Міністерство освіти і науки України

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп’ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

на тему: «Проєкт системи моніторингу мережної інфраструктури на базі Microsoft System Center Operations Manager»

Виконав студент 4-го курсу групи КІ-19-1
спеціальності 123 «Комп’ютерна інженерія»
_____ Семенчук Максим
Керівник старший викладач кафедри КІ та КБ
_____ Фальковський Ігор
Рецензент професор кафедри КІ та КБ д.т.н, доцент
_____ Воротніков Володимир

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії та
кібербезпеки
Андрій Єфіменко
1 березня 2023 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу бакалавра

Студент: Семенчук Максим Миколайович

Тема роботи: «Проєкт системи моніторингу мережної інфраструктури на базі Microsoft System Center Operations Manager»

затверджена Наказом університету від 1 березня 2023 р. № 98/С

Термін здачі студентом закінченої роботи 24 червня 2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Мережа моніторингу

Обладнання та програмне забезпечення:

1. Windows server 2019
2. Scom 2019
3. Операційна система Linux Centos
4. Маршрутизатор Cisco 7250

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Фальковський І. Г.	06.03.2023	06.03.2023
2	Фальковський І. Г.	20.04.2023	20.04.2023
3	Фальковський І. Г.	11.05.2023	11.05.2023

Студент _____ Максим Семенчук
Керівник _____ Ігор Фальковський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	1 березня 2023	Виконано
2	Пошук інформації стосовно моніторингу мережі	6 березня – 13 березня 2023	Виконано
3	Аналіз інструментів моніторингу	14 березня – 27 березня 2023	Виконано
4	Ознайомлення з SCOM	28 березня – 9 квітня 2023	Виконано
5	Вивчення принципів роботи SCOM з пристроями	10 квітня – 23 квітня 2023	Виконано
6	Побудова мережі	24 квітня –30 квітня 2023	Виконано
7	Налаштування агентів на робочих пристоях	1 травня – 14 травня 2023	Виконано
8	Налаштувння SNMP на мережних пристроях	15 травня – 28 травня 2023	Виконано
9	Тестування моніторингу	29 травня – 11 червня 2023	Виконано
10	Написання пояснювальної записки	12 червня - 21 червня	Виконано
11	Отримання відгуку та резенції	22 червня - 23 червня 2023	Виконано
12	Захист	29 червня 2023	Виконано

Студент _____ Семенчук Максим

Керівник _____ Ігор Фальковський

Анотація

Кваліфікаційна робота складається з проекту системи моніторингу, її реалізації та пояснювальної записки до нього. Пояснювальна записка містить 64 сторінки та 47 ілюстрацій

Метою роботи є розробка та реалізації проекту системи моніторингу мережної інфраструктури на базі Microsoft System Center Operations Manager

В роботі проведено побудову мережі, встановлення сервісу SCOM, та проведено моніторинг фізичних та віртуальних пристроїв

Ключові слова: SCOM, моніторинг, Agent, мережа, SNMP, Operations Console, alert

					ККІК<.КР.Б – 123 –16 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Семенчук М.М.		20.06.23	Проєкт системи моніторингу мережної інфраструктури на базі Microsoft System Center Operations Manager	Літ.	Арк. / Аркушів
Керівник		Фальковський І.Г.		20.06.23			
Реценз.		Воротніков В.В		20.06.23		ФІКТ, Гр. КІ-19-1	
Н. контр.							
Затверд.		Єфіменко А.А		20.06.23			

ANNOTATION

The qualification work consists of a draft policy of the investigation, its implementation, and an explanatory note to it. The explanatory note contains 64 page and 41 illustrations.

The purpose of the work is the development and implementation of the network infrastructure monitoring system project based on Microsoft System Center Operations Manager

In the work, the network was built, the SCOM service was installed, and physical and virtual devices were monitored

Keywords: SCOM, monitoring, Agent, network, SNMP, Operations Console, alert

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SCOM - System Center Operations Manager

SNMP – Simple Network Management Protocol

IT - Інформаційні технології

WMI – Windows Management Instrumentation

MP – Management packs

AD – Active Directory

SQL – Structured query language

LAN – Local Area Network

IP – Internet Protocol

DNS – Domain Name System

ЗМІСТ

ВСТУП 9
Розділ 1: Теоретичні основи моніторингу мережної інфраструктури 10
1.1 Значення та принципи моніторингу мережної інфраструктури 10
1.2 Методи моніторингу мережної інфраструктури 12
1.3 Огляд Microsoft System Center Operations Manager 16
1.4 Порівняння альтернативних рішень моніторингу 18
1.5 Основні вимоги до системи моніторингу мережної інфраструктури 27
Висновки до розділу 1: 29
Розділ 2: Огляд принципів та архітектури MS SCOM та проектування мережі моніторингу 30
2.1 Інфраструктура Operation Manager 30
2.2 Принципи виявлення об’єктів та моніторингу за ними 33
2.3 Розробка схеми мережі 39
Висновки до розділу 2 44
Розділ 3: Встановлення та базове налаштування системи моніторингу SCOM 45
3.1 Встановлення SCOM 45
3.2 Підключення пристроїв для моніторингу 49
3.3 Перевірка роботи моніторів та попереджень 57
Висновки до розділу 3 60
Висновки 61
Список використаних джерел 62
Додатки 63

ВСТУП

Актуальність теми: Сучасні підприємства та організації стикаються з постійно зростаючим обсягом мережної інфраструктури, що включає сервери, мережеві пристрої, додатки та інші компоненти. Ефективне функціонування цієї інфраструктури є вирішально важливим для забезпечення безперебійної роботи бізнес-процесів. Однак, великі та складні мережні інфраструктури потребують постійного контролю та моніторингу для виявлення можливих проблем, попередження виникнення аварійних ситуацій та забезпечення швидкого реагування на події. У зв'язку з цим, розробка та впровадження систем моніторингу стають актуальними завданнями для підприємств.

Мета дослідження: розробка та реалізація проєкту системи моніторингу мережної інфраструктури на базі Microsoft System Center Operations Manager. У роботі буде проведено аналіз теоретичних основ моніторингу мережної інфраструктури, вивчення можливостей та функціональності Microsoft System Center Operations Manager, проєктування та реалізація системи моніторингу, а також впровадження та експлуатація розробленої системи.

Задачі дослідження: Основні завдання дослідження полягають у розробці ефективного інструментарію для моніторингу мережної інфраструктури, підвищенні стабільності та надійності роботи мережних систем та забезп

Результати даної роботи будуть сприяти підвищенню ефективності моніторингу мережної інфраструктури, забезпеченню швидкого виявлення та усунення проблем, а також покращенню надійності та стабільності роботи бізнес-процесів підприємства.

Об'єктом дослідження даної роботи є система моніторингу мережної інфраструктури на базі Microsoft System Center Operations Manager.

Розділ 1: Теоретичні основи моніторингу мережної інфраструктури

1.1 Значення та принципи моніторингу мережної інфраструктури

Моніторинг IT-інфраструктури – важливий процес, який допомагає організаціям відстежувати зміни в їх IT-інфраструктури. Мета моніторингу – збір та аналіз даних про IT-сервіси і компоненти інформаційної інфраструктури та використання цих даних для контролю всіх елементів і для запобігання збоїв

Моніторинг IT є невід'ємною складовою для забезпечення неперервності діяльності бізнесу. Ця система слідкує за станом технічної інфраструктури підприємства і допомагає технічному персоналу оперативно реагувати і уникнути негативних наслідків системних збоїв та аварій. IT-моніторинг дозволяє підприємствам виявляти проблеми задовго до того, як вони почнуть впливати на користувачів, тим самим передбачаючи можливі перешкоди для нормального функціонування бізнесу.

Практика IT-моніторингу зазнала значного розвитку за останні роки, значною мірою через те, що IT-середовище стало значно складнішим. Однією з важливих змін у моніторингу IT стало зростання популярності хмарних обчислень. IT-інструменти моніторингу тепер призначені для моніторингу як локальної, так і хмарної інфраструктури.

IT-моніторинг широко поєднується з іншими суміжними дисциплінами, включаючи управління IT-операціями (ITOM), оперативну розвідку (OI), спостережливість, оркестрування безпеки, автоматизацію та реагування (SOAR) і управління інформацією та подіями безпеки (SIEM).

Інструменти IT-моніторингу надають інформацію, необхідну щоб зрозуміти, як працюють їхні системи як на даний момент, так і з часом, і, таким чином, визначити дії, які вони вживають для ефективного керування своїми мережами, системами та пристроями та робити як короткі, так і довгострокові строкові рішення.

Моніторинг мережної інфраструктури ґрунтується на кількох ключових принципах, що сприяють забезпеченню надійності та ефективності мережі:

- Повнота: Моніторинг повинен охоплювати всі ключові компоненти IT-інфраструктури, такі як сервери, мережеві пристрої, бази даних, додатки тощо. Це допомагає забезпечити повну картину стану інфраструктури та виявляти потенційні проблеми.
- Постійність: Моніторинг повинен бути постійним і здійснюватися 24/7 для виявлення можливих проблем навіть в нічний час або під час неактивності користувачів.
- Цільовість: Моніторинг має бути спрямований на конкретні цілі, відповідні потребам організації. Цілі можуть включати виявлення проблем, оптимізацію ресурсів, забезпечення безпеки тощо.
- Автоматизація: Моніторинг в IT-інфраструктурі часто вимагає автоматизованого збору даних та аналізу. Це може бути досягнуто за допомогою використання спеціалізованих інструментів моніторингу, які автоматично збирають дані та надають зрозумілу інформацію для адміністраторів.

Завдання моніторингу мережної інфраструктури включають:

1. Виявлення проблем: Моніторинг допомагає виявити можливі проблеми, такі як відмови обладнання, перевантаження, помилки в передачі даних, затримки тощо.
2. Оптимізація ресурсів: Моніторинг надає інформацію про використання ресурсів мережі, таких як пропускна здатність, використання пристроїв та сервісів. Це допомагає аналізувати навантаження та приймати рішення щодо оптимізації ресурсів.
3. Забезпечення безпеки: Моніторинг допомагає виявляти аномальну активність, загрози та атаки на мережу, що дозволяє оперативно реагувати та вживати заходів для запобігання порушенням безпеки.
4. Вимірювання продуктивності: Моніторинг дозволяє зібрати дані про швидкість передачі даних, час відповіді та інші метрики продуктивності мережі для аналізу та вдосконалення її роботи.

5. Генерація звітів та сповіщень: Моніторинг надає можливість генерувати звіти, алерти та сповіщення про стан мережі, що допомагає оперативно реагувати на проблеми та вживати відповідних заходів.

Узагалі, моніторинг мережної інфраструктури грає важливу роль у забезпеченні безперебійності, ефективності та безпеки мережі, а також у вдосконаленні її функціональності та використання ресурсів.

1.2 Методи моніторингу мережної інфраструктури

Існує два основних типи моніторингу інфраструктури: моніторинг без агентів і моніторинг на основі агентів. Обидва мають свої переваги та проблеми.

Agentless monitoring є методом моніторингу мережної інфраструктури, який не вимагає встановлення спеціальних агентів на мережних пристроях. Замість цього, цей підхід використовує протоколи зв'язку, такі як SNMP (Simple Network Management Protocol), WMI (Windows Management Instrumentation), SSH (Secure Shell), REST API (Representational State Transfer Application Programming Interface) для зв’язку з пристроями. Засоби моніторингу, які використовують метод Agentless, здатні отримувати дані з різних типів пристроїв, включаючи маршрутизатори, комутатори, сервери, принтери та інші.

Моніторинг без агентів дозволяє безперешкодно спостерігати за загальним станом і продуктивністю компонентів інфраструктури без інсталяції програмного забезпечення агента. Це допомагає швидко отримувати показники продуктивності з різних мережевих компонентів. Безагентний підхід також допомагає зменшити вартість і складність операцій і обслуговування інфраструктури (O&M). Враховуючи ці переваги, більшість рішень моніторингу на ринку переходять на безагентний моніторинг або забезпечують підтримку як агентного, так і безагентного моніторингу.

Зазвичай цей тип моніторингу використовується для відстеження стану мережних девайсів, пристроях зберігання інформації, гіпервізорах, віртуальних серверах

Agentless моніторинг використовує різні протоколи (SNMP, WMI тощо) і решту API для швидкого пошуку та спостереження за серверами, програмами та іншими пристроями, підключеними до вашої мережі. Цей метод допомагає побудувати оновлену карту мережі, щоб зрозуміти складний зв'язок між компонентами мережі, включаючи залежності програм. Це також дозволяє відстежувати загальний стан мережі та визначати ключові тенденції, аналізуючи ключові показники продуктивності на єдиній інформаційній панелі, такі як використання процесора та пропускна здатність мережі.

Програмне забезпечення для керування мережею з можливостями моніторингу без агентів також може надавати своєчасні сповіщення щоразу, коли певний пристрій або програма перевищують критичний поріг. Це допоможе вам швидко виявити та виправити критичні проблеми та уникнути несподіваних збоїв у мережі. Ви можете налаштувати ці сповіщення на основі різних показників, таких як використання ЦП, швидкість втрати пакетів і час відповіді. Моніторинг без агентів також може запропонувати налаштовані звіти з багатими даними, які допоможуть вам ретельно відслідковувати та порівнювати продуктивність мережі за певні проміжки часу. Це також дозволяє ефективно контролювати ваші віртуалізовані ресурси, такі як віртуальні сервери та програми SaaS, збираючи показники їх продуктивності через хмарні API.

До переваг Agentless monitoring можна додати простоту реалізації, через непотрібність встановлювати агенти на кожному мережному пристрої, масштабованість, адже можна контролювати достатньо велику мережу та доступність через сумісність більшості пристроїв з протоколами зв'язку такими як SNMP.

До недоліків цього методу відноситься доволі обмежена функціональність та залежність від протоколів зв'язку. Хоч майже всі пристрої в наш час можуть підтримувати протоколи зв'язку типу SNMP або WMI, але якщо вони не будуть здатні то використання цього методу буде недоступне

Agent-based monitoring — це метод моніторингу продуктивності та стану комп'ютерних систем і мережевих пристроїв шляхом встановлення програмних

агентів на пристрої, що контролюються. Агенти збирають і повідомляють дані на центральну платформу моніторингу.

Agent-based моніторинг також зазвичай є більш гнучким і настроюваним, ніж моніторинг без агентів. Агентів можна налаштувати для збору певних даних, а платформу моніторингу можна налаштувати для попередження про певні умови.

Моніторинг на основі агентів також дає змогу контролювати системи, які знаходяться за брандмауером або іншими засобами безпеки, або він може надавати інформацію про моніторинг систем, які не піддаються впливу мережі.

Ще одна перевага моніторингу на основі агентів полягає в тому, що він може продовжувати збирати дані, навіть якщо мережеве з'єднання між моніторинговою системою та платформою моніторингу втрачено. Агенти можуть буферизувати дані та надсилати їх на платформу моніторингу, коли з'єднання буде відновлено.

Agent-based моніторинг — це потужний метод моніторингу систем і мережевих пристроїв, який надає детальну інформацію про продуктивність системи. Це може бути корисним у середовищах, де необхідно мати детальну інформацію про системи, що контролюються, або коли безагентний моніторинг неможливий через міркування безпеки чи інші обмеження.

До недоліків цього методу можна віднести те, що: Встановлення агентів на мережних пристроїв може потребувати багато додаткових ресурсів, що може привести до збоїв слабких пристроїв та а агенти потребуються управління ними та постійного оновлення. Контролювати Agent-based моніторинг потрібно вручну, що вимагає додаткових зусиль управління мережею.

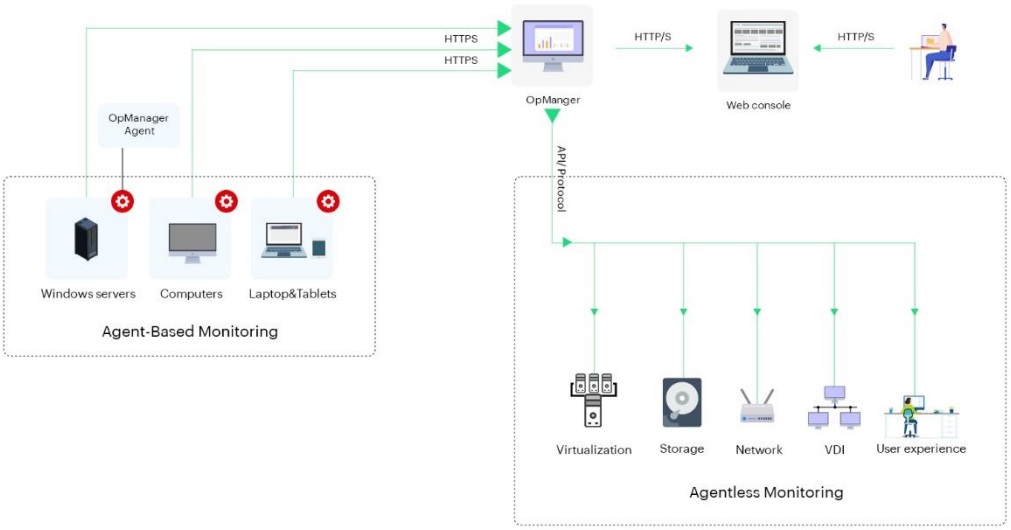


Рисунок 1.1 Agent-based і Agentless моніторинг

Мережевий світ не такий, як був раніше. Речі змінюються все швидше. Організації використовують мережі, які з кожним днем стають усе складнішими. Така складність викликає потребу в методах моніторингу як агента, так і без агента. І агентні, і безагентні методи моніторингу мають достатню частку плюсів і мінусів. Отже, адміністратор мережі повинен використовувати професіонали та методи, які найкраще підходять для конкретної ситуації. Замість того, щоб зосереджуватися на типі техніки, яка буде використана, адміністратор мережі повинен зосередитися на кінцевому результаті та способах його ефективного досягнення.

Окрім поділу на моніторинг з агентами та без, існує поділ також на активний та пасивний моніторинг.

Активний і пасивний моніторинг - це два основних підходи до збору даних в процесі моніторингу мережі або системи. Давайте розглянемо кожен з цих підходів та їх переваги та недоліки, але важливо врахувати, що кращий підхід залежить від конкретних потреб та контексту.

В пасивному моніторингу система просто спостерігає та аналізує трафік, що проходить через мережу або систему, не втручаючись у сам процес комунікації. В основному, це означає, що система слідкує за пакетами даних, що надходять та відправляються, і аналізує їх характеристики, пропускну здатність, час відповіді та інші параметри. Пасивний моніторинг не заважає нормальній роботі системи або мережі, оскільки не втручається у комунікаційний процес. За допомогою нього можна отримати загальну картину про стан системи, виявити загрози або проблеми.

Активний моніторинг включає в себе відправку спеціально сформованих запитів або пакетів даних до системи або мережі з метою отримання відповідей та оцінки реакції. Це можуть бути запити на доступність, пропускну здатність, швидкість відповіді, тестування функцій тощо. Активний моніторинг дозволяє отримати детальну інформацію про стан системи, включаючи внутрішні параметри та можливі проблеми. Він дозволяє негайно реагувати на проблеми та вживати автоматичних заходів для їх виправлення.

Вибір між активним та пасивним моніторингом залежить від конкретних потреб і контексту. У багатьох випадках комбінація обох методів може бути найкращим підходом для отримання повної та збалансованої інформації про систему чи мережу.

1.3 Огляд Microsoft System Center Operations Manager

Microsoft SCOM (System Center Operations Manager) - це програмне забезпечення для моніторингу, управління та автоматизації інфраструктури IT-систем, у тому числі для активного спостороження за станом мережі. З останніх версій Microsoft SCOM підтримується не тільки з системами Windows, але і є доступним для роботи з UNIX та Linux.

Інформаційна панель керування SCOM використовує кольорове кодування світлофора для вказівки стану працездатності об’єкта. Зелений означає здоров’я, жовтий – попередження, а червоний – критичну проблему. За потреби адміністратор може налаштувати ці рівні.

Основними можливостями цього моніторингового додатку є:

- Моніторинг всієї інфраструктури: SCOM здатний моніторити різні компоненти інфраструктури, починаючи від серверів і закінчуючи мережними пристроями та базами даних.
- SCOM може автоматично виконувати дії на основі певних умов та подій. Він не потребує постійного нагляду, і може автоматично запускати процеси відновлення після виявлення проблеми
- SCOM надає можливість аналізувати дані, зібрані з інфраструктури, і генерувати звіти про різні показники, такі як продуктивність, використання ресурсів, доступність систем та інші.

Основними перевагами цього продукту є:

1. Сумісність з другими продуктами Microsoft, такими як Active Directory, Exchange Server, Sharepoint.
2. Централізоване керування, що дає можливість моніторити всю нашу систему за допомогою одного централізованого інтерфейсу
3. уніфікований контроль в рамках приватних і загальнодоступних хмарних сервісів;

В цілому, Microsoft SCOM є потужним інструментом для моніторингу та управління інфраструктурою IT-систем, що використовується зазвичай в організаціях з великою кількістю машин, що включають також мережеве обладнання, однак він також має декілька недоліків.

Першим недоліком є доволі складне налаштування, адже потребує певних знань для використання повного потенціалу. Неправильне налаштування часто може привести до збоїв, надзвичайного завантаження системи та різних неполадків.

Також система підходить більше для моніторингу загального стану системи більше, ніж для огляду конкретних показників та пристроїв. Також до одних з недоліків SCOM можна віднести її вартість, адже вона є платною, що може бути обмеженням для деяких організацій.

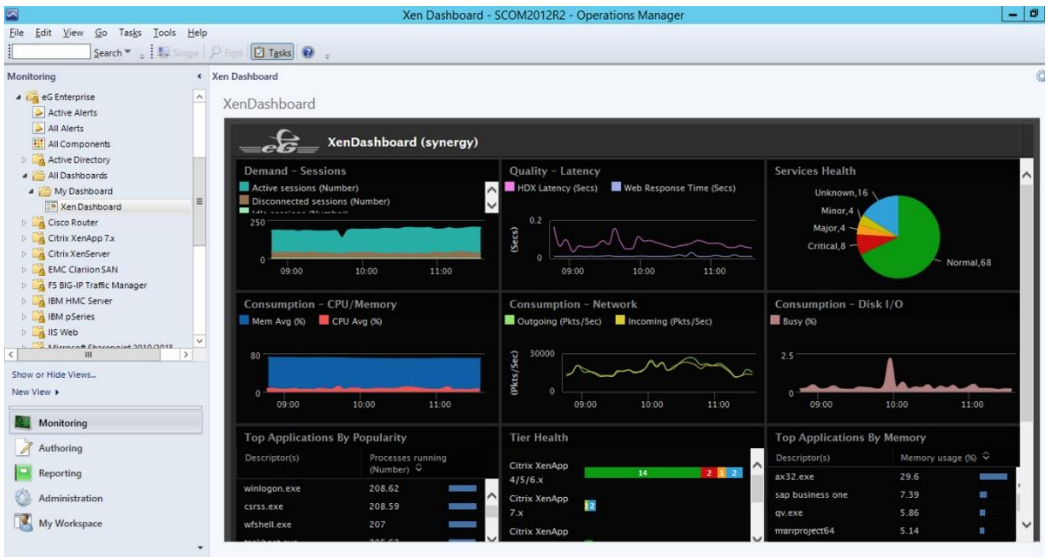


Рисунок 1.2 – Інтерфейс MS SCOM

1.4 Порівняння альтернативних рішень моніторингу

Оскільки моніторинг є доволі поширеною задачею в IT-інфраструктурі, очевидно, що окрім MS SCOM є багато аналогів, які можуть справитися з цією задачою. Для порівняльної характеристики розглянемо найпоширеніші з них: Zabbix, Nagios та PRTG Network monitor

1.4.1 Zabbix

Zabbix - це відкрите програмне забезпечення для моніторингу, тривоження та управління мережами і серверами. Він надає засоби для збору, аналізу та візуалізації даних про стан різних компонентів інфраструктури IT.

Zabbix є універсальною системою моніторингу, яка з успіхом:

- відстежує тенденції в роботі серверів і мережевої техніки;
- оперативно реагує на різні процеси;
- передупреждает про потенційні проблеми з навантаженням;
- збирає статистичні дані в певній робочій середі;
- діє в конкретних ситуаціях за заданим алгоритмом.

Zabbix має веб-інтерфейс, який може відображати всю зібрану інформацію з баз даних, віртуальних машин, мережних пристроїв у вигляді графіків, діаграм та звітів, що дозволяє зручно аналізувати інформацію та виявляти аномалії.

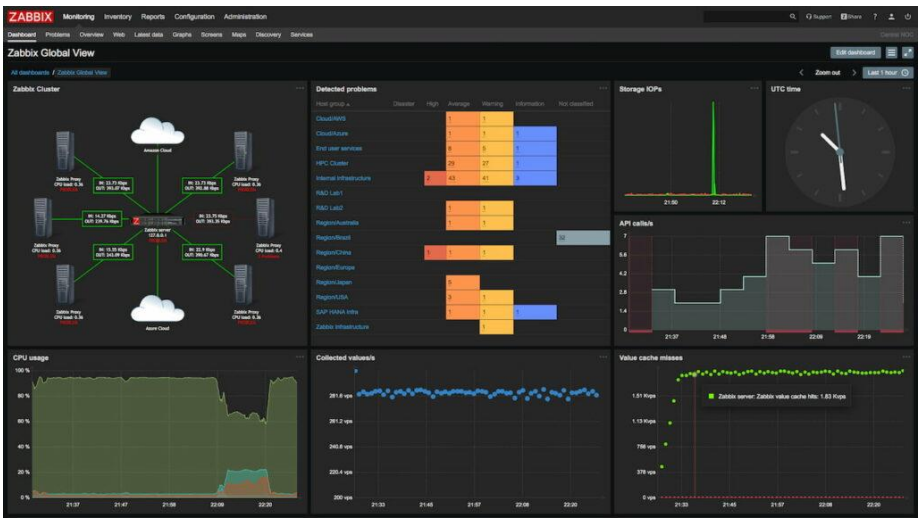


Рисунок 1.3 – Веб-інтерфейс Zabbix

Zabbix в процесі своєї роботи аналізує різну інформацію починаючи від навантаження на ЦП, закінчуючи моніторингом веб-серверів, NTP, та значенням пінгу.

При аваріях чи неполадках зазвичай спрацьовують налаштовані завчасно тригери, які відправляють інформацію адміністратору, або навіть самостійно піднімають сервіс, який вийшов з ладу.

Окрім цього Zabbix є програмою з відкритим кодом, що дозволяє вільно використовувати його при потребі.

До недоліків Zabbix можна віднести доволі складне налаштування та громізкість сервісу. Він потребує доволі високих вимог до ресурсів і підходить для пристроїв з високими характеристика. Також Zabbix потребує встановлення агентів на всіх машинах у мережі.

1.4.2 Nagios

Nagios є однією з найпопулярніших систем моніторингу з відкритим джерелом (open-source) і використовується для нагляду за інфраструктурою IT-системи, включаючи сервери, мережеві пристрої, програмне забезпечення та інші компоненти. Основною метою Nagios є постійний моніторинг різних параметрів системи та сповіщення адміністратора про будь-які проблеми або неполадки, що можуть виникнути. Спочатку розроблена для операційних систем на базі Linux, зараз однаково добре працює також і під Sun Solaris, FreeBSD, AIX і HPUX.

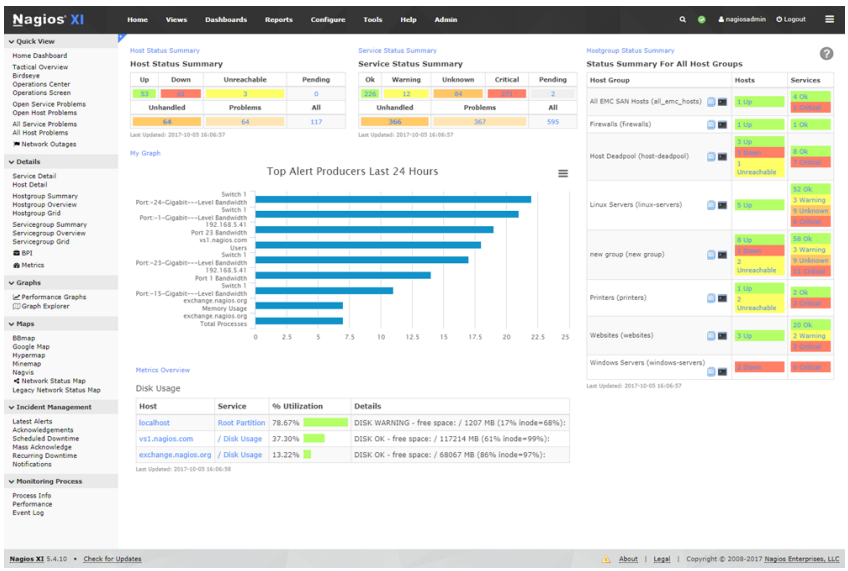


Рисунок 1.4 – Моніторинг мережі в Nagios

Nagios підтримує як управління за допомогою командної строки, так і за допомогою веб-інтерфейсу, що дозволяє юзерам працювати з тим, що їм більш практично.

Nagios підтримує плагіни, які є самостійними доповненнями та розширеннями, щоб користувач міг визначити цілі та параметри, які слід моніторити. Плагіни використовуються для перевірки стану пристроїв. Завдяки плагінам Nagios, може моніторити різні параметри, наприклад час відгуку пристрої при пінгуванні, чи температуру або вологість при роботі з сенсорами. Це дозволяє йому бути «гнучким» і працювати з різними пристроями.

Також Nagios підтримує використання шаблонів, що дозволяє швидко налаштувати подібні один до одного пристрої, і дає можливість швидкого налаштування мережі.

Але окрім всіх переваг Nagios має і недоліки.

Основним недоліком є погана сумісність з серверами під управлінням Windows. Оскільки Nagios переважно працює з сервісами Linux, сумісність з Windows не передбачена розробниками, і часто стає проблемою цієї програми.

Nagios не завжди якісно працює при великій і складній інфраструктурі. При дуже великій кількості моніторингових об’єктів або високій частоті моніторингу, він може виявитись недостатньо ефективним, що часто приводить до затримок або збоїв.

Також Nagios більш спрямований на «мережний» моніторинг.

Загалом, Nagios є потужним інструментом для моніторингу систем, який надає широкі можливості налаштування та сповіщення про проблеми. Однак, перед використанням Nagios слід врахувати, що він не зовсім підходить для великих мереж та погано працює з сервісами Windows

1.4.3 PRTG Network Monitor

PRTG Network Monitor є потужним інструментом для моніторингу та управління мережею, який надається компанією Paessler AG. Цей програмний продукт дозволяє підприємствам та організаціям здійснювати нагляд за їх мережевою інфраструктурою, виявляти проблеми та забезпечувати безперебійну роботу систем.

PRTG Network Monitor працює на основі агент-базованої архітектури. Основний компонент, відомий як "ядро PRTG", встановлюється на центральному сервері або комп'ютері, який виконує функцію сервера моніторингу. Це ядро відповідає за збір даних, обробку, зберігання і відображення інформації про стан мережі.

Крім моніторингу кількох типів пристроїв, Paessler PRTG також може контролювати різні типи ресурсів у цих пристроях. Наприклад, ви можете використовувати його для моніторингу використання процесора, пам’яті, місця на диску тощо. Це дозволяє легко отримати повну картину продуктивності ваших пристроїв і виявити потенційні проблеми.

Користувальницький інтерфейс Paessler PRTG дуже інтерактивний, тож ви можете легко налаштовувати пристрої та датчики, переглядати дані в реальному часі та налаштовувати сповіщення з одного інтерфейсу

Інтерфейс користувача також працює як односторінкова програма, що означає, що він набагато швидший і чуйніший, ніж традиційні веб-інтерфейси.

Крім того, користувальницький інтерфейс пропонує альтернативний користувальницький інтерфейс, який можна використовувати для підключення до локальної інсталяції PRTG — ідеально підходить для тих випадків, коли немає доступу до інтерну

Paessler PRTG має вбудований інструмент звітності, який дозволяє легко створювати детальні звіти про вашу мережеву активність. Ви можете налаштувати ці звіти, щоб вони включали лише ту інформацію, яку ви хочете бачити, що робить звіти безцінним ресурсом для усунення несправностей і планування потужностей.

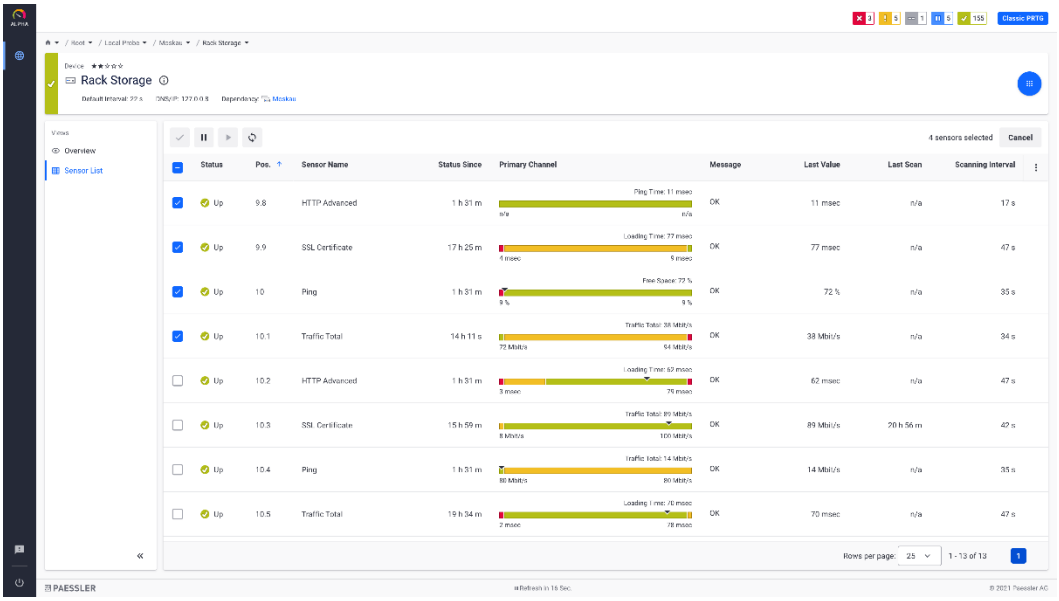


Рисунок 1.5 – Інтерфейс PRTG

Paessler PRTG Network Monitor має широкі можливості інтеграції з іншими програмами, що робить його дуже гнучким інструментом управління мережею. Серед найбільш популярних програм, які можна інтегрувати з Paessler PRTG Network Monitor, можна виділити Microsoft Azure, Amazon Web Services, Slack, ServiceNow, Zabbix, Nagios та багато інших.

Але окрім всіх плюсів, PRTG має і недоліки. Основним недоліком є його вартість. Він коштує доволі багато, і не всі компанії мають бюджет для його підтримки.

Окрім цього він вимагає постійного підключення до мережі і не працює в автономному режимі.

1.4.4 Cacti

Cacti – це безкоштовний і відкритий сервіс моніторингу, який використовується для збору статичних даних та відображення їх графічно у вигляді графіків та діаграм за допомогою RDD утиліти, що збирає інформацію

про пропуску здатність мережі, навантаження на сервери, використання інших ресурсів.

Cacti розроблений в інфраструктурі Apache-PHP-MySQL, дозволяє налаштовувати збір і відображення даних моніторингу на основі вебінтерфейсу, з юзер-френдлі організацією. Є можливість дописування власних агентів збору даних

Cacti дозволяє моніторити різні типи обладнання та систем, включаючи мережеві маршрутизатори, комутатори, сервери, додатки, бази даних та інші пристрої. Він підтримує протоколи моніторингу, такі як SNMP (Simple Network Management Protocol), які використовуються для збору даних зі змоніторених пристроїв.

Cacti надає веб-інтерфейс, необхідний для швидкого запуску, включаючи керування користувачами, пристроями та графіками. На серверній частині, Cacti використовує RRDTool для зберігання даних часових рядів, зібраних з усіх пристроїв, які ви налаштували.

RRD зберігає дані протягом встановленого періоду часу, оскільки файл ніколи не збільшується. Cacti забезпечує більш тривале зберігання, зберігаючи дані в кількох циклічних архівах (RRA). RRA визначають, скільки точок даних зберігати протягом певного періоду часу (Часовий проміжок) і як агрегувати ці дані (Кроки). Кроки – це кількість точок даних для усереднення в одну точку даних для цього RRA.

До унікальних особливостей Cacti відноситься:

- Висока швидкість встановлення
- Простота і зручність інтерфейсу
- Можливість для кожного графіка визначити необмежену кількість елементів графіка, додатково використовуючи CDEF або джерела даних із Cacti.
- Юзер-базоване управління для створення користувачів і призначення різних рівнів дозволів.



Рисунок 1.6 Графікі Cacti

Але окрім плюсів, Cacti має і недоліки.

Він має доволі обмежені можливості в моніторингу пристроїв окрім мережених девайсів. Також при великій кількості девайсів, цей сервіс немає можливості дублювати монітори, що вимагає створювати для кожного девайсу свій. Це значно ускладнює моніторинг за великими мережами.

Окрім цього Cacti перестав оновлюватися, і його підтримка була закінчена, що означає неможливість добавлення нових функцій в майбутньому.

1.4.5 SolarWinds Network Performance Monitorє програмним засобом, розробленим компанією SolarWinds, який призначений для моніторингу та управління комп'ютерними мережами. Його основна мета - забезпечити адміністраторам мережі інструменти для виявлення, аналізу та усунення проблем у мережевому середовищі з метою підтримки нормальної роботи мережі.

SolarWinds NPM надає цілісний погляд на мережеві ресурси, включаючи маршрутизатори, комутатори, сервери, фізичні та віртуальні машини, датчики, мережеві послуги і т.д. Він працює на основі протоколів мережевого моніторингу, таких як Simple Network Management Protocol (SNMP), і збирає дані про роботу цих ресурсів, їхню продуктивність, завантаженість, використання пропускної здатності та інші метрики.

NPM включає інформаційну панель із комплексними елементами керування, які можуть допомогти вам налаштувати перегляд мережевих даних, а також фільтрувати події, про які повідомляє система. Це дуже гнучка система, яка підходить для будь-якого розміру мережі. Операційні процедури Network Performance Monitor базуються на простому протоколі моніторингу мережі. Це галузевий мережевий стандарт, який вимагає встановлення агентської програми на кожному пристрої. На кожному пристрої, який можна підключити до мережі, уже буде встановлено агент SNMP як частину мікропрограми. Для SNMP потрібен центральний контролер, і мережевий монітор продуктивності забезпечує цю функцію.

У SolarWinds Network Performance Monitor є кілька дуже приємних додаткових функцій, яких зазвичай немає в програмному забезпеченні для моніторингу мережі. До них входить можливість установлювати налаштовані умови сповіщення з об’єднаних мережевих джерел даних.Модуль NetPath — ще одна чудова утиліта, яка розширює можливості усунення несправностей Network Performance Monitor на територію аналізатора пропускної здатності. Можливість моніторингу віртуальних середовищ, бездротових мереж та інтернет-маршрутів доповнює функції моніторингу локальної мережі, щоб створити справді глобальну службу моніторингу, яка дуже добре працюватиме для гібридних і складних мережевих топологій.



Рисунок 1.7 Генерація повідомлень у Solarwinds

Головним недоліком цього сервісу є дуже висока вартість. Це комерційний продукт, і може бути дорогим для невеликих організацій. Також він є не практичним для великих мереж та потребує доволі високих апаратнів ресурсів.

1.4.6 Порівняльний аналіз моніторингових систем

Кожен із інструментів моніторингу має свої плюси та мінуси, підходить для різних типів мережі та використовується по своєму. Для пошуку оптимальної системи управління проведемо порівняння систем моніторингу за параметрами наведеними в табл. 1.1.

Таблиця 1.1

Порівняння систем моніторингу

Функція	SCOM	Nagios	Zabbix	PRTG	Cacti	Solarwinds
Моніторинг мережних пристроїв	+	+	+	+	+	+
Оповіщення	+	+	+	+	+	+
Моніторинг продуктивності	+	+	+	+	-	+
Підтримка SNMP	+	+	+	+	+	+
Безкоштовне використання	-	+	+	-	+	-
Хмарний моніторинг	+	-	+	-	-	-
Моніторинг в реальному часі	+	-	-	-	+	+
APM	+	-	+	-	-	-
Аналіз топології мережі	+	-	-	+	+	-

1.5 Основні вимоги до системи моніторингу мережної інфраструктури

Моніторинг значно видозмінюється з плином часу. Якщо раніше була необхідність відстежувати стан тільки фізичних серверів, то тепер на кожному з них може бути ще кілька віртуальних

При розробці, впровадженні систем моніторингу спочатку необхідно визначити об’єкти за якими планується нагляду, а також критичні події та показники, які будуть визначати кількість повідомлень при поломці, частоту сканування та інші наслідки і параметри.

Система моніторингу повинна здійснювати постійний збір інформації про стан мережних компонентів, включаючи сервери, маршрутизатори, комутатори, принтери та інші пристрої. Це включає моніторинг параметрів, таких як навантаження процесора, використання пам'яті, доступність сервісів та інші метрики, які відображають стан компонентів.

Система моніторингу повинна забезпечувати зручну візуалізацію стану мережних компонентів та подій. Це може включати графіки, діаграми, таблиці та інші елементи візуалізації для зручного сприйняття і аналізу даних. Крім того, система повинна надавати можливість створення звітів зі зібраних даних, які допомагають у вирішенні проблем та прийнятті рішень.

Окрім цього всього, для корректної роботи з мережними пристроями, всі вони повинні підтримувати протокол SNMP, Netflow або sFlow.

SNMP — це мережевий протокол, який використовується для керування та моніторингу підключених до мережі пристроїв у мережах Інтернет-протоколу. Протокол SNMP вбудовано в численні локальні пристрої, такі як маршрутизатори, комутатори, сервери, брандмауери та бездротові точки доступу, доступ до яких здійснюється за їхньою IP-адресою. SNMP забезпечує загальний механізм для мережевих пристроїв для передачі керуючої інформації в середовищах LAN або WAN від одного та кількох постачальників. Це протокол прикладного рівня в структурі моделі OSI. Без цього протоколу збирати інформацію про стан мережних пристроїв неможливо.

Також Забезпечення безпеки є важливим аспектом системи моніторингу мережної інфраструктури. Вона повинна містити авторизацію та аутентифікацію, щоб забезпечити недоступність системи моніторингу для сторонніх користувачів та зловмисників. Окрім цього повинний бути забезпечений захист баз даних та всієї інформації про мережу.

NetFlow – це протокол мережевого моніторингу, розроблений компанією CISCO, і є аналогом протоколу SNMP.

Принцип роботи NetFlow полягає у зборі статистики про мережевий трафік на мережевих пристроях, таких як маршрутизатори або комутатори. Він аналізує IP-пакети, що проходять через ці пристрої, і генерує записи (звані "NetFlow-записи" або "потоки") з інформацією про цей трафік. Кожен NetFlow-запис містить дані, такі як джерело й призначення IP-адрес, порти, протоколи, обсяги переданих даних тощо. Він дає можливість більш детальніше розібрати інформацію про трафік, ніж SNMP.

В свою чергу sFlow — це вбудована технологія, яка реалізована через спеціальні апаратні мікросхеми, які вбудовані в маршрутизатор/комутатор. Програмний компонент, який називається агентом sFlow, працює як частина програмного забезпечення для керування мережею, знову ж таки всередині пристрою.

sFlow, незважаючи на свою назву, є технологією пакетної вибірки, а не технологією «потокової вибірки». IP-потік визначається як серія IP-пакетів, що переміщуються від джерела до пункту призначення через певний порт. У той час ,як NetFlow відбирають частину кожного IP-потоку, sFlow відбирає 1 із N кожного пакета, що проходить через інтерфейс, незалежно від потоку. Виконується як випадкова, так і часова вибірка пакетів і додатків. Хоча вибірка пакетів може не відбирати кожен потік, sFlow надає результати з кількісною точністю, особливо щодо додатків із великим трафіком.

При використання SCOM найбільш ефективним буде використання SNMP, адже він не потребує додатково встановлених MP і надає весь потрібний функціонал без великих навантажень на систему

Система моніторингу SCOM також має доволі високі вимоги до обладнання.

Таблиця 1.2

Вимоги до обладнання MS SCOM

Роль сервера	Процессор	Оперативна пам’ять	Місце на диску
Management server	4-core 2.6 GHz CPU	8 GB	10 GB
Gateway server managing up to 2000 agents	4-core 2.6 GHz CPU	8 GB	10 GB
Gateway server in resource pool managing up to 500 network devices	8-Core 2.66 GHz CPU	32 GB	10 GB
Gateway Server in resource pool managing up to 100 UNIX/Linux computers	4-Core 2.66 GHz CPU	4 GB	10 GB
Web console server	4-core 2.6 GHz CPU	8 GB	10 GB
SQL Server Reporting Services server	4-core 2.6 GHz CPU	8 GB	10 GB

Висновки до розділу 1:

В цьому розділі було розглянуто актуальність та задачі, які повинна виконувати моніторингова система, розглянуто та порівняно різні моніторингові системи, і вирішено, що SCOM найбільш підходить для нашого типу мережі. Також було розглянуто вимоги до моніторингової мережі.

Розділ 2: Огляд принципів та архітектури MS SCOM та проектування мережі моніторингу

2.1 Інфраструктура Operation Manager

Використання Operations Manager серед організації полегшує спостереження за великою кількістю комп'ютерів, пристроїв, служб і додатків. Консоль управління дозволяє перевіряти працездатність, продуктивність і доступність всіх об'єктів, що відстежуються в середовищі, а також допомагає виявляти і усувати проблеми.

Operations Manager може повідомляти вам, які об'єкти, не працездатні, сповіщає при виявленні проблем і надає відомості, які допомагають визначити причину проблеми та можливі рішення. Адміністратор задає об'єкти для спостереження, вибираючи комп'ютери та пристрої та імпортуючи пакети керування, які забезпечують моніторинг конкретних компонентів та програм. Вирішити, які об'єкти слід спостерігати, і що саме спостерігати, визначає група керування.

Група керування складається з таких компонентів як: сервер керування(management server), робоча база даних(operational database), база даних сховища даних(date warehouse database), та сервер звітів(Reporting server).

Сервер керування(Management server) є центром для адміністрування групи керування та зв’язку з базою даних. Під час відкриття консолі операцій і підключення до групи керування, користувач підключаєтеся до сервера керування для цієї групи . Залежно від розміру мережі, сервер керування може використуватися як один, так і декілька. Роль сервера управління полягає в адмініструванні конфігурації групи управління, в адмініструванні агентів та взаємодії з ними, а також у взаємодії з базами даних у групі управління.

Робоча база даних — це база даних , яка містить усі відомості про конфігурації для керування групою та зберігає всі дані моніторингу, зібрані та оброблені для цієї групи. Робоча база даних зберігає оперативні дані за замовчуванням протягом 7 днів.

База даних сховища даних – це архівна база даних, яка зберігає моніторинг та попередження за тривалий проміжуток часу. Всі дані що йдуть в робочу базу даних, йдуть і сюди, але зберігаються на довший час.

Сервер звітів – це сервер, який відповдає за забезпечення функції звітності в системі. До його функцій належить: генерація звітів з баз даних, надання інформації про стан системи, дозволяє налаштовувати планову звітність та необхідні дані для збору.

Останнім компонентом SCOM є web-сервер, який дозволяє взаємодіяти з основними функціями моніторингу через браузер, без встановлення спеціального програмного забезпечення.

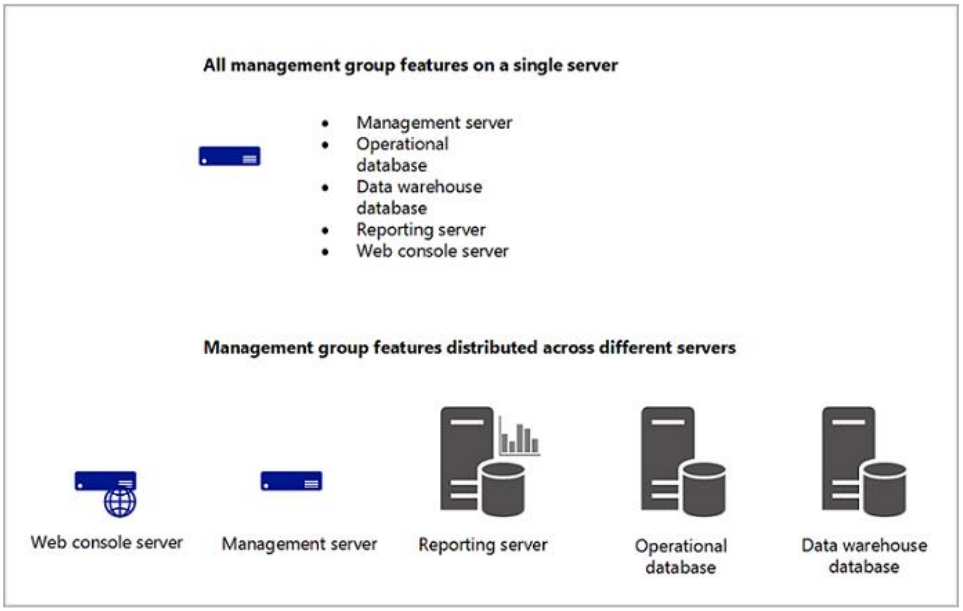


Рисунок 2.1 Структура Operations Manager

В якості баз даних Operations manager використовує SQL Server.

Microsoft SQL Server — це система керування реляційною базою даних (RDBMS), яка підтримує широкий спектр програм обробки транзакцій, бізнес-аналітики та аналітики в корпоративних IT-середовищах. Microsoft SQL Server є однією з трьох провідних на ринку технологій баз даних разом із Oracle Database і DB2 IBM. Як і інше програмне забезпечення RDBMS, Microsoft SQL Server побудовано на основі SQL, стандартизованої мови програмування, яку адміністратори баз даних (DBA) та інші IT-фахівці використовують для керування базами даних і запитів до даних, які вони містять. SQL Server

пов’язано з Transact-SQL (T-SQL), реалізацією SQL від Microsoft, яка додає набір власних розширень програмування до стандартної мови.

З боку керування даними Microsoft SQL Server включає служби інтеграції SQL Server, служби якості даних SQL Server і служби основних даних SQL Server. Також до СУБД входять два набори інструментів для адміністраторів баз даних і розробників: SQL Server Data Tools для розробки баз даних і SQL Server Management Studio для розгортання, моніторингу та керування базами даних.

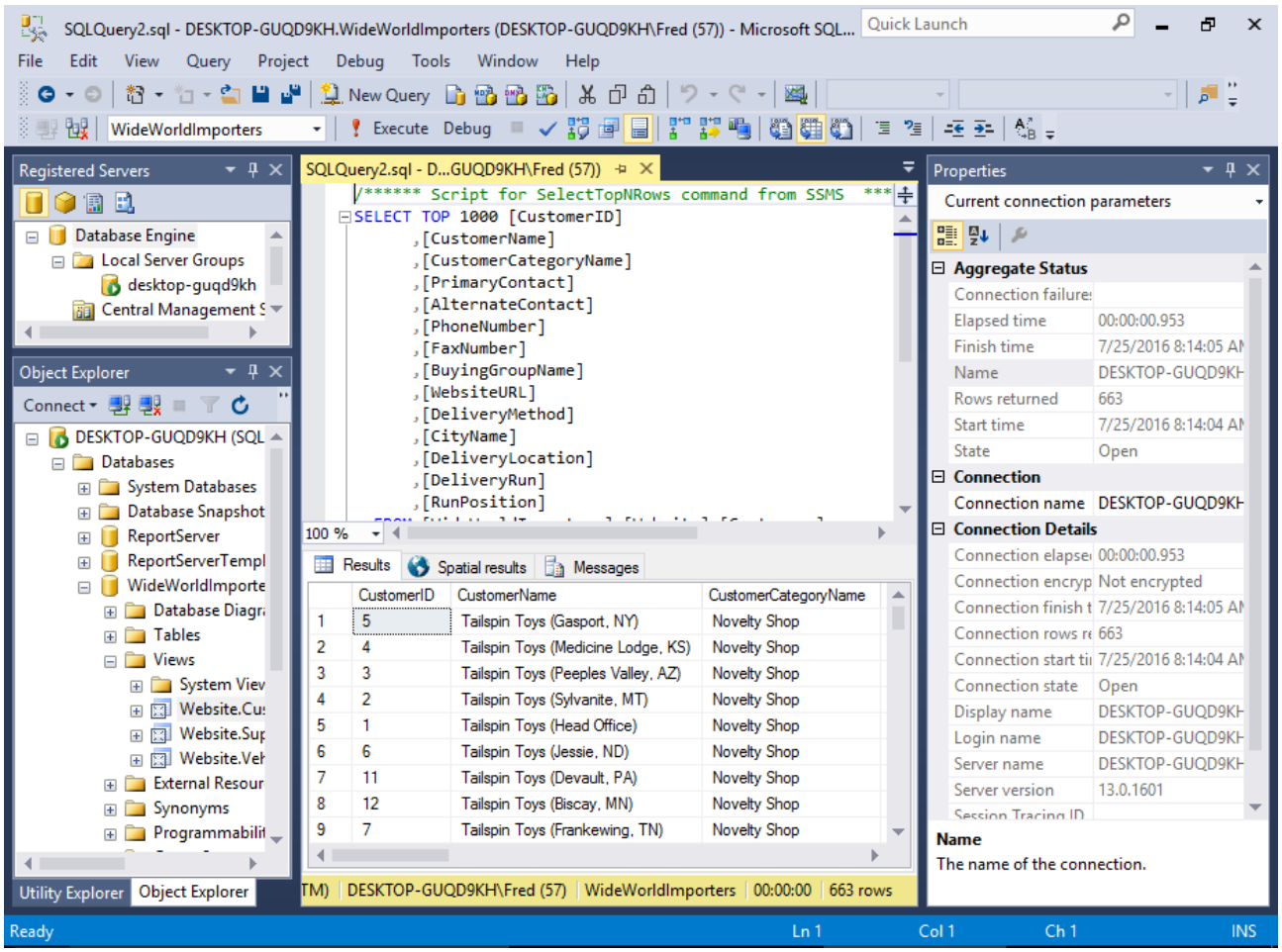


Рисунок 2.2 Інтерфейс SSMS

Окрім цього всього, для коректної роботи з мережою SCOM потребує використання сервіса Active Directory.

Active Directory (AD) є сервісом директорій, розробленим компанією Microsoft, і входить до складу їхньої серії серверних операційних систем, таких як Windows Server. Active Directory є централізованою базою даних, яка

зберігає інформацію про користувачів, комп'ютери, групи, політики безпеки та інші об'єкти в мережі комп'ютерів, що працюють під управлінням операційної системи Windows. Основними функціями цього сервісу є: централізоване управління мережою, аутентифікація та авторизація користувачів, організація в структуру та реплікація даних.

SCOM може використовувати AD для аутентифікації користувачів та операторів, які намагаються отримати доступ до системи. Користувачі можуть використовувати свої облікові записи AD для входу в SCOM, що спрощує процес керування обліковими записами та забезпечує єдиноцентрову систему ідентифікації для всіх систем, що використовують AD. SCOM може інтегруватися з AD для розпізнавання та імпорту об'єктів AD в якості моніторингових об'єктів. Це означає, що SCOM може автоматично виявляти сервери, комп'ютери, служби та інші об'єкти в AD та додавати їх до моніторингу.

Для контролю над AD використовується окремий сервер – Domain Controller(контролер домену). Він виконує ключову роль у доменній моделі AD і відповідає за керування об'єктами AD

2.2 Принципи виявлення об’єктів та моніторингу за ними

Для виявлення об’єктів SCOM використовує як і agent метод, так і agentless.

Агенти в Operations manager зазвичай використовуються для виявлення Windows та Unix комп’ютерів. Агент Operations Manager — це служба, інстальована на комп’ютери. Агент збирає дані, порівнює вибіркові дані з попередньо визначеними значеннями, створює сповіщення та запускає відповіді. Сервер керування отримує та розповсюджує конфігурації агентам на контрольованих комп’ютерах.

Агенти спостерігають за джерелами даних на контрольованому комп’ютері та збирають інформацію відповідно до конфігурації, яка надсилається йому з його сервера керування. Агент також обчислює стан

працездатності контрольованого комп’ютера та об’єктів на контрольованому комп’ютері та повідомляє сервер керування. Коли стан працездатності контрольованого об’єкта змінюється або виконуються інші критерії, агент може створити сповіщення. Це дозволяє операторам знати, що щось вимагає уваги. Надаючи дані про працездатність об’єкта моніторингу на сервер керування, агент надає актуальну картину працездатності пристрою та всіх додатків, які на ньому розміщені.

Завдяки Active Directory, встановлення агента на пк всередині домену робиться автоматично, і всі комп’ютери контролюються легко і безпечно.

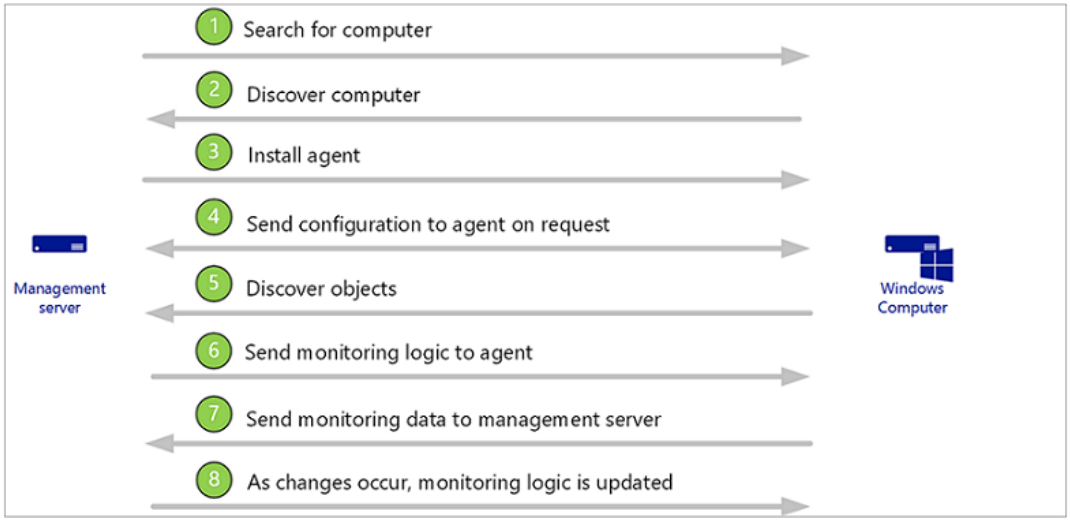


Рисунок 2.3 Принцип виявлення об’єктів в SCOM

Для комп’ютерів, які знаходяться поза доменом потрібно використовувати сертифікати. Сертифікація комп'ютерів - це процес, який дозволяє надавати довіру та встановлювати ідентичність комп'ютерів, які не входять до домену Active Directory. Цей процес може використовуватися в ситуаціях, коли комп'ютери підключаються до мережі, але не входять до централізованої інфраструктури домену. Основна функція сертифікації комп'ютерів поза доменом полягає у підтвердженні безпеки та ідентифікації цих комп'ютерів у мережі.

Для зв’язку з мережними пристроями SCOM використовує Agentless структуру з використанням Simple Network Management Protocol (SNMP) - це підхід до моніторингу, при якому не потрібно встановлювати агента (програмне

забезпечення) на самому пристрої для отримання інформації про його стан і роботу.

SNMP є протоколом, який використовується для моніторингу і керування мережевими пристроями, такими як маршрутизатори, комутатори, файрволи, сервери і т.д. Він дозволяє збирати дані про стан пристрою, такі як ресурси, потоки даних, статуси роз'ємів і т.д., а також надсилати команди для керування пристроєм.

У режимі agentless моніторингу, моніторингова система (наприклад, SCOM) взаємодіє з мережевими пристроями через SNMP. Вона відправляє запити до пристроїв через мережу, використовуючи SNMP-запити, і отримує відповіді з необхідною інформацією про стан пристрою. Запити можуть стосуватися різних параметрів, таких як стан інтерфейсів, завантаження процесора, використання пам'яті і т.д.

Agentless моніторинг за допомогою SNMP має кілька переваг:

Спрощена реалізація: Не потрібно встановлювати агенти на кожному мережному пристрої, що полегшує процес моніторингу і управління.

Зниження навантаження: Оскільки немає потреби в агентах, навантаження на мережеві пристрої зменшується, що може бути важливим для пристроїв з обмеженими ресурсами.

Універсальність: SNMP є стандартним протоколом, який підтримується більшістю мережевих пристроїв, тому agentless моніторинг можна використовувати для широкого спектру пристроїв.

Agentless моніторинг за допомогою SNMP є потрібним для забезпечення контролю і моніторингу мережевих пристроїв без потреби встановлювати агенти. Це дозволяє операторам мережі відстежувати стан пристроїв, виявляти проблеми, моніторити використання ресурсів і вчасно приймати рішення щодо управління мережею.

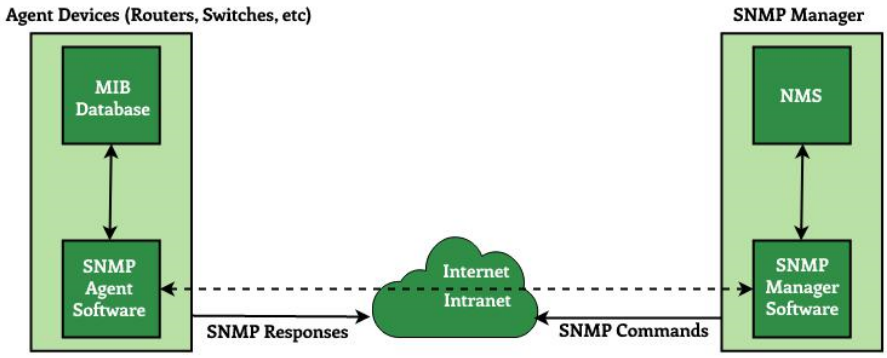


Рисунок 2.4 Архітектура SNMP

Для конфігурації моніторингу в SCOM використовуються пакети керування(Management packs)

Management packs (MP) - це пакети конфігурації, які містять набори правил, моніторів, репортів та інших об'єктів, необхідних для моніторингу конкретних технологій, продуктів або інфраструктурних компонентів. MP визначає, які метрики і стани повинні бути моніторовані, які дії слід виконати в разі виявлення проблеми, і які дані слід збирати для подальшого аналізу. SCOM постачається з набором стандартних Management packs, але можна створювати свої власні або використовувати Management packs від сторонніх виробників.

У кожному пакеті управління визначається модель керованого компонента. Ця модель виражається у вигляді одного або кількох класів, кожен з яких визначає об'єкти для відображення та управління. Коли дані з пакета керування надсилаються агенту, він використовує правила виявлення з пакету керування для пошуку фактичних екземплярів класів, заданих у пакеті.

Для зниження навантаження на набір і вимог до сховища на стороні агента, на локальне сховище агента завантажуються лише складові пакети керування, необхідні для моніторингу. Наприклад, скачуються розділи пакетів управління, що визначають правила і монітори, а розділи для знань і звітів — немає.

Кожен керуючий пак включає в себе набори моніторів, правил, завдань, звітів та профили Run as.

Монітори в SCOM використовуються для постійного моніторингу стану системи або ресурсу. Вони перевіряють стан регулярно і визначають, чи є система або ресурс у стані нормальної роботи, критичного стану або відсутності підключення. Монітори використовуються для виявлення проблем, встановлення тривог і виклику відповідних дій для виправлення проблеми.

Правила в свою чергу використовуються для моніторингу специфічних подій або станів в системі. Вони базуються на "if-then" логіці, де визначаються умови, які повинні виконуватися, і дії, які слід виконати при виконанні цих умов. Правила можуть бути використані для моніторингу подій, логів, реєстру, служб і багатьох інших аспектів системи.

Задачі відносяться до функціональності, яка дозволяє виконувати специфічні дії або команди на моніторингованих об'єктах. Завдання — це сценарій або інший код, що виконується, який запускається на сервері керування або на сервері, клієнті або іншому керованому пристрої. Задачі можуть виконувати будь-який вид діяльності, включаючи перезапуск програми, що відмовила або видалення файлів. Як і інші аспекти пакета управління, завдання пов'язуються з певними . Існують керованими класами. Існують два спеціальні типи завдань, пов'язаних з моніторами: завдання діагностики, що мають на меті виявити причину проблеми, та завдання відновлення, що служать для вирішення проблеми. Ці завдання можуть виконуватися автоматично під час переходу монітора до стану помилки, надаючи автоматичний спосіб вирішення проблеми.

Пакети керування можуть містити один або кілька профілів запуску від імені. Профілі та облікові записи запуску від імені використовуються для вибору користувачів із правами, необхідними для запуску правил, завдань та моніторів.

Автори пакета керування можуть створити профіль запуску від імені та зв'язати його з одним або декількома правилами, моніторами, завданнями або виявленнями. Названий профіль запуску від імені імпортується разом із пакетом керування в Operations Manager.

Для налаштування та керування моніторингом інфраструктури в SCOM використовується Operations Console. Це доволі зручний клієнтський додаток, який дозволяє зручно керувати всіма функціями моніторингу.

Operations Console надає зручний інтерфейс для настроювання моніторингу. Користувачі можуть створювати та налаштовувати правила, монітори, тривоги та інші компоненти моніторингу безпосередньо зі свого робочого простору. Окрім цього користувачі можуть переглядати, керувати та реагувати на триваги, згенеровані системою. Додаток дозволяє виставляти пріоритети тривогам, переглядати деталі та можливі способи вирішення проблем. Інтерфейс містить окремі розділи для моніторингу, створення різних правил чи моніторів, адміністрування та звітів, що робить інтерфейс ще зручнішим.

До недоліків цього додатку можна віднести залежність від інтернету та доволі великий поріг входу. Деякі функції можуть бути доволі складні і вимагають багатьох кроків, для ефективної роботи.

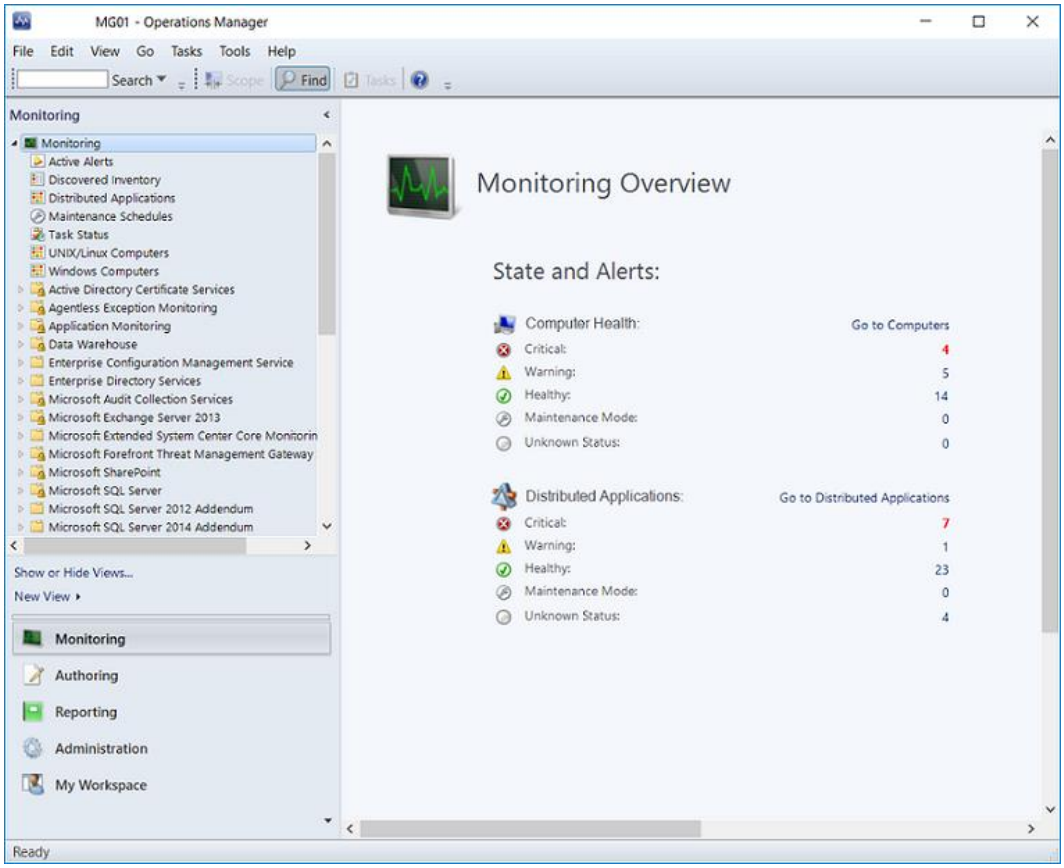


Рисунок 2.5 Головний інтерфейс Operations Manager

2.3 Розробка схеми мережі

Моніторингова мережа поділена на віртуальну і фізичну мережу.

2.3.1 Віртуальна мережа

Віртуальна мережа проекту буде побудована в графічному симуляторі GNS3. GNS3 дозволяє імітувати мережеве обладнання, таке як маршрутизатори, комутатори, файрволи та інші пристрої, із використанням реальних образів операційних систем, які використовуються в реальних мережах. Метод роботи Gns3 базується на віртуалізації. Він використовує оригінальні мережеві пристрої, такі як CISCO IOS, Juniper JunOS або інші віртуальні машини. GNS3 надає інтерфейс для взаємодії з цими віртуальними пристроями, що дозволяє налаштовувати їх, створювати мережеві топології та тестувати їх працездатність. Основним плюсом цього симулятора є можливість підключити реально фізичне обладнання до віртуальної мережі.

В якості платформи віртуалізації операційних систем найкращими рішеннями буде VirtualBox або VMWare.

Virtualbox - Це відкрита платформа віртуалізації, розроблена компанією Oracle, яка дозволяє відкривати абсолютно всі операційні системи на віртуальних машинах, незалежно від встановленої на машині. VirtualBox може розширити технічні можливості будь-якого сумісного комп’ютера, дозволяючи йому запускати кілька операційних систем на різних віртуальних машинах одночасно. VirtualBox дозволяє будь-якій системі встановлювати та використовувати стільки віртуальних машин, скільки дозволяють її пам’ять і дисковий простір. Oracle VM VirtualBox дозволяэ скористатися перевагами інновацій, представлених у сучасній системі x86 апаратної платформи, він легкий і простий у встановленні та використанні. Проте під простим зовнішнім виглядом криється надзвичайно швидкий і потужний механізм віртуалізації. Oracle VM VirtualBox має високу репутацію та має багато плюсі, таких як: чудова продуктивність; потужна система віртуалізації; і широкий спектр підтримуваних гостьових операційних систем. Oracle VM VirtualBox Enterprise — ідеальний вибір для розробки нового покоління. Останній випуск представляє підтримку

паравіртуалізації для віртуальних машин Linux і Windows і підтримку пристроїв xHCI/USB 3.0 і нові платформи, а також забезпечує розширені можливості ЦП і підтримку двонаправленого перетягування між хост і його гостьові віртуальні машини. Він також представляє шифрування образу диска та багато інших удосконалень.

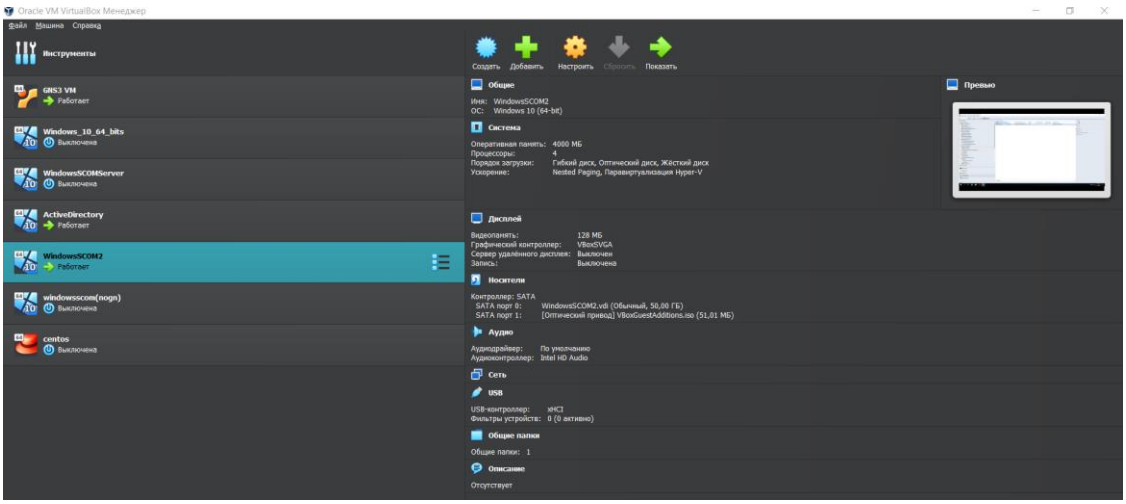


Рис 2.6 Інтерфейс VirtualBox

VMWare – аналог віртуалбокс, програмне забезпечення для віртуалізації та хмарних обчислень. VMWare базує свої технології віртуалізації на голому гіпервізорі ESX/ESXi в архітектурі x86. За допомогою віртуалізації сервера VMware на фізичному сервері встановлюється гіпервізор, який дозволяє працювати декільком віртуальним машинам (ВМ) на одному фізичному сервері. Кожна віртуальна машина може запускати власну операційну систему (ОС), що означає, що кілька ОС можуть працювати на одному фізичному сервері. Усі віртуальні машини на одному фізичному сервері спільно використовують такі ресурси, як мережа та оперативна пам’ять. У 2019 році VMware додала підтримку свого гіпервізора для запуску контейнерних робочих навантажень у кластері Kubernetes подібним чином. Команда інфраструктури може керувати цими типами навантажень так само, як віртуальні машини, а команди DevOps можуть розгортати контейнери, як вони звикли.

VirtualBox було вибрано як основну платформу для віртуалізації, оскільки він дає можливість поєднувати фізичну та віртуальну мережу в спільну.

Віртуальна мережа складається з двух відділів: Адміністративного, де знаходяться сервери, маршрутизатори та робочого, де знаходяться робочі машини типу Windows, Linux або Unix

Адміністративний відділ включає в себе сам Scom сервер, контролер домену, та маршрутизатор для зв’язку з мережою Інтернет

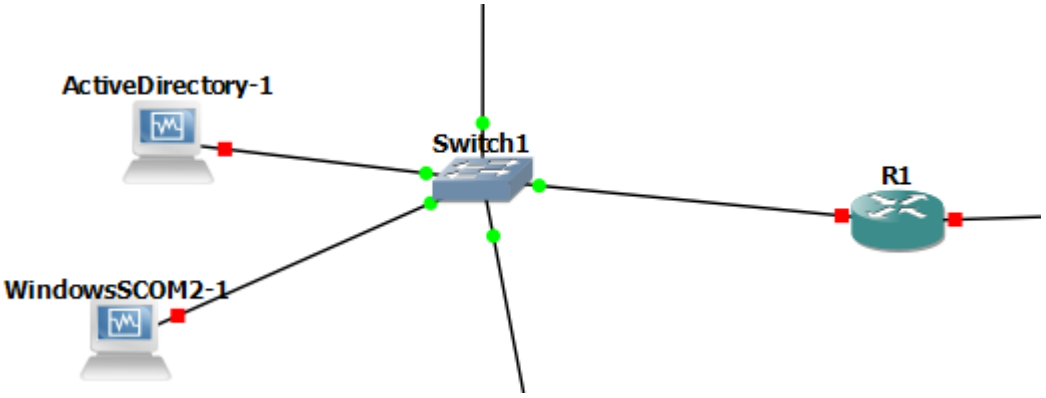


Рисунок 2.6 Адміністративній відділ

Контролер домену створює структуру, відповідає за контроль домена та аутентифікацію користувачів.

Для того, щоб моніторити маршрутизатор налаштовано SNMP. Окрім цього на ньому налаштовано DHCP для видачи ip-адрес, OSPF для зв’язку з мережою та NAT. Маршрутизатор виконує функцію зв’язку між віртуальною мережою та фізичною мережою .

Робоча мережа складається з Windows і Linux комп’ютерів

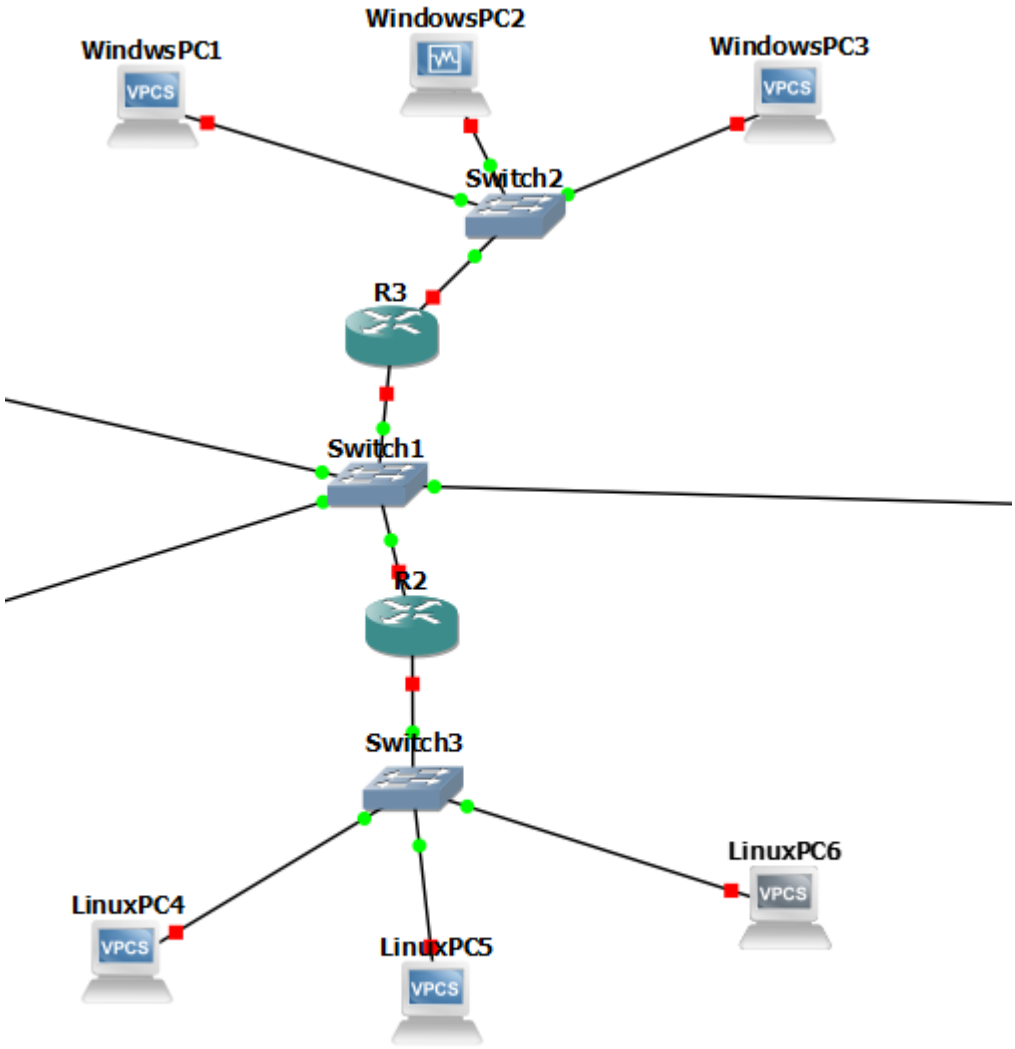


Рисунок 2.7 Локальна мережа

Завдяки тому, що всі пк в локальній мережі знаходяться всередині домену, встановлення агента на них автоматичне.

2.3.2 Фізична мережа

Фізична мережа включає в себе домашній роутер, HostPC та DNS-Server для перевірки роботи серв

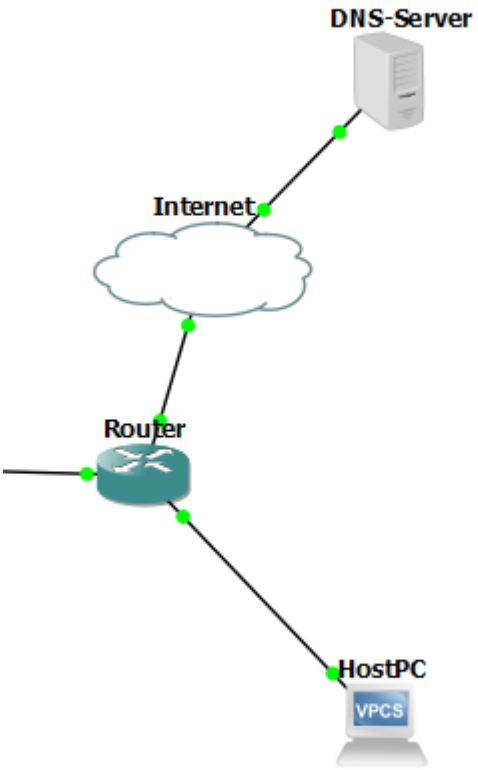


Рисунок 2.8 фізична мережа

На роутері, dns-сервері та dhcp-сервері налаштовано snmp для моніторинг за допомогою SCOM.

Для зв’язку з Хост-пк буде встановленно агент вручну та налаштування сертифікації для довіренного доступу до Management server.

Окрім цього, моніторингова мережа включає 3 віддалені сервері, які є найвідомішими сервісами банкінгу.

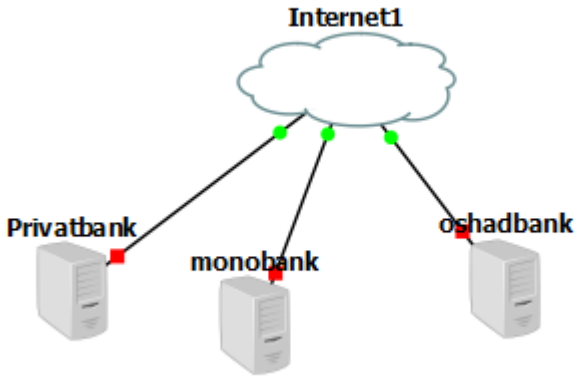


Рисунок 2.9 Віддалені веб сервери

Для моніторингу веб серверів використовується спеціальні монітори(web application availability monitoring), які дозволяють відслідковувати стан та час відгуку.

Висновки до розділу 2

В цьому розділі було розглянуто архітектуру SCOM, принципи його роботи з пристроями.

Проаналізовано вибір найбільш ефективного графічного симулятора та платформу віртуалізації

Було складено схему майбутньої мережі та налаштовано зв’язок між пристроями

Розділ 3: Встановлення та базове налаштування системи моніторингу SCOM

3.1 Встановлення SCOM

Перед встановлення сервісу System Center Operations manager проведемо базове налаштування системи. Для початку підключимо Server до домену semenchuk.

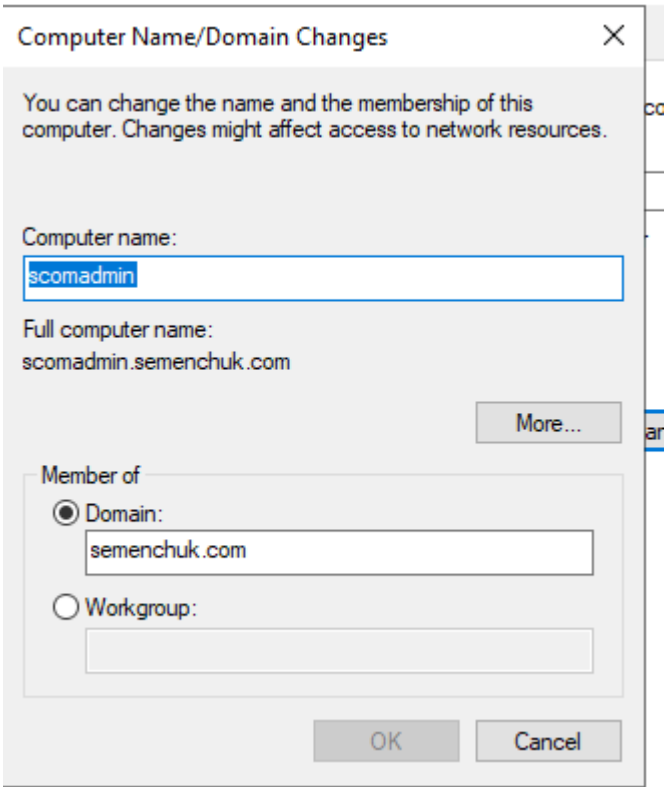


Рисунок 3.1 Підключення до домену semenchuk.com

Для коректної роботи та моніторингу проведемо встановлення відповідних ролей та компонентів, ввівши команди нижче в Powershell:

Add-WindowsFeatureNET-WCF-HTTP-Activation45,Web-Static-Content,Web-Default-Doc,Web-Dir-Browsing,Web-Http-Errors,Web-Http-Logging,Web-Request-Monitor,Web-Filtering,Web-Stat-Compression,Web-Mgmt-Console,Web-Metabase,Web-Asp-Net,Web-Windows-Auth –Restart

Для коректної роботи Microsoft SCOM потрібна сервер та база даних. Було вирішено встановити SQL Server 2017 з функціями Database Engine

Services та Full-Text and Semantic Extractions for Search. Для керування SQL Server 2017 використовується SSMS(SQL Server Management Studio)

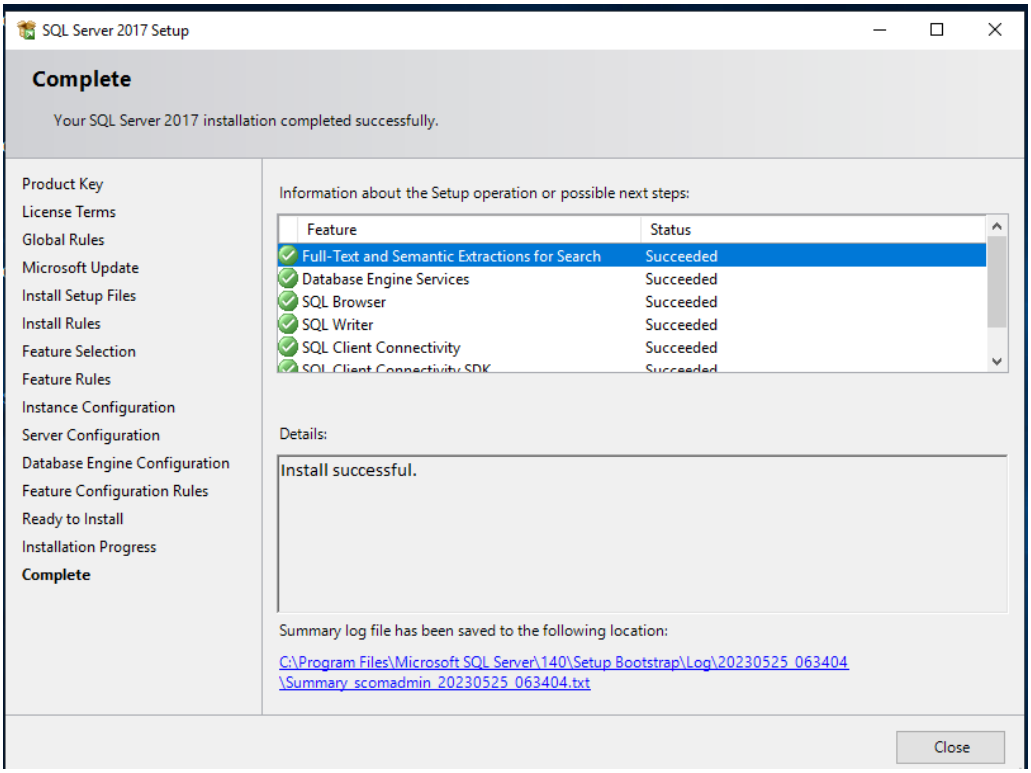


Рисунок 3.2 Встановлення SQL SERVER

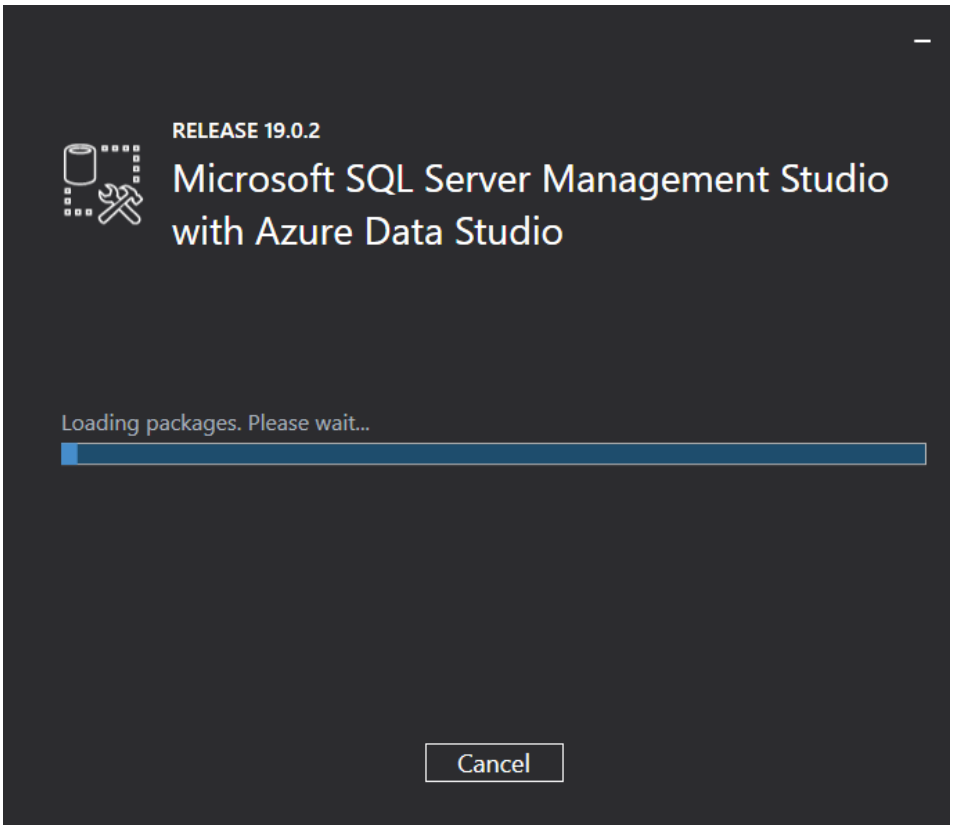


Рисунок 3.3 Встановлення SSMS

Для роботи з звітами та репортами SCOM використовує SQL Server 2017 Report Service. В ньому можна налаштувати сервісний аккаунт, створити базу даних для звіті та веб сервіс для керування SCOM.

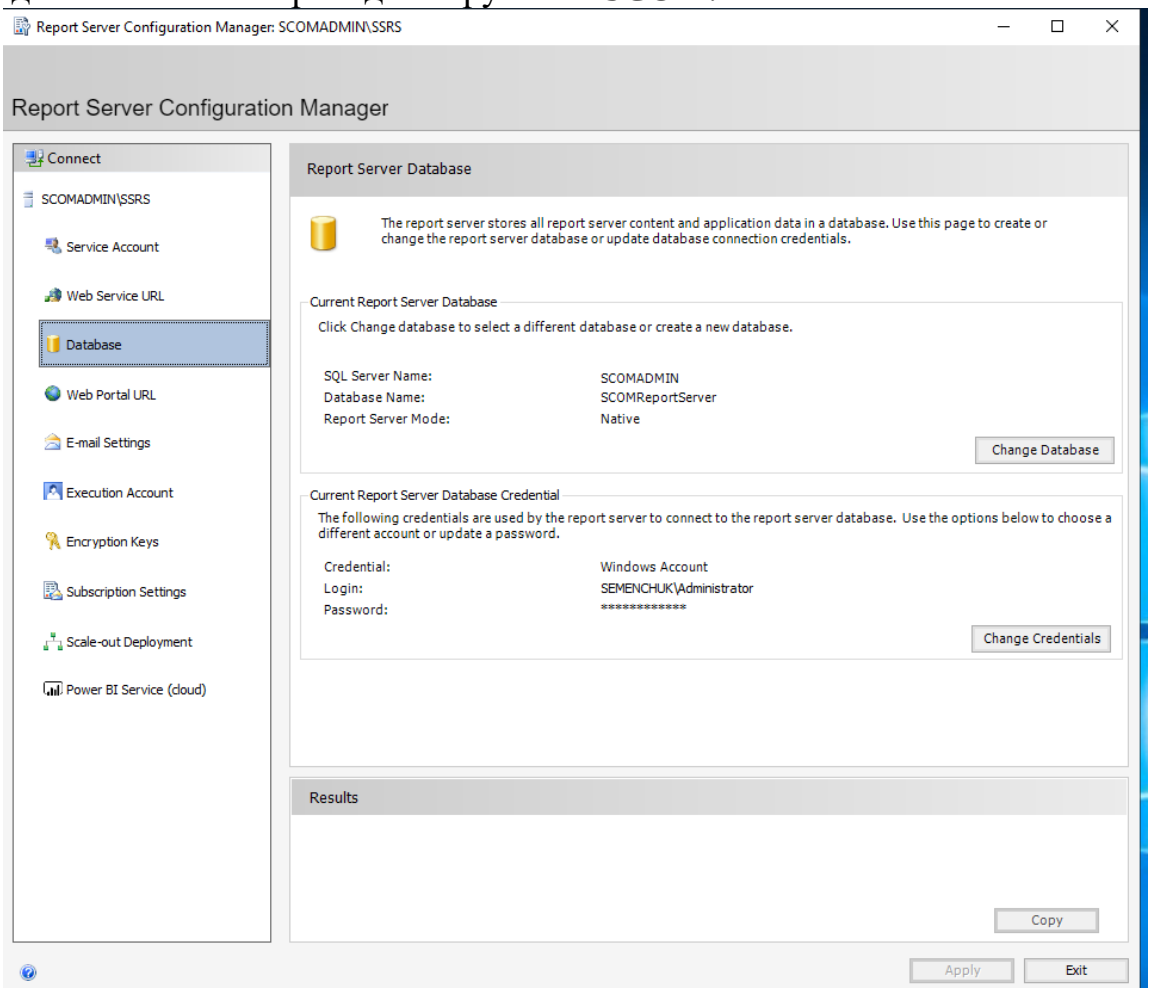


Рисунок 3.4 Створення бази даних репортів

Після всіх цій дій, можна почати встановлення MS SCOM. В розділі функцій потрібно встановити management server, operations console, web console, reporting server

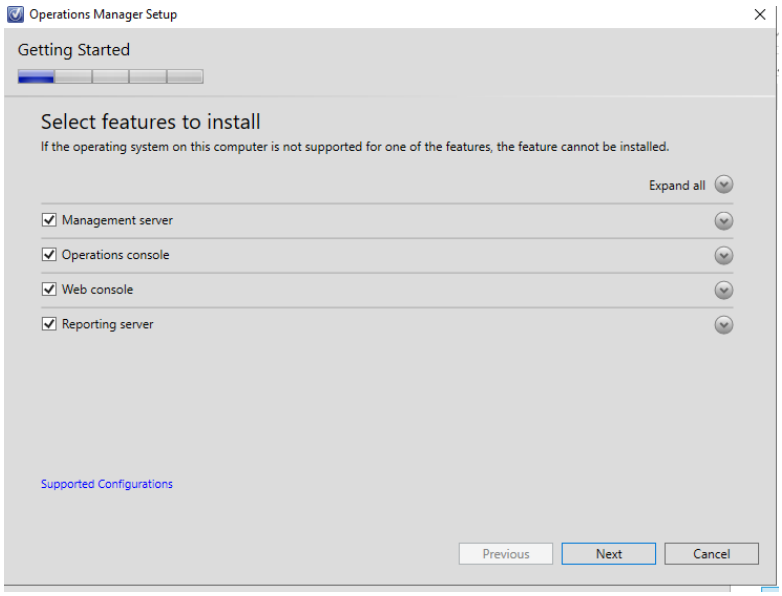


Рисунок 3.5 Функції MS SCOM

Інсталяція MS SCOM пройшла успішно.

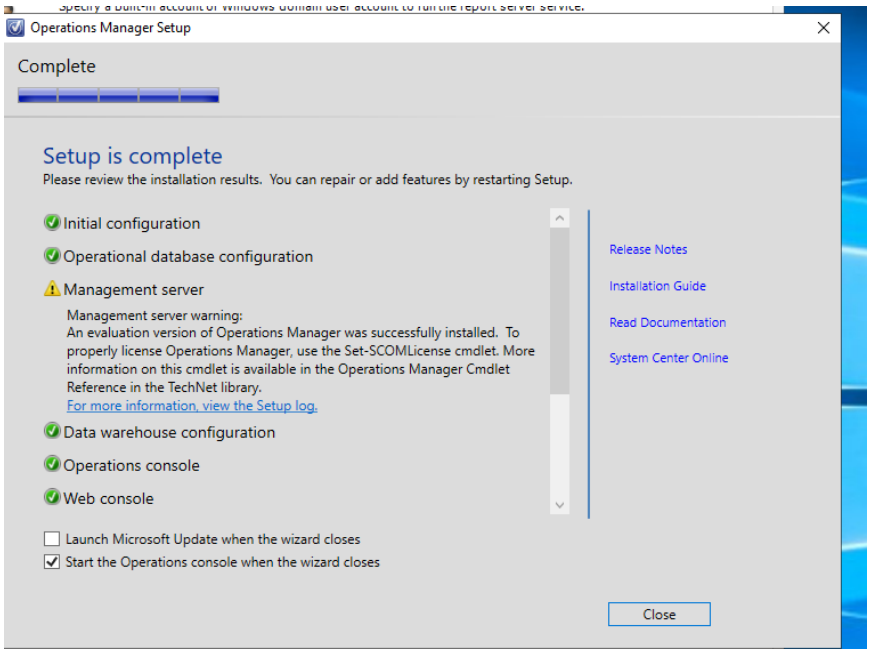


Рисунок 3.6 Успішна інсталяція

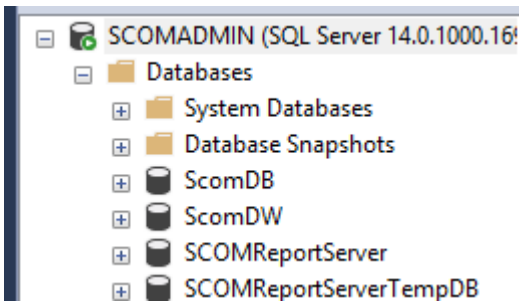


Рисунок 3.7 Створенні бази даних

3.2 Підключення пристроїв для моніторингу

Для моніторингу пристроїв мережі, буде використано, як метод з агентами так і без.

Для зв'язку з пристроями Windows, які знаходяться в межах домену використовується автоматичне встановлення агентів, як видно на рисунку 3.8

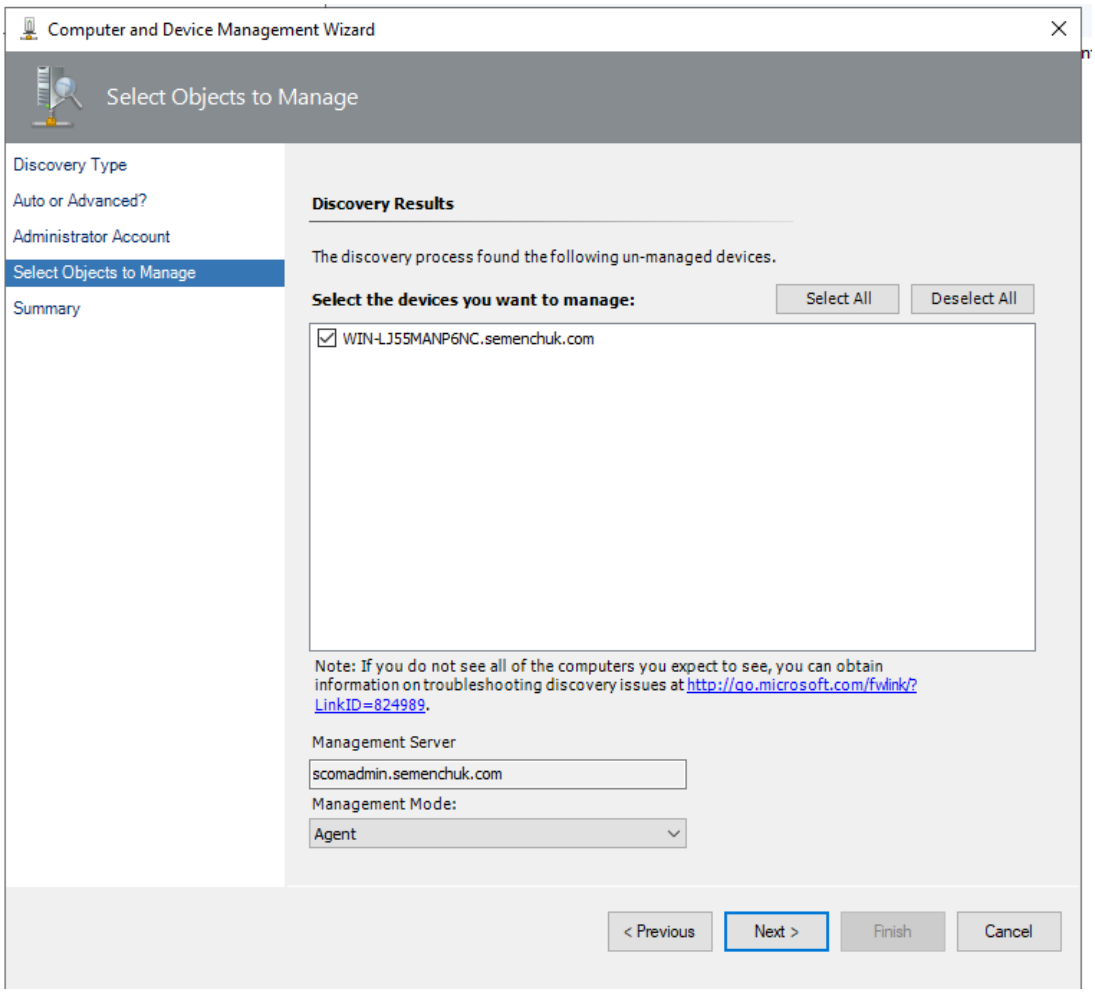


Рисунок 3.8 Автоматичне встановлення агента

Встановлення агента на Windows машину поза доменом проводиться вручну. Для забезпечення безпеки та надійності мережевих структур, потрібно

встановити сертифікати на SCOM сервер та віддалену машину. Для початку потрібно скачати довірений рут сертифікат, перейшовши на сайт сервера сертифікатів і після цього добавити його в довіренні.

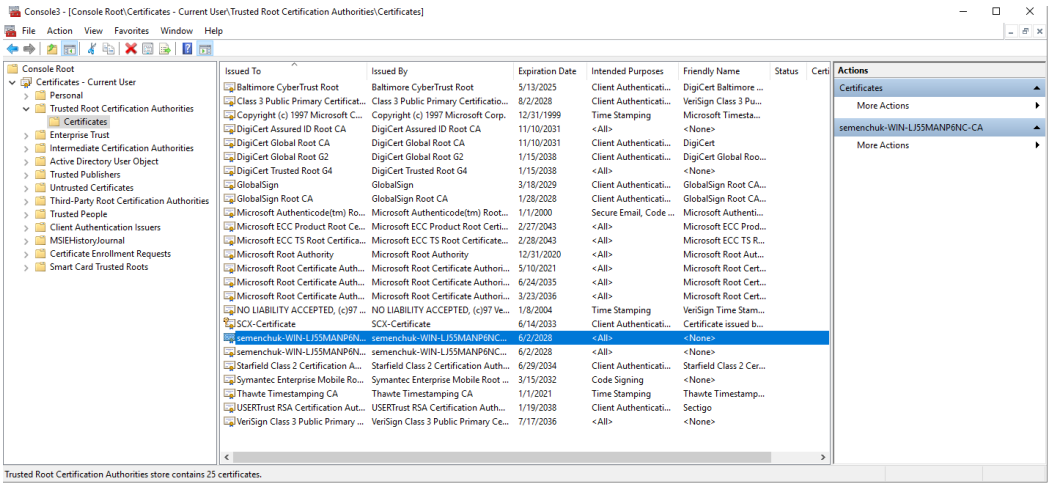


Рисунок 3.9 Довірений сертифікат

Після цього формується запит на отримання сертифіката у такому вигляді:

Subject="CN=<FQDN of computer you are creating the certificate, for example, the gateway server or management server.>"

Exportable=TRUE

KeyLength=2048

KeySpec=1

KeyUsage=0xf0

MachineKeySet=TRUE

[EnhancedKeyUsageExtension]

OID=1.3.6.1.5.5.7.3.1

OID=1.3.6.1.5.5.7.3.2

Цей запит конвертується в тип req за допомогою команди:

CertReq –New –f RequestConfig.inf CertRequest.req

Після запиту на сертифікат, потрібно скачати отриманий сертифікат, та встановити його на сервер управління та робочу машину

certreq -accept NewCertificate.cer

Після завершення роботи з сертифікати, потрібно встановити агента вручну на робочу машину

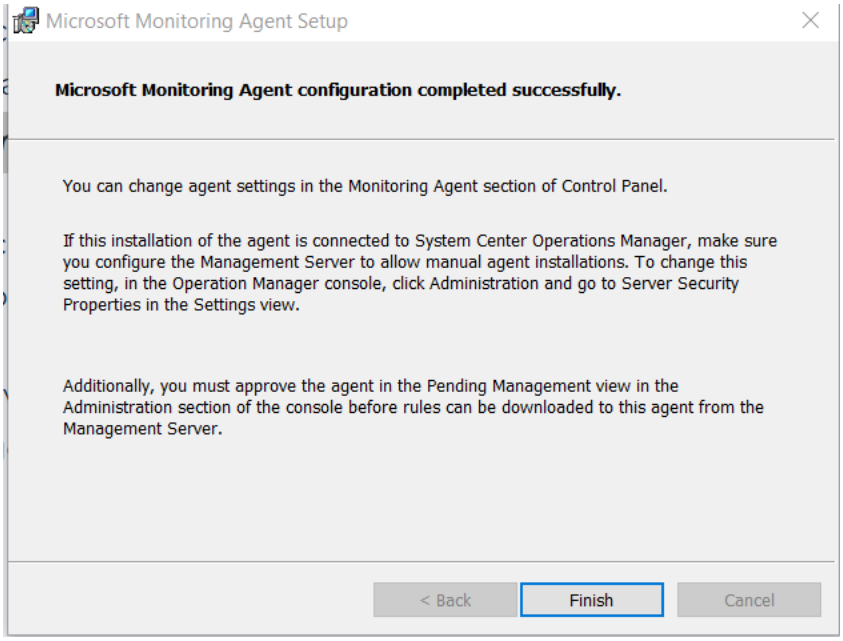


Рисунок 3.10 Встановлення агенту

Після встановлення агента потрібно імпортувати сертифікат в SCOM та машину за допомогою інструменту MOMCertImport:

MOMCertImport.exe semenchuk.pfx

Після цього, пристрій з’явиться в переліку моніторингу.

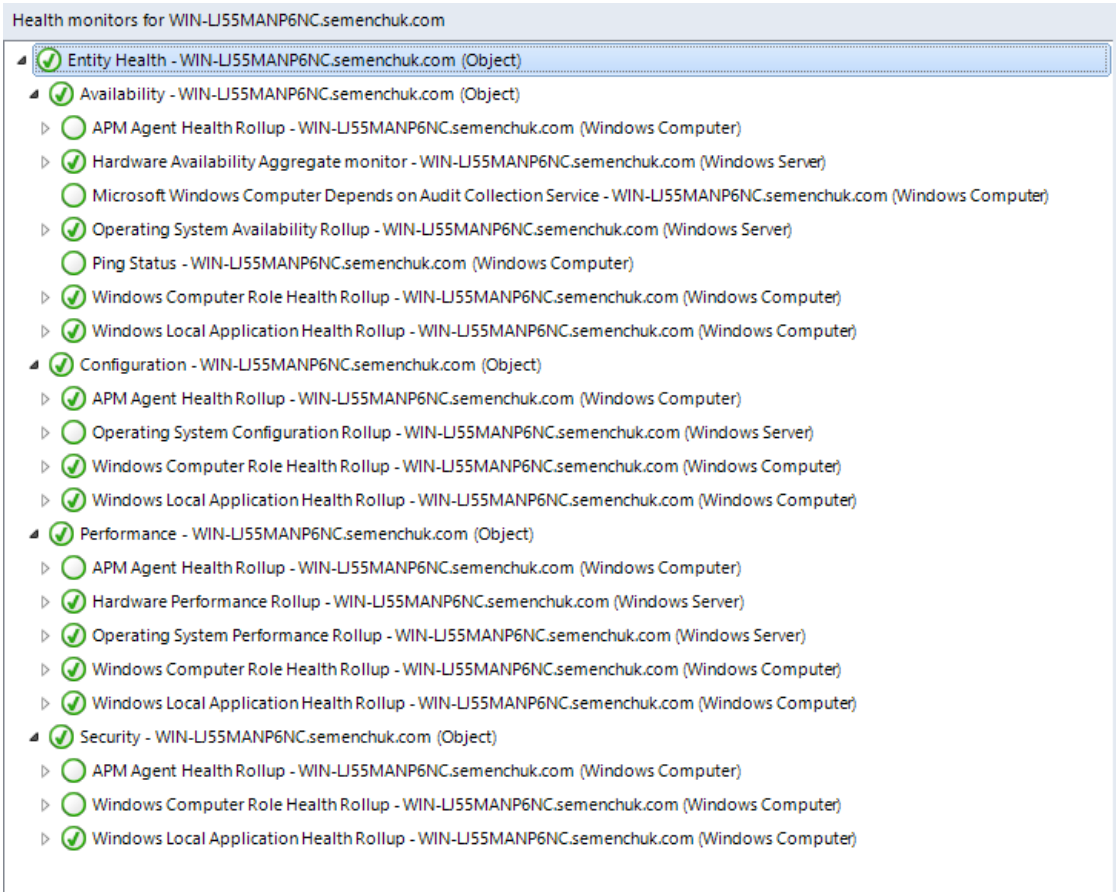


Рисунок 3.11 Перевірка стану функцій машини

Для роботи з Linux пристроями SCOM потребує окремого набору пакетів керування. На рисунок 3.11 показано імпорт цих пакетів.

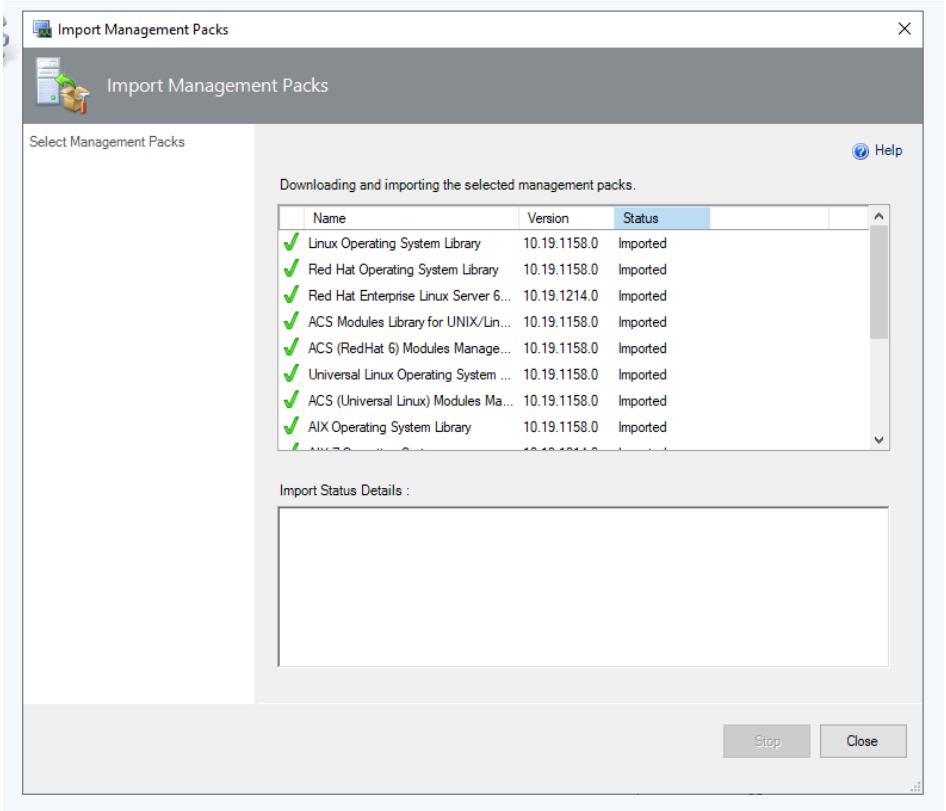


Рисунок 3.12 Імпорт пакетів для моніторингу Linux/Unix пристроїв

Для моніторингу Linux/Unix машинами потрібно 3 користувача: Unix/Linux Agent maintance Account, Unix/Linux Monitoring Account, Unix/Linux Privileged Monitoring Account.

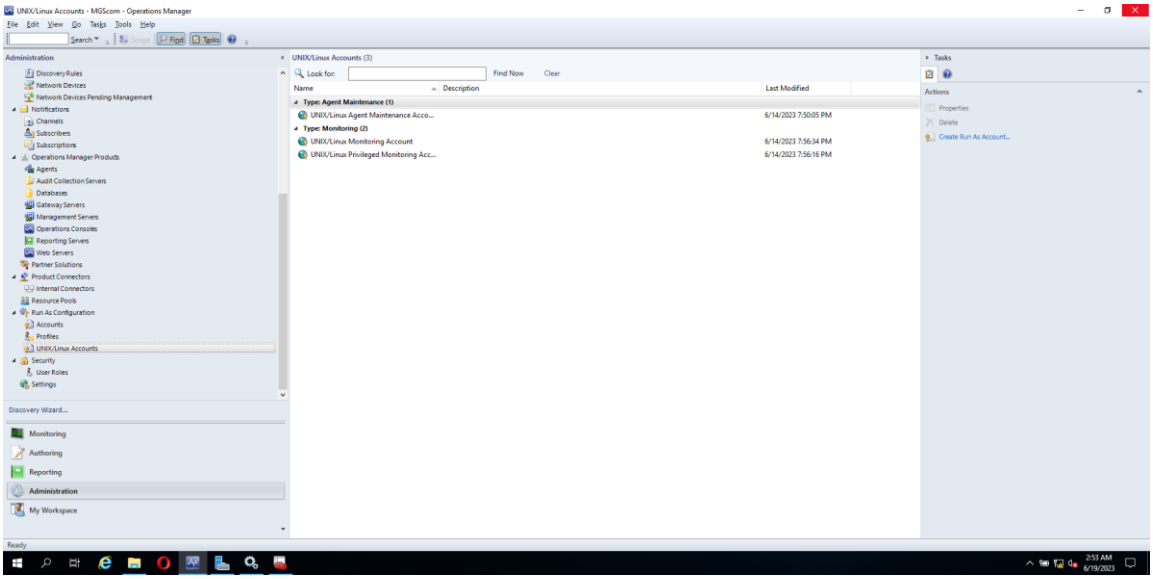


Рисунок 3.13 Аккаунти для керування Unix/Linux машинами

Для доступу до прав адміну, потрібно добавити цих користувачів в sudoers файл за допомогою строчки:

scomadmin ALL=(ALL) NOPASSWD:ALL

Для уникнення проблем з сертифікацією, згенеруємо новий сертифікат використовуючи команду:

/opt/microsoft/scx/bin/tools/scxsslconfig -f -h centos -d semenchuk.com

Після проведення всіх вище перерахованих етапів, можна автоматично встановити агента на Unix/Linux машину, і моніторити основні дані.

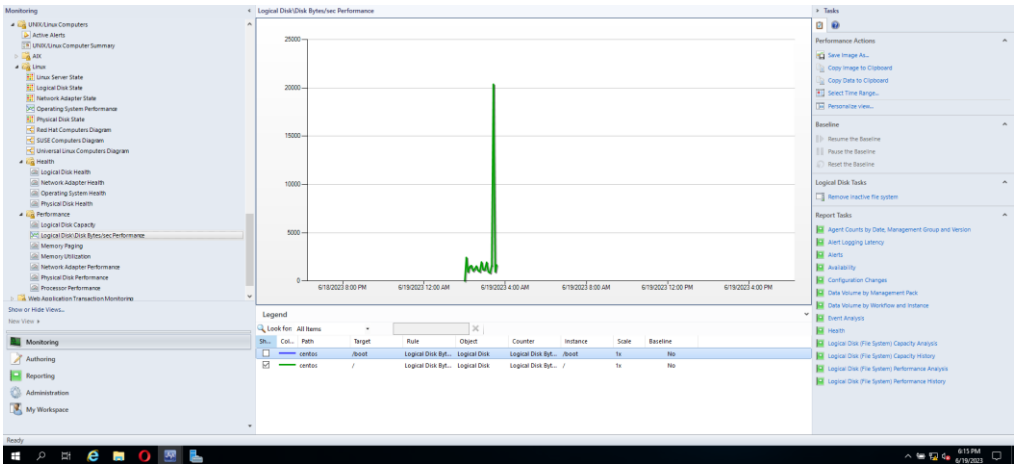


Рисунок 3.14 Успішний моніторингу Linux машини

Для моніторингу мережевих пристроїв потрібно на кожному з них налаштувати SNMP. Налаштування SNMP показано на рисунках нижче:

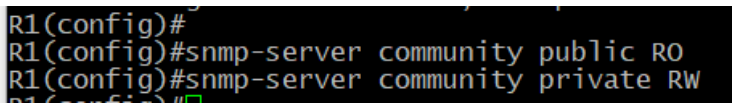


Рисунок 3.15 Налаштування SNMP на CISCO7200

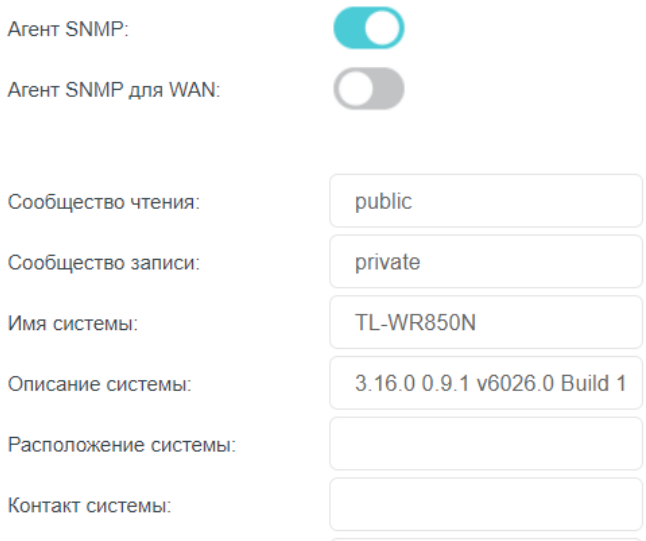


Рисунок 3.16 Налаштування SNMP на TP-Link

Після налаштування SNMP потрібно включити пошук агентів в Operations console та задати ip-адреси для пошуку. Окрім моніторингу мережних пристроїв своєї мережі, також можна додати сервіси провайдера, такі як DHCP або DNS.

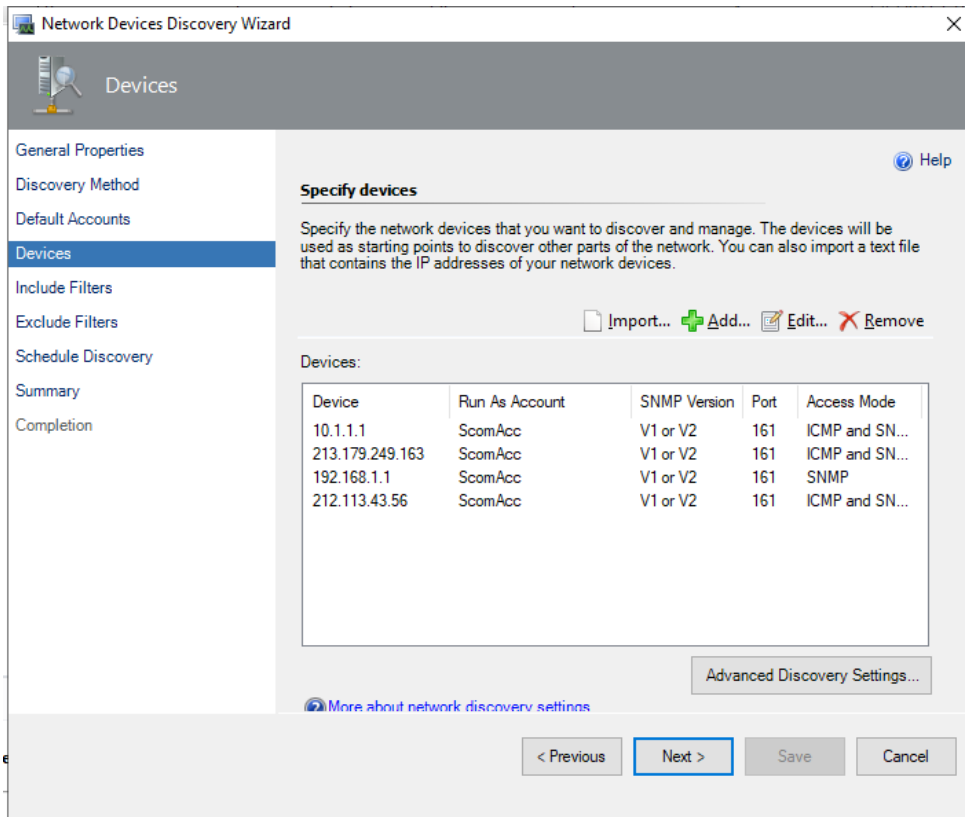


Рисунок 3.17 Задання ip-адрес

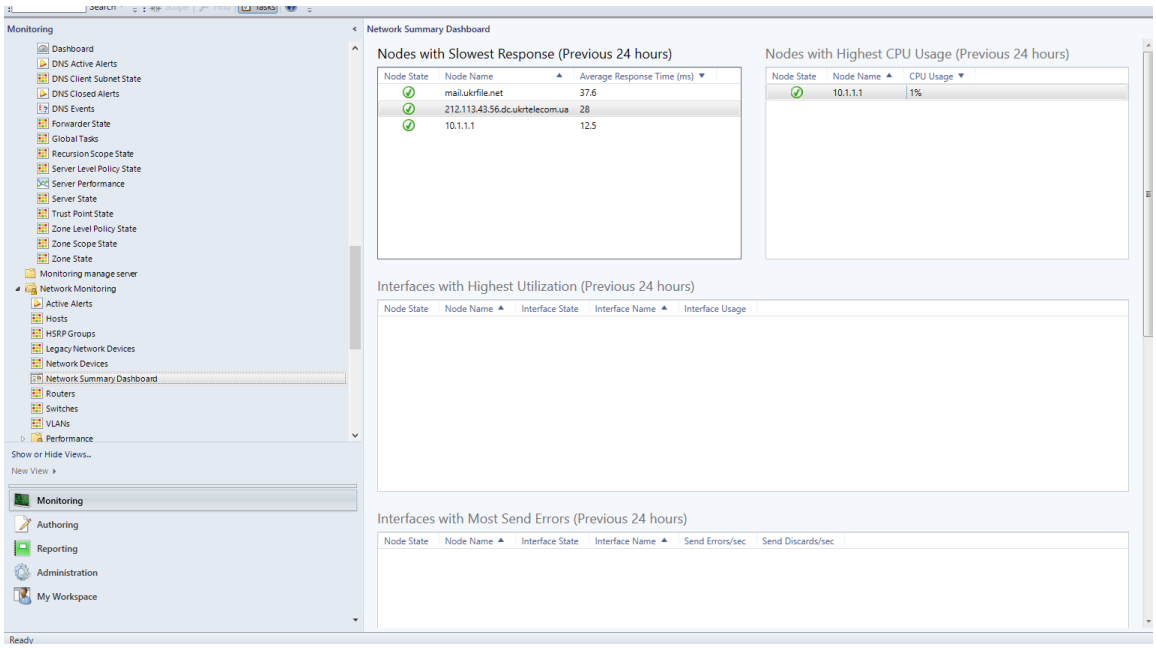


Рис 3.18 Статус моніторингу мережевих пристроїв

Створимо монітор для моніторингу віддалених серверів банкінгу. Для цього потрібно перейти в Authoring та створити Web Application Availibility Monitor, створити монітор з назвою Bank_ID та добавити веб-адресу банків.

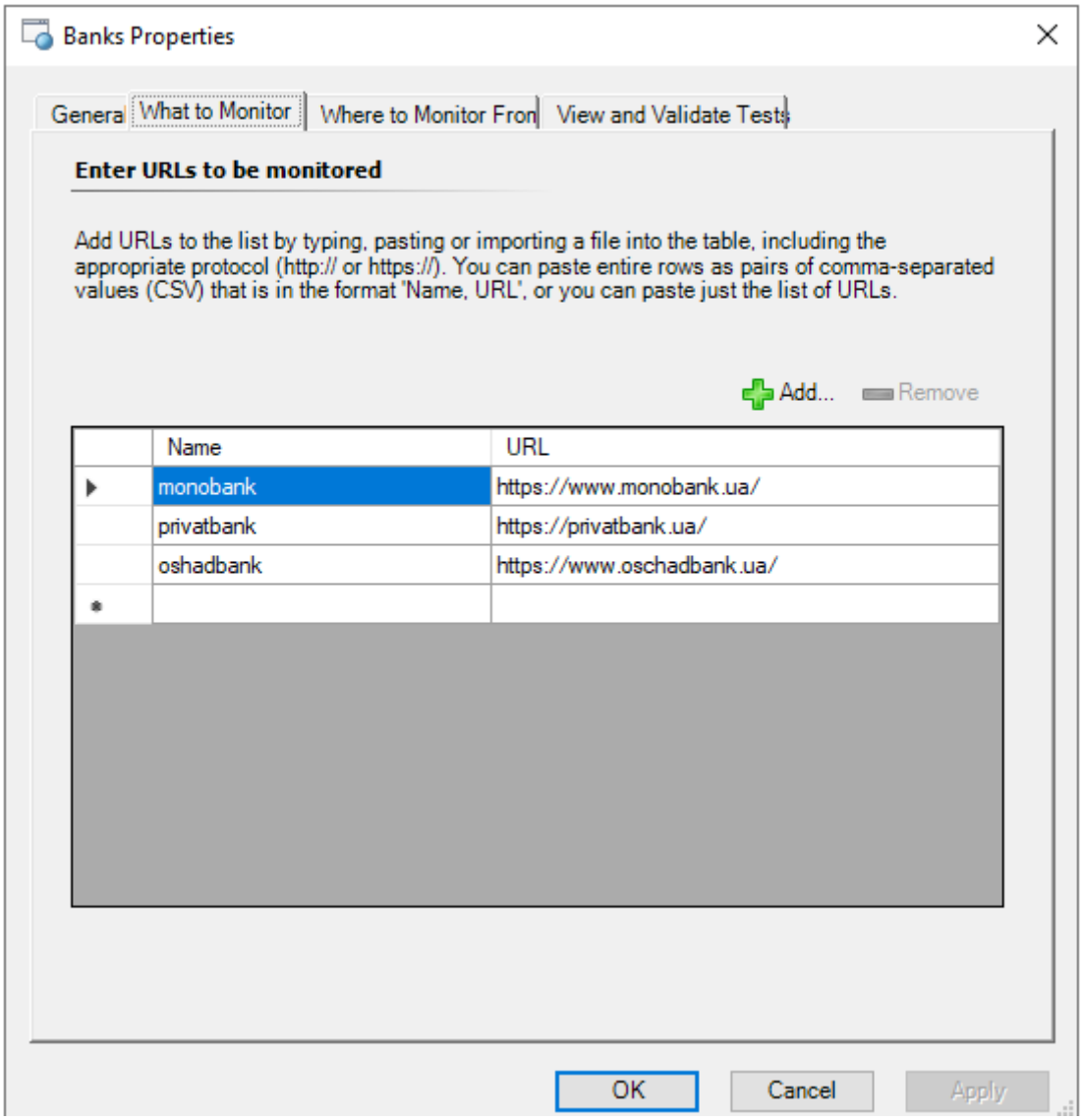


Рисунок 3.19 Моніторинг сервісів банкінгу

Тепер в SCOM сервер можна моніторити статус цих серверів та порівнювати час відклику від кожного з них

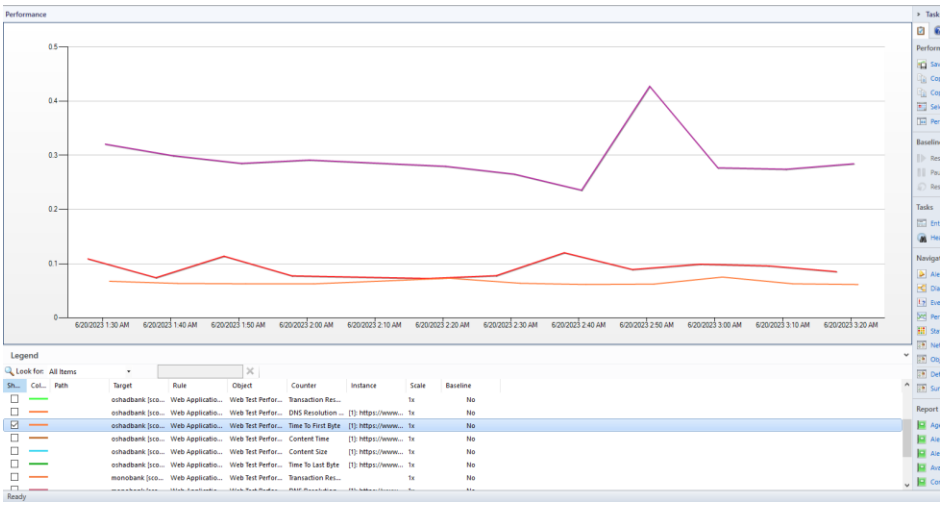


Рисунок 3.20 Порівняння сервісів банкінгу у вигляді графіку

3.3 Перевірка роботи моніторів та попереджень

В якості прикладу для перевірки буде використано монітор Logical Disk Free Space Monitor. Цей монітор відповідає за вільне місце на логічному диску робочого компьютера та вибиває попередження загрози при заповненому на 75% диску, та критичну помилку при заповненому на 90% диску. Налаштування цього монітора можна побачити на рисунку 3.21

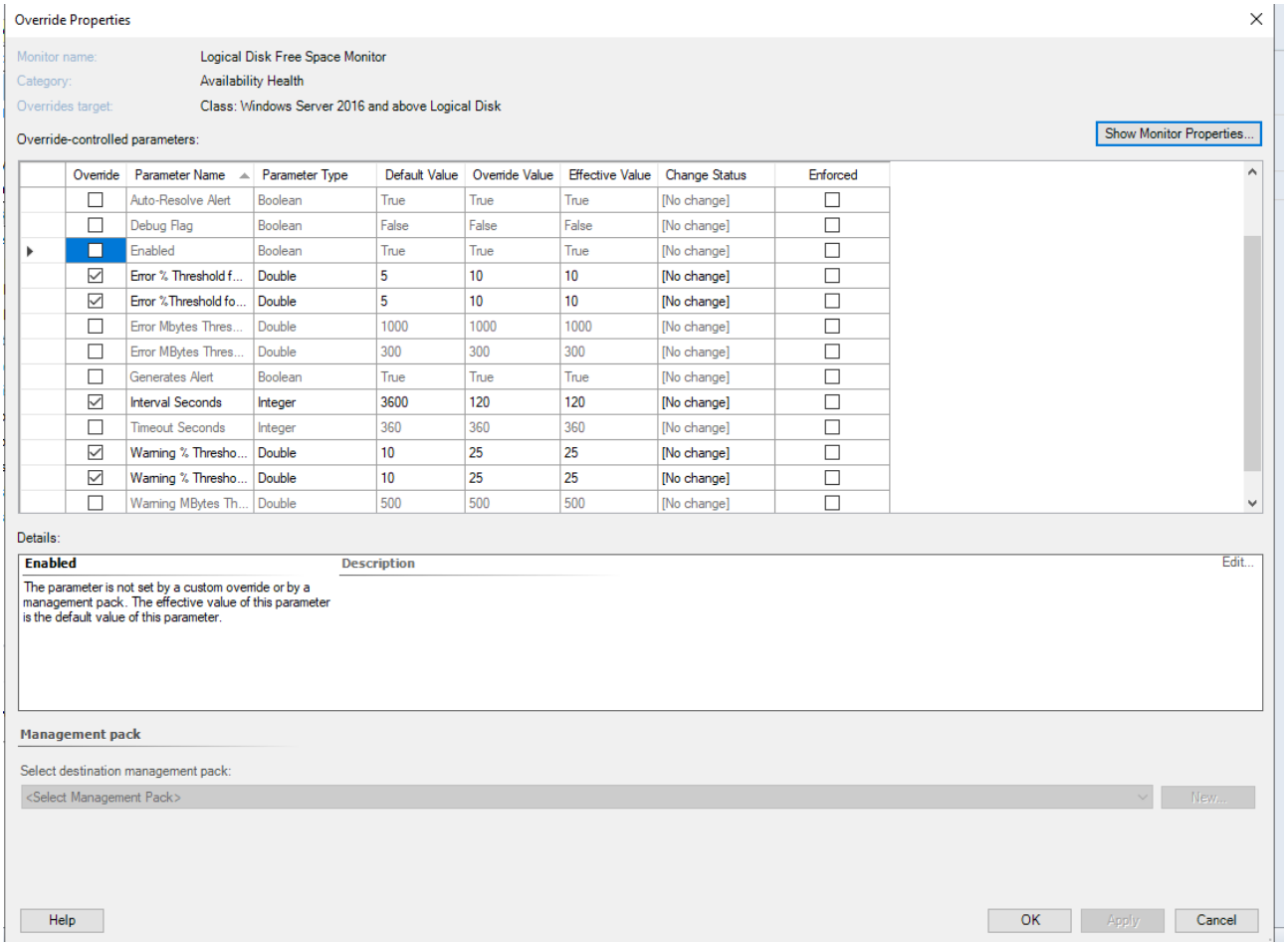


Рисунок 3.21 Налаштування монітору вільного простіру

Спробуємо забити простір на диску на одній з наших робочих машин:

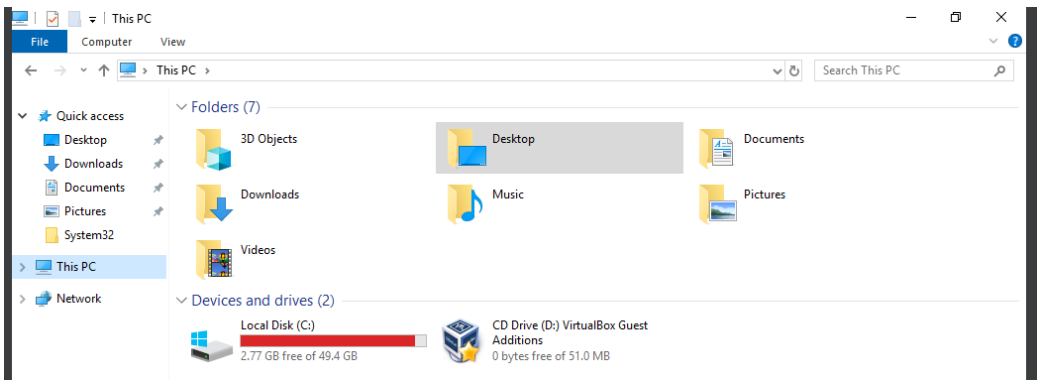


Рис 3.22 Заповнений простір на диску

Як видно на графіку нижче, кількість вільного простіру різко зменьшилася

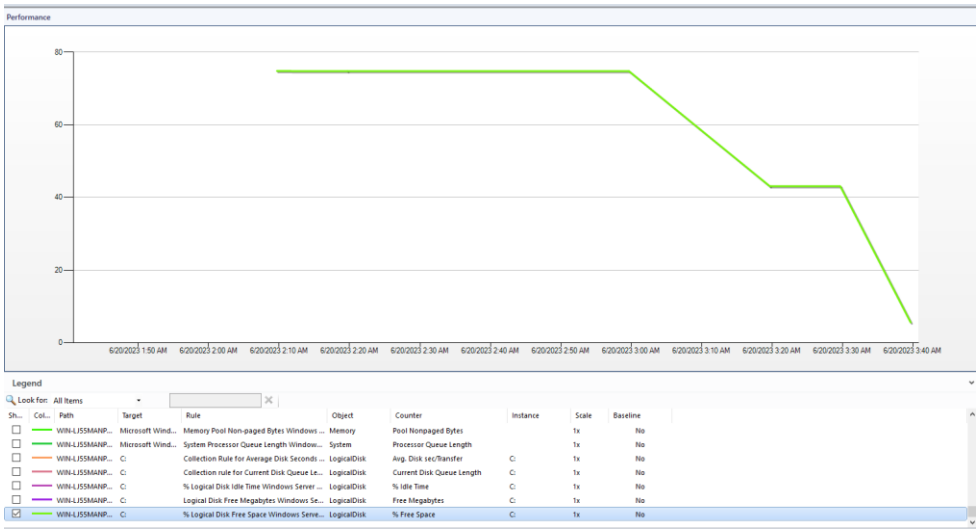


Рис 3.23 Графік зміни вільного простіру на диску

Через 120 секунд, як і зазначено в налаштуваннях, монітор переходить в Critical стан.

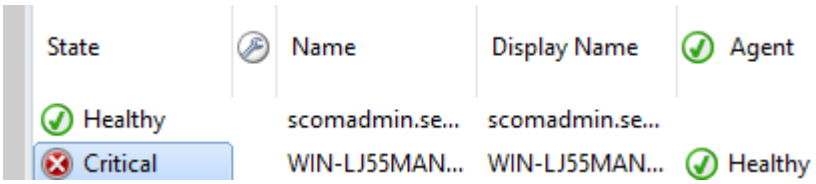


Рисунок 3.24 зміна стану

Якщо розкрити повну інформацію, то можна побачити, що Logical Disk Free Space монітор в критичному стані

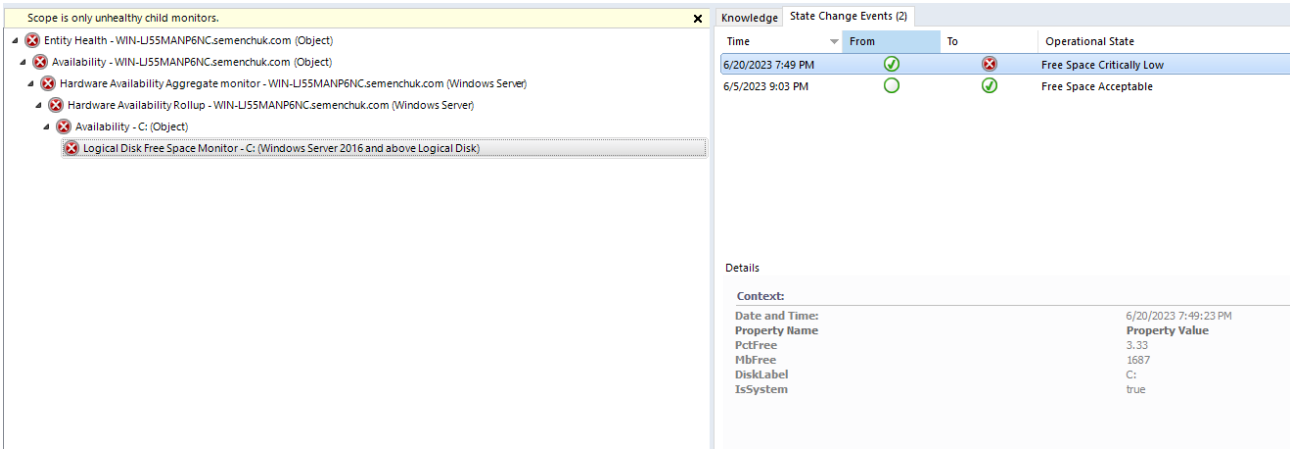
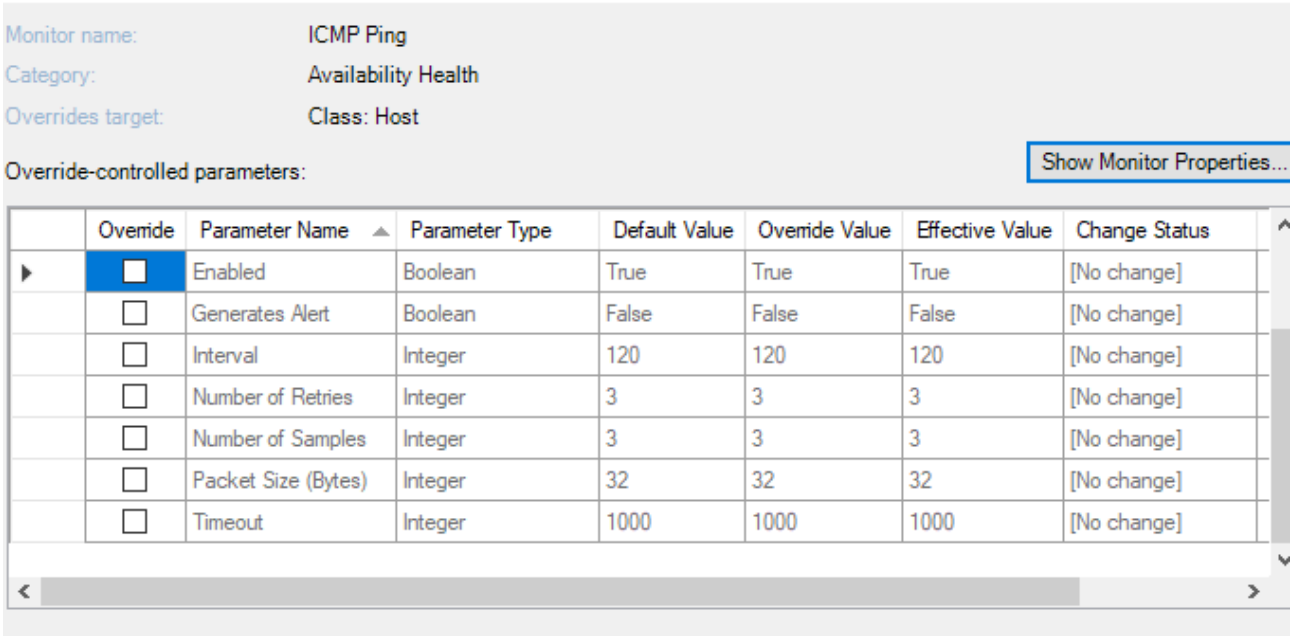


Рисунок 3.25 Розгорнута інформація про вільне місце на машині

Окрім перевірки моніторів операційних систем, перевіримо роботу моніторів для мережних девайсів. Для перевірки буде використано монітор ICMP Ping, налаштування якого зображено на рисунок 3.26



Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
☐	Enabled	Boolean	True	True	True	[No change]
☐	Generates Alert	Boolean	False	False	False	[No change]
☐	Interval	Integer	120	120	120	[No change]
☐	Number of Retries	Integer	3	3	3	[No change]
☐	Number of Samples	Integer	3	3	3	[No change]
☐	Packet Size (Bytes)	Integer	32	32	32	[No change]
☐	Timeout	Integer	1000	1000	1000	[No change]

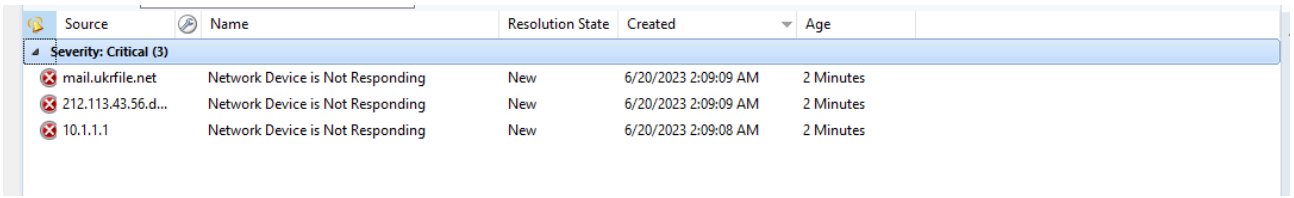
Рис 3.24 Налаштування ICMP Ping

Цей монітор робить 3 запити з інтервалом в 120 секунд. Якщо мережений пристір не дає відповідь на 3 запити, монітор повідомляє про критичну помилку. Спробуємо відключити один з мережних пристроїв



Рисунок 3.25 Відключений маршрутизатор

Через 6 хвилин мережний пристрій перейшов в стан Critical та повідомив про помилку



Source	Name	Resolution State	Created	Age
Severity: Critical (3)				
mail.ukrfile.net	Network Device is Not Responding	New	6/20/2023 2:09:09 AM	2 Minutes
212.113.43.56.d...	Network Device is Not Responding	New	6/20/2023 2:09:09 AM	2 Minutes
10.1.1.1	Network Device is Not Responding	New	6/20/2023 2:09:08 AM	2 Minutes

Рис 3.26 Попередження про відсутність зв’язку з пристроєм

Якщо перейти в Health Explorer відключеного пристрою, можна помітити, що він видає помилку про неотримання відповіді на ping

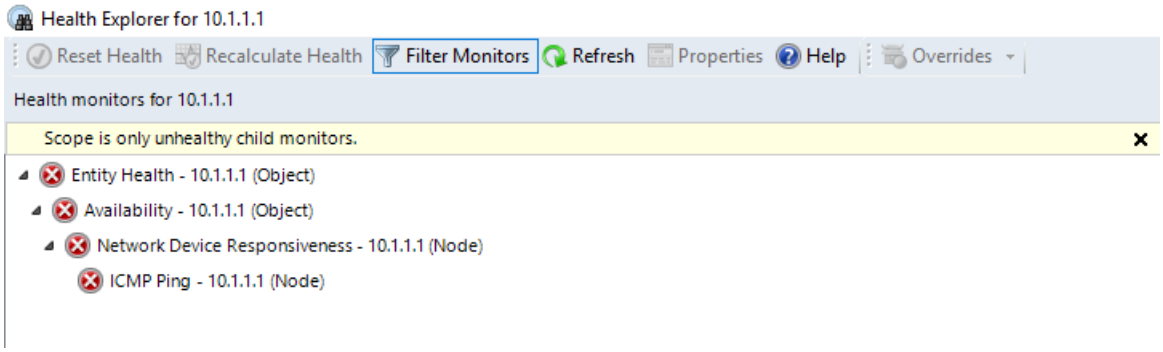


Рис 3.27 Health Explorer

Висновки до розділу 3

У цьому розділі було проведено установку та базове налаштування SCOM 2019. Підключено Windows, Unix/Linux та мережні машини до моніторингу. Протестовано моніторинг та надсилання сповіщень при помилка в роботі пристроїв

Висновки

У цій роботі було розглянуто систему моніторингу мережної інфраструктури та встановлення MS SCOM. Досліджено різні аспекти моніторингу, включаючи типи моніторингу, методи дослідження та інші релевантні питання

Розділ 1 надав загальний огляд теми дипломної роботи, починаючи з вступу, де була визначена актуальність розробки системи моніторингу мережної інфраструктури. Були розглянуті методи дослідження, що дозволяють провести обґрунтування вибору Microsoft SCOM як основи для реалізації системи моніторингу.

Розділ 2 надав загальний огляд про структуру SCOM. Було розглянуто способи моніторингу, зв’язку з робочими пристроями та розібрано архітектуру. Також було побудовано загальну схему мережі

Розділ 3 дозволив ознайомитися з системою моніторинга SCOM, встановити програму. В ньому було проведено налаштування SCOM, розібрано роботу з агентами на Windows та Linux машинах, підключено мережні пристрої за допомогою SNMP, та протестовано реакцію на помилки в роботі машин.

Загальним висновком дослідження є те, що Microsoft System Center Operations Manager є потужним інструментом для моніторингу мережної інфраструктури. Вона надає широкі можливості збору, аналізу та візуалізації даних, а також має інтеграцію з іншими продуктами Microsoft, що забезпечує повний огляд стану мережі та ефективне управління ним.

Список використаних джерел

1. William S. Snmp, Snmpv2, Snmpv3, and Rmon 1 and 2, 1999, 619 c.
2. Slawek L. Effective Monitoring and Alerting, 2012, 164 c.
3. Kevin G. Getting Started with Microsoft System Center Operations Manager, 2016, 560 c.
4. Ed W. Network Monitoring and Analysis: A Protocol Approach to Troubleshooting, 2000, 359 c
5. Brian D. Active Directory: Designing, Deploying, and Running Active Directory, 2013, 738 c.
6. Brian B. Prometheus: Up & Running: Infrastructure and Application Performance Monitoring, 2018, 368 c.
7. All about operations manager. URL: https://learn.microsoft.com/en-us/system-center/scom/welcome?view=sc-om-2019
8. What is SCOM? URL: https://www.techtarget.com/searchwindowsserver/definition/Microsoft-System-Center-Operations-Manager-Microsoft-SCOM
9. Microsoft Active directory. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
10. What is network monitoring? URL: https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring

Додатки

ДОДАТОК А

Схема віртуальної мережі

