшенням обчислювальних потужностей;

- інші зміни в завданнях, складі і характеристиках IT-інфраструктури замовника.

Важливою особливістю модернізації ЦОД, як правило, являється необхідність проведення робіт без зупинки критичних сервісів замовника. Для виконання цієї умови у рамках проектування центрів обробки даних потрібно розробити спеціальні заходи з підготовки об'єкту до виконання усіх етапів робіт, що впливають на безперервну роботу ЦОД. Також в процесі модернізації центрів обробки даних може знадобитися створення тимчасових елементів окремих інженерних систем.



(Рис. 2.3 — телекомунікаційні системи та мережі)

Сервіс

Планове технічне обслуговування - планове профілактичне обслуговування ЦОД, що проводиться відповідно до рекомендацій від виробників. За результатами проведення технічного обслуговування замовник отримує комплексний звіт про стан усіх інженерних систем з детальними рекомендаціями з поліпшення стану підтримуваних систем. Якщо на технічний супровід приймається система, що вже знаходиться в експлуатації, перед проведенням першого планового технічного обслуговування ЦОД проводиться попередній аудит системи. Серверне приміщення відноситься до приміщень підвищеного класу надійності. Це спричиняє за собою підвищені вимоги до підтримки чистоти в ЦОД, а також до кваліфікації обслуговуючих фахівців. Тому в якості додаткової опції у рамках послуг з технічного обслуговування ЦОД пропонується послуги клінінгу у рамках проведення робіт по технічному обслуговуванню інженерних систем.

Клінінг включає в себе:

- загальне прибирання ЦОД: видалення пилу і забруднень з поверхні підлоги за допомогою пилососа, вологе прибирання серверного приміщення з використанням очисників;
- видалення пилу і забруднень під фальшполом;
- вологе прибирання підлоги: протирання підлоги, опорних ніжок, опорної рами і кабельних жолобів;
- збір і вивезення сміття.

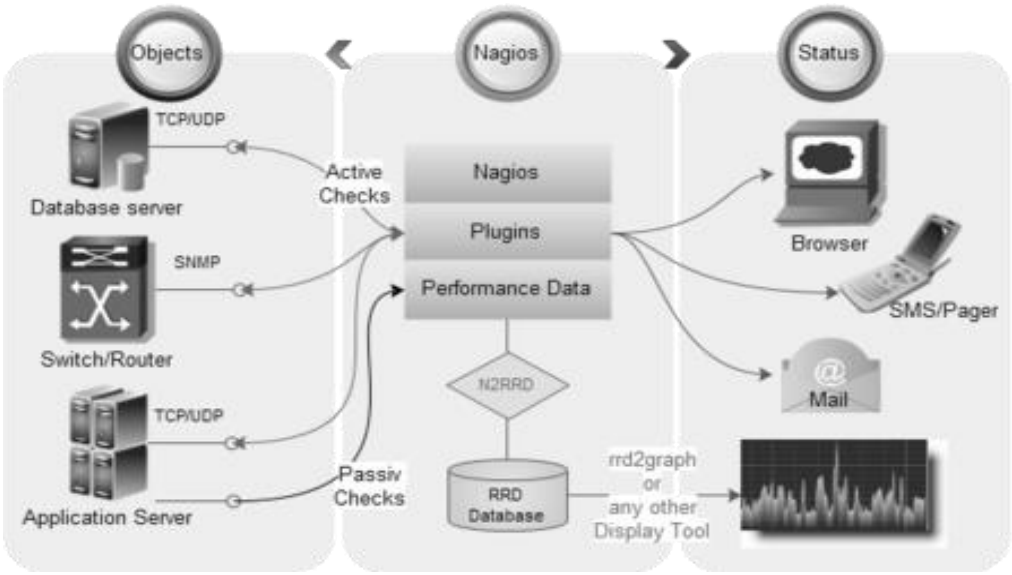
Якісний рівень прибирання приміщень ЦОД не наражає IT-устаткування на небезпеку відключення або ушкодження.

РОЗДІЛ 3. Порівняльний аналіз систем моніторингу

3.1. Огляд системи моніторингу Nagios

Моніторинг є однією з основних складових якісного сервісу. Складно уявити собі якісного хостинг-провайдера без системи моніторингу, яка б своєчасно сповіщала системних адміністраторів щодо будь-яких проблем із серверами. Nagios - це безкоштовна система для Unix-платформ всередині якої стеження за статусом віддалених сервісів та надсилання повідомлень через e-mail та sms при виникненні будь-яких проблем у просторі хостингу.

Вочевидь, системи розташовані на одному з серверів, за яким спостерігають найбільше, не мають достатнього ступеня надійності. Якщо впаде сам сервер, то в них не буде жодного сенсу. Їх застосовують, коли потрібно зробити автоматичний рестарт впавших серверів. Зовнішній моніторинг повідомить вас щодо проблеми у разі якщо сервер взагалі не буде пінгуватися.



(Рис. 3.1 — використання Nagios)

Однак не тільки хостингу сайтів php (Hypertext preprocessor в перекл. «гіпертекстовий препроцесор») mysql (вільна система керування

реляційними базами даних) може знадобитися централізована система моніторингу. Якщо у вас велика кількість серверів на різних майданчиках, то спостереження за їх станом, точно не буде зайвим. У разі, якщо у вас колокація (різновид хостингу), або ваш провайдер надає сервери без адміністрування, то стежити за роботою сервера доведеться самотужки. Крім того, моніторинг деяких сервісів передбачає віддалений доступ до нього з сервера, де розташований моніторинг і тому зробити це зможете тільки Ви. Можна звісно піти іншим шляхом, але у цьому випадку потрібно буде передати дані доступу третім особам, що не є дуже добре та надійно.

Встановлення Nagios можлива з вихідних кодів, завантажених з офіційного сайту або через пакетні менеджери ОС. Другий варіант - кращий, адже при вході оновлення, користувачеві буде простіше встановити нову версію.

(Рис. 3.2 — Nagios у роботі)

При встановленні системи моніторингу Nagios особливу увагу зверніть на те, що плагіни встановлюються окремо. Без цих плагінів, моніторинг матиме змогу стежити лише за обмеженим колом стандартних сервісів. У Nagios є веб-інтерфейс, тож для його роботи знадобиться, і веб-сервер, і php. Однак щодо цього моменту можна не турбуватися, адже пакетні менеджери ОС самостійно завантажать та проведуть встановлення,

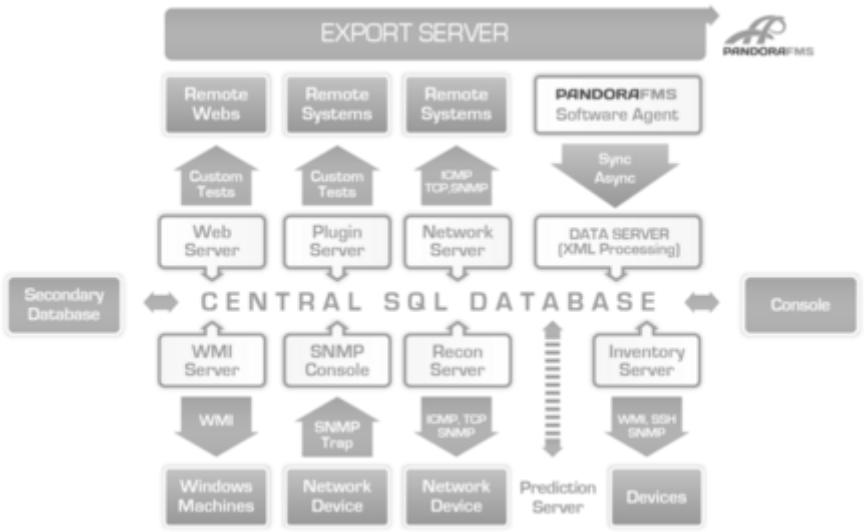
в залежності від пакета Nagios. У разі встановлення з вихідних кодів, вам доведеться встановлювати ще і всі додаткові програми самостійно. Вони знаходяться в межах хостингу сервера lineage.

Веб-сервіс системи моніторингу Nagios досить інформативний, тут можна подивитися список хостів, сервісів, журнал виниклих проблем та повідомлень про них. Проблемні сервіси підсвічуються червоним і жовтим кольорами, в залежності від рівня проблеми. Водночас веб-інтерфейс має один головний мінус - саме через нього і не можна нічого змінити. На жаль, всі налаштування, наприклад додавання, редагування хостів і сервісів, контактів для повідомлень - здійснюються вручну, через конфігураційні файли програми.

3.2. Огляд системи моніторингу Pandora FMS

Pandora FMS (Pandora Flexible Monitoring System) - програмне рішення для моніторингу. Pandora FMS дозволяє здійснювати моніторинг з візуалізацією станів і продуктивністю декількох параметрів з різних операційних систем, серверів, додатків і апаратних систем, таких як брандмауери, проксі, баз даних, веб-серверів або маршрутизаторів.

Pandora FMS можуть бути розгорнуті практично у будь-якій операційній системі. Моніторинг здійснюється за допомогою WMI, SNMP, TCP, UDP, ICMP, HTTP, тощо і агентів. Агенти доступні для кожної платформи. Вона може також контролювати апаратні системи з TCP / IP стеком. Наприклад балансування навантаження, маршрутизатори, мережеві комутатори, принтери і брандмауери.



(Рис. 3.3 – архітектура Pandora FMS)

Можливості Pandora FMS:

- виявлення нових систем в мережі;
- перевірка на наявність або продуктивність;
- попереджати про небезпеку коли щось піде не так;
- дозволяють отримувати дані усередині систем зі своїм агентами;
- дозволяють отримувати дані зовні, використовуючи тільки зонди мережі. Включаючи SNMP;
- отримання SNMP пасток із загальних мережевих пристроїв;
- створення в реальному часі звітів і графіків;
- зберігати дані впродовж декількох місяців, готовий для використання на звітність;
- графіки в реальному часі для кожного модуля;
- висока доступність для кожного компонента;
- масштабність і модульна архітектура;
- підтримує до 2500 модулів на сервері;
- сповіщення користувача. Також можуть бути використані для реагування на інциденти;

- інтегрований інцидент менеджер;
- інтегроване управління БД: чищення і БД ущільнення;
- розраховані на багато користувачів, багатопрофільні, групові;
- профілі можуть персоналізовано використовуватися з кількістю атрибутів безпеки до 8, без обмежень по групах або профілях.

(Рис. 3.4 – Pandora FMS у роботі)

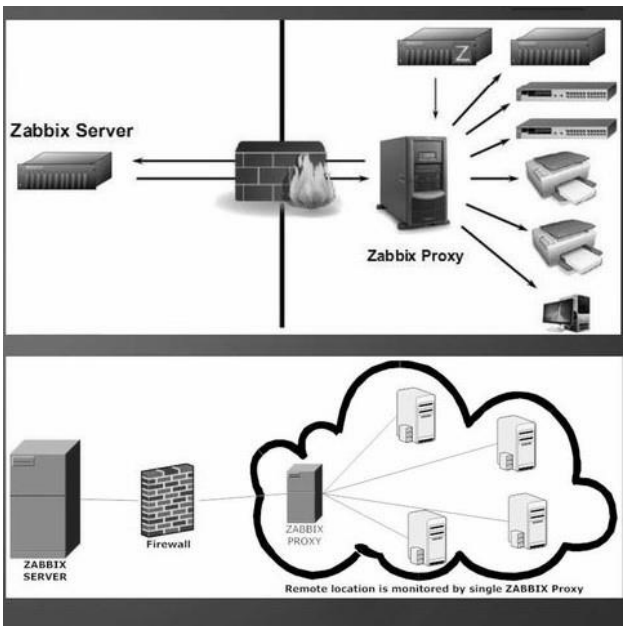
3.3. Огляд системи моніторингу Zabbix

Zabbix можна вважати відкритим рішенням розподіленого моніторингу корпоративного класу.

Zabbix - це багатофункціональна система моніторингу з веб-інтерфейсом, яка підлаштовується під потрібні системи, збираючи з них статистику, і діюча заданим чином в передбачених випадках. Zabbix використовує гнучкий механізм повідомлень, що дозволяє користувачам налаштовувати сповіщення поштою практично для будь-якої події. Це дає можливість швидко реагувати на проблеми з сервером. Zabbix пропонує прекрасні можливості звітності і візуалізації даних, базуючись на зібраних даних. Це робить Zabbix ідеальним інструментом для планування і масштабування.

Підтримує кілька видів моніторингу:

1) Simple checks - може перевіряти доступність і реакцію стандартних сервісів, таких як SMTP або HTTP, без установки якого-небудь програмного забезпечення на спостережуваному хості;
2) Zabbix agent - може бути встановлений на UNIX-подібних або Windows-хостах для отримання даних про навантаження процесора, використання мережі, дисковому просторі і так далі;
3) External check - виконання зовнішніх програм, також підтримується мониторинг через SNMP.



(Рис. 3.5 – архітектура Zabbix)

Zabbix підтримує опитування даних (пуллер) і отримання даних (траппер). Усі звіти і статистика Zabbix, також як і параметри налаштувань, доступні через веб-інтерфейс. Веб-інтерфейс забезпечує щоб стан вашої мережі і життєдіяльність ваших серверів можна було оцінити з будь-якого місця. Добре налагоджений Zabbix може відігравати важливу роль в моніторингу IT інфраструктури. Це так само важливо як для малих організацій з декількома серверами, так і для великих компаній з множиною серверів.

Zabbix безкоштовний. Zabbix написаний і поширюється під ліцензією General Public License (GPL) версії 2. Це означає, що його початковий код вільно поширюється і у вільному доступі. Так само доступна комерційна підтримка, яка надається компанією Zabbix.

Багато організацій різних розмірів по всьому світу покладаються на Zabbix як на головну систему моніторингу.

Zabbix пропонує:

- автоматичне виявлення серверів і інших пристроїв в мережі;
- розподілений моніторинг з централізованим адмініструванням;
- підтримка обох механізмів: пуллерів та трапперів;
- серверне програмне забезпечення для Linux, Solaris, HP - UX, AIX, FreeBSD, OpenBSD, OS X;
- різні агенти з високою продуктивністю (клієнтське програмне забезпечення для Linux, Solaris, HP - UX, AIX, FreeBSD, OpenBSD, OS X, Tru64/OSF1, Windows NT4.0, Windows 2000, Windows 2003, Windows XP, Windows Vista);
- моніторинг без агентів;
- безпечна аутентифікація користувачів;
- гнучка система прав доступу користувачів;
- Web- інтерфейс;
- гнучка система повідомлень по e-mail про зумовлені події;
- високорівневий вид контролю ресурсу (класу «Бізнес»);
- журнал аудитора.

(Рис. 3.6 – Zabbix у роботі)

Очевидні плюси Zabbix:

- відкрите програмне забезпечення;
- агенти з високою ефективністю для UNIX і WIN32 платформ;
- легко вивчається;
- збільшує рентабельність;
- низька вартість обслуговування;
- дуже проста конфігурація;
- централізована система моніторингу. Уся інформація (конфігурація і дані про продуктивність) зберігаються в реляційній базі даних;
- високорівневе дерево послуг;
- дуже просте встановлення підтримки SNMP (v1, v2, v3). Обидва режими пуллера і траппера;
- можливість візуалізації;
- вбудований механізм очищення застарілих динних.

3.4. Порівняльний аналіз

Будь-яка система моніторингу, у тому числі моніторингу мережевих пристроїв - це складна інформаційна система, що включає в себе:

- метрики мережевих пристроїв (центральний процесор, температура, доступність пристроїв, втрати пакетів, помилки на інтерфейсах, доступна смуга пропускання та інші критично важливі параметри, за значеннями яких необхідно вести спостереження;
- моніторинг - процес збору, агрегації і аналізи метрик для поліпшення розуміння характеристик і проведення компонентів системи. У цей пункт входить також візуалізація зібраних даних по метриках в різні графіки, діаграми, гістограми;
- систему сповіщень - не менш важливий компонент, оскільки виконує дії на основі змін метрики. Досягши критичного порогу значення метрики може спробувати самостійно виправити проблему за заготовленим сценарієм або відправити сповіщення відповідальній особі засобами sms, електронної пошти і т. д.

В результаті аналізу порівнюваних систем моніторингу виявлені наступні критичні недоліки:

- при використанні RRD (Файл набору даних зі зниженим розширенням) в Nagios втрачається деталізація старих даних;
- конфігурація в Pandora FMS та Nagios змінюється за допомогою змінення файлу конфігурації, але нова конфігурація застосовується тільки під час перезапуску служби Nagios, що при великій кількості зібраних метрик може займати декілька десятків хвилин, а отже, система не функціонуватиме в цей час;
- Zabbix має менш критичні недоліки, пов'язані з візуалізацією даних, що слабо впливає на основні функціональні можливості системи;

Система	**Автоматичне виявлення**	**Підтримка SNMP**	**Плагіни**	**Система сповіщень**	**Спосіб зберігання даних**	**Ліцензія**
Pandora FMS	Через плагін	Так	Так	Через плагін	RRDTool	GPL
Nagios	Через плагін	Через плагін	Так	Так	RRDTool, MySQL через плагін	GPL
Zabbix	Так	Так	Так	Так	Oracle, MySQL, PostgreSQL, IBM DB2, SQLite	GPL

(Рис. 3.7 – зведена таблиця можливостей порівнюваних систем)

Система	**CPU, %**	**RAM, %**
Pandora FMS	10	22
Nagios	14	25
Zabbix	12	25

(Рис. 3.8 – споживання ресурсів системами)

Загалом, найменш ресурсоємною системою є Pandora FMS, найбільш ресурсоємною - Nagios. Але через описані недоліки і необхідність використання великої кількості сторонніх плагінів для Pandora FMS і

Nagios, а також через складнощі масштабування цих систем, найкращим вибором для моніторингу великої кількості метрик визнаний - Zabbix.

ВИСНОВКИ

Для компанії знадобляться одна або декілька програм-інструментів, які б охопили всі елементи, що потребують моніторингу.

Плануючи купувати моніторинговий інструмент, важливо заздалегідь запланувати перелік характеристик, які він контролюватиме. З таким списком буде простіше підібрати інструмент, контролюючий їх. При цьому варто розуміти, що якщо конкретний інструмент не робить моніторинг важливого для вас параметра, то заповнити цей пропуск можливо, завдяки недорогій або навіть безкоштовній утиліті.

Програм-інструментів для перевірки мережі компанії сьогодні пропонується багато. Велика їх частина припускає моніторинг комутаторів, серверів, баз даних і комп'ютерів підприємства.

За допомогою інструменту для моніторингу можливо:

- дізнатися про виниклі проблеми (розривах з'єднання, зупинці процесів і служб, ушкодженні каналу зв'язку, відсутності місця на диску);
- усунути проблему відразу, ще до того, як вона стане нерозв'язною: будуть порушені процеси, втрачені дані;
- вести перевірку файлів, хостів, серверів, служб і баз даних на мережевому устаткуванні і комп'ютерах, які розміщені в загальній виробничій мережі.

Дуже важливо, щоб будь-яка сучасна програма моніторингу локальної мережі підприємства накопичувала і зберігала статистику опитувань. З її допомогою можна провести IT аудит і проаналізувати продуктивність і поведінку конкретних пристроїв і мережі в цілому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1) Sophon Mongkolluksamee, Panita Pongpaibool, Chavee Issariyapat, “Strengths and Limitations of Nagios as a Network Monitoring Solution” Proceedings of the 7th International Joint Conference on Computer Science and Software Engineering (JCSSE 2010) Vol. 1, pp. 96-101, Bangkok, Thailand, May 2010
2) Центры обработки данных [Електронний ресурс] – Режим доступу до ресурсу: http://www.tadviser.ru/index.php
3) Ahmed D. Kora and Moussa Moindze Soidridine, “Nagios based enhanced IT management system,” Interntional Journal of Engineering Science and Technology, vol. 4, no. 3, pp. 818–822, 2012.
4) https://www.ussc.ru/solutions/inzhenernye-sistemy/tsentry-obrabotki-dannykh/
5) SpringGraph Flex Component. (n.d). [Електронний ресурс] – Режим доступу до ресурсу: http://markshepherd.com/SpringGraph/
6) NSClient++ for Windows, Secure monitoring daemon, Retrieved December 2012). [Електронний ресурс] – Режим доступу до ресурсу: http://www.nsclient.org/nscp/wiki/doc/about/0.4.x
7) https://alp-itsm.ru/interesting/monitoring_seti_predpriyatiya/
8) https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BC%D0%BE%D0%BD%D1%96%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3%D1%83
9) D. Doug, B. James R., M. High, “Best of open source networking software,”infoworld.com, Aug 31, 2009.
10) Cisco Systems, Inc., "Enterprise Campus 3.0 Architecture: Overview and Framework," 2008. [Електронний ресурс] – Режим доступут до ресурсу:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html.