SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #7. Впровадження систем моніторингу на основі Wazuh та MS SCOM.*

План лекції . Тема 7. Впровадження систем моніторингу на основі Wazuh та MS SCOM.

- Огляд Wazuh як відкритої платформи для моніторингу безпеки.
- Огляд MS SCOM як інструменту системного моніторингу від Microsoft.
- Моніторинг та виявлення загроз безпеки за допомогою Wazuh та MS SCOM.

Вступ.

Сучасна інформаційна безпека стає невід'ємною складовою успішної діяльності будь-якої організації, незалежно від її розміру або сфери діяльності. Однак, із зростанням кількості та складності кіберзагроз, потреба у забезпеченні безпеки стає все більш критичною.

Саме тому сьогодні ми розглянемо дві потужні платформи: ***Wazuh*** і ***Microsoft System Center Operations Manager (SCOM)***. Wazuh, як відкрита платформа для моніторингу безпеки, надає широкі можливості з виявлення та реагування на потенційні загрози для інформаційної безпеки вашої організації. З іншого боку, MS SCOM, розроблений Microsoft, є потужним інструментом системного моніторингу, який допомагає у виявленні, діагностиці та вирішенні проблем у реальному часі.

Метою лекції є детальний розгляд цих двох систем, від їх огляду та основних принципів функціонування до базового налаштування та практичного застосування для моніторингу та виявлення загроз безпеки. Ми розглянемо процес підготовки та налаштування як Wazuh-сервера та агентів, так і MS SCOM, а також проаналізуємо методи моніторингу та реагування на потенційні загрози з використанням цих інструментів.

Огляд Wazuh як відкритої платформи для моніторингу безпеки

Wazuh - це відкрита платформа для моніторингу безпеки, яка поєднує в собі можливості ELK Stack та розширення Wazuh до ELK Stack для виявлення загроз безпеки та реагування на них. Нагадаю, що ELK Stack це комплект відкритих програмних рішень Elasticsearch, Logstash та Kibana.

Wazuh починався як проект, заснованої у 2015 році однойменної компанії, що розширює функціональність ELK Stack, додавши можливості моніторингу безпеки. В основі Wazuh лежить інтеграція з ELK Stack, що дозволяє збирати, аналізувати та візуалізувати журнальні дані безпеки.
З часом, розвиток проекту Wazuh призвів до того, що він став самостійною платформою для моніторингу безпеки, яка включає в себе не тільки ELK Stack, але й інші компоненти та функціонал. Таким чином, Wazuh не просто розширює ELK Stack, але створює власну платформу, спеціалізовану на моніторингу безпеки. Вона використовується для виявлення та реагування на загрози безпеки в IT-інфраструктурі.

Основні версії Wazuh:

- ✓ Wazuh 2.x: Випущений близько 2017 року.
- ✓ Wazuh 3.x: Був випущений приблизно в 2018 році.
- ✓ Wazuh 4.x: Остання версія, яка була випущена приблизно у 2020 році.

Ці роки є лише наближеними і можуть відрізнятися залежно від конкретних випусків підверсій та точних дат. На момент написання цього документу актуальна версія Wazuh – 4.7.2.

Платформа Wazuh надає функції захисту робочих навантажень хмари, контейнера та серверу за допомогою двох важливих інструментів кібербезпеки:

XDR (Extended Detection and Response):

- ✓ **Розширене виявлення та реагування**: XDR – це комплексна стратегія кібербезпеки, яка використовує дані з різних джерел для виявлення та реагування на кіберзагрози.
- ✓ **Консолідація даних**: XDR об'єднує дані з телеметрії кінцевих точок, мережевого трафіку, журналів та інших джерел для отримання цілісного уявлення про кібербезпеку організації.
- ✓ **Автоматизація**: XDR використовує машинне навчання та інші методи автоматизації для пришвидшення виявлення та реагування на кіберзагрози.

SIEM (Security Information and Event Management):

- ✓ **Управління інформацією та подіями безпеки**: SIEM – це програмний продукт, який збирає та аналізує журнали безпеки та інші дані з різних джерел для виявлення кіберзагроз.
- ✓ **Кореляція подій**: SIEM корелює події з різних джерел, щоб ідентифікувати потенційні кіберзагрози, які інакше могли б залишитися непоміченими.
- ✓ **Моніторинг та оповіщення**: SIEM використовується для моніторингу мережі та систем на наявність ознак кібератак та для надсилання оповіщень про виявлені загрози.

XDR та SIEM доповнюють один одного, XDR фокусується на виявленні та реагуванні, а SIEM – на зборі та аналізі даних. Використання XDR та SIEM разом може значно покращити кібербезпеку організації.

Переваги Wazuh:

- ➢ **Відкритість:** Wazuh - це проект з відкритим кодом, що дає користувачам доступ до його коду та можливість його модифікації.
- ➢ **Безкоштовність:** Wazuh можна використовувати безкоштовно, що робить його доступним для організацій з обмеженим бюджетом.
- ➢ **Гнучкість:** Wazuh може використовуватися для моніторингу різних типів систем, включаючи сервери, робочі станції, мережеві пристрої та хмарні середовища.
- ➢ **Кросплатформенність**: Є кросплатформеним рішенням, що означає, що воно підтримується та може бути встановлене на різних операційних системах. Основні операційні системи, на яких можна встановити Wazuh, включають:
  - ✓ **Linux**: Wazuh підтримує багато дистрибутивів Linux, таких як Ubuntu, CentOS, Debian, Fedora, Red Hat Enterprise Linux (RHEL), openSUSE тощо.
  - ✓ **Windows**: Wazuh також може бути встановлено на операційних системах Windows, що дозволяє користувачам моніторити безпеку в їхніх середовищах Windows.
  - ✓ **macOS**: Версії Wazuh також доступні для встановлення на комп'ютери з операційною системою macOS, що дозволяє користувачам забезпечити безпеку своїх систем Mac.

SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #7. Впровадження систем моніторингу на основі Wazuh та MS SCOM.*

Кросплатформеність Wazuh робить його дуже гнучким і придатним для різних установок та інфраструктур. Це означає, що незалежно від того, яка операційна система використовується в вашій організації, ви можете встановити та використовувати Wazuh для моніторингу та забезпечення безпеки вашої інфраструктури.

- **Масштабованість:** Wazuh може масштабуватися для моніторингу великих IT-інфраструктур.
- **Простота використання:** Wazuh має інтуїтивно зрозумілий інтерфейс користувача, що робить його доступним для користувачів з різним досвідом.

Компоненти Wazuh

Рішення Wazuh базується на агентах Wazuh, які розгортається на контрольованих кінцевих точках, і на трьох центральних компонентах:

- Сервері – Wazuh Server
- Індексаторі – Wazuh indexer
- Інформаційній панелі – Wazuh dashboard

Wazuh Indexer

Індексатор Wazuh (Wazuh indexer) — це система повнотекстового пошуку та аналітики даних безпеки в реальному часі. Дані журналу, що надходять на сервер Wazuh, аналізуються та пересилаються до індексатора для індексування та зберігання. Ці події потім запитуються на інформаційній панелі Wazuh.

Індексатор Wazuh зберігає дані як документи JSON. Кожен документ пов'язує набір ключів, імен полів або атрибутів із відповідними значеннями, якими можуть бути символи, числа, логічні значення, дати, масиви значень, геолокації чи інші види даних.

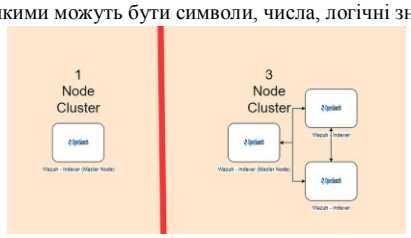


Рис. 07.01. Кластер з 1 вузлом і 3 вузлами

Індексатор Wazuh можна налаштувати як одновузловий або багатовузловий кластер, що забезпечує масштабованість і високу доступність. Він розподіляє документи між різними контейнерами, відомими як сегменти. У свою чергу, він розподіляє ці фрагменти між вузлами кластера. Розподіляючи документи між декількома шардами та розподіляючи ці сегменти між кількома вузлами, індексатор Wazuh забезпечує надлишковість. Надлишковість забезпечує доступність індексатора Wazuh у разі збою та збільшує пропускну здатність для запитів між вузлами кластера.

Індекси індексатора Wazuh. Покажчик — це сукупність документів, які пов'язані між собою. Індексатор Wazuh використовує індекси для зберігання та організації даних безпеки для швидкого пошуку. Wazuh використовує такі шаблони індексів для зберігання цих даних:

- wazuh-alerts-* : це шаблон індексу для сповіщень, створених сервером Wazuh.
- wazuh-archives-* : це шаблон індексу для всіх подій, надісланих на сервер Wazuh.
- wazuh-monitoring-* : це шаблон індексу для статусу агентів Wazuh.
- wazuh-statistics-* : це шаблон індексу для статистичної інформації сервера Wazuh.

Система підтримує створення спеціальних шаблонів індексу або зміну стандартного шаблону індексу.

Інформація про індекси Wazuhможе бути перевірена двома способами.

- З використанням веб-інтерфейсу користувача.
- Створенням запиту до API індексатора Wazuh.

Переіндексація. Коли в схему даних вносяться зміни, виникає необхідність повторно індексувати дані, щоб відобразити ці зміни. Існуючі дані можуть не відповідати оновленій схемі без повторного індексування, що призведе до невідповідності даних або помилок під час запитів. Повторне індексування дає змогу копіювати всі або частину ваших даних із вихідного індексу в індекс призначення.

Стандарти безпеки вимагають зберігати дані доступними для аудиту протягом мінімального періоду часу. Дані, які зберігаються довше цього терміну, можуть бути видалені, щоб заощадити місце для зберігання.

Також можливо визначити спеціальні політики для автоматичного видалення даних.

Wazuh Server

Сервер Wazuh аналізує дані, отримані від агентів. Він обробляє їх через декодери та правила, використовуючи аналіз загроз для пошуку добре відомих індикаторів компрометації (IOC). Один сервер може аналізувати дані від сотень або тисяч агентів і масштабувати горизонтально, якщо налаштувати його як кластер. Цей центральний компонент також використовується для керування агентами, налаштування та оновлення їх віддалено, коли це необхідно.

Сервер Wazuh складається з кількох перелічених нижче компонентів, які мають різний функціонал, наприклад реєстрацію нових агентів, перевірку ідентифікації кожного агента та шифрування зв'язку між агентом Wazuh і сервером Wazuh.

- **Служба реєстрації агентів** використовується для реєстрації нових агентів. Служба надає та розповсюджує унікальні ключі автентифікації кожному агенту. Процес працює як мережева служба та підтримує автентифікацію за допомогою сертифікатів TLS/SSL або шляхом надання фіксованого пароля.
- **Служба підключення агентів** отримує дані від агентів. Служба використовує ключі, спільні для служби реєстрації, для перевірки ідентифікації кожного агента та шифрування зв'язку між агентом Wazuh і сервером Wazuh. Крім того, служба підключення агентів забезпечує централізоване керування конфігурацією, що дозволяє віддалено надсилати нові параметри агентам.
- **Механізм аналізу** це - серверний компонент, який виконує аналіз даних. Він використовує декодери для визначення типу інформації, що обробляється (події Windows, журнали SSH, журнали веб-сервера та інші). Ці декодери також «витягують» відповідні елементи даних із повідомлень журналу, такі як IP-адреса джерела, ідентифікатор події або ім'я користувача. Потім, використовуючи правила, механізм визначає конкретні шаблони в розшифрованих подіях, які можуть ініціювати сповіщення та, можливо, навіть викликати автоматичні контрзаходи (наприклад, блокування IP-адреси, зупинка запущеного процесу або видалення артефакту зловмисного програмного забезпечення).

SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #7. Впровадження систем моніторингу на основі Wazuh та MS SCOM.*

- **Wazuh RESTful API**. Необхідно розпочати з значення абревіатури назви компоненту. RESTful API розшифровується як Representational State Transfer Application Programming Interface. REST - це архітектурний стиль для веб-сервісів, API - це інтерфейс програмування, який дозволяє двом програмам взаємодіяти одна з одною. Таким чином, RESTful API - це API, який використовує архітектурний стиль REST для надання доступу до ресурсів. RESTful API надає інтерфейс для взаємодії з інфраструктурою Wazuh. Він використовується для керування параметрами конфігурації агентів і серверів, моніторингу стану інфраструктури та загального стану здоров'я, керування та редагування декодерів і правил Wazuh, а також запиту про стан контрольованих кінцевих точок. Інформаційна панель Wazuh також використовує його.
- **Wazuh cluster daemon** використовується для горизонтального масштабування серверів Wazuh, розгортаючи їх як кластер. Така конфігурація в поєднанні з балансувальником мережевого навантаження забезпечує високу доступність і балансування навантаження. Демон кластера Wazuh — це те, що сервери Wazuh використовують для спілкування один з одним і підтримки синхронізації.
- **Filebeat** використовується для надсилання подій і сповіщень до індексатора Wazuh. Він зчитує вихід аналітичної системи Wazuh і передає події в реальному часі а також забезпечує балансування навантаження при підключенні до багатовузлового кластера індексатора Wazuh.

Рис. 07.02. Wazuh Server та агенти у структур Wazuh

Wazuh dashboard

Інформаційна панель Wazuh — це веб-інтерфейс користувача для візуалізації та аналізу даних. Він включає в себе готові інформаційні панелі для

- ✓ подій безпеки
- ✓ нормативної відповідності
- ✓ виявлені вразливості програм
- ✓ дані моніторингу цілісності файлів
- ✓ результати оцінки конфігурації
- ✓ моніторинг хмарної інфраструктури
- ✓ події та ін.

Інформаційна панель Wazuh також використовується для керування конфігурацією Wazuh і моніторингу її стану.
Агенти Wazuh встановлюються на кінцевих точках, таких як ноутбуки, настільні комп'ютери, сервери, хмарні екземпляри або віртуальні машини. Вони забезпечують запобігання загрозам, їх виявлення та реагування. Вони працюють на таких операційних системах, як Linux, Windows, macOS, Solaris, AIX і HP-UX.
На додаток до можливостей моніторингу на основі агентів, платформа Wazuh може контролювати безагентні пристрої, такі як брандмауери, комутатори, маршрутизатори або мережі IDS, серед іншого. Наприклад, дані системного журналу можна збирати через Syslog, а його конфігурацію можна відстежувати шляхом періодичного тестування даних, через SSH або через API.
На діаграмі нижче показано компоненти та потік даних Wazuh.

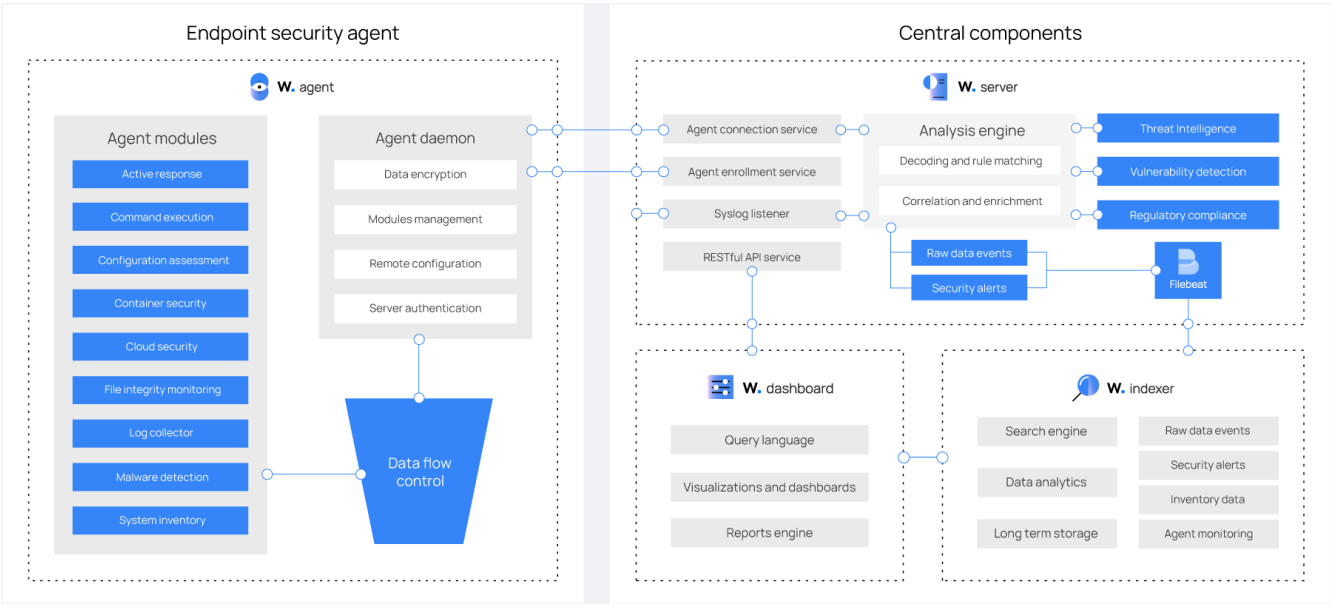


Рис. 07.03. Компоненти та потоки даних Wazuh

Архітектура Wazuh

Архітектура Wazuh базується на агентах , які працюють на контрольованих кінцевих точках і передають дані безпеки на центральний сервер . Безагентні пристрої, такі як брандмауери, комутатори, маршрутизатори та точки доступу, підтримуються та можуть активно надсилати дані журналу через Syslog, SSH або за допомогою свого API. Центральний сервер декодує та аналізує вхідну інформацію та передає результати в індексатор Wazuh для індексування та зберігання.

Кластер індексатора Wazuh — це набір з одного або кількох вузлів, які спілкуються один з одним для виконання операцій читання та запису в індексах. Невеликі розгортання Wazuh, які не вимагають обробки великих обсягів даних, можуть бути легко оброблені кластером з одним вузлом.

SNM. #3. Інструменти моніторингу та аналізу даних ***

Системний *та мережевий моніторинг. Лекція #7. Впровадження систем моніторингу на основі Wazuh та MS SCOM.*

Багатовузлові кластери рекомендуються, якщо є багато контрольованих кінцевих точок, коли очікується великий обсяг даних або коли потрібна висока доступність.

Кластеризація серверів Wazuh це цікавий та сучасний приклад реалізації масштабування. Реалізація можлива починаючи з версії Wazuh 3.x (2018 рік). По суті, може бути кілька серверів, які працюють разом у режимі кластера та містять протокол, що дозволяє їм обмінюватися інформацією, необхідною для керування підключенням агентів. Іншими словами, агенти зможуть звітувати перед будь-яким нодом (сервером) у кластері, який розподілятиме навантаження між різними вузлами (нодами) та забезпечуватиме можливості високої доступності.

Як показано на рис 07.02, архітектура кластера базується на головному/клієнтському серверах. Головні вузли будуть відповідати за централізацію всієї конфігурації та керування Wazuh.

У рамках кластеризації можливе групування агентів, щоб налаштувати конкретну конфігурацію, політику кореневої перевірки та перевірку надійності для певної групи. Для кожної групи, сервер дистанційно надсилатиме агентам відповідні файли, автоматично застосовуючи зміни

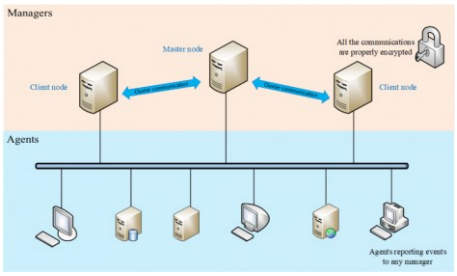


Рис. 07.04. Кластерізація менеджерів Wazuh

Для робочих середовищ рекомендується розгортати сервер Wazuh та індексатор Wazuh на різних хостах. У цьому сценарії Filebeat використовується для безпечного пересилання сповіщень Wazuh і заархівованих подій до кластера індексатора Wazuh (з одним або кількома вузлами) за допомогою шифрування TLS.

На рис.07.03 показано архітектуру розгортання Wazuh. Він показує компоненти рішення та те, як сервер Wazuh і вузли індексатора Wazuh можуть бути налаштовані як кластери, забезпечуючи балансування навантаження та високу доступність.

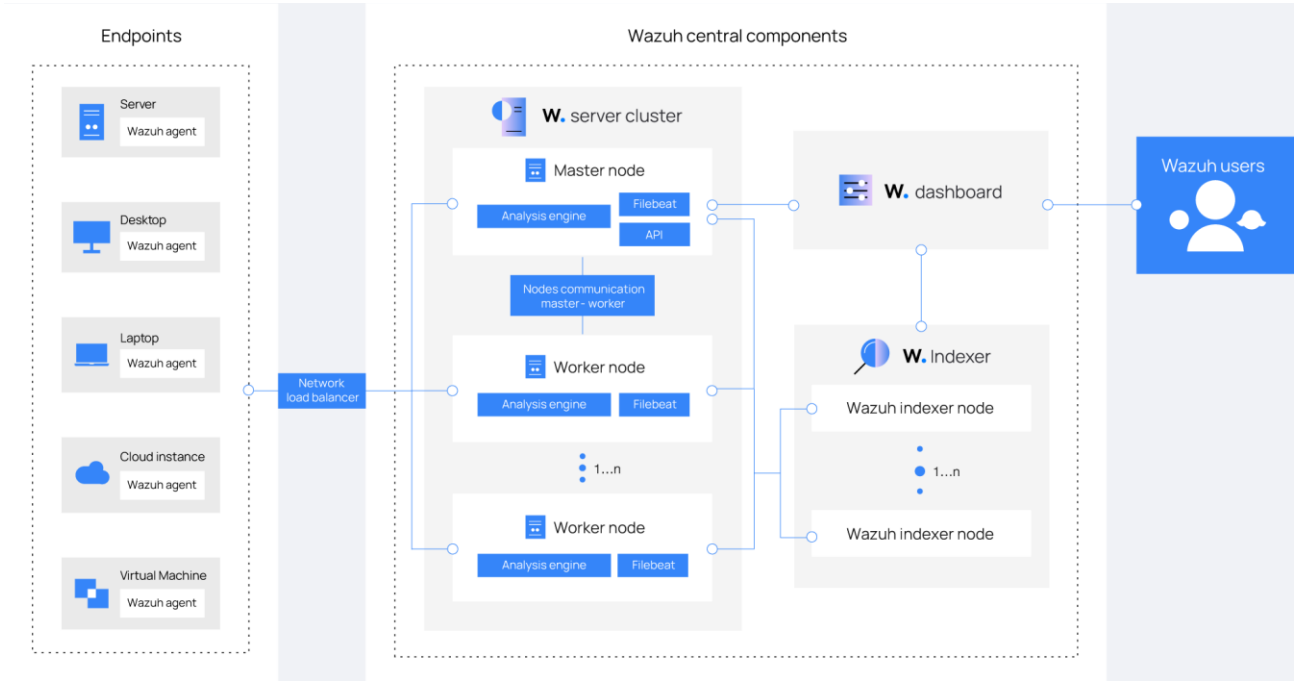


Рис. 07.05. Архітектура розгортання Wazuh

Агент Wazuh постійно надсилає події на сервер Wazuh для аналізу та виявлення загроз. Щоб розпочати надсилання цих даних, агент встановлює з'єднання зі службою сервера для підключення агента, який прослуховує порт 1514 за замовчуванням (номер порту можливо змінити налаштуванням). Потім сервер Wazuh декодує та перевіряє за правилами отримані події, використовуючи механізм аналізу. Події, які запускають правило, доповнюються даними попередження, такими як ідентифікатор правила та назва правила. Події можуть бути передані в один або два файли журналів, в залежності від того, чи спрацьовує правило:

- /var/ossec/logs/archives/archives.json містить усі події незалежно від того, чи спрацювало вони правило чи ні.
- /var/ossec/logs/alerts/alerts.json містить лише події, які спрацювали за правилом із достатньо високим пріоритетом (поріг можна налаштувати).

Протокол повідомлень Wazuh за замовчуванням використовує шифрування AES 128 біт на блок і 256-бітними ключами. Шифрування Blowfish необов'язкове.

Сервер Wazuh використовує Filebeat для надсилання даних попереджень і подій до індексатора Wazuh за допомогою шифрування TLS. Filebeat зчитує вихідні дані сервера Wazuh і надсилає їх до індексатора Wazuh (за замовчуванням прослуховує порт 9200/TCP). Коли дані проіндексовано індексатором Wazuh, інформаційна панель Wazuh використовується для аналізу та візуалізації інформації.

SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #7. Впровадження систем моніторингу на основі Wazuh та MS SCOM.*
Інформаційна панель Wazuh запитує Wazuh RESTful API (за замовчуванням прослуховує порт 55000/TCP на сервері Wazuh), щоб відобразити конфігурацію та інформацію про стан сервера та агентів Wazuh . Він також може змінювати параметри конфігурації агентів або сервера через виклики API. Цей зв'язок шифрується за допомогою TLS і автентифікується за допомогою імені користувача та пароля.

Кілька служб використовуються для зв'язку компонентів Wazuh. Не будемо детально зупинятися на списку стандартних портів, які використовуються цими службами. При потребі їх можна розглянути у документації.

Як сповіщення, так і події, що не стосуються сповіщень, зберігаються у файлах на сервері Wazuh, а також надсилаються до індексатора Wazuh. Ці файли можуть бути записані у форматі JSON (.json) або звичайному текстовому форматі (.log). Файли щодня стискаються та підписуються за допомогою контрольних сум MD5, SHA1 і SHA256. Структура каталогу та імені файлу наступна:
root@wazuh-manager:/var/ossec/logs/archives/2024/Mar# ls -l

```
total 176
-rw-r----- 1 wazuh wazuh 234350 Mar  2 00:00 ossec-archive-01.json.gz
-rw-r----- 1 wazuh wazuh    350 Mar  2 00:00 ossec-archive-01.json.sum
-rw-r----- 1 wazuh wazuh 176221 Mar  2 00:00 ossec-archive-01.log.gz
-rw-r----- 1 wazuh wazuh    346 Mar  2 00:00 ossec-archive-01.log.sum
-rw-r----- 1 wazuh wazuh 224320 Mar  2 00:00 ossec-archive-02.json.gz
-rw-r----- 1 wazuh wazuh    350 Mar  2 00:00 ossec-archive-02.json.sum
-rw-r----- 1 wazuh wazuh 151642 Mar  2 00:00 ossec-archive-02.log.gz
-rw-r----- 1 wazuh wazuh    346 Mar  2 00:00 ossec-archive-02.log.sum
-rw-r----- 1 wazuh wazuh 315251 Mar  2 00:00 ossec-archive-03.json.gz
-rw-r----- 1 wazuh wazuh    350 Mar  2 00:00 ossec-archive-03.json.sum
-rw-r----- 1 wazuh wazuh 156296 Mar  2 00:00 ossec-archive-03.log.gz
-rw-r----- 1 wazuh wazuh    346 Mar  2 00:00 ossec-archive-03.log.sum
```

Рекомендується ротація та резервне копіювання архівних файлів відповідно до обсягу пам'яті сервера Wazuh . Використовуючи завдання cron, легко налаштовується зберігання лише певного часового проміжку архівних файлів локально на сервері, наприклад, минулого року чи останніх трьох місяців.
З іншого боку, можна відмовитися від зберігання архівних файлів і просто покластися на індексатор Wazuh для зберігання архіву. Ця альтернатива може бути кращою, якщо періодично виконується резервне копіювання моментальних знімків індексатора Wazuh або є багатовузловий кластер індексатора Wazuh з копіями фрагментів для високої доступності. Для цього також можна використовувати завдання cron, щоб перемістити знімки індексів на кінцевий сервер зберігання даних і підписати їх за допомогою алгоритмів хешування.

Можливості Wazuh

- **Моніторинг цілісності файлів:** Wazuh може відстежувати зміни файлів та повідомляти про підозрілу активність.
- **Моніторинг журналів:** Wazuh може збирати та аналізувати журнали з різних систем для виявлення загроз безпеки.
- **Моніторинг мережі:** Wazuh може відстежувати мережевий трафік та повідомляти про підозрілу активність.
- **Виявлення вторгнень:** Wazuh може використовувати правила Snort для виявлення вторгнень.
- **Моніторинг аномалій:** Wazuh може використовувати машинне навчання для виявлення аномальної поведінки.
- **Реагування на інциденти:** Wazuh може автоматизувати дії реагування на інциденти.

Wazuh – це система виявлення вторгнень (IDS) та система запобігання вторгненням (IPS), а не всебічний інструмент моніторингу та кібербезпеки. Треба розуміти, що Wazuh не має вбудованих функцій для моніторингу продуктивності та веб-додатків, не є антивірусом, не має вбудованих функцій для шифрування даних, не може моніторити хмарні інфраструктури без додаткових плагінів або інтеграцій, не може автоматично виправляти вразливості, не має вбудованих функцій для моніторингу IoT-пристроїв та не має вбудованих функцій для моніторингу контейнерів та баз даних.

Використання Wazuh для моніторингу цілісності файлів
Для цієї задачі Wazuh використовує модуль File Integrity Monitoring (FIM), що відстежує та сповіщає про зміни критичних файлів і каталогів та швидко виявляти зміни файлів, які вказують на компрометацію чи кібератаку. Використання FIM надає Wazuh наступні особливості:

- **Моніторинг в реальному часі - виявлення змін файлів і реакція на них у реальному часі.** Wazuh відстежує системні файли та каталоги в режимі реального часу, щоб виявляти зміни, коли вони відбуваються, і запускає сповіщення, які дозволяють негайно вжити заходів. Це допомагає організаціям пом'якшити вплив інцидентів безпеки

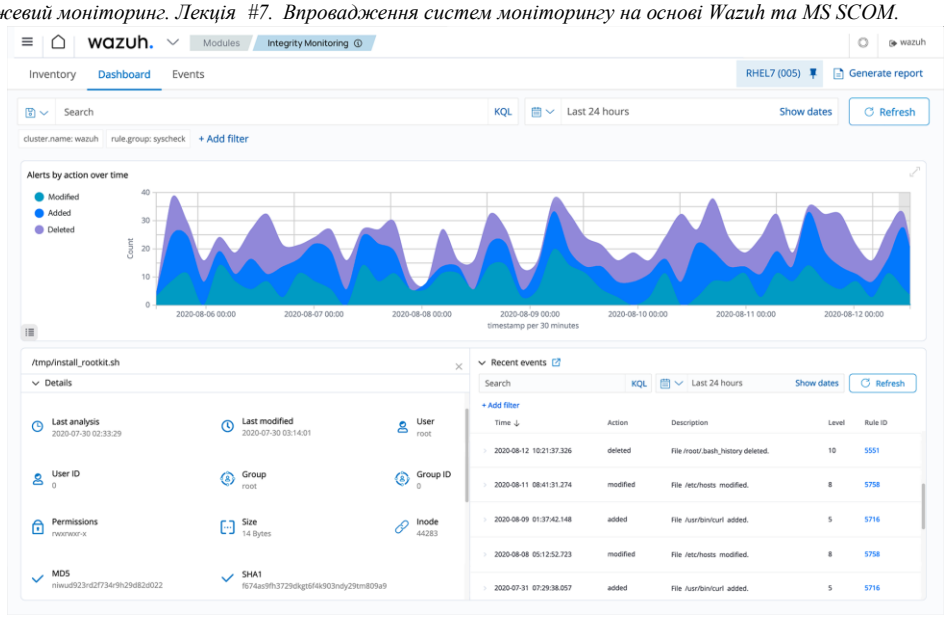
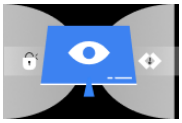


Рис. 07.06. DashBoard Wazuh



- **Виявлення порушень безпеки та втручання в систему за допомогою Wazuh FIM (File Integrity Monitoring)** - модуль вбудований в Wazuh, що використовується для моніторингу та оповіщення про зміни в критичних файлах та директоріях. Wazuh відстежує файли та каталоги, відстежуючи атрибути, дозволи, право власності та вміст. Він використовує хеш-значення для виявлення змін у файловій системі, виявлення зловмисних дій і зменшення внутрішніх загроз від окремих осіб або постачальників.
  Як працює Wazuh FIM:
  1. **Сканування**: Модуль FIM періодично сканує певні шляхи та моніторить певні директорії в режимі реального часу. Ви можете встановити, які шляхи моніторити в конфігурації агентів та менеджера Wazuh.
  2. **Базова лінія**: FIM створює базову лінію, зберігаючи криптографічну контрольну суму та інші атрибути моніторингових файлів.
  3. **Порівняння**: FIM порівнює інформацію базової лінії з інформацією про останню версію файлу. Це порівняння дає видимість змін та оновлень критичних файлів.
  4. **Оповіщення**: Якщо FIM виявляє будь-які зміни в моніторингових файлах, він генерує сповіщення, яке може бути відправлене на різні канали, такі як електронна пошта, SNMP або syslog.
- **Відповідність нормативним вимогам щодо безпеки даних і конфіденційності.** Wazuh допомагає відстежувати модифікації важливих файлів і каталогів, щоб вони відповідали нормам, таким як PCI DSS, HIPAA, NIST 800-53, TSC і GDPR. Використовуючи модуль Wazuh FIM, ви можете продемонструвати аудиторам і регуляторам, що вжили заходів для підтримки безпеки та цілісності даних.

- **Централізоване управління** - відстеження змін файлів на кількох кінцевих точках із центрального розташування. Інформаційна панель Wazuh дозволяє налаштовувати політики FIM і керувати ними, аналізувати сповіщення та виконувати адміністративні завдання. Він пропонує вичерпні звіти про зміни файлів, надаючи докладну інформацію про повідомлені зміни

- **Масштабованість** - ефективне відстеження файлів та каталогів незалежно від обсягу даних. Розподілена архітектура Wazuh забезпечує масштабовану роботу модуля FIM шляхом розподілу робочого навантаження між кількома вузлами. Це забезпечує ефективне керування великою кількістю файлів і каталогів.

Кросплатформена підтримка – захист важливих та системних файлів в кількох операційних системах за допомогою модуля Wazuh FIM. Wazuh FIM підтримує різні операційні системи, включаючи Windows, Linux і macOS. Він забезпечує міжплатформну підтримку для моніторингу змін файлів у всій вашій IT-інфраструктурі, дозволяючи захистити вас від несанкціонованих змін і потенційних порушень безпеки.

Методи встановлення Wazuh

- **Вимоги до обладнання** значною мірою залежать від кількості захищених кінцевих точок і хмарних робочих навантажень. Це число може допомогти оцінити, скільки даних буде проаналізовано та скільки сповіщень безпеки буде збережено та проіндексовано.
  Комплекту центральних компонентів (Wazuh server, indexer, dashboard) на одному хості достатньо для моніторингу до 100 кінцевих точок і для 90 днів запитуваних/індексованих даних попереджень. У таблиці нижче показано рекомендована конфігурація для швидкого розгортання:

Агенти	CPU	RAM	Зберігання (90 днів)
1–25	4 vCPU	8 Гб	50 ГБ
25–50	8 vCPU	8 Гб	100 ГБ

50–100	8 vCPU	8 Гб	200 ГБ

Для великих середовищ ми рекомендуємо розподілене розгортання. Конфігурація кластера з кількома вузлами доступна для сервера Wazuh і для індексатора Wazuh, що забезпечує високу доступність і балансування навантаження.

- **Операційна система.** Центральні компоненти Wazuh можна встановити на 64-бітну операційну систему Linux. Wazuh рекомендує будь-яку з наступних версій ОС: Amazon Linux 2, CentOS 7, 8, Red Hat Enterprise Linux 7, 8, 9, Ubuntu 16.04, 18.04, 20.04, 22.04

- **Стандартне встановлення Wazuh.** Завантажте та запустіть помічника встановлення Wazuh.
  curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh –a
  Коли помічник завершить інсталяцію, у вихідних даних відобразяться облікові дані доступу та повідомлення, яке підтверджує, що інсталяція пройшла успішно.

  INFO: --- Summary ---
  INFO: You can access the web interface https://<wazuh-dashboard-ip>
  User: admin
  Password: <ADMIN_PASSWORD>
  INFO: Installation finished.

  Wazuh встановлено та налаштовано. Доступ до веб-інтерфейсу Wazuh за допомогою
  https://<wazuh-dashboard-ip>
  Облікові дані:
  Ім'я користувача: admin
  Пароль: <ADMIN_PASSWORD>
  Коли доступ до інформаційної панелі Wazuh отримано вперше, браузер показує попередження про те, що сертифікат не був виданий довіреним центром. Це очікувано, і користувач має можливість прийняти сертифікат як виняток або, альтернативно, налаштувати систему на використання сертифікату від довіреного центру.
  Можливо розпочати розгортання агентів Wazuh, що використовуються для захисту ноутбуків, настільних ПК, серверів, хмарних примірників, контейнерів або віртуальних машин. Агент легкий і багатоцільовий. Інструкції щодо розгортання агентів Wazuh можна знайти у веб-інтерфейсі користувача Wazuh або в документації .

- **Встановлення Wazuh розгортанням готових до використання машини**
  - ✓ **Віртуальна машина (OVA).** Wazuh надає попередньо зібраний образ віртуальної машини (OVA), який можна імпортувати безпосередньо за допомогою VirtualBox або інших систем віртуалізації, сумісних з OVA.
  - ✓ **Образи машини Amazon (AMI).** Попередньо створений образ машини Amazon (AMI), який можна запускати безпосередньо в хмарному екземплярі AWS.

- **Встановлення контейнерів.**
  - ✓ **Розгортання на Docker**. Docker — це набір продуктів платформи як послуги (PaaS), які доставляють програмне забезпечення в пакетах, які називаються контейнерами. За допомогою Docker ви можете встановити та налаштувати розгортання Wazuh як архітектуру з одним хостом.
  - ✓ **Розгортання на Kubernetes**. Kubernetes — це система з відкритим кодом для автоматизації розгортання, масштабування та керування контейнерними програмами. Цей тип розгортання використовує зображення Wazuh із Docker і дозволяє створювати середовище Wazuh.

Порівняння Wazuh з іншими платформами моніторингу безпеки

Порівняємо Wazuh з іншими популярними платформами моніторингу безпеки, що підтримують більшість сучасних операційних платформ. Порівняння виконується з Splunk Enterprise Security, IBM QRadar, та Elastic Security (раніше відомий як Elasticsearch SIEM).

Платформа	Особливості платформи	Ліцензійна політика	Агентна структура
Wazuh	Відкритий код: Wazuh - це відкрита платформа з відкритим вихідним кодом, що дозволяє користувачам переглядати, змінювати та розповсюджувати його за власним бажанням. Інтеграція з ELK Stack: Wazuh інтегрується з ELK Stack (Elasticsearch, Logstash, Kibana), що надає потужні можливості для збору, аналізу та візуалізації даних безпеки. Правила виявлення загроз: Wazuh надає готові правила виявлення загроз, а також можливість створювати власні правила для виявлення конкретних видів загроз. Масштабованість: Wazuh може бути масштабований для використання великими організаціями та корпораціями.	Відкрита ліцензія: Wazuh використовує ліцензію GNU General Public License (GPL), що означає, що він є відкритим програмним забезпеченням і доступний для використання, модифікації та розповсюдження безкоштовно. Проте, при комерційному використанні можуть виникати вимоги до додаткових платних підтримки або послуг.	Агентно-серверна архітектура. Агенти Wazuh встановлюються на кожному хості, який потрібно моніторити і збирають дані безпеки та події з хостів, надсилаючи їх на Wazuh manager для аналізу та обробки. **«Важкість агентів»** Агенти Wazuh вважаються легкими та ефективними. Вони не використовують значні ресурси системи і можуть ефективно працювати на різних операційних системах. **Протоколи спілкування** Агенти Wazuh використовують протоколи TLS (Transport Layer Security) та syslog для комунікації з Wazuh manager. TLS забезпечує захищену та шифровану комунікацію, а syslog використовується для надсилання журналів подій.
Splunk Enterprise Security	Можливості аналізу даних: Splunk Enterprise Security володіє потужними можливостями аналізу даних,	Пропрієтарна ліцензія: Splunk Enterprise Security використовує пропрієтарну ліцензію, що означає, що доступ до продукту надається за	Агентно-серверна архітектура. Агенти Splunk Forwarder встановлюються на кожному хості для збору та передачі

	включаючи машинне навчання та аналітику в реальному часі. Широкий вибір інтеграцій: Splunk має велику кількість готових інтеграцій з іншими системами безпеки та інструментами моніторингу. Комерційна підтримка: Splunk пропонує комерційну підтримку для своїх продуктів та послуг, що може бути корисним для підтримки великих підприємств.	плату, і користувачам може знадобитися купувати ліцензії для використання та отримання підтримки.	даних до Splunk Indexer або Splunk Heavy Forwarder. **«Важкість агентів»** Splunk Forwarder вважається важким, особливо при великому обсязі даних або при роботі на ресурсозмінних системах. **Протоколи спілкування** Splunk Forwarder використовує протоколи Splunk Data Stream Protocol (SDSP) або HTTP Event Collector (HEC) для надсилання даних на Splunk Indexer або Splunk Heavy Forwarder.
IBM QRadar	Події в реальному часі: IBM QRadar пропонує можливості моніторингу та аналізу подій в реальному часі для виявлення загроз безпеки. Кореляція подій: QRadar використовує алгоритми кореляції подій для виявлення складних загроз та інцидентів безпеки. Широкі можливості налаштування: QRadar надає широкі можливості налаштування для відповідності потребам конкретних організацій.	Пропрієтарна ліцензія: IBM QRadar також використовує пропрієтарну ліцензію, тому доступ до продукту надається за плату, і користувачам може знадобитися купувати ліцензії для використання та отримання підтримки.	Агентно-серверна архітектура. Агенти QRadar Event Collector (QEC) встановлюються на кожному хості для збору та передачі подій до QRadar Console або QRadar Event Processor. **«Важкість агентів»** Агенти QRadar Event Collector вважаються важкими у великих розподілених мережах або при великому обсязі даних. **Протоколи спілкування** QRadar Event Collector використовує протоколи Syslog або IBM QRadar Protocol (QRPT) для надсилання подій на QRadar Console або QRadar Event Processor.
Elastic Security	Вбудована аналітика безпеки: Elastic Security має вбудовану систему аналізу безпеки, яка використовує машинне навчання та аналітику в реальному часі. Масштабованість: Elastic Security може бути легко масштабований для використання в різних масштабах організацій. Еластичність: Використання Elastic Stack дозволяє легко розширювати функціональність та інтегрувати різноманітні джерела даних.	Elastic має змішану модель ліцензування, яка включає в себе як безкоштовний відкритий код, так і комерційні рішення. Elastic Security, як частина Elastic Stack, може бути доступним для використання на безкоштовній основі за умови відповідності умовам ліцензування Elastic. Проте, для використання деяких просунутих функцій або для підтримки може знадобитися купівля комерційної ліцензії.	Агентно-серверна архітектура. Beats агенти (наприклад, Filebeat або Winlogbeat) встановлюються на кожному хості для збору та передачі даних до Elasticsearch. **«Важкість агентів»** Beats агенти вважаються легкими та ефективними. Вони не потребують значних ресурсів системи і можуть працювати на різних операційних системах. **Протоколи спілкування** Beats агенти використовують протоколи HTTP або HTTPS для відправлення даних до Elasticsearch. Вони також можуть використовувати Logstash для обробки даних перед їхнім зберіганням у Elasticsearch.

Кожна з цих платформ має свої унікальні переваги та можливості, і вибір між ними залежить від конкретних потреб вашої організації, бюджету та інших факторів. Відмітимо, що всі порівняні платформи мають агентно-серверну архітектуру, у якій лише агенти Wazuh та Elastic Security відрізняються своєю «легкістю» в незалежності від розмірів мережі, обсягу даних та ресурсозмінності.

Огляд MS SCOM як інструменту системного моніторингу від Microsoft.

Що ж таке Microsoft SCOM (System Center Operations Manager)?

Microsoft SCOM (System Center Operations Manager) — це набір інструментів для моніторингу інфраструктури та керування продуктивністю програм. SCOM є частиною Microsoft System Center, продукту, який допомагає спростити розгортання інфраструктури підприємств, налаштування, керування та моніторинг. Це також дозволяє організаціям підвищити гнучкість і продуктивність своєї інфраструктури та віртуалізованих програмно-визначених центрів обробки даних (SDDC). Microsoft System Center містить численні інструменти для спрощення керування центром обробки даних як локально, так і в хмарі . Ці інструменти спрощують моніторинг, автоматизацію та надання програмно визначених корпоративних центрів обробки даних і дозволяють адміністраторам центрів обробки даних діагностувати та усувати проблеми в усій інфраструктурі.

SCOM — це гнучкий і економічно ефективний інструмент для моніторингу інфраструктури та управління продуктивністю. Це програмне забезпечення дозволяє IT-адміністраторам контролювати операції, встановлені служби та програми, а також підключені пристрої на кількох комп'ютерах з однієї централізованої консолі.

Консоль відображає справність, продуктивність і доступність усіх цих відстежуваних об'єктів, визначає проблеми та вирішує їх за допомогою списку пріоритетних рекомендацій SCOM. За допомогою SCOM адміністратори можуть контролювати центр обробки даних і хмарну інфраструктуру (загальнодоступну та приватну) і вживати заходів для забезпечення сталої продуктивності та постійної доступності життєво важливих корпоративних програм.

Важливі компоненти Microsoft SCOM

System Center Operations Manager відстежує різні комп'ютери, пристрої, програми та служби в корпоративному IT-середовищі та повідомляє адміністраторам, які з цих об'єктів моніторингу справні, а які – ні. Він також надсилає сповіщення, коли виявляє проблеми, надає корисну інформацію про виявлену проблему, знаходить її причину та впроваджує можливе рішення.

Для виконання всіх вищезазначених завдань різні компоненти працюють разом у SCOM. Ці компоненти є частиною групи керування, яка створюється під час інсталяції SCOM і є основною функціональною одиницею. Компоненти можуть існувати на одному сервері або можуть бути розподілені між кількома серверами. Компоненти SCOM включають наступне:

- **Оперативна база даних**. База даних SQL Server , яка містить усі конфігураційні дані та зберігає дані моніторингу на короткий термін.
- **База даних сховища даних.** Також база даних SQL Server, хоч і така, яка зберігає дані моніторингу та сповіщень для історичних цілей, тобто довгострокового зберігання.
- **Сервер керування.** Адмініструє групу керування та спілкується з базою даних.
- **Сервер звітності.** Створює та представляє звіти, створені з даних у базі даних сховища даних .
- **Агент.** Служба, встановлена на комп'ютері для збору даних моніторингу, створення сповіщень і запуску відповідей; він повідомляє серверу керування в групі керування.
- **Послуга Агент моніторингу.** Збирає дані про продуктивність, виконує завдання та надсилає зібрані дані на сервер керування.

SCOM, як вказує його назва, не є вузькоспеціалізованим інструментом моніторингу MS. Це скоріше набір програмного забезпечення для розгортання, налаштування, керування та моніторингу всіх серверів, компонентів і служб IT-інфраструктури Windows.

Operations Manager призначений для моніторингу всієї інфраструктури, тому часто це складний звір із багатьма рухомими частинами, попередніми умовами та залежностями, ролями сервера, агентами тощо. Корпорація Майкрософт детально описує їх у своєму посібнику щодо системних вимог для SCOM, але ми трошки пізніше коротко пробіжимося по цим вимогам. Архітектура SCOM виглядає приблизно так, як показано на рис. 07.07.

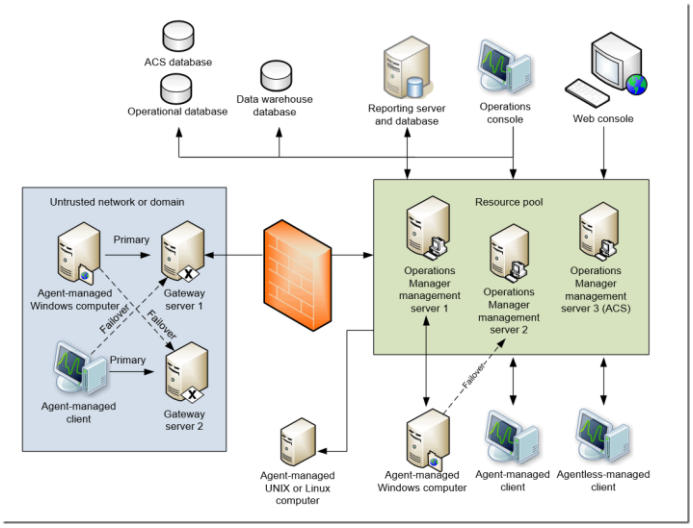


Рис. 07.07 Архітектура SCOM

Агенти Microsoft SCOM

У System Center Operations Manager агент — це служба, встановлена на комп'ютері, яка шукає дані конфігурації і заздалегідь збирає відомості для аналізу та створення звітів, вимірює стан працездатності об'єктів, що відстежуються, таких як база даних SQL або логічний диск, і виконує завдання на вимогу оператора або у відповідь умову. Вона дозволяє Operations Manager відстежувати операційні системи Windows, Linux та UNIX, а також компоненти IT-служби, встановлені на них, наприклад веб-сайт або контролер домену Active Directory.

- **Агент Windows**

  На відстежуваному комп'ютері Windows агент Operations Manager вказаний як служба Microsoft Monitoring Agent (MMA). Служба Microsoft Monitoring Agent збирає дані про події та продуктивність, виконує завдання та інші робочі процеси, визначені в пакеті керування. Навіть якщо ця служба не може підключитися до сервера керування, якому вона підпорядковується, вона продовжує працювати і поміщає зібрані дані та події в чергу на диску комп'ютера, що спостерігається. Під час відновлення підключення служба Microsoft Monitoring Agent надсилає зібрані дані та події на сервер керування.

  Іноді Microsoft Monitoring Agent називають службою працездатності.

  Служба Microsoft Monitoring Agent також працює на серверах керування. На сервері керування ця служба виконує робочі процеси моніторингу та керує обліковими даними. Для запуску робочих процесів служба викликає процеси MonitoringHost.exe за допомогою вказаних облікових даних. Ці процеси виконують спостереження та збирають дані журналів подій, дані інструментарію керування Windows (WMI), а також виконують такі дії, як запуск скриптів. Агент Operations Manager надсилає попередження та дані виявлення на призначений основний сервер управління, який записує ці дані до робочої бази даних. Крім того, агент відправляє дані про події, продуктивність та стан на основний сервер управління, який одночасно записує ці дані в робочу базу даних і в базу даних сховища даних.

Агент надсилає дані відповідно до параметрів розкладу для кожного правила та монітора. У разі оптимізованих правил збору даних дані передаються тільки в тому випадку, якщо вибірка лічильника відрізняється від попередньої вибірки на вказану величину допуску, наприклад, на 10%. Це допомагає скоротити мережевий трафік та обсяг даних, що зберігаються у робочій базі даних.

Крім того, всі агенти регулярно відправляють пакет даних, званий пульсом , на сервер управління: за умовчанням це відбувається кожні 60 секунд. Мета пульсу полягає у перевірці доступності агенту та зв'язку між агентом та сервером управління. Детальний опис реалізації механізму пульс див. у статті How Heartbeats Work in Operations Manager (Принципи роботи пульсу в Operations Manager) .

Якщо коротко, то SCOM використовує тактові сигнали для моніторингу каналів зв'язку між агентом і основним сервером керування агентом. Пакет даних регулярно, за замовчуванням кожні 60 секунд, надсилається від агента на сервер керування через порт 5723 (TCP).

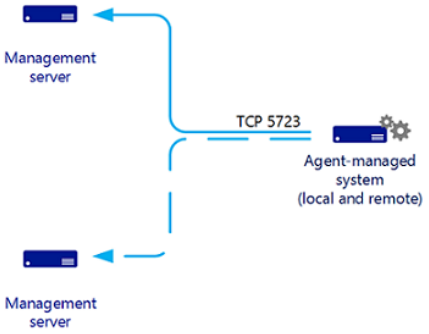


Рис. 07.08 Management server - Agent-managed host

Якщо агент чотири рази не може надіслати Heartbeats сигнал, створюється сповіщення про збій серцевого ритму служби працездатності, і сервер керування намагається зв'язатися з комп'ютером за допомогою ping. Якщо комп'ютер не відповідає на запит ping, створюється сповіщення, що не вдалося підключитися до комп'ютера.

Для кожного агенту, Operations Manager запускає спостерігач служби працездатності, який спостерігає стан віддаленої служби працездатності з точки зору сервера управління. Агент взаємодіє із сервером управління через TCP-порт 5723.

- **Агент Linux/UNIX**

Архітектура агенту UNIX та Linux істотно відрізняється від архітектури агенту Windows. Агент Windows має службу працездатності, відповідальну за оцінку працездатності комп'ютера, що відстежується. Агент UNIX та Linux не запускає службу працездатності. Натомість він передає відомості до служби працездатності на сервері управління для оцінки. На сервері керування запускаються всі робочі процеси для моніторингу стану операційної системи, визначені у реалізації пакетів керування UNIX та Linux:

- ✓ Диск
- ✓ Процесор
- ✓ Пам'ять
- ✓ Мережеві адаптери
- ✓ Операційна система
- ✓ Процеси
- ✓ Файли журналу

Агенти UNIX та Linux для Operations Manager складаються з диспетчера об'єктів CIM (тобто сервера CIM) та набору постачальників CIM.

CIM - Common Information Model. Це модель даних, яка використовується для представлення та обміну інформацією про керовані об'єкти в середовищі SCOM. Диспетчер об'єктів CIM - це серверний компонент, що реалізує WS-Management зв'язку, автентифікації, авторизації та відправки запитів постачальникам.

WS-Management (Web Services Management) - це відкритий стандарт, який описує протокол на основі SOAP для управління серверами, пристроями, програмами та різними веб-сервісами. Постачальники є ключовим елементом реалізації CIM в агенті, визначаючи класи та властивості CIM, взаємодіючи з API ядра для отримання необроблених даних, форматуючи дані (наприклад, обчислюючи різниці та середні значення) та обслуговуючи запити, надіслані диспетчером об'єктів CIM. В операційних системах з System Center Operations Manager 2007 R2 по System Center 2012 SP1 диспетчер об'єктів CIM, що використовується в агентах UNIX та Linux Operations Manager, є сервером OpenPegasus. Постачальники, які використовуються для збору даних моніторингу та складання відповідних звітів, розробляються Майкрософт та надаються на сайті CodePlex.com з відкритим кодом.

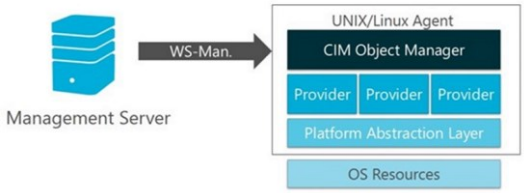
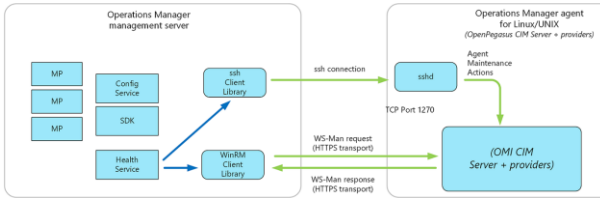


Рис. 07.09 Management server – Unix/Linux host

У System Center 2012 R2 Operations Manager цей підхід було змінено, а в основі агентів UNIX і Linux як диспетчер об'єктів CIM тепер лежить повністю узгоджена реалізація інфраструктури ***Open Management Infrastructure (OMI).*** У випадку агентів UNIX/Linux Operations Manager OMI замінює OpenPegasus. Як і OpenPegasus, OMI - це спрощена і переносима реалізація диспетчера об'єктів CIM з відкритим кодом, хоча вона легша за вагою і портативніша, ніж OpenPegasus. Ця реалізація, як і раніше, використовується в System Center 2016 — Operations Manager та пізніших версій.



Обмін даними між сервером управління та агентом UNIX та Linux ділиться на дві категорії: обслуговування агента та моніторинг працездатності. На сервері керування для взаємодії з комп'ютером UNIX або Linux використовуються два протоколи:

- ✓ Secure Shell (SSH) та протокол SFTP. Використовується для завдань з обслуговування агента, включаючи встановлення, оновлення та видалення агентів.
- ✓ Веб-служби для керування (WS-Management). Використовується для всіх операцій моніторингу та виявлення вже встановлених агентів.

Взаємодія між сервером керування Operations Manager та агентом UNIX та Linux здійснюється за допомогою WS-Man за протоколом HTTPS та інтерфейсом WinRM. Усі завдання з обслуговування агента виконуються за протоколом SSH через порт 22. Спостереження за працездатністю виконується за допомогою WS-MAN через порт 1270. Сервер управління запитує дані конфігурації та продуктивності через WS-MAN, перш ніж оцінити дані та повідомити стан працездатності. Усі дії, такі як обслуговування агентів, моніторів, правил, завдань та відновлень, налаштовуються для використання попередньо заданих профілів відповідно до вимог застосування непривілейованого або привілейованого облікового запису.

На зміну синхронним інтерфейсам API WSMAN, які використовувалися за умовчанням, прийшли нові асинхронні API інфраструктури керування (MI) Windows. Вони дозволяють виконувати масштабування та моніторинг кількох систем UNIX та Linux на одному сервері управління в System Center Operations Manager 2016 та пізніших версій.

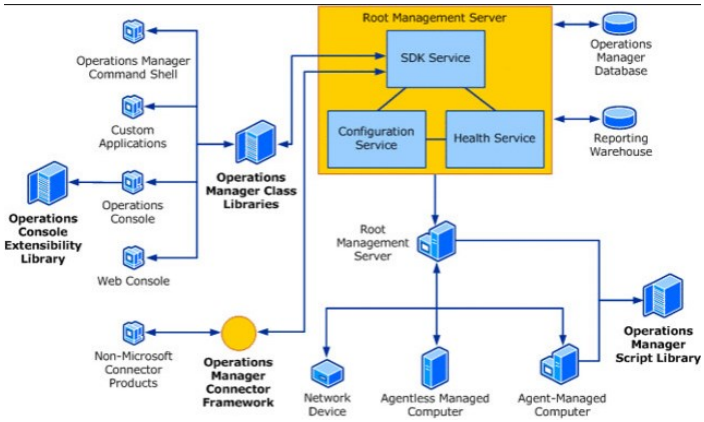


Рис. 07.10 Архітектура SCOM

Не будемо зупинятись на деталях того, як усе це працює, оскільки це велика тема, і ці деталі добре описано в документації, яку Ви будете вивчати, якщо доведеться налаштовувати такого звіра☺ . Проте, коротко кажучи, Operations Manager виявляє сервери для моніторингу та встановлює на кожному з них агента, який «збиратиме дані, порівнюватиме вибіркові дані з попередньо визначеними значеннями, створюватиме сповіщення та запускатимемо відповіді». Сервер керування надсилає деталі конфігурації та логіку моніторингу кожному агенту, використовуючи пакети керування (про це трохи пізніше), які визначають логіку моніторингу для кожного компонента. Монітори збирають дані про стан «здоров'я» об'єкта, що контролюється, а правила визначають, які події та дані продуктивності збирати та що з ними робити.

Стандартна інсталяція SCOM — це, по суті, лише базова структура, на якій можна розмістити пакети керування. Кожен пакет визначає як структуру програми або служби, яку слід відстежувати, так і всі її компоненти та їхні взаємозв'язки (модель служби), а також дані, які слід збирати для оцінки працездатності цієї програми (модель працездатності).

Агент автоматично виявляє всі попередньо визначені «об'єкти» в моделі обслуговування для пакета керування. Наприклад, для SQL Server це включатиме бази даних, файли баз даних, завдання тощо. Для кожного об'єкта (логічно згрупованого в класи) він збирає дані моніторингу, визначені моделлю працездатності, і надсилає їх назад на сервер керування, який зберігає дані моніторингу та сповіщень в операційній базі даних (тут зберігається поточна звітність) і в сховищі даних (для історичних даних).

SCOM — це гарний інструмент моніторингу на системному рівні для звітування про загальний стан і продуктивність різноманітної серверної інфраструктури та служб, які на ній працюють. Він збирає дані про широкий спектр системних показників, служб, станів процесів і лічильників продуктивності Windows для кожного сервера. Він відстежуватиме журнали подій сервера. Він повідомлятиме про будь-які невдалі входи на сервер та інші помилки та попередження сервера. Він попередить вас про проблеми з процесором, пам'яттю чи вводом/виводом або помилки мережі. Він сповістить вас, коли на фізичному диску чи логічному томі буде мало місця для зберігання.

Проблеми справді виникають, лише якщо ви намагаєтеся розширити функціональність SCOM для моніторингу складних програм або служб, таких як SQL Server. SCOM не розроблявся для того, щоб заглиблюватися в «нутрощі» складної служби, щоб допомогти зрозуміти, що саме там відбувається, коли щось йде не так. Продукт створений та задуманий як спосіб надання загальної картини моніторингу.

Налаштування правил, моніторів і сповіщень SCOM для пакетів керування певними конкретними ролями є складною справою, що ускладнюється відносно поганою документацією. Для цього потрібні спеціальні знання як SCOM, так структури та алгоритмів ролі чи служби, моніторинг якої налаштовується. Зазвичай, налаштування такого моніторингу за допомогою SCOM передбачає написання користувацьких правил і моніторів, або, в крайньому випадку, навіть написання власного пакету керування. Навіть після того, як усе налаштовано та запрацює, багато команд все одно виявляють, що отримані дані моніторингу важко зрозуміти. Знову ж таки, для інтерпретації даних і дій на основі них потрібна спеціальна експертиза. Складність для організації такого моніторингу полягає в розумінні межі між тим, що SCOM може і повинен контролювати, і тим, що можна зробити краще та більш масштабованим способом за допомогою інструменту, розробленого спеціально для моніторингу спеціалізованих служб.

Таким чином, SCOM є чудовим інструментом системного рівня, але в ньому будуть відсутні важливі діагностичні дані та дані для усунення несправностей, необхідні для дослідження деталей проблеми продуктивності нижчого рівня, таких як статистика виконання, плани запитів, стани очікування, ланцюг блокування тощо.

Щоб зовсім Вас не розчарувати у можливостях SCOM розглянемо його інформаційну панель

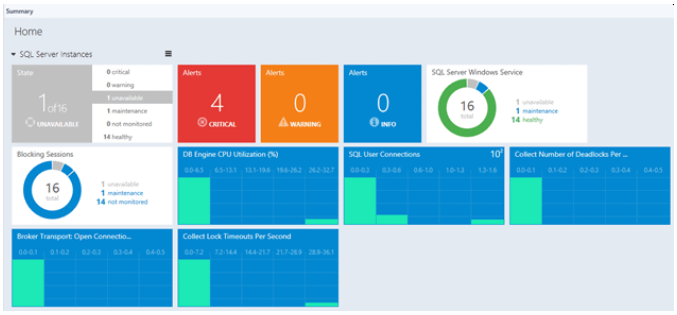


Рис. 07.11 Інформаційна панель SCOM

Користувач сам налаштовуєте інформаційну панель із інформацією, яку хоче бачити. Якщо необхідно побачити базову лінію для метрики, щоб порівняти поточну поведінку з «нормою», потрібно буде створити базову лінію. Як зазначалося раніше, команди часто створюють необхідну інформаційну панель фрагментарно, оскільки вони дізнаються, які дані їм дійсно потрібні для діагностики кожного типу проблеми. Це - класичний, нормальний підхід до побудови гарної системи моніторингу.

SNM. #3. Інструменти моніторингу та аналізу даних ***
Системний *та мережевий моніторинг. Лекція #7. Впровадження систем моніторингу на основі Wazuh та MS SCOM.*
Загальним результатом є те, що, хоча SCOM пропонує єдиний координаційний центр для всього моніторингу всіх систем, він недоступний для тих у IT-команді, яким може знадобитися реагувати на попередження, але яким бракує повних, детальних знань про домен всі елементи та складові інфраструктури, що моніториться. Але, погодьтеся, такі знання необхідні для побудови будь якої моніторингової системи.

Функціонал SCOM 2022, що базується на RBAC
В останній версії 2022 року SCOM підтримує вдосконалений контроль доступу на основі ролей і нові вбудовані ролі для покращення взаємодії з користувачем. Наприклад, він підтримує роль адміністратора лише для читання, яка надає дозволи на читання в SCOM, включаючи звітування. Роль уповноваженого адміністратора подібна до ролі адміністратора лише для читання, за винятком дозволів на звітування. Адміністратори також можуть створювати спеціальні ролі користувачів із певними дозволами в SCOM.
Трошки докладніше про контроль доступу на основі ролей (RBAC). Це метод обмеження доступу до мережі на основі ролей окремих користувачів на підприємстві. Організації використовують RBAC, також званий ролевою безпекою , для аналізу рівнів доступу на основі ролей і обов'язків співробітника.
Обмеження доступу до мережі є важливим для організацій, які мають багато співробітників, підрядників або дозволяють третім сторонам , таким як клієнти та постачальники, мати доступ до мережі, оскільки ефективний моніторинг доступу до мережі може бути складним. Компанії, які залежать від RBAC, краще можуть захистити свої конфіденційні дані та критично важливі програми. RBAC гарантує, що користувачі отримують доступ лише до інформації, необхідної для виконання своєї роботи, запобігаючи доступу до інформації, яка їх не стосується.
Роль працівника в організації визначає дозволи, які надаються особі, гарантуючи, що працівники нижчого рівня не зможуть отримати доступ до конфіденційної інформації або виконувати завдання високого рівня.

RBAC базується на концепції ролей і привілеїв. Доступ залежить від таких факторів, як повноваження, компетентність і відповідальність. Доступ до мережі та інших ресурсів, як-от доступ до певних файлів або програм, може обмежувати працівник. Наприклад, певні файли можуть бути доступними лише для читання, але до певних файлів або програм можна надати тимчасовий доступ для виконання завдання. Організації можуть визначити, чи є користувач кінцевим користувачем, адміністратором чи спеціалістом. Ці ролі також можуть збігатися або давати різні рівні дозволів для окремих ролей.

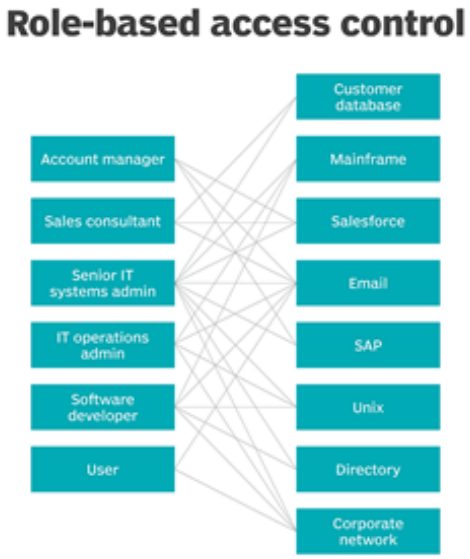


Рис. 07.12 Ілюстрація RBAC моделі

Використання RBAC має багато переваг, зокрема такі:
- **Покращена ефективність роботи.** За допомогою RBAC компанії можуть зменшити потребу в паперовій роботі та зміні паролів , коли вони наймають нових співробітників або змінюють ролі існуючих співробітників. RBAC дозволяє організаціям швидко додавати та змінювати ролі, а також застосовувати їх на різних платформах, операційних системах і програмах. Це також зменшує можливість помилок під час призначення дозволів користувача. Крім того, за допомогою RBAC компанії можуть легше інтегрувати сторонніх користувачів у свої мережі, надавши їм попередньо визначені ролі.
- **Покращена відповідність.** Кожна організація повинна дотримуватися місцевих, державних і федеральних норм. Компанії зазвичай вважають за краще впроваджувати системи RBAC, щоб відповідати нормативним і законодавчим вимогам щодо конфіденційності та конфіденційності, оскільки керівники та IT-відділи можуть ефективніше керувати доступом до даних і їх використанням. Це особливо важливо для фінансових установ і організацій охорони здоров'я, які керують конфіденційними даними.
- **Підвищена видимість.** RBAC надає мережевим адміністраторам і менеджерам більше видимості та нагляду за бізнесом, а також гарантує, що авторизованим користувачам або гостям надається доступ лише до того, що їм потрібно для виконання своєї роботи.
- **Зменшені витрати.** Заборонивши користувачам доступ до певних процесів і додатків, компанії можуть зберегти або більш економно використовувати такі ресурси, як пропускна здатність мережі, пам'ять і сховище.
- **Зменшення ризику зламу та витоку даних.** Впровадження RBAC означає обмеження доступу до конфіденційної інформації, таким чином зменшуючи ймовірність порушення даних або витоку даних.

Ще одна нова функція в SCOM 2022 полягає в тому, що організації з вимкненими протоколами безпеки Windows LAN Manager New Technology можуть вибрати тип автентифікації Reporting Manager як Windows Negotiate під час встановлення. Крім того, адміністратори можуть закрити сповіщення про несправний монітор здоров'я. Вони також можуть оновити бази даних SCOM за допомогою наявної установки SQL Always-On без необхідності вносити зміни після налаштування.
У SCOM 2022 сертифікат Secure Hash Algorithm-1 зашифровано за допомогою SHA-256. Крім того, groupId підтримується в API даних Get Alert, а джерело — повне доменне ім'я — можна переглянути під час налаштування пакета керування. Серед інших корисних функцій SCOM 2022:
- Підтримка опції сортування за стовпцем у Підсумку замін (Overrides Summary)
- Значення налаштованих реєстрів зберігаються під час оновлення до SCOM 2019.
- Деталі реєстру сховища даних зберігаються під час оновлення неосновних серверів керування.
- Веб-консоль використовує Hypertext Markup Language 5 (HTML5) замість Silverlight.
- Підтримка .NET 48, Ubuntu 20, Oracle Linux 8, Debian 10 і Debian 11.
- Джерело сповіщення (монітор/правило), яке можна переглянути в розділі Консоль > Моніторинг > Активні сповіщення.
- Вилучено залежність від облікового запису LocalSystem.
- Усі звіти про відстеження змін доступні в одній папці (Change Tracking).

Системні вимоги для SCOM
Щоб отримати максимальну користь від SCOM, важливо спочатку перевірити системні вимоги та переконатися, що ці вимоги виконуються. Тим не менш, SCOM розроблений як гнучкий і масштабований, тому вимоги до апаратного та програмного забезпечення для певних сценаріїв можуть відрізнятися від наведених нижче рекомендацій.

SNM. #3. Інструменти моніторингу та аналізу даних ***

Системний *та мережевий моніторинг. Лекція #7. Впровадження систем моніторингу на основі Wazuh та MS SCOM.*

- Необхідно дотримуватися рекомендованих обмежень для всіх контрольованих елементів, включаючи комп'ютери, які контролює агент, консолі одночасних операцій, комп'ютери, керовані агентом і Unix або Linux на групу керування, а також мережеві пристрої, якими керує пул ресурсів із трьома або більше серверами керування.
- Кількість додатків для моніторингу продуктивності додатків має бути менше 400.
- Кількість URL-адрес, які відстежуються на агента, має бути менше 50.
- Мінімум 8 гігабайт пам'яті та 10 ГБ дискового простору потрібні для конфігурації таких ролей, як сервер керування, сервер шлюзу, який керує до 2000 агентів, сервер веб-консолі та сервер SQL Server Reporting Services.
- Для будь-якої ролі сервера SCOM мінімальною вимогою до процесора x64 є чотириядерний центральний процесор 2,66 ГГц.
- Для налаштування сервера керування Operations Manager потрібна мінімальна версія Windows Server 2019 Standard або Datacenter.
- Для компонента сервера звітів Operations Manager потрібна версія Windows Server 2019 або Windows Server 2022 Standard або Datacenter.

Крім того, під час оновлення інсталяцій System Center 2019 – Operations Manager, інтегрованого з одним або кількома компонентами System Center, адміністратори повинні переконатися, що спочатку оновлено Orchestrator, а потім Service Manager, Data Protection Manager, Operations Manager і Virtual Machine Manager.

Серед інших мінімальних системних вимог для налаштування Microsoft SCOM:

- Internet Explorer (IE) 11 і Silverlight 5 для забезпечення зворотної сумісності клієнтських браузерів із інформаційними панелями з підтримкою Silverlight.
- Windows PowerShell версії 2.0 або 3.0 для консолі Operations Manager. Налаштування Command Shell Operations Manager виконується у консолі SCOM розділ "Administration" (Адміністрування), вкладці "Settings" (Налаштування) - "Security" (Безпека) активацією відповідної опції.
- .NET Framework 4.7.2 або 4.8 для сервера керування та сервера шлюзу.
- Microsoft Edge версії 88, IE версії 11, Google Chrome версії 88 для клієнтського веб-браузера для веб-консолі HTML5.
- Налаштований протокол передачі гіпертексту або безпечне прив'язування HTTP .
- Клієнтська операційна система Windows 10 і Windows 11 .
- Служби доменів Active Directory (AD DS) справні та підтримуються на певних мінімальних рівнях конфігурації. AD DS використовується для керування автентифікацією та авторизацією користувачів, а також для розподілу та організації об'єктів, таких як сервери, комп'ютери, служби та ролі, у доменній мережі. Мінімальні рівні конфігурації AD DS зазвичай відповідають певним версіям операційної системи Windows Server, які підтримуються SCOM. Наприклад, у хмарній реалізації, використовується Azure Active Directory (Azure AD) від Microsoft, можливе також використання гібридної служби доменів. Основні аспекти, пов'язані з використанням дерева каталогів у роботі SCOM, включають:
  - ✓ **Автентифікація і авторизація**. SCOM використовує службу доменів AD DS для автентифікації користувачів та надання їм відповідних дозволів на доступ до ресурсів системи моніторингу.
  - ✓ **Розподіл об'єктів**. Об'єкти, що моніторяться SCOM, такі як сервери, комп'ютери, програмне забезпечення та служби, організовуються відповідно до структури дерева каталогів AD DS. Це дозволяє керувати об'єктами моніторингу та надавати доступ до них з різних компонентів SCOM.
  - ✓ **Ролі та дозволи**. AD DS дозволяє налаштовувати ролі та дозволи користувачів SCOM з використанням Role-Based Access Control (RBAC). Це дозволяє диференціювати доступ користувачів до функціональності SCOM відповідно до їхніх обов'язків та повноважень.
  - ✓ **Розгортання і реплікація**. AD DS може бути використане для керування процесом розгортання та реплікації SCOM, дозволяючи ефективно розподіляти об'єкти моніторингу та забезпечувати доступність служби моніторингу у різних географічних регіонах.
- Система доменних імен встановлена та справна для належної підтримки AD DS і SCOM.

Інтеграція з іншими продуктами управління підприємством

Багато організацій використовують одну або декілька платформ для моніторингу своєї IT-інфраструктури. Ці платформи збирають дані про роботу серверів, мереж, програмного забезпечення та інших компонентів IT-системи. Одна з цих платформ використовується як центральна. Вона збирає дані з інших платформ та надає загальну картину роботи IT-інфраструктури. Ця платформа також використовується для:

- Запису та ескалації інцидентів: Коли виникають проблеми, платформа може записати їх та повідомити про них відповідним людям.
- Аналізу та візуалізації даних: Платформа може аналізувати дані, щоб виявити проблеми та тенденції. Вона також може візуалізувати дані за допомогою інформаційних панелей, щоб їх було легше зрозуміти.

SCOM може бути частиною цієї структури. Взаємодія між Operations Manager та іншими продуктами досягається багатьма різними методами залежно від технічних і бізнес-вимог. Нижче наведено загальні методи взаємодії з Operations Manager:

- System Center – Orchestrator із пакетами інтеграції, доступними від Microsoft, сторонніх розробників і спільноти, щомістять додаткові дії, які розширюють функціональні можливості Orchestrator для зв'язку та обміну даними з іншими сторонніми системами.
- Конектори, створені на основі Operations Manager Connector Framework (OMCF), розроблені з Operations Manager SDK , надають методи та типи, які можна використовувати для ініціалізації та керування конектором, а також для отримання чи надсилання операційних даних. Деякі приклади конекторів, які використовуються для інтеграції з Operations Manager, — це інші продукти System Center, як-от Service Manager і Virtual Machine Manager (VMM), а також сторонні продукти, такі як Nagios або IBM Netcool. Підключення до зовнішніх систем зазвичай виконується за допомогою веб-служби.
- Надсилання запитів до операційних баз даних SQL або баз даних сховищ для отримання певних наборів даних для спеціальних звітів або інформаційних панелей.

Інші користувацькі конектори розроблено та впроваджено для підтримки розширених сценаріїв, таких як збагачення сповіщень, включаючи додаткову інформацію перед тим, як сповіщення пересилається в систему керування інцидентами, виконує кореляцію попереджень або забезпечує розширені функції сповіщень за допомогою Operations Manager.

Operations Manager також інтегрується з Azure Monitor для пересилання зібраних подій, сповіщень і даних продуктивності для подальшого аналізу та забезпечує кращу видимість для організації.

Інтеграція між Operations Manager та іншими продуктами моніторингу та керування зазвичай налаштовується між одним сервером керування та іншим продуктом керування. Або в інших випадках між декількома серверами керування або вказуючи назву групи керування Operations Manager. Підтримка кількох підключених груп керування не підтримується, і кожній групі керування потрібно буде інсталювати окремий екземпляр конектора для кожної групи керування. Це включає інтеграцію між System Center Orchestrator, VMM і Service Manager.

Плануючи безперервність обслуговування, важливо оцінити та визначити ризики, вплив і варіанти відновлення для розгортання Operations Manager, щоб підтримувати цільовий рівень обслуговування.

Якщо сервер керування підтримує інтеграцію (через з'єднувач, розміщений безпосередньо на сервері керування або з іншого продукту System Center, наприклад VMM, Orchestrator або Service Manager), потрібно спланувати це за допомогою ручних або автоматичних кроків відновлення залежно від інтеграції. налаштування та послідовність кроків, необхідних для повернення до нормальної функціональності.

Корисні посилання
Ресурси для вивчення Wazuh:

Офіційний сайт Wazuh: https://wazuh.com/
Документація Wazuh: https://documentation.wazuh.com/
Блог Wazuh: https://blog.wazuh.com/
GitHub Wazuh: https://github.com/wazuh/wazuh

Ресурси для вивчення MS SCOM
Microsoft SCOM: https://www.techtarget.com/searchwindowsserver/definition/Microsoft-System-Center-Operations-Manager-Microsoft-SCOM
Heartbeats in SCOM: https://learn.microsoft.com/en-us/system-center/scom/manage-agent-heartbeat-overview?view=sc-om-2022