ВІДЗИВ НАУКОВОГО КЕРІВНИКА НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ

Студента (ки) **Клименко О.П.**

(прізвище та ініціали)

представлену на здобуття освітнього ступеня «бакалавр»
зі спеціальності 123 «Комп'ютерна інженерія»

1. Робота виконана на тему Проект підсистеми журналювання подій комп'ютерної мережі на базі ОС Windows

2. Актуальність. Читання журналів подій є невід'ємною частиною роботи будь-якого адміністратора безпеки. Мережеве обладнання, операційні системи і практично всі бізнес-додатки здійснюють журнал подій безпеки, таких як: вдалий / невдалий вхід в систему, запуск / зупинка системи, звернення до закритого порту для міжмережевих екранів і інші події.

(зазначити, які питання теоретичного і практичного характеру визначають актуальність роботи)

3. Основний зміст роботи викладено на 85 сторінках тексту, містить 14 таблиць та 44 ілюстрації. Список використаних літературних джерел налічує 12 найменувань.

4. Зміст розділів роботи *(зазначити за кожним розділом, які питання досліджені та з якою метою)*

Розділ 1. Аналіз напрямків використання інформаційних технологій для реалізації журналювання подій. У розділі проаналізовано журнал подій Windows, приклади таких журналів, викликів журналів, проведено аналіз даних журналу, досліджено кореляцію журналу.

Розділ 2. Порівняльний аналіз існуючих систем моніторингу локальних мереж та вибір оптимального для проекту. У розділі наведено класифікацію засобів моніторингу та аналізу, проведено порівняльний аналіз наявних систем моніторингу локальних мереж. Здійснено вибір системи моніторингу.

Розділ 3. Порядок розробки та роботи підсистеми журналювання. Описано про взаємодію пристроїв з системою моніторингу і приклад налаштування в мережі.

5. Висновки обгрунтовані, повністю відповідають поставленим завданням, мають теоретичне та практичне значення. Практичне значення отриманих результатів полягає у розробці проекту підсистеми журналювання подій комп'ютерної мережі на базі ОС Windows.

(обгрунтованість, теоретичне і практичне значення)

6. Список використаних літературних джерел. Джерела опрацьовані у повному обсязі, відповідають змісту роботи.

(обсяг і повнота опрацювання за змістом роботи)

7. Додатки

(перелік додатків та повнота їх опрацювання за змістом роботи)

8. Таблиці та ілюстрації Ілюстрації носять інформаційний характер, є доповненням до змісту роботи.

(призначення таблиць та їх використання для підтвердження досліджень в роботі)

9. Якість оформлення роботи на достатньому рівні

10. Ставлення студента (ки) до виконання випускної кваліфікаційної роботи відповідально

11. Висновок

В цілому при написанні випускної кваліфікаційної роботи студент (ка) **Клименко О.П.**

(прізвище та ініціали)

вміння /невміння/ підібрати необхідну літературу, інформаційну базу, проаналізувати їх, зробити відповідні висновки і оформити свої дослідження у випускній кваліфікаційній роботі.

Випускна кваліфікаційна робота студента (ки) **Клименко О.П.**

(прізвище та ініціали)

написана на достатньо /недостатньо/ високому рівні та може /не може/ бути допущена до захисту в Екзаменаційній комісії.

Науковий керівник д. п.н., доцент, професор кафедри інженерії програмного забезпечення

(вчений ступінь, звання, посада)

(підпис) Вакалюк Т.А.

(прізвище та ініціали)

«20» 06 2020 р.

РЕЦЕНЗІЯ

на кваліфікаційну роботу
студента 4 курсу групи КІ-2 спеціальності 123 «Комп'ютерна інженерія»
факультету інформаційно-комп'ютерних технологій
Державного університету «Житомирська політехніка»
Клименко Олени Петрівни
на тему: „ Проект підсистеми журналювання подій комп'ютерної мережі на базі ОС Windows ”

Кваліфікаційна робота студента Клименко О.П. „ Проект підсистеми журналювання подій комп'ютерної мережі на базі ОС Windows ” присвячена актуальній тематиці – розробці та впровадженню у практику діяльності організації захищених комп'ютерних мереж.

Робота містить реалізований у середовищі моделювання проект мережі та пояснювальну записку наступного складу: вступ, три розділи основного тексту, висновки, список використаної літератури, два додатки.

У першому розділі пояснювальної записки описано два основні механізми реєстрації журналів, Syslog та Журнал подій Windows, і як вони працюють. Також дізнались інформацію про безпеку та систему управління подіями (SIEM). Та вияснили, як збирати, аналізувати та аналізувати журнали.

У другому розділі пояснювальної записки здійснено порівняльний аналіз існуючих систем моніторингу локальних мереж та вибір оптимального для проекту.

У третьому розділі пояснювальної записки здійснено вибір обладнання для розробленого проекту мережі, наведено опис процесу налагодження та тестування побудованої мережі. Також у цьому розділі здійснено перевірку функціоналу підсистеми журналювання подій в мережі.

Зміст роботи відповідає поставленому завданню. У цілому кваліфікаційна робота виконана на високому рівні. Тема роботи розкрита повністю. Студентом продемонстровані ґрунтовні теоретичні знання та практичні фахові навички, що отримані як під час навчання, так і у процесі виконання роботи. Матеріал пояснювальної записки викладено логічно, науково і технічно грамотно. Ілюстративний матеріал (рисунки, таблиці), що наведений у роботі, оформлений якісно і наведений у відповідних місцях. Оформлення роботи у цілому відповідає вимогам стандартів. Його функціонал відповідає заявленому.

Позитивною стороною є те, що отримані результати мають практичну цінність – розроблений проект планується до впровадження в діяльності підприємства. Недоліками роботи є наступні: наявність деяких відхилень від вимого щодо оформлення пояснювальної записки (відсутні посилання на літературні джерела у розділі 1, помилки в оформленні деяких таблиць). Зазначені недоліки у цілому не впливають на високу якість і актуальність роботи.

У цілому кваліфікаційна робота студентки Клименко О.П. „ Проект підсистеми журналювання подій комп'ютерної мережі на базі ОС Windows ” відповідає вимогам рівня вищої освіти «бакалавр» спеціальності 123 «Комп'ютерна інженерія» і рекомендується до захисту в ЕК.

За відповідного захисту студентка Клименко О.П. заслуговує на оцінку – «відмінно».

Рецензент,
ст. викл. Каф. БІ та Т
20 червня 2020 р.



Д.С. Морозов

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра інженерії програмного забезпечення

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

на тему: «Проект підсистеми журналювання подій комп'ютерної мережі на базі ОС Windows»

Виконала студентка 4-го курсу, групи КІ-2
спеціальності 123 «Комп'ютерана інженерія»
_____ Клименко О.П.

Керівник д.п.н., доц., професор кафедри ІПЗ
_____ Т.А. Вакалюк

Рецензент ст. вик. кафедри БІ та Т
_____ Морозов Д.С.

Житомир – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки
_____ Єфіменко А. А.
«06» квітня 2020 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу

Студентки **Клименко Олени Петрівни**
Тема роботи: **Проект підсистеми журналювання подій комп'ютерної мережі на базі ОС Windows**
затверджена Наказом по університету від **«06» квітня 2020 р. № 98с**
Термін здачі студентом закінченої роботи – **21 червня 2020 р.**
Вихідні дані для роботи:

1. Фізична топологія мережі
2. Брандмауер Fortigate 140D
3. Комутатори Fortiswitch 124D
4. Операційні системи Windows Server2012, Windows 10

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Вакалюк Т.А.	06.03.2020	06.03.2020
2	Вакалюк Т.А.	20.03.2020	20.03.2020
3	Вакалюк Т.А.	11.05.2020	11.05.2020

Керівник _____ Вакалюк Т.А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналізування вимог до програмного продукту	11 квітня 2020 – 1 травня 2020	виконано
2	Пошук, огляд та аналіз аналогічних розробок	2 травня 2020– 10 травня 2020	виконано
3	Вивчення матеріалу по даній тематиці	11 травня 2020– 20 травня 2020	виконано
4	Планування структури програми	21 травня 2020 – 25 травня 2020	виконано
5	Проектування та реалізація архітектури нейронної мережі	26 травня 2020 – 31 травня 2020	виконано
6	Написання програмного коду	1 червня 2020 – 5 червня 2020	виконано
7	Тестування роботи програми	6 червня 2020– 9 червня 2020	виконано
8	Аналіз одержаних результатів	10 червня 2020– 12 червня 2020	виконано
9	Оформлення пояснювальної записки	13 червня 2020– 20 червня 2020	виконано
10	Захист	21 червня 2020	

Студент _____
(підпис)

Керівник _____
(підпис)

					КІ.КР.Б – 123 – 09 – ПЗ		
		№ докум.	Підпис				
		Клименко О.П.		23.06.20	Проект підсистеми журналювання подій комп'ютерної мережі на базі ОС Windows Пояснювальна записка	Літ.	Арк. 4 / Аркушів 83
Керівник		Вакалюк Т.А.		23.06.20			
Н. контр.		Єфіменко А.А.		23.06.20		Житомирська політехніка, група КІ-2	
		Морозов Д.С.		24.06.20	Пояснювальна записка		
Зав. каф.		Єфіменко А.А.		23.06.20			

РЕФЕРАТ

Випускна робота бакалавра являє собою підсистеми журналювання подій комп’ютерної мережі на базі ОС Windows. Пояснювальна записка до випускної роботи місить 85 сторінок, 44 ілюстрації, 14 таблиць, 1 додатки та 12 літературних джерел.

Метою випускної роботи є обґрунтування вибору інструментальних засобів розробки програмної системи, вміти збирати та аналізувати журнали.

В роботі визначені головні завдання для розробки системи, проаналізовано методи вирішення поставленої задачі, обґрунтовано вибір програми для моніторингу мережі та наведено перелік бібліотек які на сьогоднішній день активно використовуються для вирішення задач. Представлено алгоритм роботи програмного комплексу, структуру та взаємодію його деяких компонентів. Також описана реалізація моніторингу мережі.

В рамках випускної роботи проводились експерименти з журналювання подій комп’ютерної мережі на базі ОС Windows в результаті яких були визначені оптимальні налаштування моніторингу мережі.

КЛЮЧОВІ СЛОВА: SYSLOG, WINDOWS, PRTG, SNMP, ЗАХИСТ, МЕРЕЖА, ПЕРИМЕТР МЕРЕЖІ

ABSTRACT

The bachelor's thesis is a subsystem for logging computer network events based on Windows. The explanatory note to the thesis contains 85 pages, 44 illustrations, 15 tables, 1 appendix and 12 references.

The purpose of the thesis is to justify the choice of tools for software development, to be able to collect and analyze journals.

The main tasks for system development are determined in the work, the methods of solving the set task are analyzed, the choice of the program for network monitoring is substantiated and the list of libraries which are actively used for solving tasks today is given. The algorithm of software development, structure and interaction of some of its components are presented. The implementation of network monitoring is also described.

In the final work, experiments on logging computer network events based on Windows were performed, as a result of which the optimal network monitoring settings were determined.

KEY WORDS: SYSLOG, WINDOWS, PRTG, SNMP, PROTECTION, NETWORK, NETWORK PERIMETER

ЗМІСТ

РЕФЕРАТ 4

ЗМІСТ 6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 8

ВСТУП 9

РОЗДІЛ 1. АНАЛІЗ НАПРЯМКІВ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ РЕАЛІЗАЦІЇ ЖУРНАЛЮВАННЯ ПОДІЙ 11

1.1. Журнал подій Windows 11

1.2. Syslog 15

1.3. Приклад журналу подій Windows 19

1.4. Виклик журналу Analytics 21

1.5. Аналіз даних журналу 30

1.6. Особливості SIEM 33

1.7. Дослідження кореляції журналу 34

ВИСНОВОК ДО РОЗДІЛУ 1 36

РОЗДІЛ 2. ПОРІВНЯЛЬНИЙ АНАЛІЗ ІСНУЮЧИХ СИСТЕМ МОНІТОРИНГУ ЛОКАЛЬНИХ МЕРЕЖ ТА ВИБІР ОПТИМАЛЬНОГО ДЛЯ ПРОЕКТУ 37

2.1. Класифікація засобів моніторингу та аналізу 37

2.2. Порівняльний аналіз існуючих систем моніторингу локальних мереж 39

2.3. PRTG 40

2.4. NetXMS 44

2.5. Nagois 45

2.6.Вибір системи моніторингу 46

ВИСНОВОК ДО РОЗДІЛУ 2 52

РОЗДІЛ 3. ПОРЯДОК РОЗРОБКИ ТА РОБОТИ ПІДСИСТЕМИ ЖУРНАЛЮВАННЯ 54

3.1. Простий протокол управління мережею 54
3.2. Вимоги Технічні умови 60
3.3. Мережа 62
3.4. Впровадження 64
3.4.1. Обладнання 64
3.4.2 Брандмауер Fortigate 140D 64
3.4.3. Fortigate кластер високої доступності 65
3.4.4. Fortigate мережеві інтерфейси 66
3.4.5. Посилення політики брандмауера 68
3.4.6. Увімкніть конфігурацію SNMP, NetFlow та Syslog 68
3.4.7. Fortiswitch 124D 71
3.4.8. Сервери Dell PowerEdge 72
3.4.9. Конфігурація сервера PRTG Core 72
3.4.10. Конфігурація пристроїв PRTG 74
3.4.11. Створення датчиків у PRTG 77
3.4.12. Визначення значень порогу та сигналізації датчиків 80
ВИСНОВОК ДО РОЗДІЛУ 3 81
ВИСНОВКИ 82
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 83
ДОДАТОК 85

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CLI Інтерфейс командного рядка

CPU Центральний процесор

DMZ Демілітаризована зона, підмережа, яка надає зовнішнім службам доступ в Інтернет

GPS Глобальна система позиціонування

GUI Графічний інтерфейс користувача

HA Відмовостійкий кластер, кластер високої доступності

HMI Інтерфейс людської машини

iDRAC Вбудований контролер(плата) віддаленого доступу Dell

IIS Інтернет-інформаційні послуги

ISL Протокол Cisco Inter-Switch Link

LACP Протокол контролю агрегації посилань

MIB Інформаційна база управління - база даних, що використовується для управління суб'єктами комунікаційної мережі

PRTG Монітор мережевої трафіку Paessler Router

ОЗП Оперативна пам'ять

SFP Промисловий стандарт модульних компактних приймачів даних

SNMP Простий протокол управління мережею

SOAP Простий протокол доступу до об'єктів

UDP Протокол датаграм користувача, один із протоколів в стеку TCP/IP.

UPS Джерело безперебійного живлення

USB Універсальна послідовна шина

VLAN Віртуальна локальна мережа

WBEM Веб-управління підприємством

WMI Інструментарій управління Windows

ВСТУП

Актуальність теми. Читання журналів подій є невід'ємною частиною роботи будь-якого адміністратора безпеки. Мережеве обладнання, операційні системи і практично всі бізнес-додатки здійснюють журнал подій безпеки, таких як: вдалий / невдалий вхід в систему, запуск / зупинка системи, звернення до закритого порту для міжмережевих екранів і інші події.

Однак при наявності в мережі навіть десяти серверів читання журналів подій на кожному з них стає досить трудомістким завданням, що вимагає витрати великої частини робочого часу. Для того щоб автоматизувати процес обробки журналів подій, наприклад, в частині пошуку спроб невдалого входу в систему, існує безліч різних рішень. Для Windows систем існує безліч безкоштовних додатків, які дозволяють здійснювати автоматичний пошук заданої події в журналі і реакцію на цю подію, наприклад, відправлення поштового повідомлення адміністратору. Для Windows є безліч комерційних продуктів, таких як: ArcSight, Symantec Information Manager або Tivoli Security Operations Manager, які вміють не тільки збирати події від різних джерел, але і перевіряти дані події на відповідність різним моделям загроз (наприклад, підбір пароля або DDoS атака), реагувати на події, будувати звіти і багато іншого. Але ці потужні засоби моніторингу коштують дуже недешево і в нинішніх непростих економічних умовах багатьом організаціям просто не по кишені. Symantec Information Manager або Tivoli Security Operations Manager, які вміють не тільки збирати події від різних джерел, але і перевіряти дані події на відповідність різним моделям загроз (наприклад, підбір пароля або DDoS атака), реагувати на події, будувати звіти і багато іншого. Як було зазначено вище, ці потужні засоби моніторингу мають чималу вартість. Однак якщо в мережі на серверах використовується операційна система Windows Server 2012, то можна самостійно організувати централізований моніторинг подій безпеки.

Важливе джерело цифрових доказів - файли журналів. Одним із запорук успіху в проведенні ефективного цифрового розслідування в комп'ютерній

системі є знання того, що відбувається в ній. Комп'ютерні системи та програми генерують журнали, коли щось відбувається або потребує уваги (наприклад, комп'ютерна система, налаштована для запису спроб входу користувача.). Ці журнали можуть надати ґрунтовні криміналістичні докази, які дозволять виявити недобросовісну діяльність користувача та дізнатись, як, коли та де трапився інцидент та допоможуть виявити кіберзлочинців. У цій роботі ви дізнаєтесь про основні механізми реєстрації журналів, Syslog та Журнал подій Windows, а також про те, як вони працюють.

Існує безліч програмних продуктів, що дозволяють осувати моніторинг мережі. У кожної програми є свої переваги і недоліки. Спочатку я проведу аналіз журналювання подій в комп’ютерній системі Windows. У другому розділі я проведу порівняльну характеристику деяких відомих систем моніторингу таких, як: PRTG, Zabbix, NetXMS і Nagios. У наступному розділі я розповім про те, як встановити та налаштувати систему моніторингу IT ресурсів мережі, а також підготувати пристрої до взаємодії з сервером моніторингу. У третьому розділі піде мова про взаємодію пристроїв з системою моніторингу і приклад налаштування в мережі.

Метою дипломної роботи розробити, впровадити та протестувати працюючу мережу розв’язування рішення для Windows. Відповідно до мети було поставлені такі завдання:

1) Вивчення журналів і фільтрів на моніторинг подій.
2) Знайти популярні механізми реєстрації журналів, Syslog та Журнал подій Windows, і зрозуміти, як вони працюють.
3) Обґрунтування вибору інструментальних засобів розробки моніторингу системи, вміти збирати, аналізувати журнали.

Об’єктом дослідження є журналювання подій комп’ютерної мережі на базі ОС Windows.

Предметом дослідження є проект підсистеми журналювання подій комп’ютерної мережі на базі ОС Windows.

РОЗДІЛ 1. АНАЛІЗ НАПРЯМКІВ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ РЕАЛІЗАЦІЇ ЖУРНАЛЮВАННЯ ПОДІЙ

1.1. Журнал подій Windows

Комп'ютерні системи та програми генерують велику кількість журналів для вимірювання та запису інформації протягом тривалості періоду моніторингу. Дані системного журналу є одними з найцінніших, що містять категоричний запис про трансакції користувачів, діяльність клієнтів, зчитування датчиків, поведінку машини, загрози безпеці, шахрайська діяльність тощо. Коли трапляються порушення безпеки, журнали можуть бути найкращою захисною лінією. Системні журнали також є однією з найбільш швидко зростаючих, найскладніших областей великих даних, особливо при швидкому розвитку розподілених обчислень. Саме створення та аналіз даних журналів дозволить ефективно покращити безпеку системи, посилити обороноздатність системи та атакувати криміналістику.

Журнал подій Windows syslog - це основний механізми реєстрації журналів. Зазвичай вони розгортаються одночасно у складному мережевому фізичному середовищі для управління журналом, і обидва вони можуть бути налаштовані на замовлення кінцевими користувачами. Існують інструменти для інтеграції журналу подій Windows, щоб зробити управління журналом більш ефективним у сьогоднішньому середовищі підприємства. Наприклад, SolarWinds форвард журналу подій для Windows може автоматично пересилати журнали подій Windows у вигляді повідомлень syslog до колектора syslog. Однак деякі загальні проблеми в галузі аналітики зумовлені традиційним управлінням даними журналів і обмежені сучасними технологіями. Поряд з деякими з цих викликів, які включають генерування, збирання, транспортування, зберігання, аналіз та прогнозування з точки зору безпеки, будуть представлені в цьому розділі.

Microsoft поступово збільшувала ефективність та ефективність своїх аудиторських засобів протягом багатьох років. Сучасні системи Windows можуть записувати велику кількість інформації з мінімальним впливом на систему. При відповідному зниженні ціни на носії інформації виправдання. Налаштування адекватного журналу в системах Windows та ідеальна агрегація цих журналів у SIEM або інший агрегатор журналів - це важливий крок до забезпечення того, що ваше середовище може підтримувати ефективну реакцію на інцидент. Ця робота надає огляд деяких найважливіших журналів Windows та подій, які там записані.

Одне з найбільш часто використовуваних і найбільш важливих засобів контролю за системою - це реєстрація різних подій в журналах операційної системи Windows. Реєстрацію подій в системі Windows здійснює служба "Журнал подій" (Event Log). У будь-якій системі сімейства Windows завжди присутні три журнали:

- журнал "Система" (System) - події, записані в журнал компонентами операційної системи (наприклад, збій в запуску служби при перезавантаженні); розташування журналу за замовчуванням - в папці "% SystemRoot% \ system32 \ config \ SysEvent.Evt ";
- журнал "Безпека" (Security) - реєстрація подій, що відносяться до системи безпеки (наприклад, спроби реєстрації користувачів, зміни в політиках безпеки, спроби доступу до різних ресурсів); набір подій, що реєструються в журналі «Безпека»; розташування за замовчуванням - "% SystemRoot% \ system 32 \ config \ SecEvent.Evt ";
- журнал "Додаток" (Application) - події, спричинені різними додатками (наприклад, збій MS SQL при доступі до бази даних); набір подій, що реєструються в журналі "Додатки", визначається розробниками додатків; розташування за замовчуванням - "% SystemRoot% \ system32 \ config \ AppEvent.Evt ".

При установці в системі будь-яких компонентів можуть з'явитися журнали, які реєструють події, що стосуються роботи даних компонентів.

При установці служби DNS з'являється журнал "DNS-сервер" (DNS Server), реєструючий події, пов'язані з роботою служби DNS (розташування за замовчуванням - " % SystemRoot% \ system32 \ config \ DNSEvent.Evt ").

При створенні контролера домена в системі з'являються журнали:

- журнал "Служба каталогів" (Directory Service) - події, пов’язані зі службою каталогів Active Directory ; розташування за замовчуванням - "% SystemRoot% \ system32 \ config \ NTDS.Evt ";
- журнал "Служба реплікації файлів" (File Replication Service) - події, пов'язані з реплікацією файлів (в першу чергу файли в папці SYSLOG і файли в мережевих папках, керованих рапределеніе файлової системою DFS); розташування за замовчуванням - "% SystemRoot% \ system32 \ config \ NtFrs.Evt".

Як і багато інших функцій Windows журнали подій були істотно перероблені і доповнені новими можливостями. За визначенням Майкрософт, подія - це будь-яка значна проява в операційній системі або додатку, що вимагає відстеження інформації. Подія - це не завжди негативно, оскільки успішний вхід в мережу, успішна передача повідомлень або реплікація даних також можуть генерувати події в Windows. У кожному журналі з його подіями пов'язані загальні властивості.

Level (рівень) - Це властивість визначає важливість події.

Date and Time (дата і час) - Це властивість містить інформацію про дату і час виникнення події.

Source (джерело) - Це властивість вказує джерело події: додаток, віддалений доступ, служба і так далі.

Event ID (Код події) - Кожній події призначений ідентифікатор події ID, число, згенероване джерелом і унікальне для всіх типів подій.

Task Category (Категорія завдання) - Це властивість визначає категорію події. Наприклад, Security або System.

Отже, ми розібралися з тим, що вдає із себе подія в журналі Windows Event Log. Тепер нам необхідно спочатку налаштувати аудит подій інформаційної безпеки.

Для налаштування аудиту необхідно зайти на контролер домену і відкрити редактор групових політик Start-> Administrative Tools-> Group Policy Management. Далі вибираємо домен і, натиснувши праву кнопку миші, вказуємо Create a GPO in this domain ... Взагалі, для включення аудиту можна скористатися політиками домену за замовчуванням, але краще створити окрему політику з відповідною назвою, так як це спрощує адміністрування. Далі в новій політиці йдемо в Computer Configuration-> Windows Settings -> Security Settings -> Local Policies -> Audit Policy. Відкриється список можливих параметрів налаштування аудиту. Включати всі підряд параметри немає особливого сенсу, так як в такому випадку журнал подій наповниться величезною кількістю малоінформативних повідомлень. Рекомендується наступний набір параметрів:

Таблиця 1.1.

Таблиця параметрів настройки аудиту

Категорія аудиту	Тип аудиту	Примітка
Audit account logon events	No auditing	
Audit account management	success / failure	
Audit directory service access	No auditing	
Audit logon events	success / failure	
Audit object access	No auditing	включити, тільки якщо необхідно відстежувати доступ до певних об'єктів (наприклад, каталогам на диску).
Audit policy change	success / failure	
Audit privilege use	success / failure	
Audit process tracking	No auditing	
Audit system events	success / failure	

Тепер ми налаштували аудит в домені. Відкривши журнал подій Security, можна переконатися в тому, яка кількість подій сиплеться в нього щомиті. Для того щоб не навантажувати контролери домену та інші сервера завданнями з обробки подій, ми повинні спочатку переслати події безпеки на виділений сервер, на якому і буде здійснюватися автоматична обробка всіх отриманих подій. Цей виділений сервер також повинен працювати під управлінням операційної системи Windows Server 2012 і входити в домен Active Directory. Для пересилання подій нам необхідно скористатися Subscriptions, підписками на події.

1.2. Syslog

Syslog - це стандарт для надсилання та отримання повідомлень у певному форматі – з різних мережевих пристроїв. Повідомлення включають часові позначки, повідомлення про події, суворість, IP-адреси хоста, діагностику та інше. Щодо вбудованого рівня тяжкості, він може передавати діапазон між рівнем 0, надзвичайною ситуацією, рівнем 5, попередженням, нестабільною системою, критичним та рівнем 6 та 7, які є інформаційними та налагодженими.

Більше того, Syslog є відкритим. Syslog був розроблений для моніторингу мережевих пристроїв та систем для надсилання повідомлень про повідомлення, якщо є якісь проблеми з функціонуванням. Він також надсилає сповіщення про попередньо повідомлені події та відстежує підозрілу активність через журнал змін / журнал подій мережевих пристроїв-учасників.

Протокол Syslog спочатку був написаний Еріком Аллманом і визначений в RFC 3164 . Повідомлення надсилаються через IP-мережі на колектори повідомлень про події або на сервери syslog. Syslog використовує для спілкування протокол User Datagram (UDP), порт 514 . Хоча сервери syslog не повертають підтвердження про отримання повідомлень. Починаючи з 2009 року, syslog був стандартизований IETF в RFC 5424 .

Syslog (системний журнал) є стандартом для ведення журналів повідомлень і широко використовується в Unix та Linux, а також багатьох

продуктах безпеки, таких як: брандмауер, система виявлення вторгнень (IDS). Повідомлення журналу системного журналу класифікуються за двома категоріями: Механізм та суворість. "Суворість" використовується для позначення пріоритету, який показаний у наступній таблиці (табл.1.2).

Таблиця 1.2.

Таблиця серйозності повідомлень системного журналу

Числовий код	Суворість
0	Надзвичайна ситуація: система непридатна
1	Попередження: потрібно вжити заходів негайно
2	Критичні: критичні умови
3	Помилка: умови помилки
4	Попередження: умови попередження
5	Помітка: нормальна, але значна умова
6	Інформаційні: інформаційні повідомлення
7	Налагодження: повідомлення на рівні налагодження

Таблиця 1.3.

Засоби повідомлення Syslog

Числовий код	Об'єкт	Опис
0	kern	ядро
1	user	"Користувацькі" процеси (немає конкретних)
2	mail	sendmail
3	daemon	"Системні" демон, такі як "маршрутизовані"
4	Auth	безпека та пов'язані з авторизацією
5	syslog	Syslog внутрішніх повідомлень
6	LPR	Демон-лінійний принтер BSD
7	news	система новин Usenet
8	UUCP	для (старовинної) послуги UUCP (копія unix-unix)
9	Cron	кронський демон
10	authpriv	схожий на "auth", увійшов до захищеного файла
11	ftp	Демон FTP
16–23	local0–local7	використовується для місцевих / інших демонів

«Об'єкт» описує частину системи або програми, яка генерувала повідомлення журналу, що показано в наступній таблиці (табл 1.3).

Коли користувач намагається увійти в машину, наприклад, за допомогою ssh (захищеної оболонки), користувач перевіряє аутентифікацію, ввівши своє ім’я / пароль. Потім подія аутентифікації буде реєструватися незалежно від того, успішна чи невдала спроба входу. Далі наведено кілька прикладів системних повідомлень про успіхи / збої входу в систему:

May 16 17:10:30 localhost sshd[5124]: Accepted password for root from 192.168.220.1 port 1643 ssh2

May 16 17:10:31 localhost sshd[5127]: pam_unix(sshd:session): session opened for user root by root(uid=0)

May 16 17:10:51 localhost sshd[5154]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid 0 tty ssh ruser rhost=192.168.220.1user=root

May 16 17:10:53 localhost sshd[5154]: Failed password for root from 192.168.220.1 port 1645 ssh2

May 16 17:10:59 localhost sshd[5154]: Failed password for root from 192.168.220.1 port 1645 ssh2

Очевидно, якщо ми можемо продовжувати моніторинг цих повідомлень журналу, ймовірно ми можемо виявити багато атак / зловживань. Наприклад, якщо за короткий період ми виявимо багато невдалих спроб входу проти облікового запису користувача, то дуже схоже, що система піддається атаці відгадки пароля.

Хоча синтаксис і семантика даних в повідомленнях журналу зазвичай залежать від постачальника, усі вони повинні слідувати протоколу syslog (RFC 5424). Протокол використовує шарувату архітектуру, яка дозволяє використовувати будь-яку кількість транспортних протоколів для передачі системних повідомлень. Без цього протоколу один одному стандарту необхідно визначити власний формат пакетів системного журналу та механізм транспортування, що може спричинити тонкі проблеми сумісності. Протокол Syslog визначає три шари

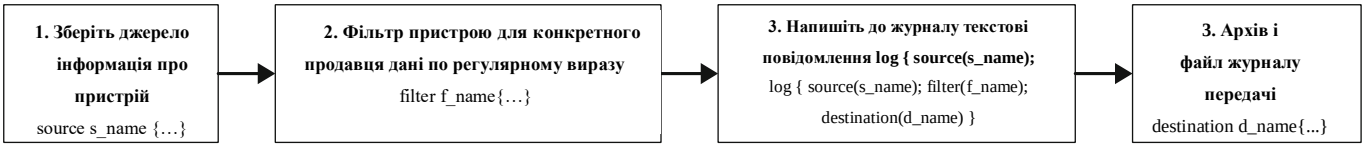


Рис. 1.1. Механізм обробки системного протоку

- вміст syslog - інформація про управління, що міститься в повідомленні syslog
- додаток syslog - обробляє генерацію, інтерпретацію, маршрутизацію та зберігання повідомлень syslog
- syslog transport - розміщує повідомлення на дроті та знімає їх з проводу

Потік обробки системного журналу в цілому може бути виявлений декількома стадіями. По-перше, потрібно збирати інформацію про вихідні об'єкти. Після того як необроблені дані фільтруються за специфічним механізмом, який зазвичай є регулярним вираженням, інформацію про події слід записувати в масаж тексту журналу. Тим часом, якщо файли журналів будуть архівовані або перенесені, подальші дії слід також реєструвати з інформацією про призначення (рис. 1).

Коли вперше був введений syslog, він підтримував лише UDP для доставки повідомлень журналу. Це означає, що немає гарантії, що повідомлення журналу будуть успішно доставлені до його попередньо визначеного пункту призначення. Пізніше вдосконалені версії протоколу syslog стали сьогодні багатообіцяючими механізмами реєстрації для широкого кола обчислювальних пристроїв, що мають більше функціональних можливостей, ніж їх предки. Наприклад, Syslog-ng (Syslog Next Generation) розширює базовий протокол syslog з новими функціями, включаючи фільтрацію на основі вмісту, вхід безпосередньо в базу даних, надійний транспорт за допомогою TCP та безпечну передачу за допомогою TLS (Security Layer Security) . Ще одна вдосконалена версія, яку варто згадати, - rsyslog, а найбільш помітне вдосконалення rsyslog - це її

високопродуктивні та чудові функції безпеки. На сьогоднішній день у багатьох дистрибутивах Linux доступний попередньо створений пакет або Syslog-ng, або rsyslog. Наприклад, у Kali Linux встановлено пакет rsyslog. Згодом я буду використовувати rsyslog для аналізу журналів.

Приклади сценаріїв розгортання колекції журналів з використанням syslog працюють таким чином: повідомлення журналу створюються «відправником» і пересилаються «збирачеві». Збирач syslog - це, як правило, централізований сервер реєстрації або сервіс для централізованого ведення журналів та управління подіями.

Централізоване ведення журналу має багато переваг. По-перше, це дозволяє перевіряти журнали різних систем в одній системі, і в результаті може простіше з'ясувати першопричину інцидентів. Найголовніше, що вона все-таки забезпечує слід, коли підхідник порушений. Це тому, що дуже часто трапляється, що хакер завжди очищає файли журналів після того, як щось зробив на компрометованій комп'ютерній системі.

1.3. Приклад журналу подій Windows

На відміну від UNIX syslog Windows системні журнали структуровані. Реєстрацію в системі Windows можна переглянути через "Переглядач подій". Журнали подій відрізняються для різних варіантів, але Windows 10 зробив важливі покращення безпеки. У дереві консолі відкрийте Журнали Windows та натисніть Захист.

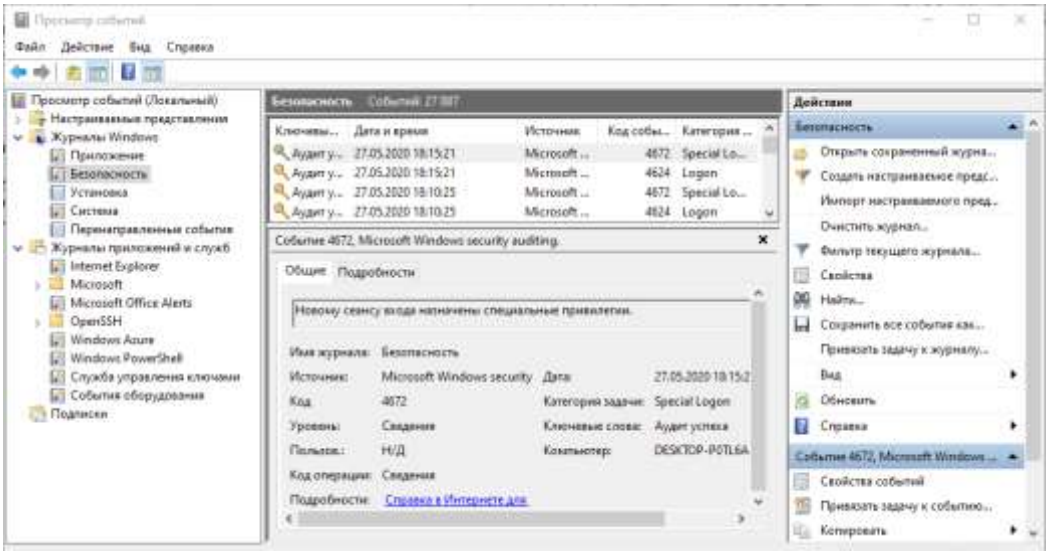


Рис. 1.2. Журнали безпеки в системі Windows

Поточна інфраструктура ведення журналів Windows для настільних та серверних операційних систем складається з рамки TraceLogging та журналів подій. Новий випущений фреймворк TraceLogging ґрунтується на відстеженні подій для Windows (ETW) та забезпечує спрощений спосіб коду інструменту. Однак журнал безпеки, призначений для використання системою, генерується в рамках журналу подій.

Система надає доступ на основі прав доступу, наданих обліковому запису, під яким працює нитка. Користувачі можуть читати та очищати журнал безпеки, якщо їм було надано привілей SE_SECURITY_NAME, і лише Місцевий орган безпеки (Lsass.exe) має дозвіл на запис журналу безпеки, і жоден інший обліковий запис не може вимагати цього привілею. Журнал для категорії подій аутентифікації повинен включати функцію AuthzReportSecurityEvent для створення журналів. А параметри аудиту також можуть бути визначені у функції AUDIT_PARAM_TYPE (Рис. 1.3).

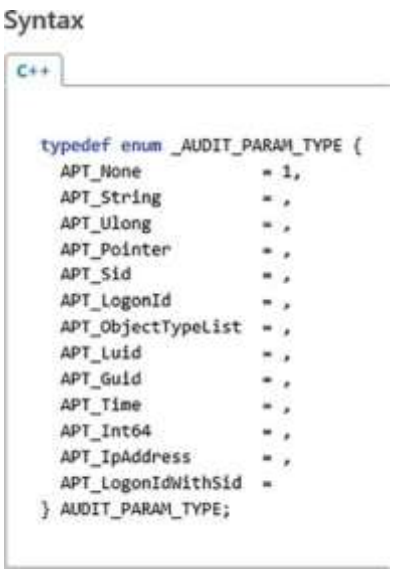


Рис. 1.3. Тип параметрів аудиту Windows для подій аутентифікації

Однак Windows не може обмежувати привілей адміністратора як SELinux, єдиний спосіб запобігти перезапису системи Windows на свої файли журналів - це налаштувати її на припинення реєстрації, коли у неї не вистачає місця на диску, або повністю вимкнути апарат. Так само очевидна і читабельна слабкість журналу додатків Windows. У конфігурації журналу подій Windows програмісти записують "Словник повідомлень", який відображає кодовані номери помилок, які випускає Microsoft. У такому випадку, код "80010105" з файлу журналу на відповідні повідомлення в DLL, користувачеві може знадобитися служба підтримки, щоб знати, що таке "80010105".

1.4. Виклик журналу Analytics

Сьогодні корпоративні середовища стали більш складними з багатьма комп'ютерними системами та мережами різного типу. Крім того, вони забезпечують себе різноманітними сторонніми технологіями захисту від ряду постачальників, які розповсюджуються в різних місцях мережі підприємства. Складні середовища створюють проблеми для аналізу журналів.

По-перше, комп'ютерні пристрої в умовах підприємства надають переважну кількість інформації. Це стає нездійсненним для огляду людини. Крім того, повідомлення журналу надходять у різних форматах, а також можна визначити формат журналів з деяких пристроїв. І що ще гірше, деякі пристрої

використовують спеціалізовані коди або підписи для ідентифікації того, який тип типу сповіщення або помилки генерується. Наприклад, у Windows NT "Переглядач подій" має такі коди, як 529, що представляє помилку входу через невідоме ім'я користувача або неправильний пароль.

По-друге, журнали сильно різняться від системи до системи і навіть від версії до версії для тієї ж системи. Перетинання кореляції джерел даних для дослідження першопричини, виявлення поведінкових зв’язків та виключення дублюючої інформації між різними подіями є одним із найсильніших вузьких місць аналізу даних журналів. Власне кажучи, докази щодо видобутку криміналістики безпеки можуть записуватися в декілька файлів журналів і навіть перетинати декілька пристроїв. Виявлення відносин між декількома джерелами може збільшувати складність при роботі з більш ніж двома джерелами. Більшість сучасних технологій просто пересилають усі дані журналу в одне централізоване місце і через складну мову пошукових запитів для досягнення попередньої кореляції, що призводить до високої вартості, але з невеликим успіхом.

По-третє, сучасні підприємства прийняли різноманітні продукти безпеки. Різні продукти фокусуються на наданні технологій точкового рішення для відомих проблем безпеки. Наприклад, для контролю доступу до внутрішніх мереж компанії існують Брандмауери та VPN, такі як FireWall-1 Checkpoint; щоб зберегти комп'ютерні ресурси та / або мережі фізично недоступними для сторонніх людей, існує фізична безпека або біометрична безпека, наприклад, сканери відбитків пальців та розпізнавання відбитків пальців; для виявлення можливих вторгнень існують системи виявлення вторгнень (IDS), такі як Cisco Firepower NGIPS; для аналізу пакетів даних, що передаються в мережу і виходять з неї, такі як Sniffer Sniffer Technologies; щоб зменшити ризики вірусних атак, існує антивірусне програмне забезпечення; щоб забезпечити цілісність системних файлів та даних у вашій мережі та отримувати своєчасне виявлення та повідомлення про зміни в системі, існує Tripwire; для захисту ваших конфіденційних даних, що надсилаються через загальнодоступну мережу, наприклад, Інтернет, існують криптографічні технології та протоколи безпеки,

такі як IPSec, SSL / TLS тощо; хоча існують сканери безпеки, які дозволяють сканувати та картографувати мережі та пов'язані з ними вразливості, а також аналізу рівнів безпеки, які потенційні слабкі місця перевіряються, ідентифікуються та аналізуються. Крім того, операційні системи (ОС) можуть бути налаштовані для реєстрації та / або передачі подій, залежних від безпеки. Кожен тип продуктів безпеки захищає від класу ризику або більше. Однак не всі інциденти із безпекою можуть бути виявлені правильно та ефективно одним продуктом безпеки без допомоги іншої інформації. Наприклад, співробітник запускає DoS-атаку на один з серверів своєї корпорації всередині організації, ми хочемо відразу дізнатися, хто атакує сервер і чи є це успішної атакою. Це нам неможливо знати, якщо ми залежатимемо лише від системи IDS.

Крім різних форматів журналів, аналіз продуктивності є ще одним головним обмеженням для аналізу даних журналу. У традиційних рішеннях для ведення журналів індекс можна використовувати для прискорення пошуку журналів, хоча він не може ефективно забезпечити запит у великих масштабах даних журналу, особливо для усунення несправностей у реальному часі та судових експертиз.

З точки зору вищезазначених тверджень ми можемо чітко бачити, що система аналізу журналів потребує співвіднесення інформації з різних джерел таким чином, щоб визначити першопричину інциденту та пояснити цифровий артефакт. Ось чому вступає в дію система захисту інформації та управління подіями (SIEM).

2. Інформація про безпеку та система управління подіями (SIEM)

Інформація про безпеку та система управління подіями (SIEM) також відома як управління безпекою підприємства (ESM) або управління подіями безпеки (SEM) та управління інформацією про безпеку (SIM). SIEM управляє інформацією, зібраною з комп’ютерів, мережевих пристроїв та продуктів безпеки на підприємстві, і ця інформація додатково корелює для пошуку зв'язку між ними та виявлення першопричини інциденту. Крім того, це дозволяє визначити пріоритетність інцидентів та визначити, які є критичними для

процесів, а також позиції безпеки організації. Таким чином, SIEM ефективно керує інформацією з комп'ютерних пристроїв на підприємстві, що підвищує безпеку підприємства.

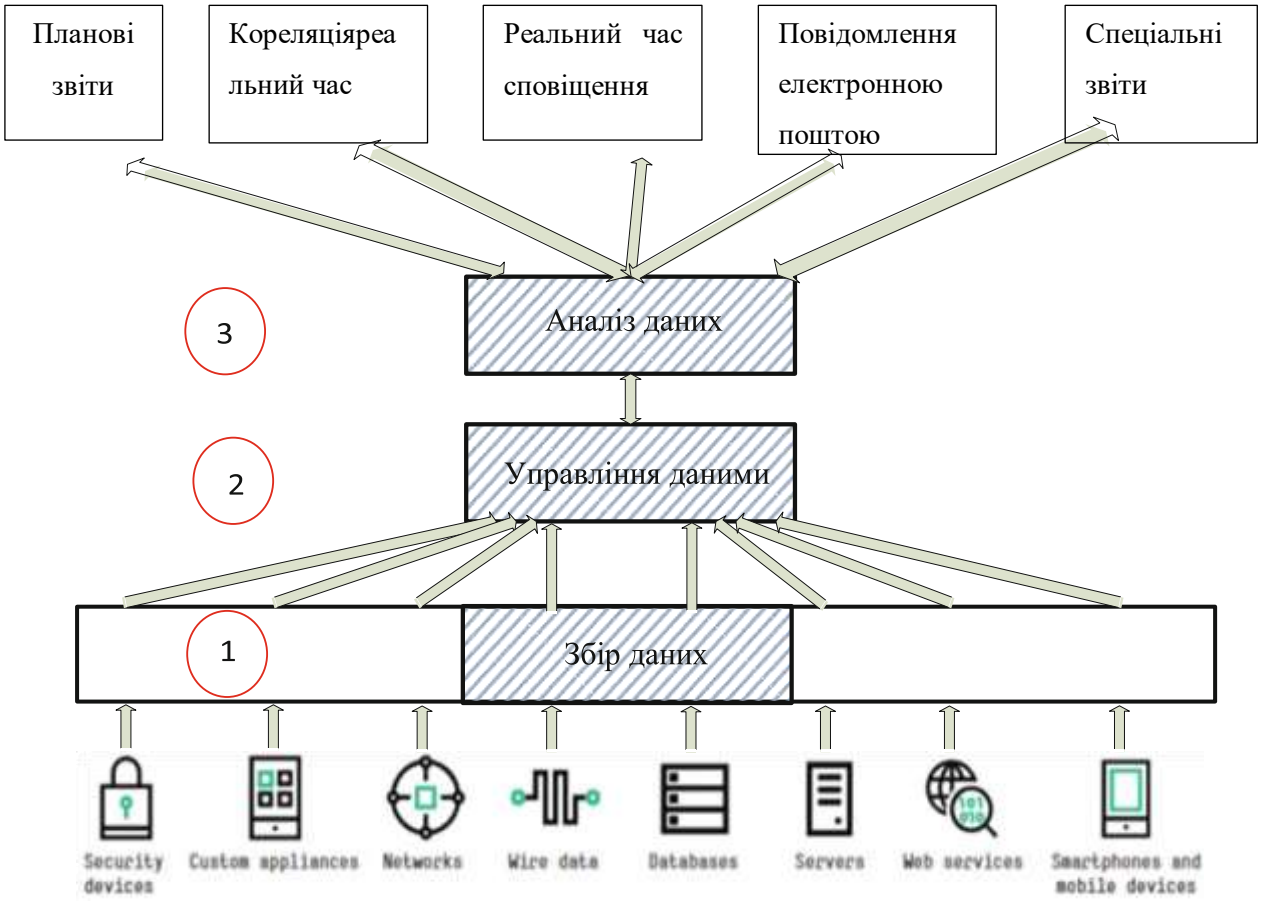


Рис. 1.3.SIEM архітектура

Система інформації про безпеку та управління подіями (SIEM) передбачає можливість збирати, обробляти та співвідносити повідомлення журналу з усіх комп'ютерних пристроїв, що контролюються. Різноманітність різних форматів журналів та типів повідомлень зобов'язує SIEM співвідносити всі активізації та події в системах та навіть у мережах. Як правило, типову архітектуру SIEM можна розділити щонайменше на три процедури. Як показано на рис.1.4, від збору та стандартизації даних журналу, до управління та аналізу даних журналу.

Існує щонайменше вісім таких функцій, які повинен мати SIEM:

1. Збір: централізований збір даних та звітування для комп'ютерних систем та мережевих продуктів безпеки на всьому підприємстві, гарантуючи,

що системи відповідають політиці безпеки та моніторингу подій з Firewall, IDS, веб-серверів, Windows та Linux серверів.

2. Класифікування: Однією з проблем журналів подій та сповіщень, що генеруються комп'ютерними пристроями, є те, що вони використовують спеціалізовані коди, щоб визначити, який тип типу помилок чи попередження створюється. Наприклад, у Windows "Переглядач подій" має такі коди, як 6005, 6009, 20 і т. д. Але це не показує вам, що 6005 означає "Початок служби подій", або що 20 означає "Файл було надруковано ». Самі продукти роблять погану роботу, показуючи, що відбувається. Оскільки ніхто не може бути експертом у всьому, системним адміністраторам дуже важко зрозуміти, про що повідомляють велика кількість пристроїв на підприємстві. SIEM має забезпечити новий тип класифікаційної схеми, яка не базується на числовому коді. Він повинен базуватися на простих, зрозумілих для людини та легко зрозумілих "типах", таких як: "ids.detect.dos", "auth.login.success" або "auth.login.failed", "auth.logoff".

3. Нормалізувати : Це перевести різні формати необроблених даних журналу в стандартизований. У такому випадку програми парсера журналів включаються до самого SIEM, і кожна з них відповідає за аналіз необроблених даних журналу з одного конкретного комп'ютерного пристрою у стандартизованому форматі. Вихідні файли журналу Parser можуть мати різні типи форматів. Нині XML, SQL і JSON - найбільш популярні формати для аналізу даних журналу. Вибір формату, який відповідає організації, залежить від потреб. XML - це дуже потужний формат, який дозволяє отримати величезну кількість гнучкості як у виведенні конкретних даних, так і у форматі. Log Parser може визначити використання декількох структур XML та схеми XML. Формат SQL дозволяє користувачам перетворювати дані журнальних файлів у таблицю SQL та зберігати їх у реляційній базі даних. JSON походить від JavaScript, і він розглядався як найкращий формат заявок за останні роки. JSON дозволяє аналізувати журнали як великі дані. Це не просто читабельний текст, а база даних, яку можна запитати.

4. Реакція: Більшість продуктів моніторингу можуть "спрацьовувати" на наборі параметрів або порогів, щоб сповістити менеджерів системи про те, щоб звернути увагу. Типові сповіщення / реакції, поширені для програмного забезпечення, включають повідомлення електронною поштою, пейджингові повідомлення, виконання команд або генерування «усунення несправностей з квитками» в службі програмного забезпечення, що допомагає, як Remedy.

5. Кореляція подій: Кореляція подій може допомогти нам зменшити сповіщення та виявити точки вразливості безпеки в мережах, системах та (рідше) додатках. Кореляція подій може допомогти нам виявити шаблон у потоці низького рівня, наприклад Syslog, SMTP, SNMP тощо, та генерувати «похідні» події вищого рівня з метою зменшення обсягу трафіку до систем SIEM. Дослідження показує, що від 60% до 90% часу IT-менеджери витрачають на вирішення проблем, втрачається на діагностику. Кореляція подій обіцяє значно знизити цей відсоток - скорочення операційних витрат на IT та скорочення доходів, втрачених до простою, на багато мільйонів доларів для великого бізнесу. Крім того, корельована база знань може підвищити точність та ефективність для інших застосувань, таких як орієнтовані на тенденції, ефективність та управління рівнем обслуговування. У найбільш хитромудрих прикладах інформація з співвіднесеної, самоадаптивної бази знань може інформувати про такі дії, як розповсюдження програмного забезпечення, налаштування та управління змінами.

6. Аналіз: Частий аналіз відповідних для безпеки симптомів мінімізує ризик втрат ефективності та порушень безпеки.

7. Звітність: Гнучка звітність забезпечує підтримку прийняття рішень для різних груп людей на підприємстві, включаючи керівництво та технічний персонал.

8. Встановлення політики безпеки: Добре продумана політика безпеки є основою для справжньої інформаційної безпеки в будь-якому корпоративному обчислювальному середовищі. Ця політика, заснована на ризику збалансування проти витрат, повинна зосереджуватися на забезпеченні

цілісності, доступності та конфіденційності. Реалізація та вимірювання цієї політики у великих, багатоплатформних середовищах для всіх підприємств є надзвичайно важливим завданням. SIEM надає вам можливість автоматизувати планування, управління та контроль вашої політики безпеки з одного місця, тим самим заощаджуючи ваш час та гроші. SIEM робить це, надаючи вам можливість вивантажувати ці повторювані та зайві завдання, пов’язані з керуванням такою політикою на комп’ютерах, а не покладатися на працівників персоналу. Також сучасні підприємства стикаються з багатьма проблемами управління безпекою. Наприклад, нові кінцеві користувачі повинні мати швидку , простий доступ до різноманітних платформ та додатків, щоб бути продуктивними. Права доступу до користувачів також повинні бути негайно відкликані, щоб запобігти несанкціонованому доступу та захистити безпеку на рівні підприємства. Процедури безпеки призначені для припинення порушень; однак без своєчасного централізованого управління процедури безпеки не можуть бути застосовані. Крім того, підприємства повинні йти в ногу з поширенням нових IT-ресурсів, збільшенням кількості користувачів та включенням нових бізнес-каналів, таких як електронний бізнес. Координація, впровадження та відстеження цих процедур стає все більш складним на великих підприємствах з різноманітною розподіленою IT-інфраструктурою. Підхід SIEM поєднує перевірену методологію та повне комплексне обслуговування з високомасштабною технологією.

Серед перерахованих вище функцій, нормалізація журналу, кореляція та аналіз журналу - це деякі функції, які визначають, наскільки ефективно продукт SIEM відповідає потребам безпеки.

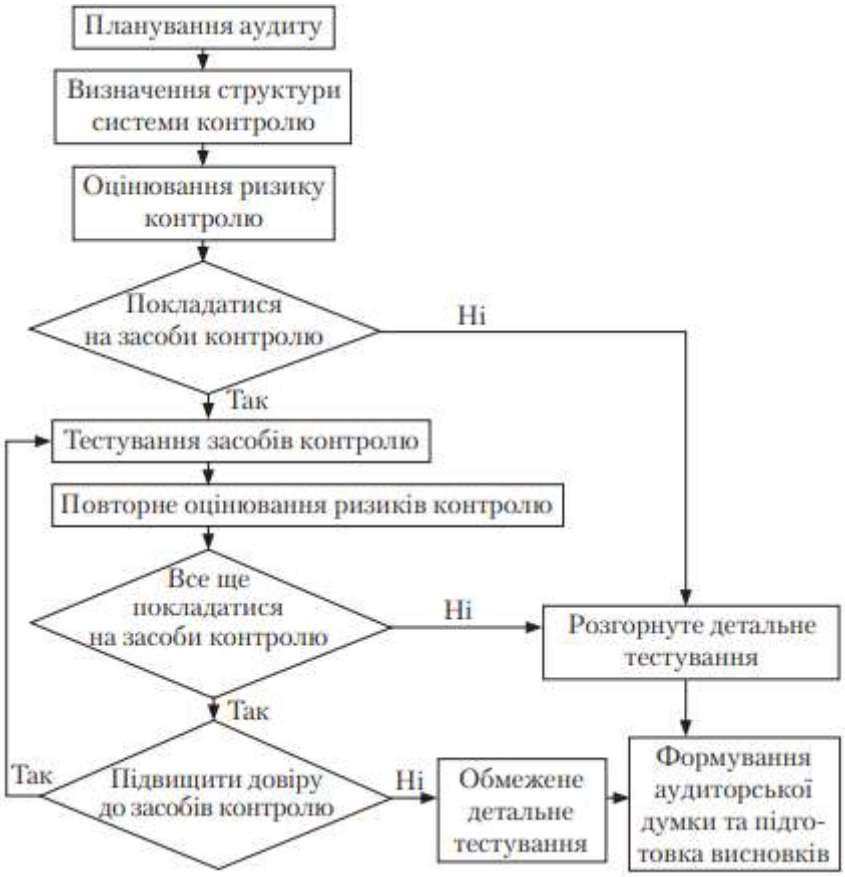


Рис. 1.5. Нормалізація і кореляція журналу

Кореляція журналу намагається зібрати всю інформацію разом, що, безумовно, буде корисним при отриманні доказів шкідливих випадків у різних джерелах даних. Використовуючи дані мережі в якості прикладу, вони можуть включати дані із систем виявлення та запобігання вторгнень (IDS / IPS), брандмауерів, веб-серверів та інших пристроїв, включаючи маршрутизатори та комутатори, таким чином, дані містять мільйони подій за короткий час. Основні дані журналу безпеки створюються попередженнями або інцидентами, які загалом охоплюють інформацію про об'єкт, поведінку, результат, техніку, групу пристроїв та часові позначки. Вони містять дані мережевого, апаратного та додаткового журналу даних. Ці набори даних мають бути відведені до того, з чим аналітик може розумно мати справу. Явні кореляційні критерії та нормування приведуть до ефективного аналізу даних.

Коли аналітик безпеки, який бажає бачити всі входи користувачів протягом певного періоду часу, повинен дізнатися, яка конкретна категорія кожного типу подій, щоб отримати цю інформацію. Відповідно до серії

таксономій для вилучення подій безпеки з необробленого файлу журналу та поділу на різні категорії, такі як аутентифікація, нове з'єднання, підпис тощо. Деякі приклади наведені нижче (рис.6):

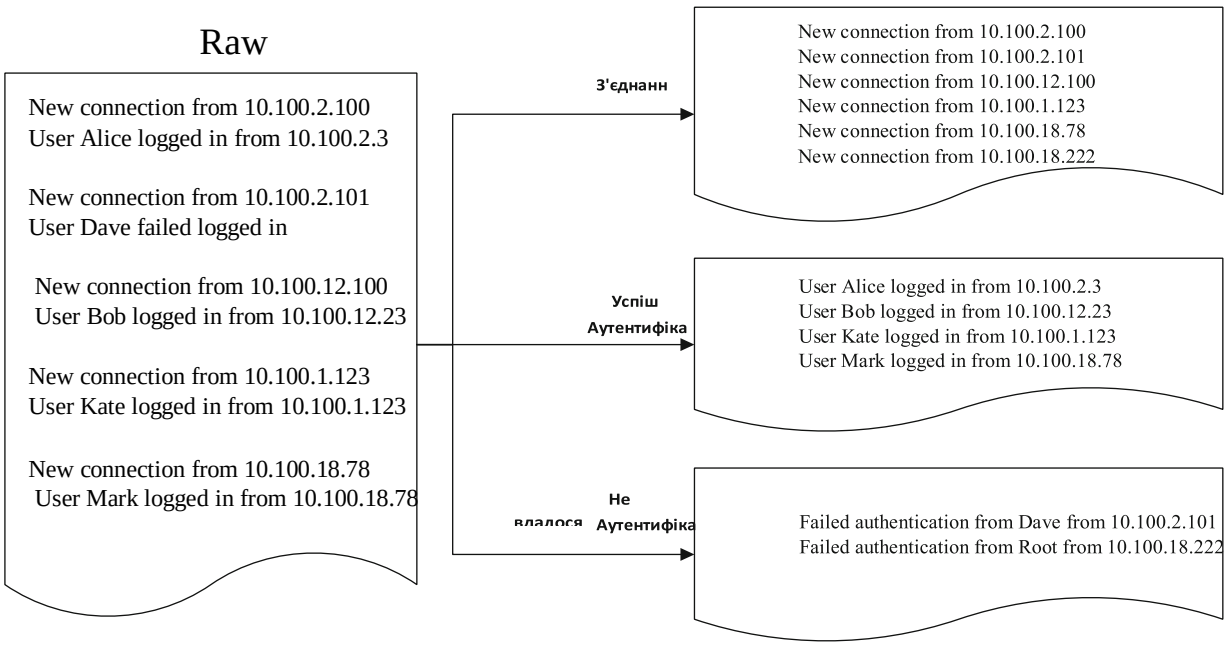


Рис. 1.6. Події безпеки, витягнуті з журналів

Критерії кореляції та нормалізації:

– Чітко сформулюйте політику, яка лежить на тому, що заборонено і що дозволено

– Переведення шкал суворості, які використовуються різними пристроями, в єдині стандарти, такі як 1-дуже низький, 2-низький, 3-середній, 4-високий і 5-дуже високий

– Оцінка взаємних зв’язків даних журналів за категорією та суворістю та наскільки важливою є ця залежність

– Кореляція реєструє дані з усіх пристроїв захисту в базі кластера про час, місцеположення та приєднання до кількох джерел даних

– Нормалізація різних форматів даних журналів з високою продуктивністю та цілісністю

– Створення ключових показників для отримання даних відповідно до політики, це істотно зменшить кількість випадків для аналітиків.

– Включаючи робочий процес, який дозволяє відрізнити будь-які випадки від хибно позитивного до потенційного нападу

– Постійно налаштовуйте оцінку вразливості та виправлення, щоб точніше та швидше з’ясувати, коли виникли проблеми із безпекою

– Запис усіх рішень та змін у міру налаштування є повторним

– Створення та налаштування індексу для прискорення передачі та пошуку даних

Відповідно до зазначених вище критеріїв, коли організація обмежує привілей "root" на доступ до певної конфігурації програми в політиці безпеки. На початку дані слід витягнути з необроблених файлів журналів усіх видів діяльності, що включає "'root" за ключовими показниками, що визначається в політиці. А потім нормалізувати пов'язані дані в єдиний формат для зберігання даних у базі даних як джерела даних для подальшого аналізу. Тим часом інформація про надзвичайні випадки буде використовуватися для покращення та налаштування політики та показників. Налаштування ключових показників також допоможе полегшити з’ясувати, який тип подій має бути на пристрої.

Інциденти або події можна відфільтрувати, ґрунтуючись на кореляційній політиці, яка вимагає багато досвіду та знань щодо безпеки IT. Це важко, а неналежне співвідношення спричинить серйозні ризики.

1.5. Аналіз даних журналу

Аналіз даних журналу визначає значення та причини проблем безпеки, це ключова частина всіх зусиль у всьому процесі. Хоча це дуже залежить від якості кореляції файлів журналу та нормалізації, подія є шкідливою чи ні, також залежить від контексту файлів журналів. Наприклад, джерело та місце призначення можуть стати зловмисниками та цілями, якщо мережевий аналізатор, такий як HIDS чи NIDS, оцінює трафік як ворожий. Після перегонки необроблених даних для структурування даних належним чином аналітичні інструменти представлять дані на інформаційній панелі, звіті чи виявленні шаблонів та інтерактивному виявленні (рис.7).

Критерії процесу аналізу журналу:

• Аналіз загальної кількості подій. Якщо кількість подій більша або нижча за звичайну, шукайте ключові показники та шаблони з позначкою часу в даних журналу і навіть переконайтесь, що політика ведення журналу є досить включною.

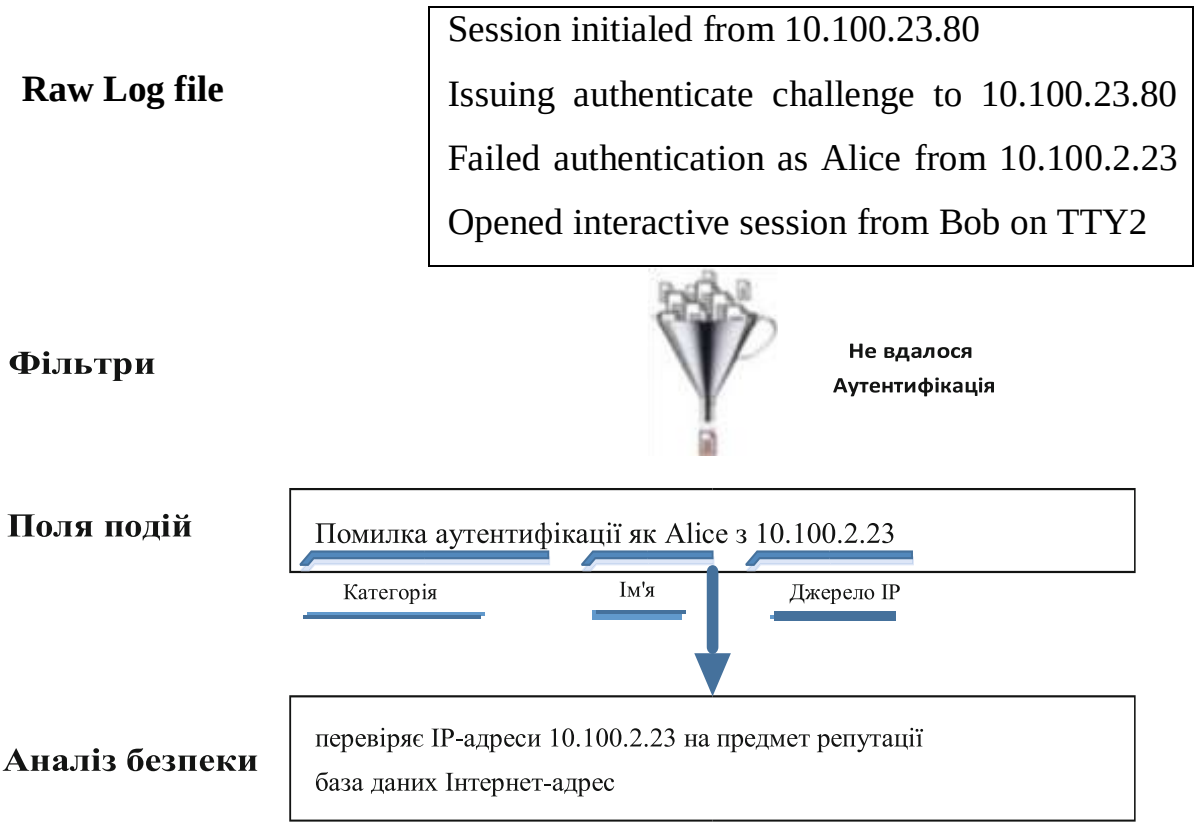


Рис. 1.7. Кореляційні директиви та аналіз безпеки

- Аналіз різноманітності подій. Якщо кількість унікальних типів подій невелика, переконайтеся, що політика журналу містить усі джерела, а ключові показники охоплюють різні події безпеки.
- Аналізуючи кількість подій, що відбувалися періодично - якщо кількість подій, мабуть, велика або нижча за минулий період, порівнюючи дані журналу, щоб з'ясувати першопричини.
- Аналіз поведінки в мережі, яка перерахована, але не обмежується
  - Дослідіть джерело
  - Пошук DNS
  - WHOIS пошук

- Показати ARP
- Перегляньте діаграми мережі
- Зверніться до власника активу та обговоріть, що бачите
- Розгляньте повну криміналістику, якщо це досить серйозно
- Оновіть підписи та виправлення антивірусу та перезавантажте
- Перезавантажте хост із завантажувального зображення та відскануйте хост на наявність шкідливих програм

• Аналіз показників доступності, потужності та продуктивності апаратних засобів. Якщо тенденція апаратних метрик ненормальна, можливі шкідливі активісти можуть статися або трапилися в системі

• Аналіз матриць захисту програмного забезпечення за деякими компрометованими методами, який перелічено, але не обмежується

- Ін'єкція
- Аутентифікація та управління сеансами
- Небезпечні прямі посилання на об’єкти
- Помилка безпеки
- Чутливе опромінення даних
- Відсутній контроль доступу на рівні функції
- Підробка міжміських запитів
- Використання компонентів з відомими вразливими місцями
- Недійсні переадресації та переадресація

Дуже важливо, що дані журналу з систем виявлення та запобігання вторгнень (IDS / IPS), брандмауера, журналів системних та мережевих пристроїв можуть вчасно контролюватися та аналізуватися. А аналіз даних журналу виконує декілька цілей. По-перше, аналіз у режимі реального часу дає адміністраторам безпеки огляд того, що зараз відбувається у ворожій системі та мережі. Інша мета - зрозуміти, як зміни діяльності з часом можуть швидко реагувати на коригування конфігурації безпеки, якщо це необхідно. Крім того, результат аналізу даних журналу є найважливішою інформацією для нападу на криміналістику.

Кілька відомих інструментів аналізу журналів з відкритим кодом випускаються із загальним робочим процесом аналізу, наприклад, OSSIM, LogRhythm, Nagios, Splunk, PRTG тощо. У реальному середовищі інструменти з відкритим кодом потрібно налаштувати на кореляцію журналів, політику ведення журналів, вилучення фільтрів та індекс. Проаналізуйте всі дані, щоб швидко виявити тенденції, сплески та аномалії, а потім подайте дані далі за допомогою графіків візуалізації та діаграм, щоб зрозуміти тенденції імпорту.

1.6. Особливості SIEM

Раніше ми обговорювали, що робить SIEM і як це працює. Далі ми переходимо до особливого розгляду SIEM. Оскільки SIEM надає всю службу безпеки для організації, при впровадженні SIEM слід враховувати три особливості - функціональність, надійність, масштабованість.

Здатність (продуктивність). Можливості рішення SIEM повинні відповідати потребам підприємства та надавати точні та змістовні дані. Також слід враховувати можливість співвідношення даних між багатьма різними джерелами даних. Більшість систем SIEM збирають дані журналу двома способами: в режимі реального часу або опитують дані із пристроїв безпеки, але кожна має свої переваги та дефекти. Механізм у режимі реального часу вимагає високої продуктивності, він забезпечує дуже актуальні дані з мінімальною затримкою, хоча навряд чи дасть неточний історичний тренд-аналіз. Централізоване сховище - це альтернативний метод у режимі реального часу. Цей механізм витягує дані в сховище по всій системі підприємства, і процес збору даних ефективно забезпечує точність даних. Однак в аспекті безпеки дані в режимі реального часу є одним з найцінніших властивостей.

Обчислювальний потенціал є величезною проблемою і для розподілених SIEM. Якщо діапазон розмірів даних в терабайт, він не зберігатиметься в одному місці, і будь-яка база даних або система зберігання знижує продуктивність. Це, очевидно, може спричинити інші серйозні наслідки для всього SIEM, коли якісь дані потребують негайно, але вони не можуть бути доступними. Тому,

використовуючи ієрархічну архітектуру, можна отримати переваги кожної методології та пом'якшити деякі недоліки.

Надійність. У системі SIEM всі пристрої та система покладаються на централізовану систему для налаштування, розгортання та моніторингу політики безпеки. Один пункт відмови спричинить загрозу в безпеці в системі SIEM і навіть призведе до непідконтрольного середовища безпеки. Клонування другого вузла для відновлення несправностей може забезпечити мінімізацію часу на ремонт системи SIEM, але з високою вартістю. Таким чином, шляхом регулярного резервного копіювання системи та тестування відновлення - це економічні та надійні способи забезпечити роботу системи відповідно до очікуваних умов.

Крім систематичних збоїв, усі відділи інформаційних технологій в організації несуть відповідальність за підтримку наявності кожного пристрою захисту. Оскільки система SIEM мала з'єднання з іншими пристроями та системами в мережі для цілей розгортання та моніторингу, зловмисники могли використовувати ці з'єднання для подальшого вторгнення.

Масштабованість. Масштабованість як основна властивість систем SIEM асоціюється з пропускною здатністю, зберіганням та розподіленими обчисленнями. Масштабування архітектури SIEM допомагає підприємству подолати деякі загальні обмеження в системах інформаційних технологій. Це слід врахувати в загальному дизайні архітектури SIEM. Незалежно від того, якого розміру може бути підприємство, створіть масштабований інструмент SIEM, щоб мати можливість підтримувати бізнес у майбутньому. Звичайно, використання витрат, щоб забезпечити реалізацію, яка може достатньо відповідати поточним цілям.

1.7. Дослідження кореляції журналу

Припустимо, що велика компанія впровадила інфраструктуру логування. Компанія розгортає систему виявлення вторгнень (IDS) за допомогою Snort. Також компанія встановлює VPN-сервер, що дозволяє телекомунікаціям

віддалено отримувати доступ до мережі компанії. Системний адміністратор також підтримує базу даних активів, яка містить дані про активи в організації. Прикладами деталей активів є ОС, IP-адреса, MAC-адреса, виробники обладнання, типи обладнання. Також Active Directory використовується для управління користувачами, автентифікації та авторизації користувачів та комп'ютерів у мережі та забезпечення доступу лише до авторизованих користувачів до ресурсів компанії. Повідомлення з необробленого журналу з сервера Snort та VPN передаються в центральне місце зберігання за допомогою Syslog, показаного на рис. 8.

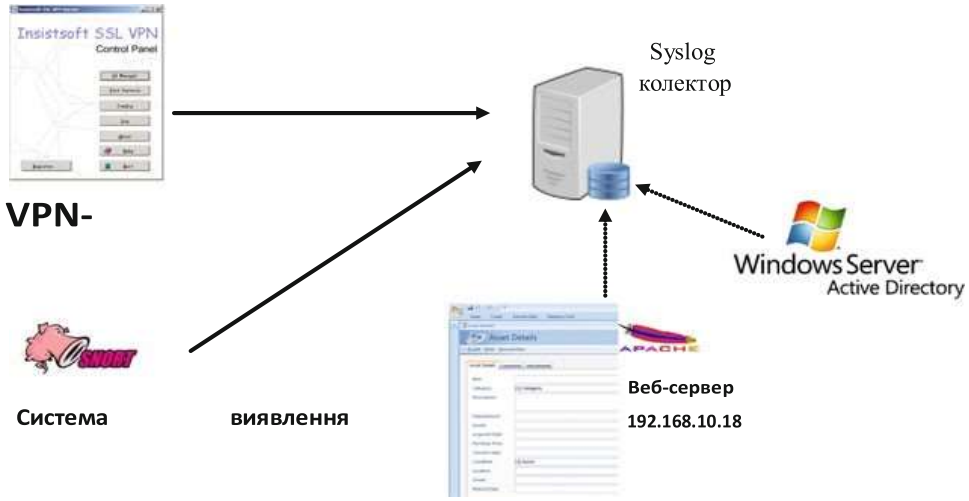


Рис.1.8. Приклад інфраструктури ведення журналів

Припустимо, сервер VPN записує подію входу для будь-якого користувача разом із розташуванням та часовою позначкою та пересилає його на централізований сервер журналу. Приблизно в той же час, що і подія входу, Snort виявив атаку DoS, що походила з 192.168.10.23, на комп'ютер компанії з IP-адресою 192.168.10.18. На основі журналів серверів VPN ви дізнаєтесь, що користувач з UID-слінгом використовує IP-адресу 192.168.10.23. Завдяки кореляції подій тепер ми знаємо, що користувач зі сідлом UID DoS атакує комп'ютер з IP-адресою 192.168.10.18. Далі ми шукаємо в базі даних активів і з’ясовуємо, що IP-адреса 192.168.10.18 призначена веб-серверу компанії, який є важливим сервером для компанії. Крім того, ми знайдемо повне ім’я користувача з UID слінгом, запитуючи Active Directory. Припустимо, повне ім'я користувача slin - Шелдон Лін. Нарешті, можна зробити висновок, що користувач Sheldon Lin

DoS атакує веб-сервер компанії. Висновок дуже корисний з точки зору двох речей порівняно із зібраними необробленими даними журналу. По-перше, ми знаємо, хто такий нападник. По-друге, ми знаємо, що це критичний випадок, і тому йому слід надавати пріоритет.

ВИСНОВОК ДО РОЗДІЛУ 1

Отже, одне важливе джерело цифрових доказів - це журнали. Одним із запорук успіху в проведенні ефективного цифрового розслідування на комп'ютерній системі є знання того, що відбувається в системі. Комп'ютерні системи та програми генерують журнали, коли щось трапляється або потребує уваги (наприклад, комп'ютерна система, налаштована для запису спроб входу користувача.). Ці журнали можуть надати ґрунтовні криміналістичні докази, які дозволять виявити недобросовісну діяльність користувача та дізнатись, як, коли та де трапиться інцидент та допоможуть виявити кіберзлочинців. У цьому розділі ми дізнались два основні механізми реєстрації журналів, Syslog та Журнал подій Windows, і як вони працюють. Також дізнались інформацію про безпеку та систему управління подіями (SIEM). Та дізнались, як збирати та аналізувати журнали.

РОЗДІЛ 2. ПОРІВНЯЛЬНИЙ АНАЛІЗ ІСНУЮЧИХ СИСТЕМ МОНІТОРИНГУ ЛОКАЛЬНИХ МЕРЕЖ ТА ВИБІР ОПТИМАЛЬНОГО ДЛЯ ПРОЕКТУ

2.1. Класифікація засобів моніторингу та аналізу

Системи моніторингу мережі – це програмне забезпечення, що дозволяє відстежувати стан мережевих пристроїв, їх працездатність, справність і інші характеристики. При цьому системи моніторингу мережі дозволяють повідомляти адміністратору про виникнення будь-яких збоїв за допомогою відправки СМС-повідомлень, повідомлень на електронну пошту тощо. Системи моніторингу мережі можна розділити на ті, що відстежують продуктивність мережі і сигналізують при перевантаженні каналів, а також на ті, що виробляють моніторинг мережі з метою пошуку збоїв і інших проблем, пов'язаних з працездатністю серверного обладнання та інших систем.

Розглянемо групи інструментів, які зазвичай використовують для моніторингу та аналізу локальних мереж:

Системи керування мережею (Network Management Systems) – централізовані програмні системи, які збирають дані про стан мережевих пристроїв і інформацію про трафік. Функціонал даних програм не обмежений моніторингом та аналізом мережі, вони також можуть здійснювати керування мережею: налаштування та зміна адресних таблиць комутаторів та іншого обладнання, включення і відключення портів пристроїв, тощо.

Вбудовані системи діагностики і керування (Embedded systems). Виконуються у вигляді програмно-апаратних модулів, які встановлюються в комунікаційне обладнання або в операційну систему. Вони дозволяють керувати діагностувати тільки той пристрій, на якому знаходяться. Зазвичай, вбудовані модулі керування також виконують роль SNMP-агентів, передаючи дані про стан пристрою в систему керування.

Засоби керування системою (System Management). Виконують функції, аналогічні функціям систем керування, але по відношенню до інших об'єктів. У

першому випадку об'єктом керування є програмне і апаратне забезпечення комп'ютерів мережі, а у другому – комунікаційне обладнання. При цьому частина функцій цих двох видів систем можуть дублюватися (наприклад, засоби керування системою можуть проводити найпростіший аналіз трафіку).

Аналізатори протоколів (Protocol analyzers) – це програмні або апаратно-програмні системи, які використовуються тільки для моніторингу і аналізу трафіку в мережах. Хорошим аналізатором вважається той, який може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються у мережах – приблизно декількох десятків. Ця група систем може встановлювати деякі логічні умови для захоплення окремих пакетів і виконувати повне декодування пакетів, тобто відображати в зручній для користувача формі вкладеність пакетів протоколів різних рівнів з розшифровкою змісту кожного з полів пакету.

Устаткування для діагностики і сертифікації кабельних систем. З назви стає зрозуміло призначення цієї групи. Умовно можна виділити чотири підтипи подібного обладнання: кабельні сканери, мережеві монітори, мультиметри і прилади для сертифікації кабельних систем.

Експертні системи з'єднують людські знання про виявлення причин аномальної роботи мереж і можливі способи повернення мережі в робочий стан. Найчастіше вони представлені у вигляді окремих підсистем інших засобів моніторингу та аналізу мереж, розглянутих раніше. До простого варіанту експертної системи відноситься контекстно залежна help-система, а більш складні є так звані бази знань, які мають елементи штучного інтелекту. Багатофункціональні пристрої аналізу і діагностики. Це недорогі портативні прилади з функціоналом декількох пристроїв: кабельних сканерів, програм мережевого управління і аналізаторів протоколів.

Також варто відзначити ще два способи моніторингу мережі. Перший – це маршрутизатор-орієнтований. Це - моніторинг, вбудований безпосередньо в маршрутизатор, і який не вимагає додаткової установки іншого забезпечення. Другий спосіб, відповідно, – це не орієнтований на маршрутизатори, тобто це

підібране самим фахівцем необхідне апаратне і програмне забезпечення для поточних потреб.

Використання систем моніторингу мережі дозволяє виконувати не тільки технічні завдання, описані вище, але і бізнес-завдання, такі як обгрунтування витрат на модернізацію обладнання або інфраструктури, що дозволило б знизити кількість проблемних вузлів. За рахунок підтримки мережі в працездатному стані і своєчасному усуненні її проблем компанія може знизити свої витрати на відновлення і повторюється усунення неполадок. А також підвищити свою репутацію в частині надійності надання власних сервісів клієнтам (це особливо актуально в разі, якщо організація надає доступ до веб-сайту, здійснює свою діяльність через інтернет або надає свої ресурси користувачам в якості хмарного сервісу). У той же час, коли керівництво може стежити за якістю надходження послуг (наприклад, канал інтернет- провайдера), при виникненні будь-яких збоїв з вини постачальника організація-споживач має право вимагати компенсацію, якщо такі збої відображені в угоді про якість обслуговування.

2.2. Порівняльний аналіз існуючих систем моніторингу локальних мереж

Розглянемо сучасні програми для моніторингу локальної мережі, які є актуальними в 2020 році.

Програми для моніторингу мережі функціонують в локальній мережі. Крім пошуку помилок, вони перевіряють доступність сервісів, відображають дані про використання мережі, формують списки комп'ютерів в мережі, перевіряють і шукають паролі, здійснюють доступ до Розшарені папках, показують дані про навантаження на процесор, оперативну пам'ять, жорсткий диск, канал зв'язку і т.д. Окремі програми даної категорії можуть не тільки збирати статистику всіх процесів, що протікають в мережі, але і відстежувати їх якість, аналізуючи помилки, і на основі зібраної інформації створюють звіт з висновками.

Системи моніторингу дозволяють істотно полегшити життя системному адміністратору, особливо якщо під його наглядом працює велика кількість мережевого обладнання.

Нині розроблені десятки програмних продуктів, які дозволяють вести моніторинг мережі. Усі їх умовно можна поділити на платні і безкоштовні. А втім, ідеальної програми все-таки не існує. У кожного продукту є як свої переваги, так і недоліки. При цьому, як правило, адміністратори виробляють моніторинг мережі з допомогою кількох програм. Розглянемо деякі з них.

2.3. PRTG

PRTG (Paessler Router Traffic Grapher) - умовно-безкоштовна програма (Пробний період - 30 днів, після чого обмежується кількість сенсорів) для моніторингу мережі, працює в сімействі операційних систем Windows, розроблена в 1997 році Дірком Песслером .

У PRTG Network Monitor є більш 200 типів сенсорів всіх стандартних мережевих служб і не тільки, включає в себе: HTTP, SMTP / POP3, FTP, певний URL-адресу, трафік мережевого підключення, порт комутатора або завантаження ЦП на комп'ютері. Кожен запис в цьому списку вважається одним сенсором. Зазвичай розрахунок ведеться за допомогою 5-10 сенсорів на пристрій.

Мабуть, найзрозуміліша система моніторингу. повністю інтуітівний інтерфейс з конфігурацією виду «наведи і клацни», легка і швидка установка (близько 2 хвилин), підтримка (правда, тільки по буднях), автоматичне виявлення вузлів мережі, готовий до роботи відразу після установки, доменна аутентифікація. Постійні оновлення і доповнення (приблизно, раз в місяць) . Можливість установки програми на Android пристрою, що дозволяє стежити за станом мережі з будь-якого місця, де є інтернет. Робота на комп'ютері зі встановленою операційною системою Windows. Можливість користуватися системою як через web-браузер, так і через додаткову встановлену програму. Чи не вимоглива до ресурсів комп’ютера: оперативна пам'ять - мінімум 1024 Мб, плюс на кожен сенсор буде потрібно 150 Кб і жорсткий диск - 200 Кб на сенсор

в день. Ця система підходить для знайомства недосвідчених системних адміністраторів зі своїм робочим простором .



Рис. 2.1. Приклад відображення інформації в PRTG

Це все плюси, але є ряд істотних недоліків. система працює тільки на Windows машині. А це покупка додаткових ліцензій для сервера. Якщо ваша мережа не така проста, а захищена, то також необхідно налаштувати firewall і антивірус для доступу до комп'ютерів та інших пристроїв, що позбавляє ще одного плюса на користь «готовий до роботи відразу після установки ». Дані та історія сенсорів програми зберігаються в незашифрованому вигляді безпосередньо в директорії програми.

ЛИЦЕНЗИЯ PRTG	ДАТЧИКИ	ЦЕНА
Бесплатный выпуск	100	Бесплатно
30 дней бесплатная версия	Неограниченно*	Бесплатно на 30 дней
PRTG 500	500	$1,600.00
PRTG 1000	1000	$2,850.00
PRTG 2500	2500	$6,150.00
PRTG 5000	5000	$10,500.00
PRTG XL1/Unlimited	Неограниченно*	$16,900.00
PRTG XL5/Unlimited	Неограниченно*	$60,000.00

Рис. 2.2. Ціни на ліцензію PRTG

Такі розцінки можуть вразити будь-яку людину, адже єдиний істотний плюс програми - це моніторинг своєї мережі через смартфон або планшет. Але установка додатково додатки в телефоні не обов'язкова, адже нам потрібна інформація про проблеми, а не діаграми, які можна подивитися, прийшовши на роботу. Однак даний продукт пропонує барвисті звіти і діаграми. У результаті ми маємо досить дороге рішення для повсякденних задач, з якими можуть впоратися інші безкоштовні системи, адже навіть в найбільшій компанії в пріоритеті є гроші, а зайві витрати на те, що можна зробити безкоштовно, їм ні до чого. Тому ми плавно переходимо до безкоштовних рішень моніторингу мережі.

2.3. Zabbix

ZABBIX - відкрите програмне забезпечення розподіленого моніторингу корпоративного класу, написане Олексієм Владішевим .

Для зберігання даних використовується MySQL, PostgreSQL, SQLite або Oracle. Веб-інтерфейс написаний на PHP. Zabbix підтримує кілька видів моніторингу. Simple checks може перевіряти доступність і реакцію стандартних сервісів, таких як: ICMP, SMTP або HTTP без встановлення будь-якого програмного забезпечення на спостережуваному хості. Zabbix agent может бути встановлений на UNIX-подібних або Windows хостах для отримання даних про навантаження процесора, використання мережі, дискового простору і т.п. External check - виконання зовнішніх програм .

Zabbix написаний і розповсюджується під ліцензією GPL (General Public License) версії 2. Це означає, що його вихідний код вільно розповсюджується і доступний для необмеженого кола осіб.

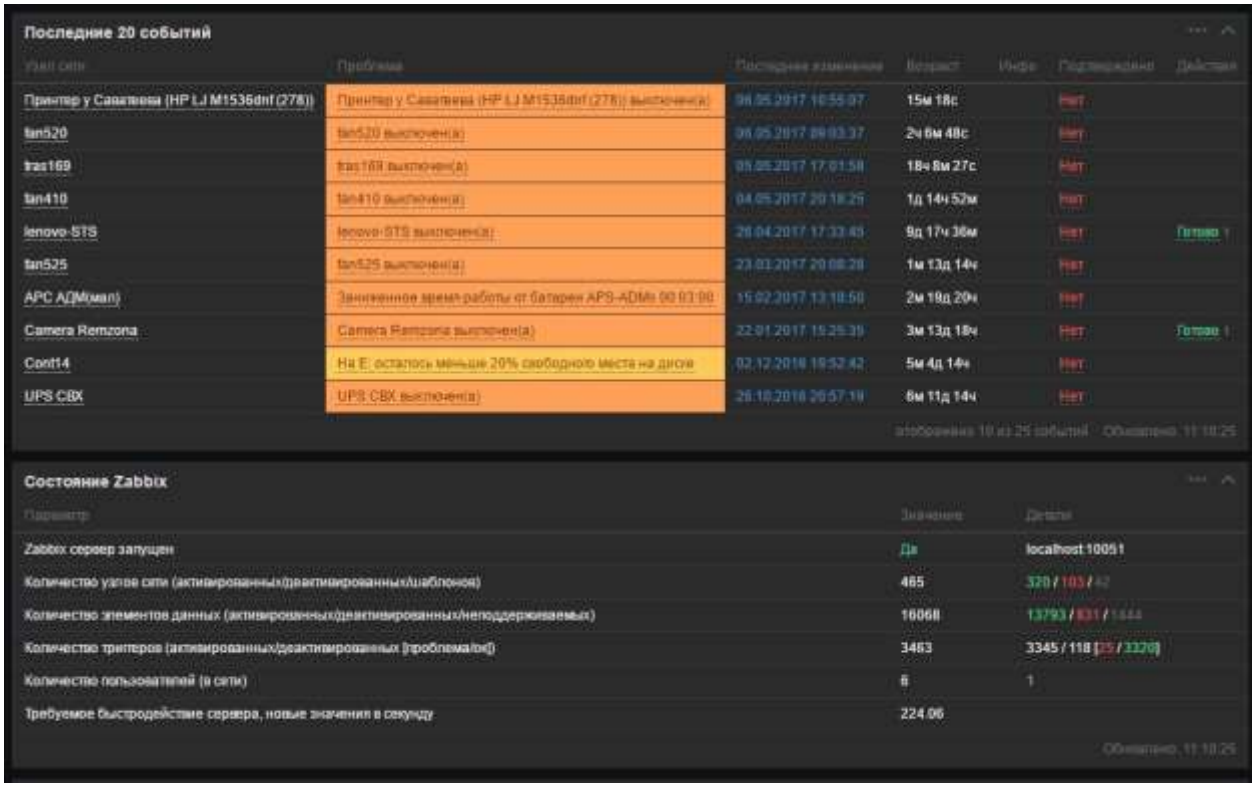


Рис.2.3. Приклад відображення інформації в Zabbix

Досить довга установка (близько 30 хвилин для занющего Unix системи адміністратора), необхідність правити конфігураційні файли після установки, налаштування шаблонів для автоматичного виявлення або ручне додавання кожного пристрою (вузла) - все це істотні недоліки, які можуть змусити відмовитися від даної системи, але після довготривалого налаштування Zabbix робитиме все сам: виявляти нові пристрої і відразу відстежувати їх стан, виконувати сценарії на основі отриманих даних, інформувати будь-яким обраним способом про проблеми (класифікацію яких також можна вибрати самостійно). У зв'язку з безкоштовністю і поширеністю в мережі Інтернет можна знайти дуже багато інформації по налаштуванню того чи іншого пристрою або скачати готові шаблони. Можливість налаштувати віддалені команди або імітацію натискань на web-сайті. Повністю налаштовується система зберігання історії та логів. Найпотужніший інструмент моніторингу і управління пристроєм за допомогою OID по SNMP. Але найважливіший плюс даної системи - підключення зовнішніх користувальницьких скриптів, з допомогою яких можна

відстежувати абсолютно все. Також Zabbix можна інтегрувати зі стороннім програмним забезпеченням .

2.4. NetXMS

NetXMS - програмне забезпечення з відкритим кодом для моніторінгу комп'ютерних систем і мереж. Може бути використана для моніторингу всієї IT-інфраструктури. Також доступний за ліцензією GNU v2 .

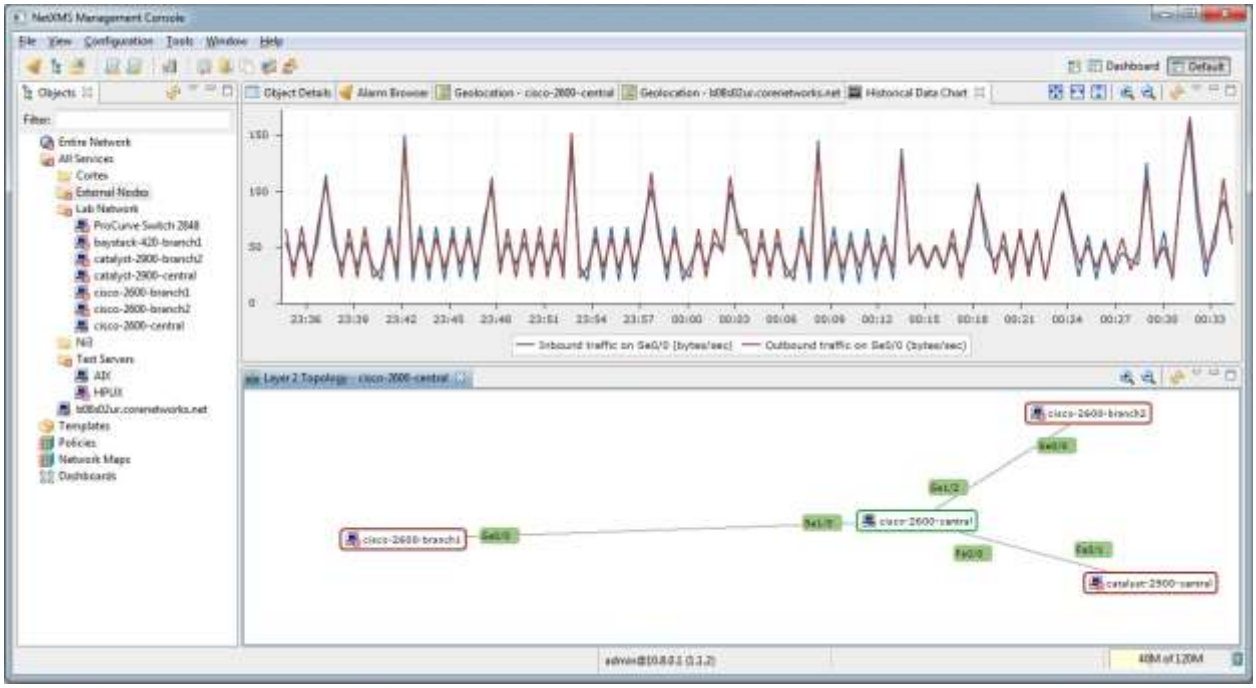


Рис. 2.3. Приклад відображення інформації в NetXMS.

Система має модульну архітектуру і дає можливість легкого розширення функціональності, можливість установки на будь-якій платформі і безкоштовне розповсюдження - ось, мабуть, усі переваги програми. З недоліків: web-інтерфейс і сама програма NetXMS Console (Може бути встановлена на Android) працює виключно на java, моніторинг пристроїв відбувається тільки після установки на них агента, зайві турботи про збіг часу. Якщо неправильні годинні пояси або неправильний час, то нічого не видно - інформація далеко в минулогму або в майбутньому. І, звичайно ж, відсутність підтримки української мови. Однак розробники живуть в Прибалтиці і добре розмовляють на російською, що дозволяє (за окрему плату) замовити у них абсолютно будь-яку функцію під Ваші потреби.

2.5. Nagois

Nagios - програма з відкритим кодом, призначена для моніторингу комп'ютерних систем і мереж. Спочатку була створена під іменем Netsaint, розроблена Ethan Galstad. Працює в UNIX-системах і випускається під ліцензією GNU v2.

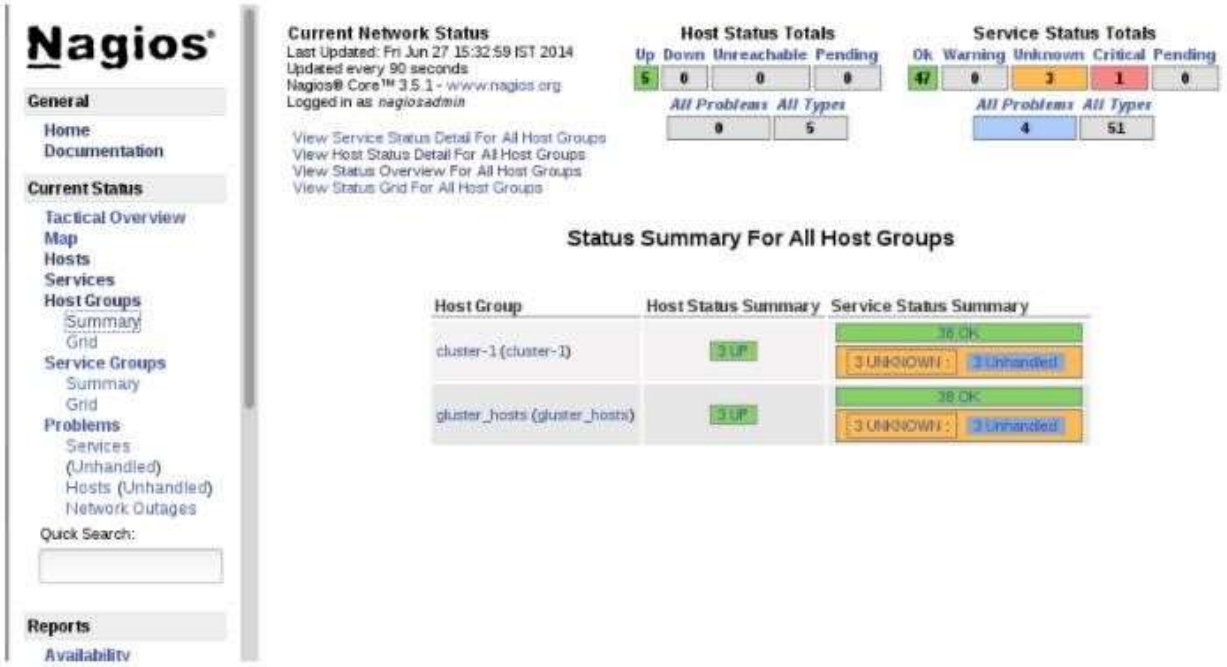


Рис. 2.5. Приклад відображення інформації в Nagios

Установка і налаштування конфігураційних файлів Nagois відбувається достатньо довго (близько години, знає UNIX-системи адміністратору). Усі налаштування моніторингу також створюються в конфігураційних файлах, що не зовсім зручно. А на пристроях необхідно налаштувати SNMP, тому що така система працює лише з цього протоколу. І знову відсутність української мови .

Підтримка віддаленого моніторингу через шифровані тунелі SSH або SSL. Проста архітектура модулів розширень (плагінів) дозволяє, використовуючи будь-яку мову програмування за вибором (Shell, C ++, Perl, Python, PHP, C # та інші), легко розробляти власні способи перевірки служб. Можливість організації спільної роботи декількох систем моніторінгу з метою підвищення надійності і створення розподіленої системи моніторингу (як правило, використовується спільно з системою моніторинг Cacti). Мінуси неістотні, а плюси недостатні. До того ж, творці перестали удосконалювати opensource систему і зайнялися

розробкою платної версії програми. Випустили Nagios XI - платна система моніторингу, що відрізняється від свого попередника лише більш яскравим інтерфейсом .

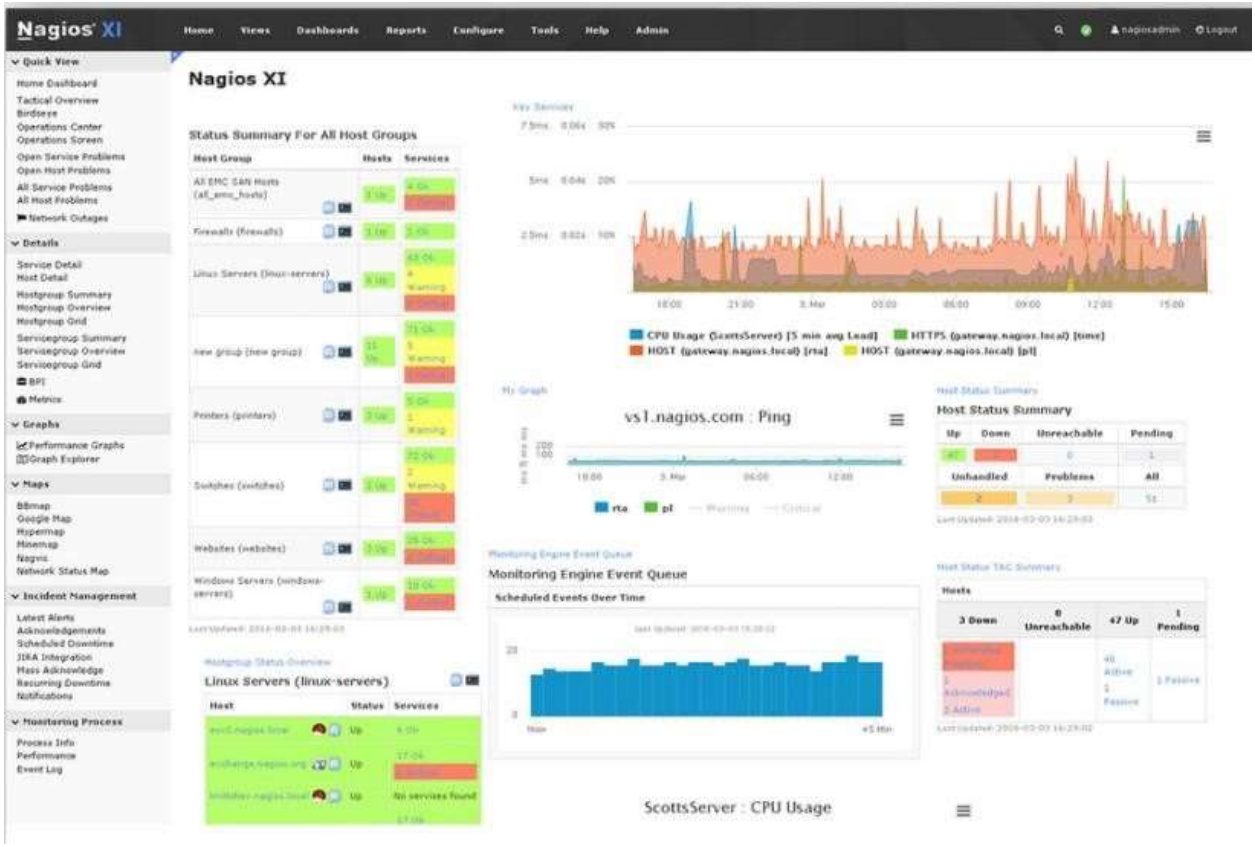


Рисунок 2.6. Приклад відображення інформації в Nagios XI

Причому вартість такого продукту - 1900 $ за Standard Edition на 100 вузлів (пристроїв). А безлімітний випуск вартий вже 6200 $. Тобто тут ми бачимо бажання позбутися шанувальників своєї продукції.

2.6.Вибір системи моніторингу

Отже, ми маємо дві платні і дві безкоштовні системи моніторингу.

Розглянемо необхідні функції для нашого підприємства:

- надійність: PRTG, Zabbix, Nagios;
- моніторинг мережевої активності пристрою: все системи;
- перевірка стану пристрою (вентилятор, CPU, пам'ять): все системи;
- сповіщення по CMC при тривогах: PRTG, Zabbix;
- віддалене управління пристроями: PRTG, Zabbix, Nagios;

- автоматичні дії при тривогах: Zabbix, Nagios;
- безкоштовність: Zabbix, NetXMS;
- Можливість розширення: Zabbix, NetXMS, Nagios;
- призначені для користувача скрипти: Zabbix, Nagios.

Між Zabbix і PRTG існує принципова відмінність. Zabbix дотримується концепції багатоагентного або безагентного моніторингу, в той час як в PRTG використовуються стандартні мережеві протоколи, наприклад: SNMP, Stream, Ping, FTP, аналіз пакетів і т.д. Zabbix вимагає установки агента на кожне контрольоване пристрій. Це не завжди можливо, і в таких випадках програма також підтримує деякі основні протоколи, наприклад: SNMP або TCP. За допомогою віддалених зондів PRTG пропонує додаткові пошукові системи, які можуть бути використані для розподілу навантаження. PRTG також найкраще підходить для моніторингу локально розподілених мереж (підмереж, VLAN і т.д.) або сегментів мережі, розділених брандмауерами (зазвичай віддаленими).

Віддалений моніторинг в PRTG.

Існує концепція віддалених зондів, які виконують функцію моніторингу мережі, відмінної від тієї, в якій встановлено PRTG. Їх установка дуже проста: на ПК з Windows необхідно звільнити правильний TCP-порт в брандмауері і IP, на якому встановлено віддалений зонд. Таким чином, ці та інші пристрої у вашій мережі видно PRTG, якщо б вони були з самої цієї мережі. Віддалений зонд періодично (дуже часто) збирає всі дані моніторингу з усіх контрольованих пристроїв і додатків в мережі, використовує стандартні протоколи і відправляє дані моніторингу на базовий сервер, використовуючи SSL-шифрування. Це досить надійнерішення! ьВіддалений моніторинг в Zabbix.

Існує концепція «агентів», які, по суті, грають таку ж роль, що й зонди PRTG, які існують для ОС Windows і для деяких дистрибутивів Linux, таких як: Ubuntu, FreeBSD, OpenBSD, AIX, і т.д. Установка агентів досить проста, однак труднощі з виділенням сенсорів на віддалених пристроях присутні так само, як і труднощі з виділенням сенсорів на локальних пристроях. Для віддаленого

моніторингу потрібно встановлене мережеве підключення. Без мережевого доступу віддалені місця розташування будуть недоступні для моніторингу.

Підтримка PRTG.

Існують групи обговорень, підтримка по електронній пошті, форуми, актуальні питання (FAQs), база знань, а для тих, хто придбав продукт, протягом 12, 24 або 36 місяців на сайті є доступ до анкети (при відкритті заявки), заповнення якої забезпечує пріоритетну підтримку по електронній пошті. План технічного обслуговування повинен актуалізуватися для оновлень і підтримки. Навіть не продовживши договір на технічне обслуговування, ви можете як і раніше використовувати ПО, але без пріоритетної підтримки або оновлень продукту.

Підтримка Zabbix.

Існують групи обговорень, форуми та можливість залучення підтримки, яка розділена на рівні: бронзовий, срібний, золотий, платиновий і корпоративний. Ціни на сайті не представлені, цінові пропозиції залежать від кожного конкретного випадку. Таким чином, продукт є безкоштовним, але підтримка оплачується, а через складність продукту вона буде необхідна.

Zabbix і PRTG допомагають досягати однієї і тієї ж мети - моніторингу мережевої інфраструктури, пристроїв, серверів, маршрутизаторів, принтерів, точок доступу Wi-Fi і т.д., проте їх способи роботи сильно відрізняються. На деяких рівнях Zabbix володіє аналогічними функціями, однак використовувати його складніше, ніж PRTG. Після тестування PRTG протягом декількох тижнів було виконано розгортання Zabbix. Чи не було наміру відтворювати повноцінний моніторинг, достатньо було невеликої його частини, щоб відчути продукт. Знадобилося кілька тижнів, щоб виконати дане розгортання на дуже невеликій кількості контрольованих елементів. Налагодження та технічне обслуговування Zabbix набагато більш трудомістке, ніж PRTG. Проте факт того, що це безкоштовне рішення, для багатьох може стати вирішальним. Однак питання моніторингу інфраструктури настільки важливий і серйозний для підтримки безперебійної роботи, що вартість безстрокової ліцензії PRTG можна

навіть назвати занадто низькою. Після закінчення першого року використання для продовження ліцензії та отримання права на поновлення та підтримку необхідно виплатити невелику суму. У Zabbix також є можливість надання платної 5-рівневої підтримки для компанії або допомоги партнера, який надає консультативні послуги з підтримки Zabbix.

Таблиця 2.1

Порівняльна таблиця PRTG і ZABBIX

Параметр	PRTG	ZABBIX
установка	Програма для Windows може бути встановлена на сервері колективного доступу або виділеному сервері (при наявності тисяч сенсорів, які необхідно контролювати).	Поетапна ручна установка і налаштування, компонент за компонентом на системі Linux або установка віртуальної машини на Hypervisor.
Користувальницький інтерфейс	Простий і зрозумілий, за останні роки був вдосконалений і модернізований. Елементи функціоналу зручно розташовані в інтуїтивно-зрозумілих місцях.	Менш зрозумілий, складна термінологія. Нема є програми для ПК, але є мобільний додаток.
Auto Discovery (автоматичне виявлення)	Після установки дана можливість пропонується для всієї мережі. Процес Auto Discovery також може бути запущений для одного пристрою.	Під час установки продукту була відсутня можливість перегляду мережі і виявлення існуючих пристроїв. Згодом це можна зробити окремо, використовуючи певні протоколи, такі як SNPM.

Додавання нових сенсорів	Просте додавання, послідовно для кожного пристрою, спеціальні сенсори. Рахунок-асистент, яка керує додаванням більш відповідних сенсорів по типу пристрою / шаблонів.	Чи не простий процес, хоча присутня гнучкість при виборі протоколів для прочісування пристрою. Для налаштування потрібні великі технічні знання. Як варіант, ви можете використовувати агенти, встановлені на кожному пристрої.
Використання агентів	З PRTG не потрібно встановлювати будь-яких агентів на кожен пристрій, моніторинг можна виконувати тільки за допомогою ядра програми, використовуючи власні технології.	Використання агента на кожному пристрої робить використання Zabbix трохи простіше, однак недоцільно встановлювати агенти на сотні або навіть тисячі пристроїв. Існують певні пристрої, наприклад, принтери, установка агентів на які неможлива.
Віддалений моніторинг	З PRTG не потрібно встановлювати будь-яких агентів на кожен пристрій, моніторинг можна виконувати тільки за допомогою ядра програми, використовуючи власні технології. Використання віддалених зондів дозволяє здійснювати моніторинг різних мереж, які або знаходяться в одному і тому ж місці, або у	Для здійснення моніторингу пристроїв потрібні агенти, для чого необхідно встановити з'єднання з мережею. При відсутності мережевої інфраструктури

	віддалених місцях, філіях і т.д. Віддалений комп'ютер збирає інформацію про місцезнаходження і об'єднує її на центральному сервері PRTG, надаючи доступ до всіх локальних і віддалених пристроїв, сенсорів, оповіщення та попереджень через мережу Інтернет, а також використовує протокол зі стійким шифруванням SSL.	компанії немає можливості проведення віддаленого моніторингу, як це робить PRTG.
Підтримка	Поширені питання (FAQs), групи обговорень, форум і підтримка через електронну пошту. При активному технічному обслуговуванні гарантується надання оновлень без додаткової плати, а також пріоритетної підтримки.	Поширені питання (FAQs), групи обговорень і підтримка через електронну пошту для тих, хто в змозі залучати зовнішніх підрядників до надання різних рівнів підтримки: бронзовий, срібний, золотий, платиновий.
Ціна	Продукт є безкоштовним для 100 сенсорів. Здійснення моніторингу 500, 1000, 2500, 5000 або необмеженої кількості сенсорів. На сайті Paessler представлені прозорі ціни, які є однаковими по всьому світу.	Продукт є безкоштовним, але і досить складним, він зажадає залучення одного з пропонованих рівнів платної підтримки. На сайті Zabbix не вказані ціни, і цінову пропозицію необхідно запитувати в кожному конкретному випадку.

ВИСНОВОК ДО РОЗДІЛУ 2

Постійний розвиток є дуже важливим фактором, і якісний моніторинг - це категорія, яка має вирішальне значення для господарської діяльності підприємств. Тестування PRTG в 2012, 2014, 2016, 2018 роках і зараз в 2020 році показали, що розвиток системи відчутно покращився Інтерфейс веб-версії отримав нову структуру, наповнився новою інформацією. На інформаційній панелі відображаються повідомлення мережі дані, пристрої, сенсори, попередження та аварійні сигнали. Додавання сенсорів до пристроїв стало простіше шляхом створення ярликів або за допомогою майстра, який дуже просто керує процедурою підключення. При зміні версії ядра PRTG віддалені зонди недоступні протягом зовсім недовгого часу. Продуктивність і навігація додатків для смартфона знаходяться на високому рівні. І нарешті, як і в кожній новій версії, набір сенсорів було розширено, що дозволяє здійснювати аналіз, моніторинг і управління все більшою кількістю ситуацій, сценаріїв і середовищ. З комерційної точки зору у компанії Paessler існує дуже зрозуміла і прозора позиція щодо PRTG. Існує тест-версія з необмеженими можливостями на 30 днів. Компанія Paessler досить прозора у своїй торговельній політиці, пропонуючи версії з 500, 1000 2500 і 5000 сенсорами. Також існують необмежені корпоративні версії навіть в загальносвітовому масштабі.Впровадження можна провести після тестування 30-денний демо-версії (з необмеженою кількістю сенсорів). Після закінчення цього терміну в залежності від реальних потреб, можна укласти договір на придбання продукту з відповідною кількістю сенсорів. У майбутньому, в разі збільшення потреби, кількість сенсорів в інструменті можна збільшити, наприклад, з 500 до 1000 (або більше). Цінність PRTG виходить за рамки технічної мотивації. Можливість реагування на технічну подію відразу після того, як воно сталося або навіть здатність його передбачення на підставі аналізу дозволяють запобігти виникненню серйозної проблеми, яка може перервати виконання критичних операцій господарської діяльності, від яких так залежні технологічні ресурси компанії. Практична

цінність тестування досить відчутна. Кількість проблем, недоступність ресурсів і час реагування на інциденти помітно скоротилися.

Внаслідок цього, я вважаю, PRTG в 2020 році передовим, зрілим, надійним продуктом, чия цінність для компаній є незаперечною, адже це вкрай важливо - отримувати інформацію по ваших бізнес-процесах, які залежать від технології. Простота установки і обслуговування, гнучкість, великий вибір сенсорів, велика кількість інформації, аварійні сигнали, звіти і графіка. Принаймні це той інструмент, який слід спробувати, якщо компанія ще не використовує таку технологію, або використовує складний і заплутаний продукт. PRTG можна завантажити з сайту у вигляді абсолютно безкоштовною тест-версії, яка буде працювати протягом 30 днів (без обмеження кількості сенсорів).

РОЗДІЛ 3. ПОРЯДОК РОЗРОБКИ ТА РОБОТИ ПІДСИСТЕМИ ЖУРНАЛЮВАННЯ

3.1. Простий протокол управління мережею

Простий протокол управління мережею (SNMP) - це набір стандартів, до яких використовується обмін інформацією про управління між SNMP-менеджером (сервером) та агентами (керовані пристрої) у мережі TCP / IP (рис. 3.1). SNMP в основному використовується для моніторингу підключених пристроїв, але він також може бути використаний як інструмент віддаленої конфігурації для зміни пристрою налаштування з відстані.

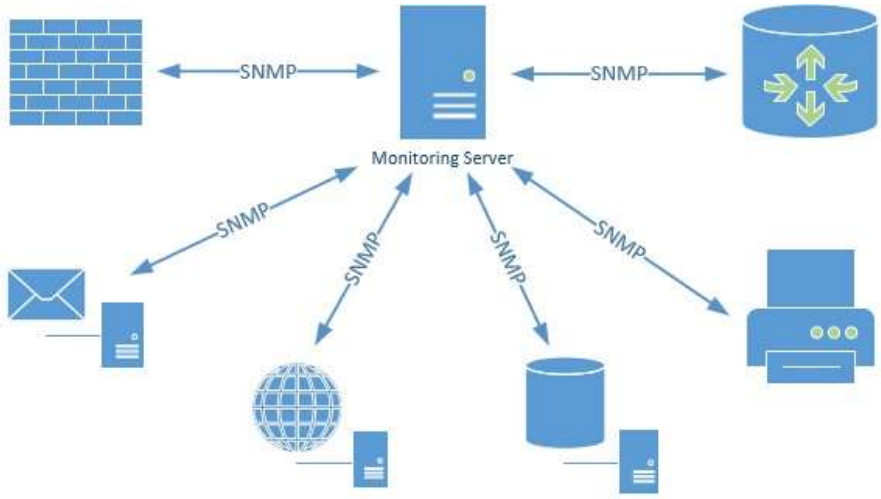


Рис. 3.1. SNMP-сервер, що спілкується з керованими пристроями.

SNMP має три різні версії; v1, v2c і v3. Версія 1 була визначена в 1988 рік, і в даний час він не використовується широко через відсутність кібербезпеки. Версія 2 є розширена версія і використовується в цій тезі. Ця версія використовує рядок спільноти як пароль між підключеними пристроями і може безпечно використовуватися в внутрішньомережевих і закритих мережах. SNMP v3 додає більше безпеки, але це також створює більше складності. Версія 3 є рекомендується використовувати загальнодоступні мережі, такі як Інтернет.

SNMP використовує зв'язок клієнт-сервер між пристроями; програмне забезпечення для моніторингу (клієнт) посилає пакет UDP на сервер SNMP, який взамін надсилає пакет SNMP як а відповідь. Цей обмін даними забезпечує результат від клієнтського пристрою, використання оперативної пам'яті або

завантаження процесора. Використовуючи програмне забезпечення для моніторингу, ця інформація візуалізується у читаному для людини форматі.

Інструментарій управління Windows

Windows Management Instrumentation (WMI) - це протокол Microsoft для управління системи на базі Windows. Він забезпечує широкий моніторинг та віддалене керування для комунікаторів під управлінням операційної системи Windows. Все можна контролювати і змінювати на цільовому комп'ютері, використовуючи вхідні облікові дані (ім'я користувача та пароль).

Веб-управління підприємством

Веб-управління підприємством (WBEM) - це набір специфікацій, що визначають, які ресурси можуть бути відкриті або доступні за допомогою загальної інформаційної моделі. Це використовується для уніфікації управління розподіленими обчислювальними середовищами. Датчики на базі WBEM, розгорнуті для контролю апаратної інформації ESXi сервер, за допомогою WBEM.

Простий протокол доступу до об'єктів

Простий протокол доступу до об'єктів (SOAP) - це протокол, який використовується для обміну інформацією в комп'ютерних мережах. SOAP використовує спосіб кодування запитів і на основі XML Відповіді в середовищі клієнт-сервер. У цьому проекті були датчики SOAP, які використовується для передачі даних віртуальної машини від ESXi до PRTG.

Протокол зв'язку між комутаторами

Два Fortiswitches пов'язані між собою за допомогою Inter-Switch Link (ISL). ISL - це власний протокол Cisco для підключення декількох комутаторів та обслуговування Інформація про VLAN Протокол також забезпечує повноцінні можливості транкінгу VLAN продуктивність швидкості проводів. Коли мережевий трафік проходить через інтерфейс ISL, оригінал - кадр інкапсульований, і додається додатковий заголовок. На приймальному кінці заголовок видаляється, і кадр пересилається до призначеної VLAN. ISL використовує Per VLAN Spanning Tree (PVST), яке використовується для

оптимізації розміщення кореневих комутаторів для кожної VLAN та запобігання створенню нескінченного циклу. ISL також дозволяє балансування навантаження VLAN між двома комутаторами. Якщо один з вимикачів вийшов з ладу, інший вимикач продовжить працювати без будь-яких збурень в мережі.

Топологія та те, як обидва Fortiswitches підключені до кожного з брандмауерів за допомогою Порти SFP в комутаторі та оптичний кабель, показані на рисунку 3.2.

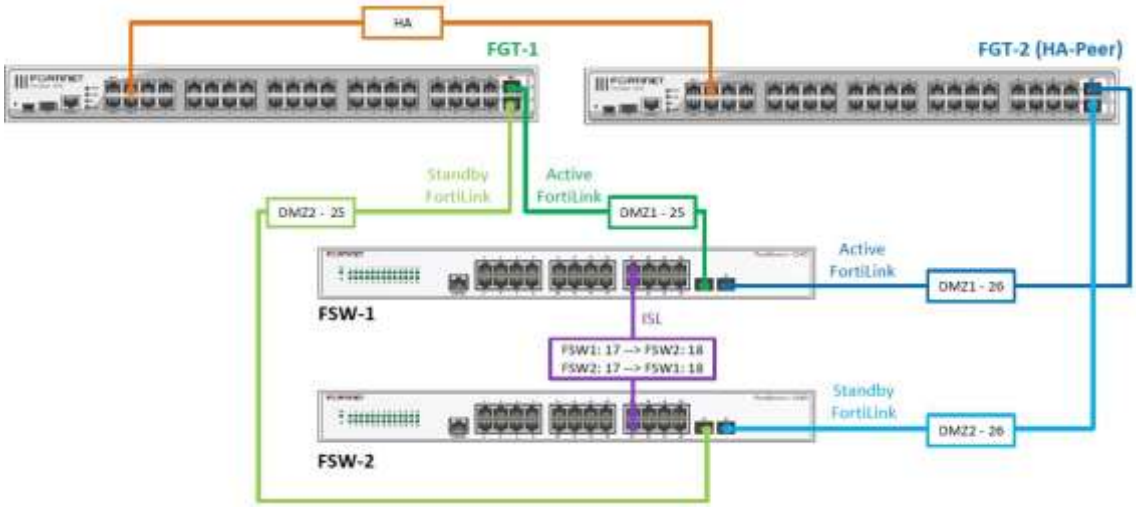


Рисунок 3.2 HA-режим «Увімкніть двома перемикачами».

Агрегація посилань 802.3ad

У міжмережевими екрані Fortigate зв'язок між міжмережевими екранами і комутаторами створюється з використанням агрегації каналів 802.3ad і її протоколу управління Протокол управління агрегацій каналів (LACP). Це протокол управління для об'єднання декількох фізичних посилань у єдине логічне посилання. Це дає можливість надмірності та збільшує потенційну пропускну здатність Між пристроями. Коли використовується LACP, мережевий трафік розподіляється між фізичними портами в каналі, що підвищує продуктивність. Члени фізичного інтерфейсу dmz1 і dmz2 знаходяться в міжмережевим екрані Fortigate, як показано на рисунку 3.3.

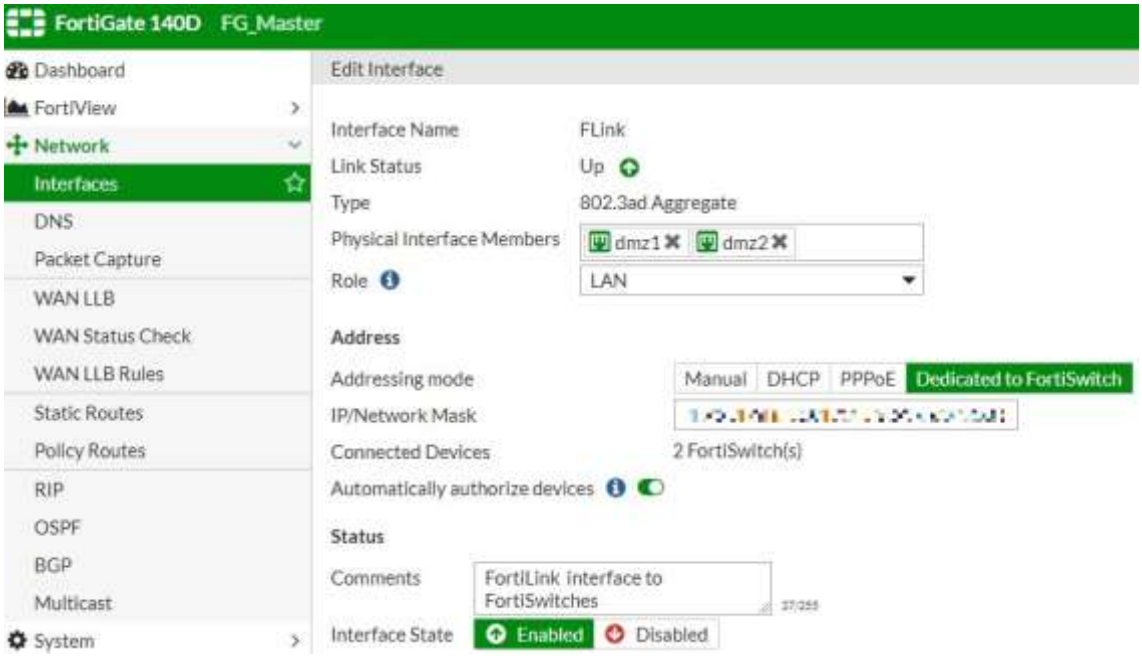


Рис. 3.3. Інтерфейс агрегації 802.3ad у графічному інтерфейсі Fortigate.

Вбудований контролер віддаленого доступу Dell

Вбудований контролер віддаленого доступу Dell (iDRAC) вбудований у кожен Dell Pow-Сервер erEdge, що використовується в схемі. Це дозволяє системним адміністраторам оновлювати, контролювати та підтримувати сервери без додаткового програмного забезпечення для управління системами. Як вбудовано на серверах, він не потребує додаткових операційних систем або гіпервізорів для роботи. Dell Сервери оснащені певними мережевими портами iDRAC, до яких може отримати доступ будь-який комп'ютер за допомогою стандартного мережевого кабелю. Причина, чому ця функція використовується в цьому дипломі полягає у його простоті отримання апаратних даних із сервера. Використовуючи iDRAC, адміністратори можуть бачити всі апаратні вимірювання (температура, процесор, використання оперативної пам’яті тощо) з GUI iDRAC.

Монітор мережевої трафіку Paessler Router

Мережевий монітор PRTG (надалі - PRTG) - це "всеєдина мережа"

Програмне забезпечення для моніторингу дозволяє системним адміністраторам контролювати та діагностувати IT-інфраструктуру швидко та

ефективно. Для аналізу мережевого трафіку PRTG використовує переважно SNMP, аналіза́тор тра́фіку, WMI та NetFlow .

Саме програмне забезпечення - це програма на базі Windows, яка встановлюється на Dell PowerEdge сервер, на якому працює 64-розрядна операційна система Windows Server 2012. Як основна причина для інструментом мережевого моніторингу повинен був відслідковувати та діагностувати HMI, PRTG встановлений на автономному сервері без будь-яких інших віртуальних машин, що працюють на тій же самій платформі. Він також матиме власну підмережу та VLAN з політикою брандмауера, створеної в закріпленому списку політики брандмауера. На рисунку 3.4 пояснено сегментацію, використану в цій тезі.

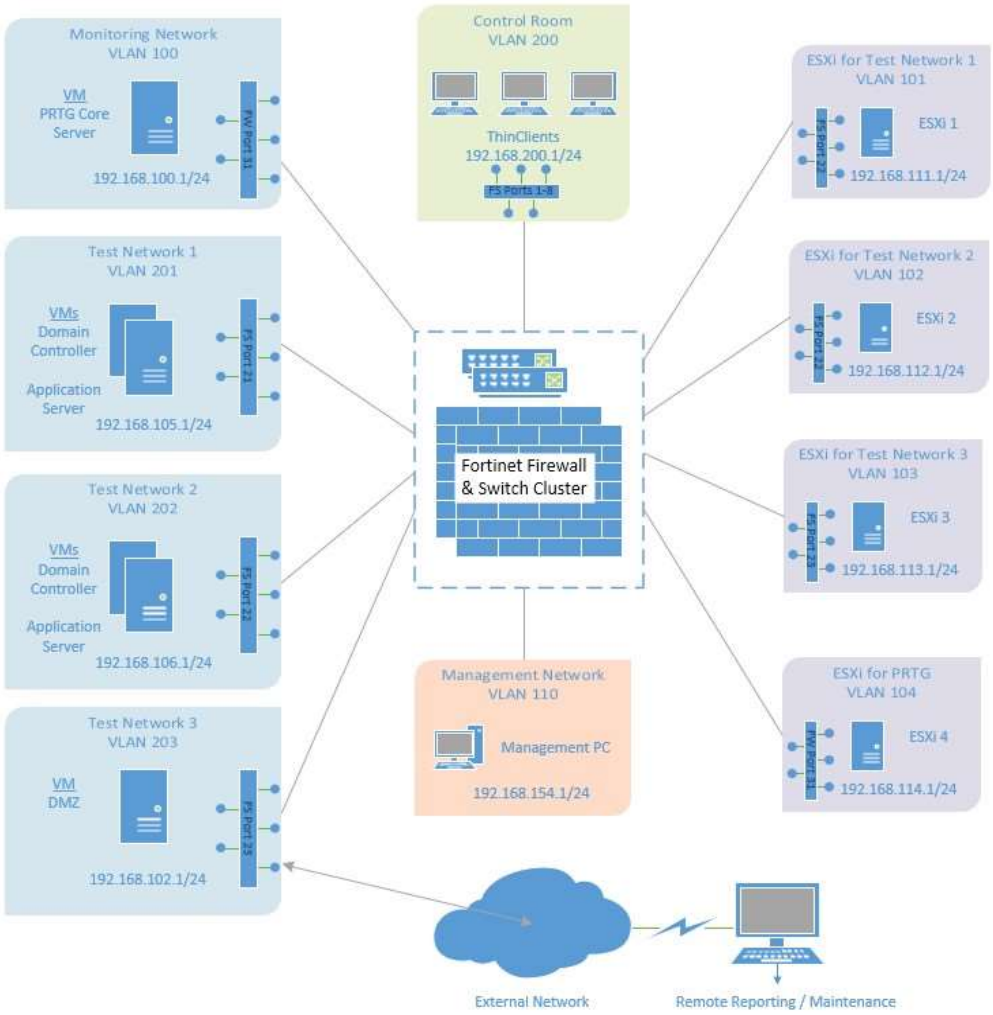


Рис.3.4. Сегментація мережі.

Операція PRTG

Основним компонентом PRTG є основний сервер. Інсталятор Windows встановлює ядро послуги PRTG, до якої також входить веб-сервер. Це дозволяє системним адміністраторам використовувати програмне забезпечення з веб-інтерфейсу за допомогою браузера. PRTG також пропонує можливість використовувати свою корпоративну консоль, яка є рідною програмою Windows, або мобільні додатки для Android, iOS, Windows Phone та Blackberry. У дипломі всі конфігурації тестування проводяться за допомогою веб-інтерфейсу (рис. 3.6).



Рис.3.5. Домашній екран веб-інтерфейсу PRTG.

Операційна модель PRTG показана на рисунку 3.7. Основний сервер посилає SNMP, ping або запити WMI до мережевих пристроїв, якщо підключений пристрій налаштовано на відповідь, вони надсилають відповідь PRTG, яка потім візуалізує результат у веб-інтерфейсі (рис. 3.7).

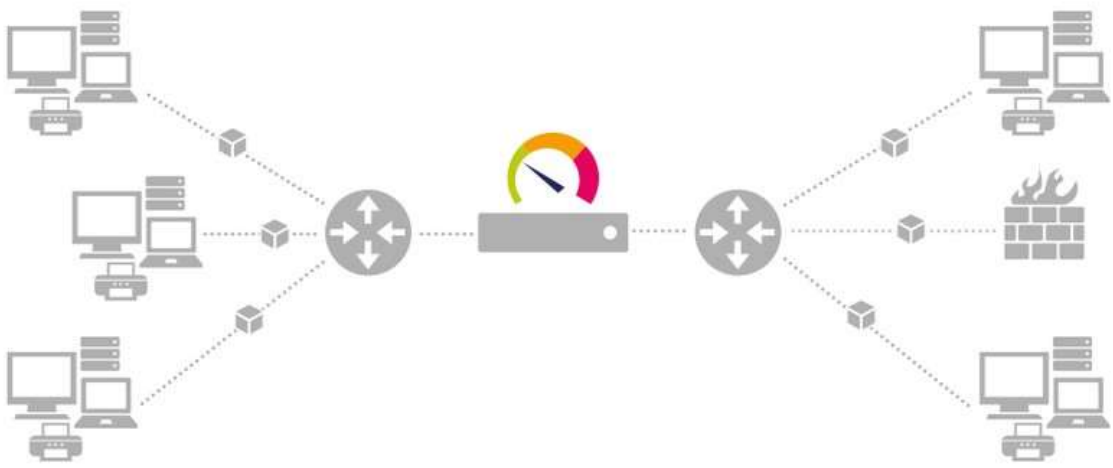


Рис. 3.6. Діюча модель PRTG .



Рис. 3.7. Закріпити датчик SNMP стану здоров'я брандмауера.

Датчики PRTG

Під час використання PRTG дуже важливо зрозуміти поняття датчика. Датчики є основними елементами моніторингу в PRTG, а один датчик контролює конкретний аспект пристрою. Датчики далі поділяються на канали, як показано на рисунку 3.8. Датчик “Fortigate HA Member / FG140D” має 4 канали; Використання процесора, використання пам'яті, сеанс Підрахунок та стан синхронізації, які об'єднані в один датчик. Цей датчик входить до складу файл інформаційної бази управління Fortigate (MIB), до якого можна завантажити PRTG. Використання спеціальних MIB-файлів для завантаження датчиків у PRTG може зберегти кількість датчиків, необхідних для створення. Це стає важливим при переході з пробної версії PRTG до ліцензованої версії.

3.2. Вимоги Технічні умови

Цей диплом був розпочатий для формування вимог специфікації проекту. Вимоги були розділені на три різні групи як показано в таблицях 3.1, 3.2 і 3.3.

Таблиця 3.1

Необхідні функції програмного забезпечення

Функції	Опис	Пріоритет
F1	Виявлення апаратних збоїв	1

F2	Читання стану системи віртуальної машини (ESXi)	2
F3	Збір стану апаратної системи (увімкнено / вимкнено)	2
F4	Основна звітність	2
F5	Оповіщення оператора WOIS про несправності HW / SW / Network	3
F6	Моніторинг Fortinet / syslog / SNMP	2
F7	Моніторинг обладнання (процесор, оперативна пам'ять, темп, RAID)	2
F8	Моніторинг ДБЖ (Eaton)	2
F9	Моніторинг порту iDRAC (бажано ESXi)	3

Таблиця 3.2

Зовнішній інтерфейс. Посилання на те, як система взаємодіє з іншими системами

Посилання	Опис	Пріоритет
I1	Веб-інтерфейс / програмний інтерфейс GUI	1
I2	Віддалений доступ до програмного забезпечення для моніторингу системи	1
I3	Інтерфейс до системи моніторингу клієнтів	3

Таблиця 3.3

Інші характеристики, необхідні для вибраного програмного забезпечення для моніторингу

Характеристики	Опис	Пріоритет
Корисність	GUI повинен бути простим в експлуатації	2
Безпека	Керувати системою може лише уповноважений персонал	1
Ціна	Доцільні варіанти ціноутворення / безкоштовна пробна версія	2
Виявлення помилок	Оператор може легко виявити помилки	1
Сегмент	Новий мережевий сегмент	1

Обладнання	Нове обладнання для системи моніторингу (сервер)	1
Мережа	Моніторинг мережевого трафіку (SNMP / NetFlow…)	2
Масштабованість	Можливість поширити моніторинг на більш високий рівень	3
Прошивка програмного забезпечення	Опція для віддаленого оновлення	2

PRTG Network Monitor був обраний для тестування на основі цих вимог та Сумісність PRTG має з існуючими мережевими пристроями в (Fortigate, Dell Сервери, ESXi). Інші варіанти програмного забезпечення також розглядалися, але були відкинуті в програмі процес тестування PRTG завдяки чудовим властивостям PRTG.

3.3. Мережа

Планування нового мережевого сегменту для програмного забезпечення для моніторингу. Це також вимагало планування нових правил брандмауера, призначення портів і маршрути, що застосовуються в конфігурації Fortigate (рисунки 10 і 11). IP-адреси і VLAN-ідентифікатори, використані в цьому документі, не співвідносять ті, які використовуються у виробництві.

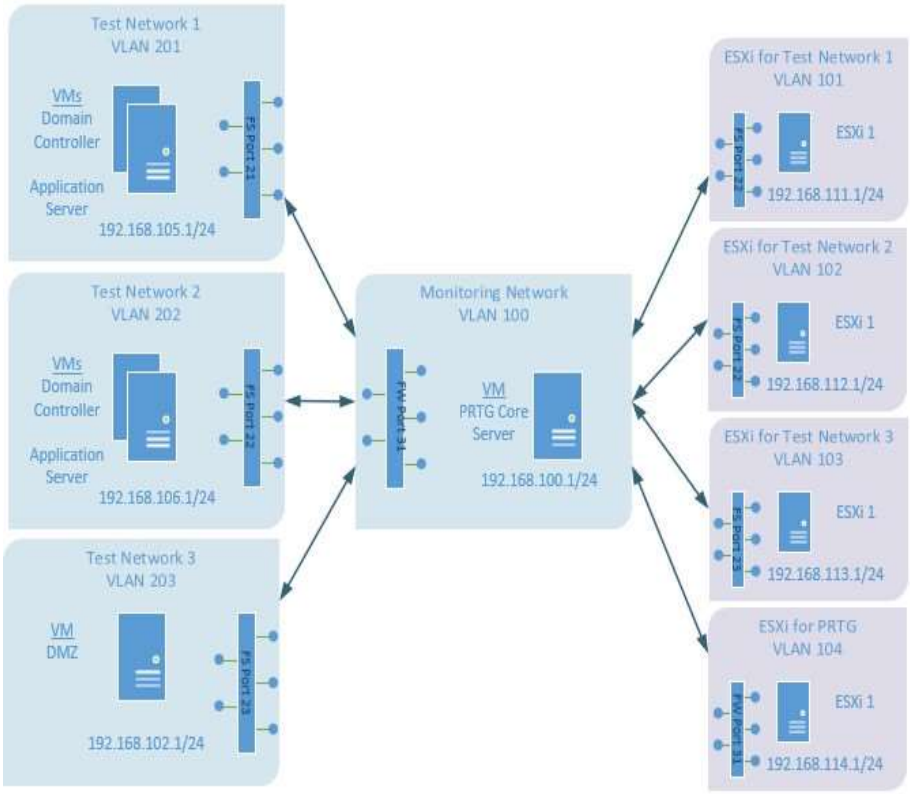


Рис.3.8. Мережеві сегменти та маршрути, створені в конфігурації Fortigate.

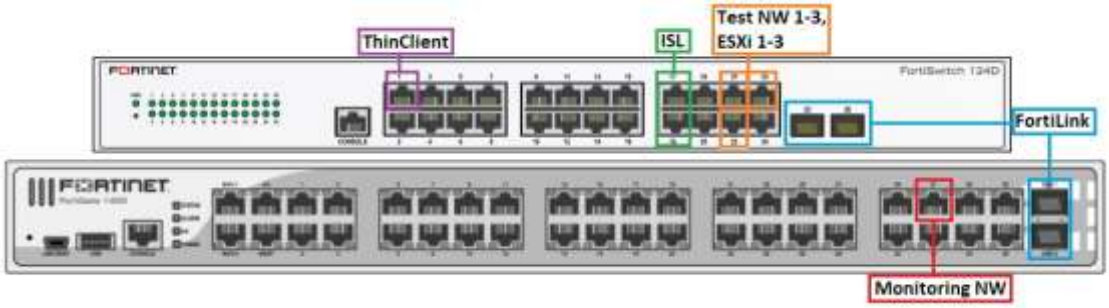


Рис.3.10. Призначення портів Fortigate та Fortiswitch.

Обладнання, яке надалі використовується для основного сервера PRTG у виробничому середовищі рішення, оскільки воно ще не є частиною за замовчуванням. У цій тезі ядро на сервер Dell T630 встановлено настільний сервер під керуванням Windows Server 2012 64-бітова операційна система.

3.4. Впровадження

Для успішного тестування рішення мережевого моніторингу - тестова версія налаштування довелося налаштувати за допомогою компонентів та пристроїв, пояснених у цьому розділі.

3.4.1. Обладнання

У таблиці 3.4 перераховано все обладнання, яке використовується в тестовому середовищі, крім мережевих кабелів.

Таблиця 3.4

Комплектуючі до апаратних компонентів

Пристрій	Операційна система	Додаткова інформація
Fortiswitch брандмауер 140D	FortiOS 5.4, build1138	2х брандмауері в кластері HA
Fortiswitch 124D	S124DN-v3.6.2-build382	2х вимикачі в ISL
Dell PowerEdge T630	Windows Server2012 R2	ESXi, основний сервер PRTG
Dell PowerEdge R430	Windows Server2012 R2	ESXi, Тестова мережа 1
Dell PowerEdge R430	Windows Server2012 R2	ESXi, Тестова мережа 2
Dell PowerEdge R420xr	Windows Server2012 R2	ESXi, Тестова мережа 3
HP Z440	Windows 10	Управління ПК

3.4.2 Брандмауер Fortigate 140D

Основним компонентом мережі є брандмауер Fortigate 140D. Він використовується для створення політики брандмауера між мережевими сегментами для маршрутизації мережевого трафіку, а також блокує та записує будь-які несанкціоновані з'єднання. Брандмауер можна налаштувати за допомогою графічного інтерфейсу користувача (GUI), інтерфейсу командного рядка (CLI) або програмного забезпечення FortiExplorer, підключившись до USB-порту пристрою. Ця документація використовує лише графічний інтерфейс.

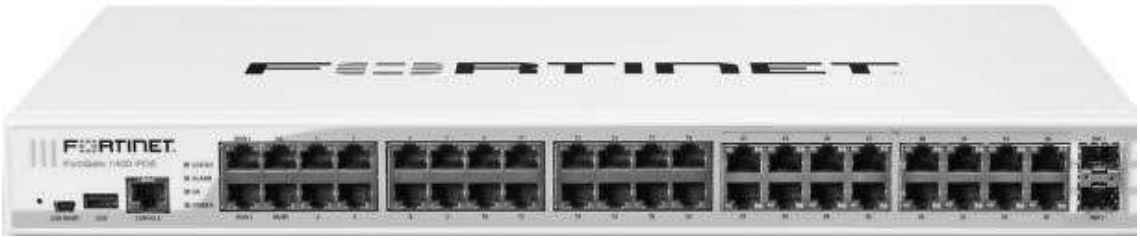


Рис.3.11. Брандмауер Fortigate 140D

3.4.3. Fortigate кластер високої доступності

Використовуючи два з цих брандмауерів, вони утворюють кластер із високою доступністю (згодом - HA) для підвищення надійності мережі. Основна мета використання кластеру HA - надмірність; якщо одна несправність брандмауера або перезавантажується, інша брандмауер займе своє місце, не викликаючи цього будь-який час простою в мережі. Два брандмауера працюють в активно-пасивному режимі, який означає, що лише одна з брандмауерів активно маршрутизує мережевий трафік, а інша залишається простоювати.

Щоб сформувати кластер HA, міжмережеві стіни з'єднані за допомогою кабелю Ethernet RJ-45 у своєму HA порти та параметри кластера встановлюються на обох брандмауерах (назва групи, пароль та пристрій, пріоритет). У цій конфігурації порти високої доступності також встановлюються в якості інтерфейсів сигналу в налаштуваннях Fortigate (рисунок 3.11).

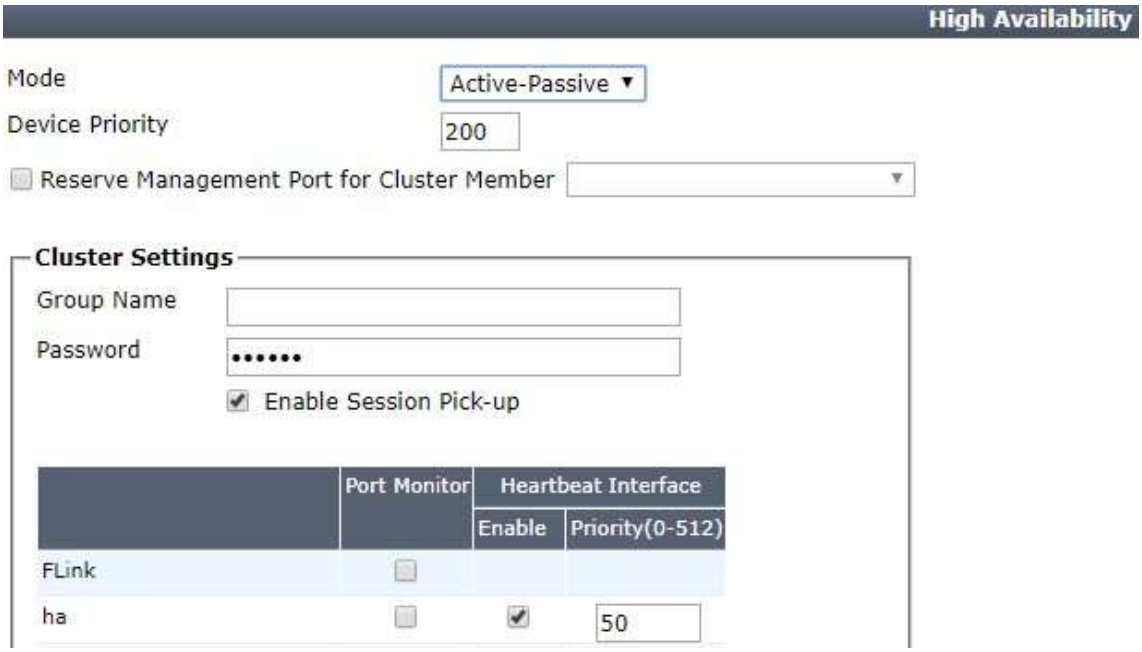


Рис.3.12 Fortigate налаштування кластера з високою доступністю.

Інтерфейс послідовного сигналу використовується між двома брандмауерами для опитування один одного - якщо він активний, брандмауер перестає реагувати на режим очікування, їх ролі перемикаються, не викликаючи жодної значні простої. Можна також додати більше одного інтерфейсу послідовного сигналу, якщо потрібно, але ця конфігурація не використовує додаткових портів для моніторингу HA. Після редагування параметрів та підключення кабелю HA, Fortigate автоматично формує кластер HA, використовуючи протокол кластеризації Fortigate (FGCP). Рисунок 3.13 відображає інформацію про систему Fortigate із синхронізованим кластером HA.



Рис.3.13. Успішно створений кластер Fortigate High Availability.

3.4.4. Fortigate мережеві інтерфейси

Кожен пристрій або підмережа потребує власного мережевого інтерфейсу в брандмауері Fortigate або Fortiswitch. Один фізичний порт в брандмауері або комутаторі може містити кілька логічних інтерфейсів або підмереж. Огляд мережевих інтерфейсів у графічному інтерфейсі Fortigate(показано в Рис. 3.14).

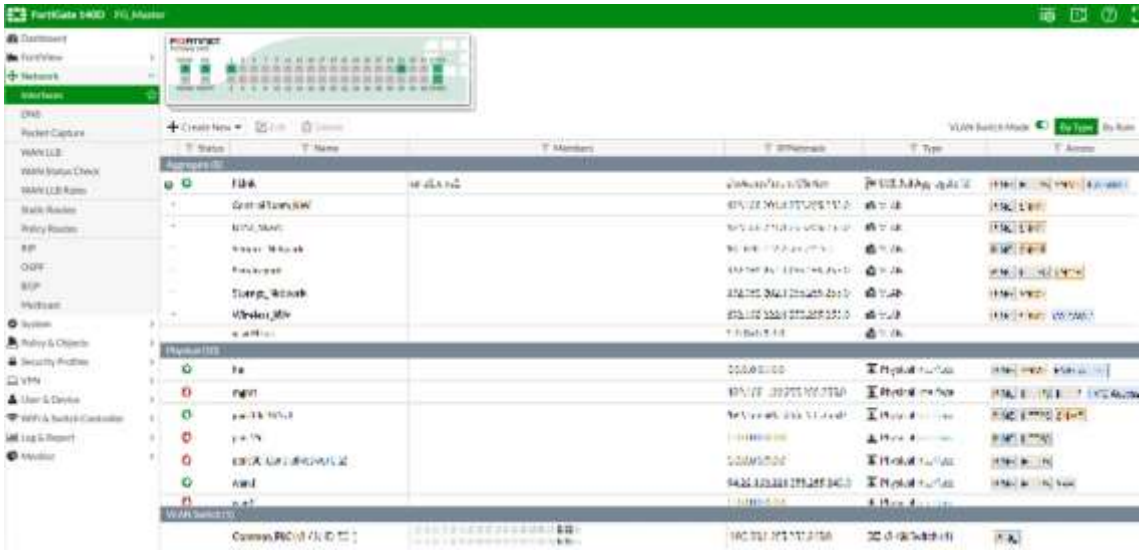


Рис.3.14. Fortigate мережеві інтерфейси.

Таблиця 5 визначає IP-адреси та мережеві сегменти, використовувані в ця теза (із зміненими IP-адресами та ідентифікаторами VLAN).

Таблиця 3.5

IP-адреси та мережеві сегменти

Мережевий сегмент	IP-адреса	Ідентифікатор VLAN	інформація
Моніторинг СЗ	192.168.100.1/24	100	Основний сервер PRTG
Тест NW 1	192.168.105.1/24	201	Два ВМ, IIS
Тест NW 2	192.168.106.1/24	202	Два ВМ, IIS
Тест NW 3	192.168.102.1/24	203	DMZ VM
Управління NW	192.168.153.1/24	110	Управління ПК
ESXi 1	192.168.111.1/24	101	ESXi для тесту NW1
ESXi 2	192.168.112.1/24	102	ESXi для тесту NW2
ESXi 3	192.168.113.1/24	103	ESXi для тесту NW3
ESXi 4	192.168.113.1/24	104	ESXi для PRTG
InTouch NW	192.168.200.1/24	200	ThinClient

Усі інтерфейси створюються за допомогою графічного інтерфейсу Fortigate. Системні адміністратори можуть створювати або модифікувати інтерфейси, як показано на рисунку 3.15.

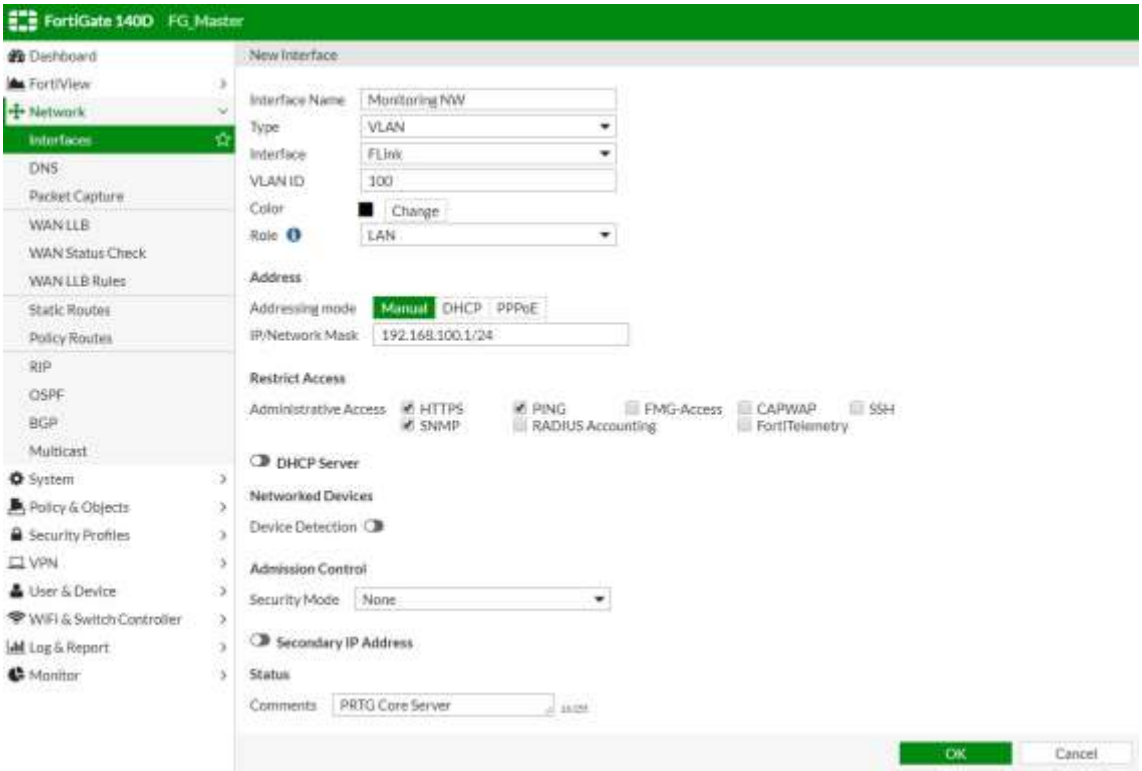


Рис.3.15. Створення нового інтерфейсу в графічному інтерфейсі Fortigate.

3.4.5. Посилення політики брандмауера

Політика брандмауера використовується для маршрутизації трафіку між мережевими сегментами, і вона є основною функція брандмауера Fortigate. Це також дає можливість адміністраторам мережі вказати протоколи, VLAN або послуги, яким дозволяється проходити через мережу. Нове створення політики відображається на рисунку 3.16.

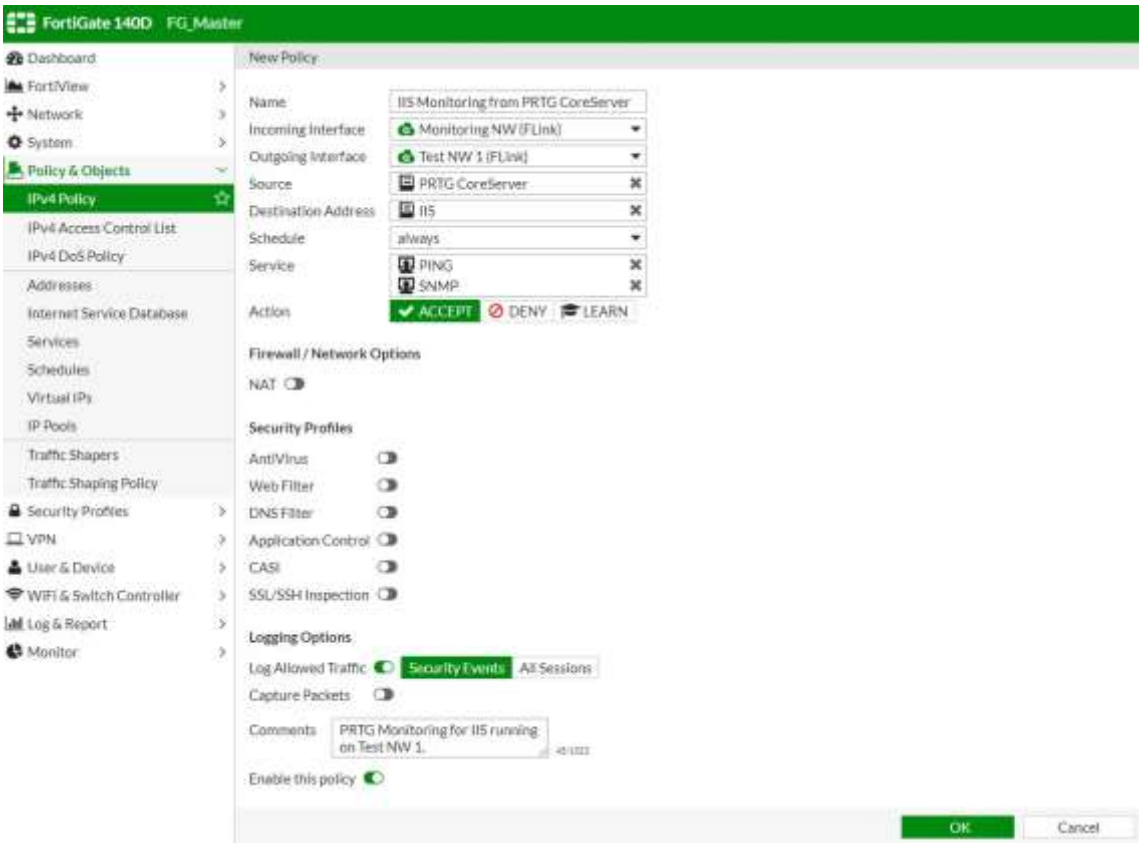


Рис.3.16.Політика брандмауера для моніторингу IIS від основного сервера PRTG до тестування NW 1 з використанням SNMP.

3.4.6. Увімкніть конфігурацію SNMP, NetFlow та Syslog

Крім політики брандмауера, для того щоб увімкнути SNMP, спільнота SNMP v2c повинна бути налаштованим у Fortigate. Використовувані налаштування відображені на рисунку 3.17.



Рис.3.17. Fortigate параметри спільноти SNMP.

Щоб дозволити спілкування в мережі між пристроями, застосовуються нижче наведені налаштування:

- IP-адреса / мережева маска
  - o Це IP основного сервера PRTG
- Порт протоколу
  - o Порт 161 використовується у всіх мережевих пристроях для спілкування за допомогою SNMP
- Події SNMP
  - o Різні події з Fortigate надсилаються до PRTG

NetFlow - це функція, яка надає можливість збирати мережевий трафік IP під час входу або виходить з інтерфейсу. У PRTG цей трафік можна візуалізувати для визначення джерела та місце руху транспорту, тип послуги та причини збоїв. Щоб увімкнути цю функцію у Fortigate конфігурацію, потрібно виконати для кожного інтерфейсу окремо за допомогою CLI. Інформація NetFlow експортується з вихідного пристрою за допомогою протоколу User Datagram (UDP) та збирається за допомогою колектора (в даному випадку PRTG). Пристроєм відправки є Fortigate Firewall, який використовує стандартний порт UDP NetFlow 2055. Команди CLI використовується для включення функції NetFlow у Fortigate, перераховані нижче.

Налаштування IP NetFlow Collector:

config system netflow

set collector-ip <ipv4_addr>

set collector-port <port_int>

end

Увімкнення NetFlow на інтерфейсі

config system interface

edit <interface name>

set netflow-sampler both

end

До цього проекту було додано Syslog для отримання повідомлень про події в PRTG. Сам Syslog, як ми вже розбирали в першому розділі дипломної роботи - це протокол, який використовується мережевими пристроями для передачі інформації на сервер syslog (у цьому випадку PRTG). Щоб дозволити Fortigate пересилати ці повідомлення, наступне оновлення було налаштовано в параметрах журналу брандмауера (Рис.3.18):



Рис.3.18. Надсилання журналів на сервер системного журналу PRTG з Fortigate.

IP-адреса сервера syslog - це базовий сервер PRTG.

3.4.7. Fortiswitch 124D



Рис.3.19. Fortiswitch 124D.

Fortiswitches використовуються в цій роботі для додавання більше фізичних портів для підключених пристроїв в більший виробничий об'єкт, кількість необхідних мережевих портів може перевищувати 50, залежно розрахована на кількість двигунів та допоміжних систем.

Крім фізичної установки Fortiswitch, все управління та конфігурація виконуються в графічному інтерфейсі Fortigate. У Fortiswitches є власні GUI та CLI, але не рекомендується використовувати ці функції, поки вони знаходяться під пультом Fortilink контроль.

На рисунку 3.20. відображені зелені кольори всіх активних портів Fortiswitches. Порти 17 і 18 є вхідними з'єднані порти ISL.

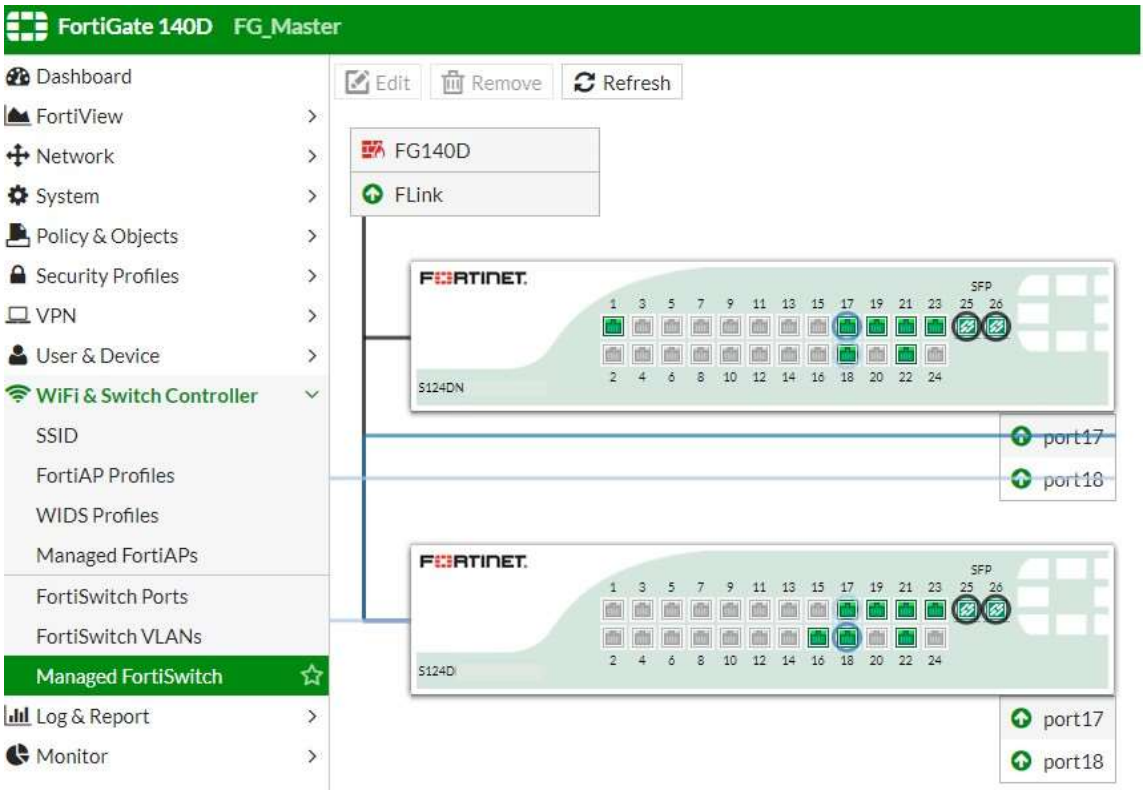


Рис.3.20. Керування Fortiswitches від графічного інтерфейсу Fortigate.

3.4.8. Сервери Dell PowerEdge

Цей проект використовує сервер PowerEdge Dell як апаратне забезпечення для віртуальних машин. Таблиця 3.6 відображає технічні характеристики пристроїв.

Таблиця 3.6

Сервери Dell PowerEdge

Модель	Процесор	ОЗП	Жорсткий диск
R430	2 процесора x Intel (R) Процесор Xeon (R) E5-2620 v4 @ 2,10 ГГц	64 Гб	1,09 ТБ
R430	2 процесора x Intel (R) Процесор Xeon (R) E5-2620 v4 @ 2,10 ГГц	64 Гб	1,09 ТБ
R420xr	Intel (R) Xeon (R) Процесор E5-2430 v2 @ 2,50 ГГц	16 ГБ	745 Гб
T630	2 процесора x Intel (R) Процесор Xeon (R) E5-2623 v3 @ 3.00GHz	32 Гб	1,09 ТБ

3.4.9. Конфігурація сервера PRTG Core

Програмне забезпечення PRTG було встановлено на сервері Dell PowerEdge T630 під управлінням Windows 64-розрядна операційна система Server 2012 R2. Інсталятор Windows доступний на PRTG веб-сайт і не потребує додаткової конфігурації до або під час встановлення процедури. Під час встановлення PRTG налаштовує всі необхідні компоненти програмного забезпечення для запуску програмного забезпечення, включаючи веб-сервер для доступу до веб-графічного інтерфейсу, базу даних для зберігання та Enterprise Console, що використовується як рідний додаток для Windows.

Після завершення інсталяції доступ до PRTG можна отримати за допомогою браузера (Google Chrome 61 або новішої версії, Mozilla Firefox 56 або новішої версії або Microsoft Internet Explorer 11) від адреса localhost 127.0.0.1, порт 8080, як показано на рисунку 3.21.



Рис.3.21. Доступ до веб-інтерфейсу PRTG.

Після установки основний сервер PRTG створює локальний зонд, який використовується для моніторингу локальної мережі. Зонди PRTG - це компоненти, які здійснюють фактичний моніторинг. У цьому випадку, оскільки мережа не відкрита для Інтернету, використовується лише локальний зонд. Також можливо відстежувати різні місця та мережі за допомогою одного основного сервера та декількох віддалених зондів, які повідомляють і надсилають дані на основний сервер. Місцевий зонд має власні вбудовані датчики, які створюються при першій установці (рис. 3.22). Ці датчики, як і будь-які інші датчики в PRTG, можуть бути змінені або видалені.



Рис.3.22. Місцеві датчики зонду створюються автоматично.

Під час першого входу системним адміністраторам також пропонується змінити вхід за замовчуванням повноваження. Це стає важливішим, якщо основний сервер піддається впливу Інтернету, щоб запобігти будь-яким несанкціонованим спробам входу.

3.4.10. Конфігурація пристроїв PRTG

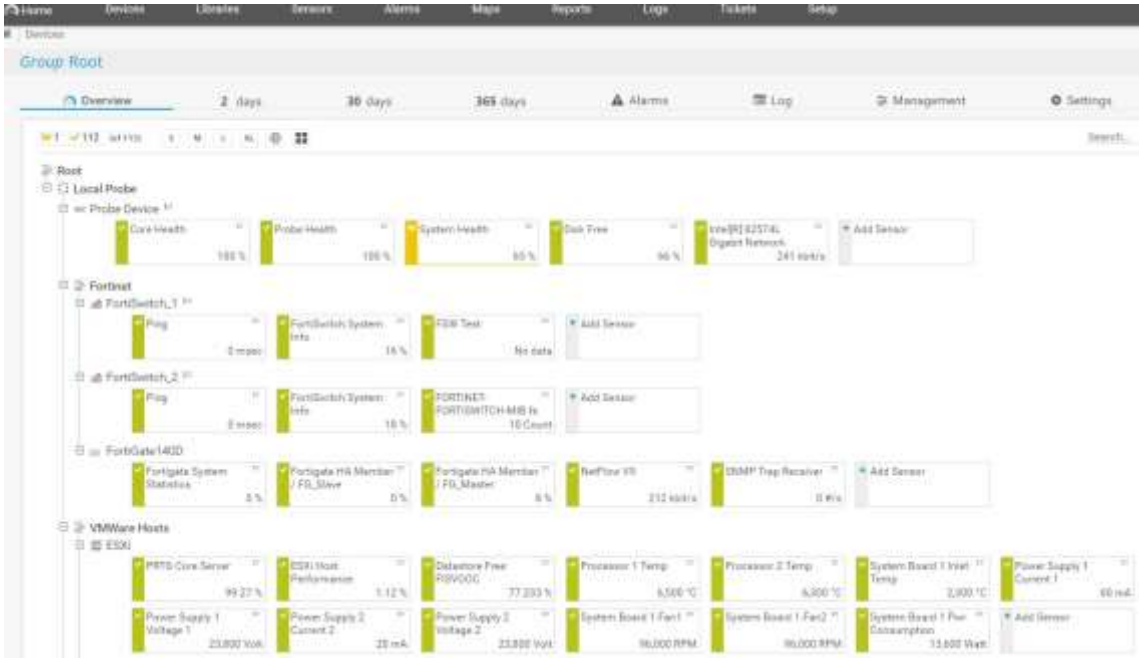


Рис.3.23. Меню пристроїв веб-інтерфейсу PRTG.

Програмне забезпечення має функцію автоматичного виявлення, яка дозволяє користувачам автоматично додавати мережеві пристрої в PRTG, якщо вони підключені і відсутні правила брандмауера, що блокують доступ. Ця функція, а також автоматичне виявлення для датчиків пристроїв не використовувалися під час цього проекту, оскільки вони виявилися неточними для цілей диплома. Всі пристрої і датчики були додані вручну.

Пристрої в PRTG відображаються в деревоподібної ієрархії. При необхідності адміністратори можуть переміщувати пристрої в різні гілки, а при необхідності можна створювати нові гілки. У цій тезі використовується ієрархія, показана на малюнку 3.23.



Рисунок 3.23. Ієрархія дерев PRTG.

Кожний фізичний і віртуальний пристрій буде додано окремо, і їх відповідні датчики відображаються під пристроєм. Перевага використання деревовидної ієрархії полягає в спадкуванні. Коли аналогічні пристрої додаються в філії в PRTG, їх можна налаштувати для наслідування облікових даних SNMP, WMI, VMware або WBEM від їх батьківського пристрою або філії, що, в свою чергу, зменшує кількість повторюваних завдань адміністратора, необхідних під час налаштування.

Щоб додати новий пристрій у PRTG, системні адміністратори можуть клацнути правою кнопкою миші потрібну гілку на панелі перегляду пристроїв та виберіть опцію «Додати пристрій» (рис. 3.26). Це відкриває меню де інформація про пристрій визначена, як показано на рисунку 3.25.

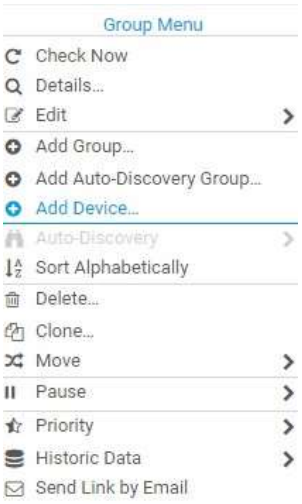


Рис.3.25. Групове меню для додавання нового пристрою до PRTG.

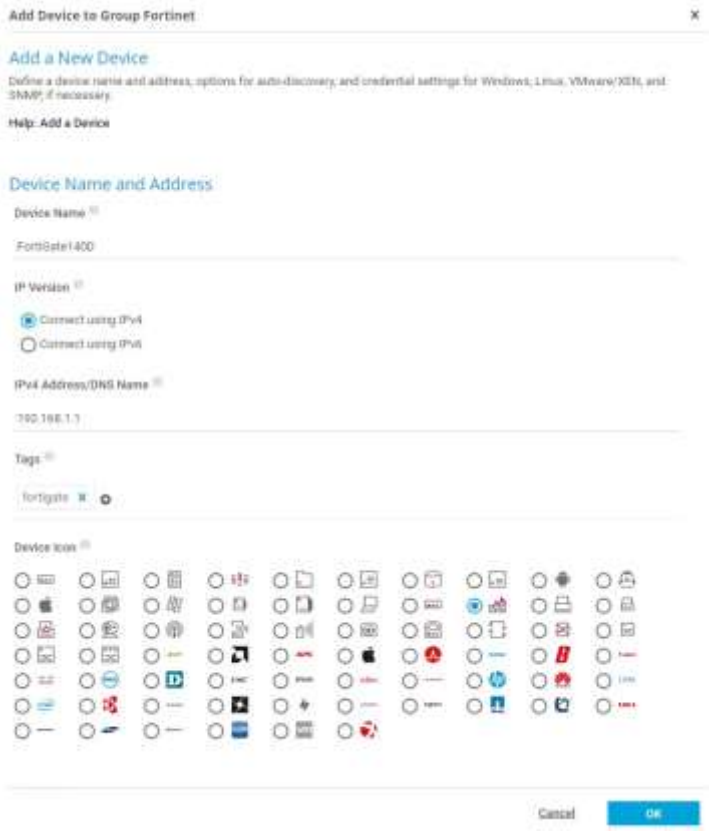


Рис.3.26. Додавання брандмауера FortiGate140D до PRTG.

PRTG має заздалегідь задані параметри датчиків, які можна використовувати для автоматичного створення датчика в програмах для різних пристроїв під управлінням датчиків показана на малюнку вище.

У цьому проекті параметр "Ручний (без автоматичного відкриття") був використаний для додавання лише необхідних датчиків для кожного пристрою. На рисунку 3.26. відображаються також успадковані облікові дані, які

обговорюються в ієрархії. Цей процес додавання пристрою виконано на всіх пристроях використовується в цьому проекті. Хоча PRTG має свою мережеву функцію Discovery, яка створює пристрої автоматично, після невеликого тестування було видно, що він не створює всі потрібні пристрої, і тому їх було простіше додавати один за одним вручну.

3.4.11. Створення датчиків у PRTG

Оскільки датчики є основною складовою процесу моніторингу PRTG, цей розділ в проекті був найбільш трудомістким і вимогливим, а також основна частина проекту теза. Кількість датчиків на пристрої, що використовуються в проекті, коливається між 3 (UPS) та 20 (Сервери) залежно від призначення пристрою. У апаратних серверах це було обов'язково для контролю самого обладнання, ESXi та віртуальних машин, що працюють на ESXi, що призвело до збільшення кількості датчиків.

Початок процесу додавання датчика аналогічно додаванню нового пристрою, за винятком того, що користувач PRTG клацає правою кнопкою миші пристрій, вказане в веб-інтерфейсі користувача, замість батьківської гілки в дереві. Замість того, щоб використовувати функцію автоматичного виявлення PRTG для додавання нових датчиків, все датчики були додані вручну, щоб оптимізувати виміряні значення Коли нові додаються датчики, то вони відображаються в огляді пристроїв з певним кольором вкажіть його стан (табл. 3.7).

Таблиця 3.7

PRTG Датчики стану

Датчик	Колір	Статус	Значення
	Червоний	Вниз	PRTG не в змозі дістатися до пристрою
	Зелений / Червоний	Вниз (частково)	Принаймні один вузол в кластер вниз

	Яскраво-червоний	Вниз (Підтвердження обрізний)	Датчик вниз, визнано Користувач PRTG
	Жовтий	Увага	Помилка читання, але PRTG буде знову
	Помаранчевий	Незвично	Незвичайні значення для цього будня та час доби
	Зелений	Вгору	Останнє сканування було добре, і сенсорт в даний час повторно зберігання даних
	Синій	Призупинено	Датчик в даний момент припинено (на певний час, на невизначений термін, викликаний залежністю)
	Чорний	Невідомо	Дані ще не отримані або сталася помилка в мережі

PRTG має функцію додавання декількох датчиків до пристрою, використовуючи параметри, визначені постачальником або протоколом. На рисунку 3.27 показаний один із апаратних серверів, що використовуються із доданими датчиками.



Рисунок 3.27. Апаратні датчики сервера.

На цьому сервері датчики змінюються від ESXi Host Performance до температури процесора і всі фізичні швидкості вентилятора. Статус віртуальних машин, встановлених на цьому ESXi відображаються на перших двох датчиках у верхньому лівому куті зображення. Коли датчик є, клацнувши в веб-інтерфейсі, доступна більш детальна інформація (рис.3.28.).



Рис.3.28. Датчик стану віртуальної машини.

Цей датчик є одним з датчиків SOAP, доступних у PRTG, він створює кілька каналів від використання процесора до мережевої активності, але він все ще вважається лише одним датчиком. Якщо всі вимірювання додавалися вручну, для цього було б потрібно 14 датчиків, що загалом це може стати проблемою, коли йдеться про вартість PRTG. Оскільки базується ціна PRTG виключно за кількістю використовуваних датчиків, більше сенсорів дорівнює більшій вартості. Використовувані типи датчиків на пристрій, перераховані в таблиці 3.8.

Таблиця 3.8.

Таблиця «Список типів датчиків, що використовуються в цьому проекті»

Пристрій	Типи датчиків	Загальна кількість датчиків
Основний сервер	Рідні датчики PRTG, sysжурнал	6
Fortiswitch_1	SNMP	27
Fortiswitch_2	SNMP	27
Fortigate140D	SNMP, syslog, NetFlow	43
ESXi_1	SOAP, WBEM	25
ESXi_2	SOAP, WBEM	25
ESXi_3	SOAP, WBEM	21
ESXi_4	SOAP, WBEM	14

VirtualServer_1	SNMP, WMI	9
VirtualServer_2	SNMP, WMI	9
VirtualServer_3	SNMP, WMI	3
VirtualServer_4	SNMP, WMI	3
VirtualServer_5	SNMP, WMI	2

3.4.12. Визначення значень порогу та сигналізації датчиків

Щоб отримати максимальне значення від використання інструменту моніторингу мережі, в PRTG додаються порогові значення і аварійні сигнали, щоб мати можливість реагувати на несправності навіть до того, як вони виникнуть. Ці значення додаються до окремих датчикам і їх каналам вручну, щоб отримати повідомлення, коли датчик передає значення за межі визначених безпечних меж. Коли значення перевищують або перевищують його обмеження протягом певного періоду часу, повідомлення електронної пошти є надіслано адміністратору PRTG. Буфер часу додається до порогу, щоб уникнути помилки тривоги. Наприклад, пристрій перезавантажується і використовує більш високий процесор і оперативну пам’ять, ніж коли він знаходиться в режимі очікування. Якщо не доданий буфер часу, це призведе до тривоги в PRTG. На рисунку 3.29. визначено пороговий тригер для температури процесора. Якщо температура понад 90 ℃ протягом 60 секунд, адміністратори PRTG отримають сповіщення електронною поштою.

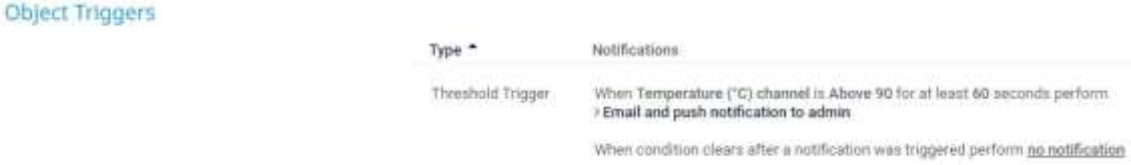


Рис.3.29. Поріг спрацьовування температури процесора.

Подібні тригери також додаються для використання оперативної пам'яті, швидкості вентилятора, використання жорсткого диска та RAID здоров'я. Інші датчики, такі як датчики інтерфейсу в Fortigate, використовують тип вгору або

вниз тривога. Якщо датчик не реагує на PRTG, він спрацьовує тривожною силою, якщо також буде наступне сканування невдале. Тригери також додаються до датчика NetFlow. Якщо використовується конкретний протокол несподіваний обсяг пропускної здатності протягом тривалого періоду, то це може бути результатом збію або перевантаженості мережі, що привертає увагу адміністратора.



Рис.3.30. Тригер доданий до протоколу WWW.

ВИСНОВОК ДО РОЗДІЛУ 3

Після того, як початкова фаза планування проекту була завершена, етапи впровадження та тестування тривали безперервно. Велика частина роботи була виконана на етапі впровадження, так як кількість датчиків в PRTG було вище, ніж передбачалося раніше.

На початку етапу впровадження потрібно налаштувати головний сервер PRTG, оновити конфігурацію брандмауера, щоб вона відповідала нової сегментації мережі, і додати всі датчики в програмне забезпечення для моніторингу, перш ніж можна буде успішно виконати тестування.

Етап тестування почався після завершення налаштування брандмауера і додавання перших датчиків в PRTG. Це було зроблено в основному методом проб і помилок, читаючи вимірювання датчика і знаючи, чого очікувати від результатів датчика. Всі типи датчиків, встановлених в PRTG, були протестовані. Система сигналізації в тому вигляді, як вона є (електронна пошта і push-повідомлення), буде перевірена за підтримки PRTG. Подальший розвиток аварійної сигналізації полягає в реалізації повідомлення для оператора в програмному забезпеченні InTouch і зменшенні кількості повідомлень по електронній пошті, необхідних для системи моніторингу.

ВИСНОВКИ

Метою дипломної роботи було розробити, впровадити та протестувати працюючу мережу розв’язування рішення для Windows. Вибране програмне забезпечення для моніторингу було впроваджено та протестоване в мережі. Нижче наведені основні точки фокусування вимог та те, як вони були виконані у дипломній роботі.

Підсумок проекту (датчики додані та перевірені успішно):

- ✓ Виявлення апаратних збоїв
- ✓ Читання стану системи віртуальної машини (ESXi)
- ✓ Збір стану апаратної системи (увімкнено / вимкнено)
- ✓ Моніторинг мережевого трафіку
- ✓ Моніторинг Fortinet / syslog / SNMP
- ✓ Моніторинг обладнання (процесор, оперативна пам’ять, темп)

Виходячи з результатів, є деякі сфери, які потребують подальшого розвитку, але поточний результат проекту можна вважати успішним. Моніторинг PRTG програмне забезпечення було успішно впроваджено в систему автоматизації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Building Scalable Syslog Management Solutions [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-557812.html#wp9000375.
2. Daumé H. A Course in Machine Learning / Hal Daumé., 2015. – 193 с.
3. Nielsen M. Neural Networks and Deep Learning / Michael Nielsen. – Determanation Press, 2017.
4. Nilsson J. INTRODUCTION TO MACHINE LEARNING / Nilsson., 2003. – 188 с.
5. Журналирование событий на маршрутизаторе Cisco [Електронний ресурс] – Режим доступу до ресурсу: http://www.opennet.ru/base/cisco/cisco_logging.txt.html.
6. Microsoft Windows Server. Повне керівництво / Морімото Автор: Р., Ноел і ін. / Видавництво: «Вільямс».
7. Моніторинг і аналіз мереж. Методи виявлення несправностей / Автор: Ед Вілсон / Видавництво: «Лорі» / Рік випуску: 2002 / К-ть сторінок: 363.
8. Zabbix 1.8 Network Monitoring / Автор: Rihards Olups / Видавництво: «Packt Publishing» / Рік випуску: 2010 / Кількість сторінок: 428
9. Microsoft Download Center [Електронний ресурс] – Режим доступу до ресурсу: http://www.microsoft.com/en-us/download/details.aspx?id=4865
10. Information about Network Monitor 3 - Microsoft Support [Електронний ресурс] – Режим доступу до ресурсу: https://support.microsoft.com/en-us/kb/933741
11. An Overview of the syslog Protocol [Електронний ресурс] – Режим доступу до ресурсу: https://www.ciscopress.com/articles/article.asp?p=426638&seqnum=3
12. Робота з Network Monitor - OSzone.net [Електронний ресурс] – Режим доступу до ресурсу: http://www.oszone.net/5688/Network_Monitor

ДОДАТОК

		Інтерфейс		Джерело	призначення		Сервіси
Індекс	Ім’я	від	до	адреса відправника	IP-адреса призначення	Порт призначення	
32	Монітор - ESXi	Монітор Network	ESXi Зона упавління	192.168.100.100	192.168.113.1, 192.168.113.1, 192.168.112.1, 192.168.111.1	135, 161, 162, 5989, 80, 443	RPC, SNMP, WBEM, HTTP, HTTPS 33
33	Монітор - Test NWs	Монітор Network	Тест NW 1 & 2	192.168.100.100	192.168.105.1/24, 192.168.106.1/24	135, 161, 162, 5989	RPC, SNMP, WBEM
34	Монітор - FortiSwitch	Монітор Network	FortiLink	192.168.100.100	192.168.50.1/24	161, 162	SNMP
35	Монітор - DMZ	Монітор Network	DMZ	192.168.100.100	192.168.102.1/24	135, 161, 162, 5989	RPC, SNMP, WBEM
36	Монітор - iDRAC	Монітор Network	iDRAC	192.168.100.100	192.1686.1/24	161, 162	SNMP