Лабораторна робота №12

Інсталяція Splunk Free, базове налаштування та збір локальних логів.

Мета: Набути практичних навичок встановлення та базового налаштування платформи Splunk Free, навчитися збирати та аналізувати локальні системні журнали Linux і Windows. Ознайомитися з принципами створення індексів, підключення джерел даних та виконання базових пошукових запитів у Splunk Search & Reporting. Засвоїти основи обробки, фільтрації та візуалізації подій для подальшого використання у задачах моніторингу та аналізу безпеки.

Інструменти: гіпервізор VirtualBox, модель комп'ютерної мережі.

Теоретичні відомості

У попередніх лабораторних роботах було створено віртуалізоване стендове середовище у VirtualBox, що складається з трьох хостів:

Serv-G-N-1 (Windows Server 2022) – контролер домену з ролями AD DS, DNS і DHCP. Налаштовано Wazuh Agent для локального моніторингу ресурсів.

Serv-G-N-5 (Ubuntu Server 24.04) – сервер на налаштовано Wazuh Agent для локального моніторингу ресурсів.

Serv-G-N-7 (Amazon Linux 2023) – сервер Wazuh Appliance, що містить компоненти Wazuh Server (Manager, API) та Elasticsearch + Kibana (Dashboard)

Serv-G-N-9 (Ubuntu Server 24.04) – сервер Splunk Free, що буде розгорнутий у цій роботі.

Мережеве середовище забезпечує взаємодію між вузлами з доменною інфраструктурою для подальшого моніторингу її елементів.

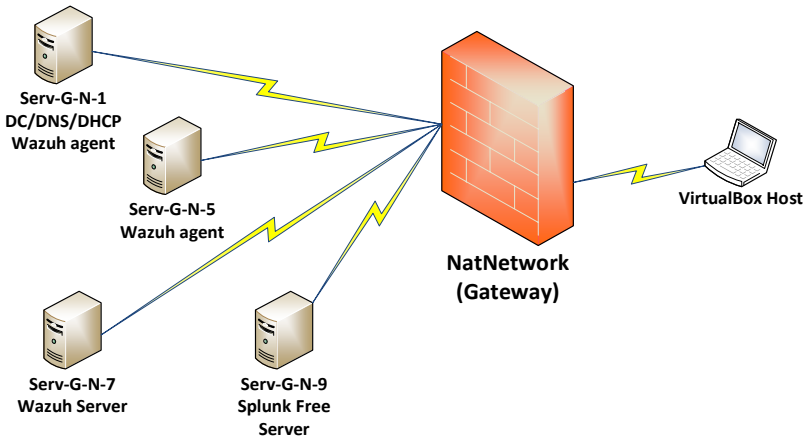

Рис. 12.1. Топологія мережі

Ознайомлення з платформою Splunk Free

Splunk — це потужна платформа для збору, індексації, пошуку та візуалізації машинних даних у режимі реального часу. Вона використовується для моніторингу системної активності, аналізу журналів подій, виявлення інцидентів безпеки та побудови звітів.

Можливі варіанти інсталяції Splunk Free.

Таблиця 12.1.

Метод розгортання	***Короткий опис***	***Переваги***	***Недоліки***
Хмарний (Splunk Cloud Free / Trial)	Доступ через веб-інтерфейс без локальної інсталяції, пробний період 14–30 днів.	Швидкий старт, не потребує ресурсів сервера.	Обмежений термін дії, неможливість підключення локальних джерел логів, немає інтеграції з Wazuh.
Віртуальний аплайнс (OVA)	Попередньо налаштований Splunk для VMware ESXi.	Мінімум ручних дій при встановленні.	Призначений лише для ESXi, проблеми сумісності з VirtualBox.
Локальна інсталяція Splunk Enterprise у режимі Free	Завантаження офіційного пакета .deb та встановлення на сервер Ubuntu.	Повна функціональність, стабільна робота у VirtualBox, підтримка локальних логів і Wazuh, без обмеження часу.	Потребує кількох ручних команд під час інсталяції.

У таблиці 12.1 приведено можливі методи інсталяції Splunk Free. Для виконання лабораторних робіт обрано локальну інсталяцію Splunk Free на сервері Ubuntu Server 24.04 (Serv-G-N-5), оскільки цей метод:

- ❖ забезпечує повний контроль над середовищем і конфігурацією Splunk;
- ❖ дозволяє збирати локальні журнали з /var/log та інших джерел системи;
- ❖ забезпечує можливість інтеграції з Wazuh, який розгорнуто в тій самій NAT-мережі;
- ❖ гарантує стабільну роботу без часових обмежень, на відміну від хмарних або демонстраційних версій;

Основні компоненти Splunk:

- ❖ Indexer – отримує вхідні дані, обробляє їх і зберігає у вигляді індексів.
- ❖ Search Head – забезпечує інтерфейс для пошуку, аналізу та візуалізації даних.
- ❖ Forwarder – агент, що збирає дані з віддалених систем і пересилає їх на Indexer.
- ❖ Deployment Server – централізоване керування налаштуваннями агентів (у розширених конфігураціях).

Splunk Free — це безкоштовна редакція Splunk Enterprise з обмеженням обсягу даних (до 500 МБ/день), але без втрати базового функціоналу. Вона ідеально підходить для навчальних стендів і лабораторних робіт.

Імпорт з аплайнсу та налаштування Serv-G-N-9

Аналогічно процедурі, описаній у одній з попередніх робіт виконуємо імпорт віртуальної машини з аплайнсу Ubuntu сервера, що доступний по лінку
https://drive.google.com/file/d/1zhqVOhGwcXdaHpjuUf7g0a8z8oXqN6kD/view?usp=drive_link
Після імпорту віртуальної машини Serv-G-N-3 (сервер на базі Ubuntu Server) необхідно перейменувати її по шаблону Serv-G-N-9 та перегенерувати MAC-адресу мережевого адаптеру (рис.12.2).

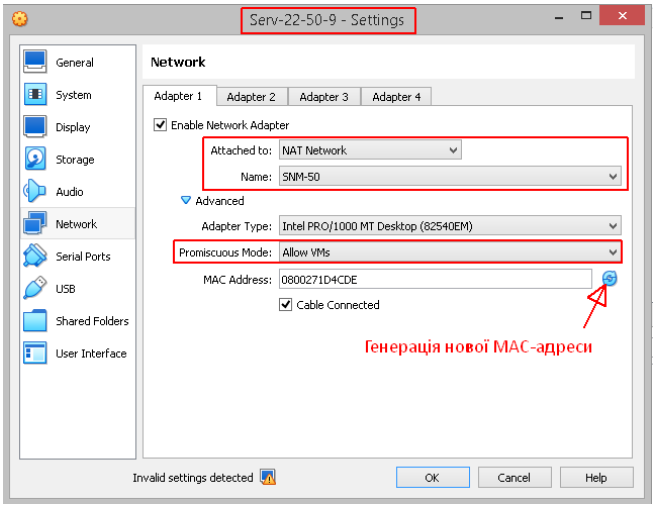

Рис. 12.2. Зміна MAC-адреси Ubuntu серверу Serv-22-50-9

Вмикаємо ВМ та повторюємо дії, що виконувались для підключення Serv-G-N-3 та Serv-G-N-5 у навчальний стенд. Авторизація – обліковий запис з правами адміністратора: ім'я користувача — student, пароль — 111111

Якщо налаштування виконані вірно, сервер автоматично отримає IP-адресу від служби DHCP у NAT-мережі, а його ім'я відповідатиме шаблону Serv-G-N-9. Для уточнення мережевих параметрів, імені хосту та його перейменування використовуємо такі команди (рис.12.3):

ip a
hostname
sudo hostnamectl set-hostname New-Name-Server
sudo reboot

Після перезавантаження нове ім'я набуде чинності.

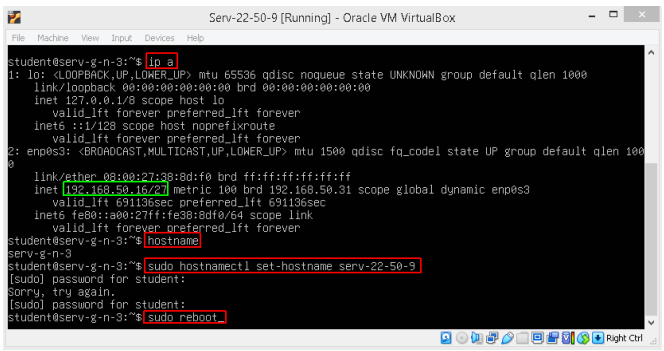

Рис. 12.3. Перегляд поточних IP-адрес, імені Ubuntu серверу Serv-G-N-3 та його перейменування на serv-22-50-9

Налаштуємо переадресацію для організації SSH доступу до Ubuntu серверу з фізичної машини – хосту VirtualBox. Пункт виконується у меню **[Oracle VirtualBox Manager] – [File] – [Tools] – [Network Manager] – [Nat Network] – [Properties] – [Port Forfarding] – [IPv4]**.

Назва правила NAT – “Serv-G-N-9 SSH”, де G – група, а N – варіант, що Ви виконуєте, протокол – “TCP”.

У якості Guest IP задаємо IP-адресу сервера, яку ми отримали за допомогою команди ***ip a*** , Port – 22 – порт «за замовчуванням» для SSH доступу.

У якості Host IP задаємо IP-адресу нашого фізичного ПК , що використовується для налаштованих раніше правил “Serv-G-N-3 SSH”, “Serv-G-N-5 SSH” та “Serv-G-N-7 SSH”.

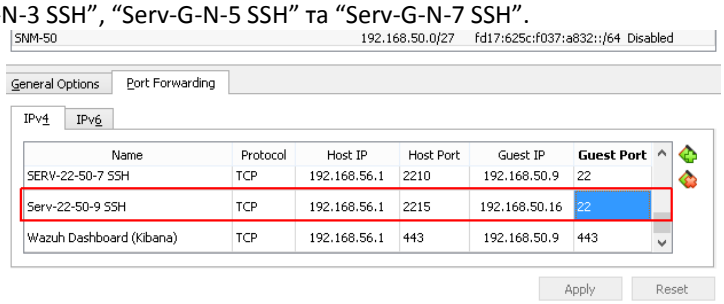

Рис. 12.4. Налаштування правила переадресації портів для SSH до серверу Serv-22-50-9.

У результаті, конфігурація Port Forwarding для забезпечення SSH-доступу з фізичного хосту до ВМ Serv-G-N-9 (Ubuntu Server) має вигляд, зображений на рис. 12.4. У якості порту переадресації обрано 2215.

Всі подальші дії з командним рядком Ubuntu рекомендовано виконувати за допомогою SSH-клієнта.

Serv-22-50-9 конфігурований на динамічну адресацію і адресу він отримує від доменного DHCP. Сервери, зазвичай, працюють на статиці. Змінюємо налаштування динамічної адреси на статичну. Шукаємо назву мережевого інтерфейсу, який необхідно відредагувати ip a

Шукаємо конфігураційні файли Netplan (з розширенням YAML), що зберігаються в каталозі /etc/netplan. Ймовірно, у цьому каталозі є один або декілька файлів YAML. Назва файлу може відрізнятися залежно від налаштувань та версії операційної системи.

dir /etc/netplan

Наприклад, у каталозі знайдено файл 50-cloud-init.yaml. Робимо його копію для редагування:

sudo cp /etc/netplan/50-cloud-init.yaml /etc/netplan/50-natnet.yaml

Відкриваємо для редагування

sudo vi /etc/netplan/50-natnet.yaml

Нижче наведено вміст файлу Netplan до та після редагування.

/etc/netplan/50-cloud-init.yaml --- DHCP

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
```

/etc/netplan/50-natnet.yaml Static 192.168.50.11/27

```
network:
  version: 2
  ethernets:
    enp0s3:
      addresses: [192.168.50.11/27]
      gateway4: 192.168.50.1
      nameservers:
        addresses: [192.168.50.3,192.168.50.1]
```

Зберігаємо відредагований Netplan та застосовуємо внесені зміни:

sudo netplan apply

Перевірка ip a показже, що на інтерфейсі enp0s3 активні дві одночасні IPv4-адреси:

192.168.50.11/27 — ручна статична адреса, задана через netplan;

192.168.50.16/27 — динамічна (DHCP) адреса позначена як secondary dynamic.

Приховуємо ☺ динамічну конфігурацію та застосовуємо зміни:

sudo mv /etc/netplan/50-cloud-init.yaml /etc/netplan/50-cloud-init.bkp

sudo netplan apply

SSH-підключення в результаті «відвалюється», бо зникла адреса Guest IP Port Forwarding. Задаємо у правилі Port Forwarding «Serv-22-50-9» налаштовану статичну адрес сервера. Перевіряємо зв’язок з хостами мережі.

Підготовка Ubuntu-хосту до встановлення Splunk Free

Перед інсталяцією Splunk необхідно переконатися, що всі системні пакети оновлені до актуальних версій. Це забезпечує сумісність компонентів та стабільну роботу сервісу.

sudo apt update

sudo apt upgrade -y

Splunk не потребує великої кількості залежностей, однак для зручності адміністрування та завантаження пакету бажано встановити базові інструменти:

sudo apt install wget curl apt-transport-https gnupg -y

- wget / curl – для завантаження інсталяційного пакету Splunk з офіційного сайту;

- apt-transport-https – забезпечує підтримку HTTPS-репозиторіїв;
- gnupg – для перевірки підписів пакетів (опціонально, але рекомендовано).

Для підвищення безпеки доцільно запускати Splunk не від імені root, чи «рідного» користувача student, а від окремого користувача. У лабораторному середовищі цей крок не є обов'язковим, але є вельми доцільним як гарна практика з точки зору безпеки. Створюємо користувача splunk:

sudo useradd -m splunk

sudo passwd splunk

Splunk Free поширюється у вигляді пакету Splunk Enterprise з безкоштовною 60-денною ліцензією. Після закінчення пробного періоду система автоматично переходить у Free Mode. Завантажуємо актуальний, на момент написання цього документу, пакет Splunk Enterprise (Free Mode)

cd /tmp

wget -O splunk-10.0.1-amd64.deb
https://download.splunk.com/products/splunk/releases/10.0.1/linux/splunk-10.0.1-c486717c322b-linux-amd64.deb

Актуальне посилання на завантаження можливо перевірити на сайтах:
https://www.splunk.com/en_us/download.html або
https://gist.github.com/devops-school/3247238bfdf8a4cbaf6039a1a38ba516

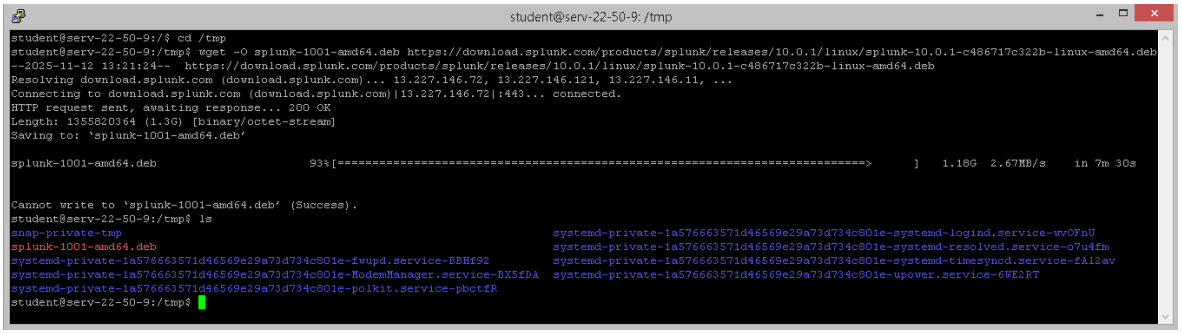

Рис. 12.5. Завантаження актуального deb-пакету Splunk Enterprise на Serv-22-50-9

Після завантаження встановлюємо Splunk за допомогою dpkg:

sudo dpkg -i splunk-10.0.1-amd64.deb

Як не дивно, ми отримуємо дуже показову і поширену помилку при інсталяції Splunk (рис.12.6).

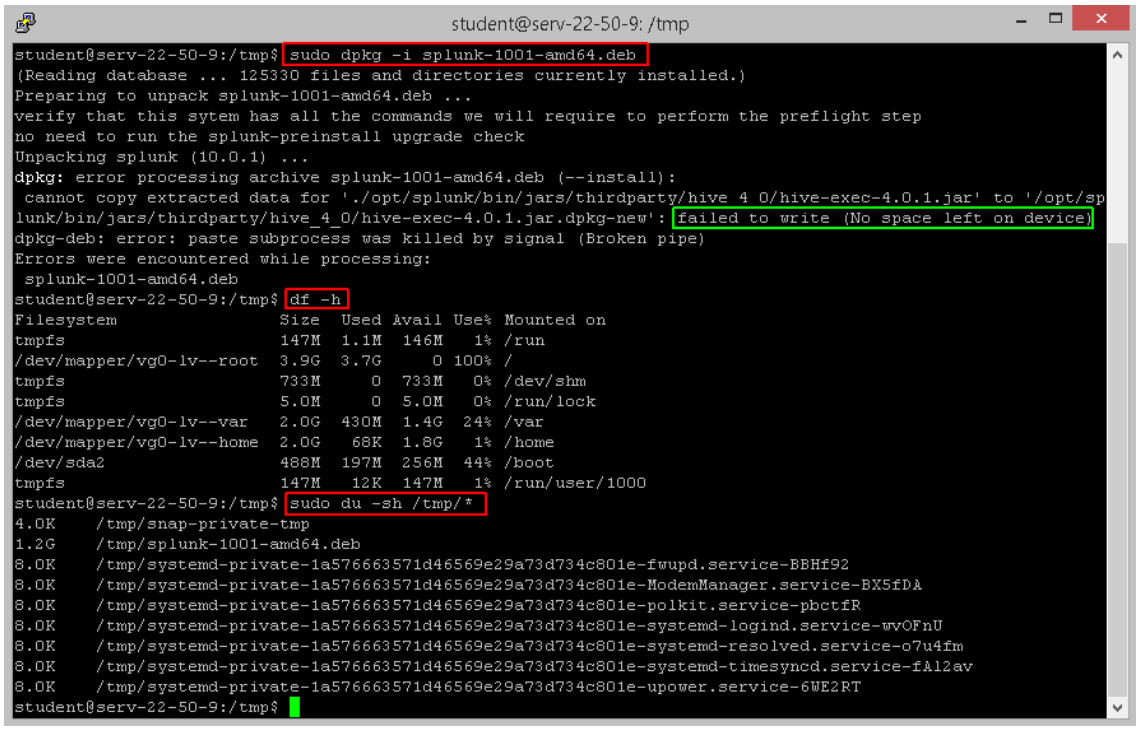

Рис. 12.6. Повідомлення failed to write (No space left on device) на Serv-22-50-9

Помилка не має відношення до пакету, а пов'язана з ресурсами віртуальної машини. Повідомлення ***failed to write (No space left on device)*** означає буквально — на диску немає вільного місця, і dpkg не зміг

розпакувати всі файли Splunk (а він важить понад 2 ГБ після розпакування). Переглядаємо заповненість файлових систем. На рисунку 12.6 у виводі команди ***df –h*** ми бачимо, що розділ / заповнений на 100% і має всього 3,9 Гб. Це і є причиною «творчої невдачі» ☺

Для комфортної роботи Splunk потрібно мінімум 20 Гб вільного місця, а краще 25–30 Гб.

Розширимо кореневий розділ системи. Система використовує LVM (/dev/mapper/vg0-lv--root), а отже це можна зробити без перевстановлення. Вимикаємо віртуальну машину та у VirtualBox переходимо у меню [File] – [Tools] – [Virtual Media Manager]. Знаходимо наш віртуальний диск та розширюємо його до 25 Гб.

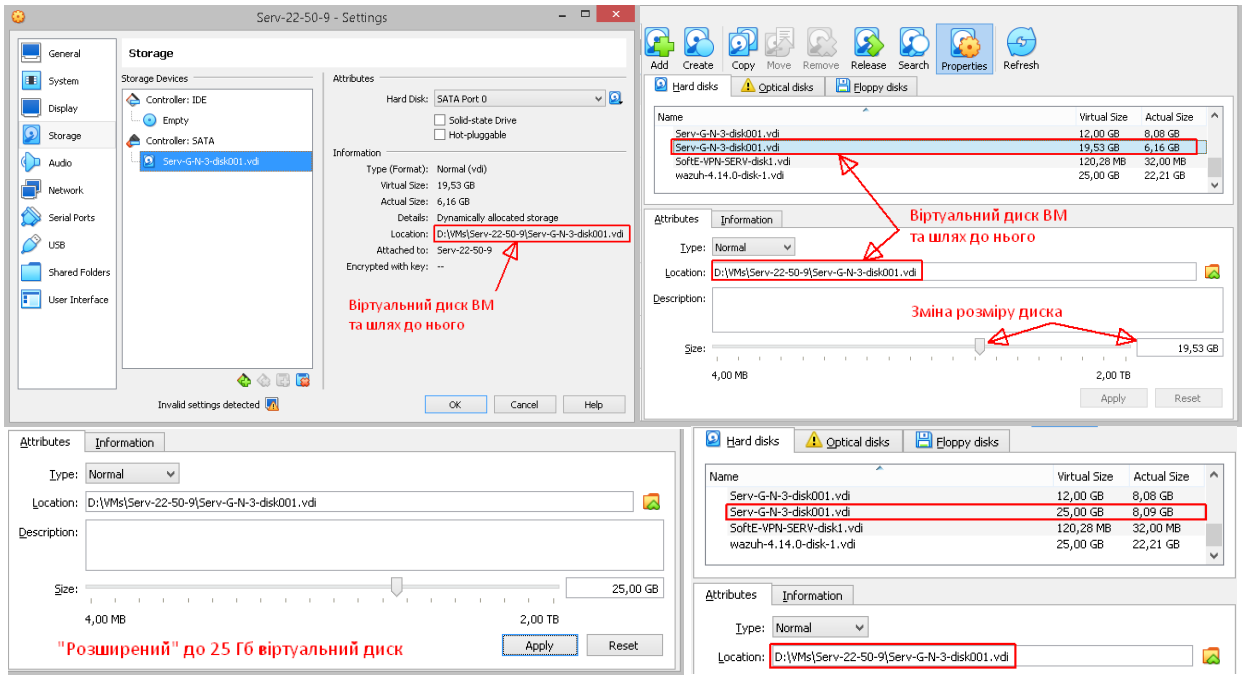

Рис. 12.7. Розширення віртуального диску до 25 Гб у Media Manager VirtualBox

Вмикаємо ВМ Serv-G-N-9. Потрібно, щоб Linux “побачив” цей додатковий простір і “приєднав” його до LVM-розділу так, як ОС ще не використовує додаткові ≈ 5,5 ГБ. Потрібно розширити фізичний том LVM а потім – логічний [root].

Переконуємось, що ядро бачить збільшений диск (≈ 25 ГБ). Знаходимо назву фізичного тому (команда ***sudo pvs***) та розширюємо знайдений фізичний том LVM.

sudo fdisk -l /dev/sda
sudo pvs
sudo pvresize /dev/sda4

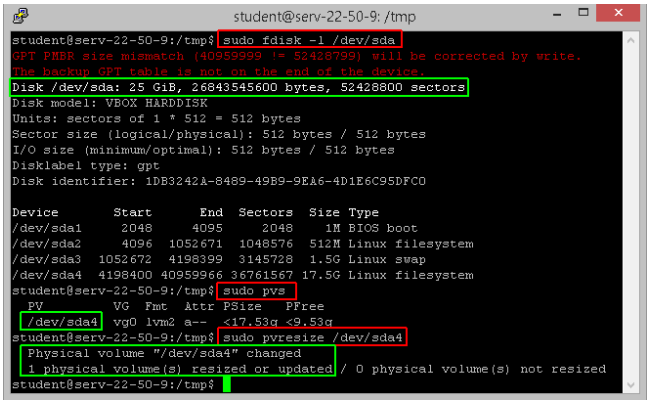

Рис. 12.8. Розширення фізичного тому LVM

Переглядаємо вірну назву root-розділу та розширюємо його розмір до максимально-можливого. У команді ***lvextend*** -l +100%FREE” означає — взяти всі вільні extents у групі vg0 та додати їх до lv-root.

Після цього оновлюємо файлову систему ext4, щоб вона «побачила» доданий простір і перевіряємо отриманий результат.

sudo lvs
sudo lvextend -l +100%FREE /dev/vg0/lv-root
sudo resize2fs /dev/vg0/lv-root
df –h

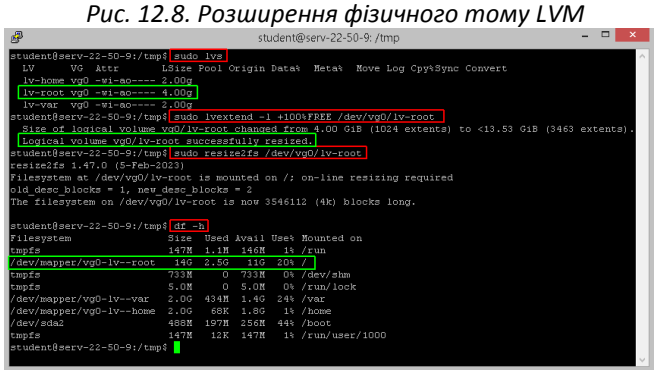

Рис. 12.9. Розширення логічного тому lv-root

З рис. 12.9 бачимо, що lv-root має розмір 14 Гб, з яких використано 20%.

Встановлення Splunk Free

Повторюємо інсталяцію Splunk:

sudo dpkg -i splunk-10.0.1-amd64.deb

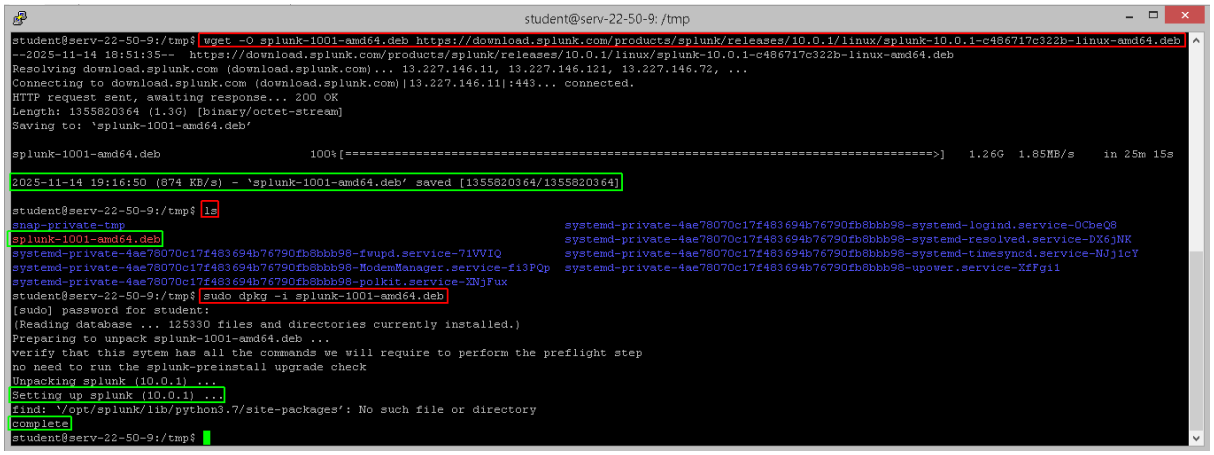

Рис. 12.10. Завантаження та встановлення splunk 10.0.1

На рис. 12.10 показано успішну інсталяцію Splunk. Повідомлення ***find: '/opt/splunk/lib/python3.7/site-packages': No such file or directory*** — не є критичною помилкою і немає причин для паніки ☺ Це типовий «warning» для Splunk 10.x, який більше не використовує Python 3.7 — Splunk просто перевіряє чи існує старий шлях, і не знаходить його.

Splunk встановлено успішно, ключовий рядок ***Setting up splunk (10.0.1) ... … complete***

Перший запуск Splunk та первинне налаштування (з окремим сервісним користувачем)

Після встановлення Splunk необхідно змінити власника його каталогу, щоб сервіс міг запускатися не від root, а від окремого користувача splunk, створеного раніше. Це відповідає рекомендованим практикам безпеки та ізоляції сервісів.

Відповідно змінюємо права на каталог програми:

sudo chown -R splunk:splunk /opt/splunk

Запускаємо Splunk від користувача splunk. Перший запуск виконуємо від імені цього користувача з прийняттям ліцензійної угоди:

sudo -u splunk /opt/splunk/bin/splunk start --accept-license

Під час першого запуску Splunk запропонує створити обліковий запис користувача, що використовується для входу в веб-інтерфейс. Також необхідно буде задати пароль для цього користувача. На рис. 12.11 показане створення користувача admin.

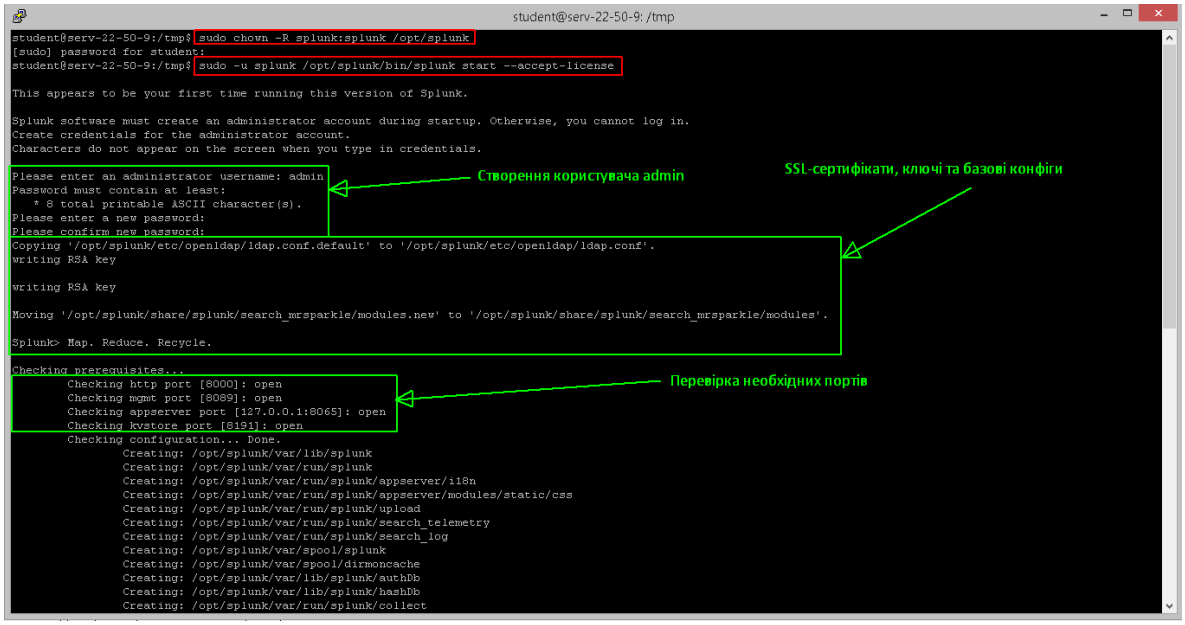

Рис. 12.11. Перший запуск splunk

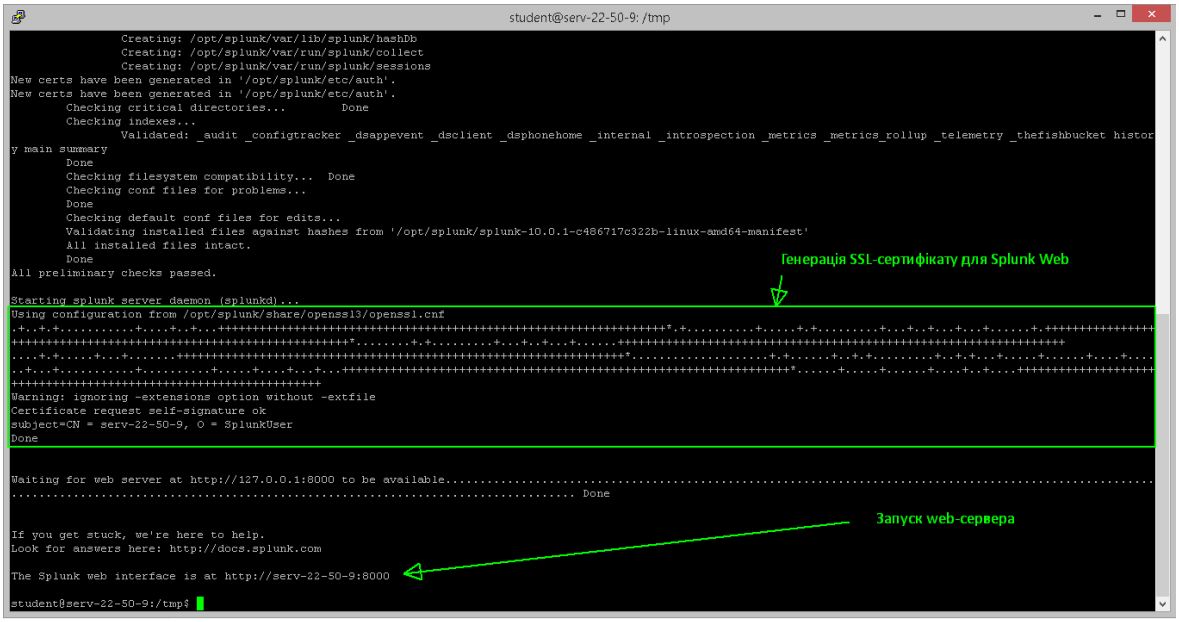

Рис. 12.11. Перший запуск splunk. Подовження скріну.

Таким чином система встановилась, ініціалізувалась, було створено адміністратора, згенеровано сертифікати, перевірена цілісність, відкриті потрібні порти та успішно запущений Splunk Web. Жодних помилок.

Базові налаштування Splunk (CLI)

Зафісуємо та увімкнемо автозапуск (boot-start). Splunk повинен автоматично підніматися після перезавантаження, і бажано — під користувачем splunk. Створюємо systemd/ініціалізаційний скрипт, який запускатиме splunkd від користувача splunk та перевіряємо стан сервісу:

sudo /opt/splunk/bin/splunk enable boot-start -user splunk
sudo /opt/splunk/bin/splunk status

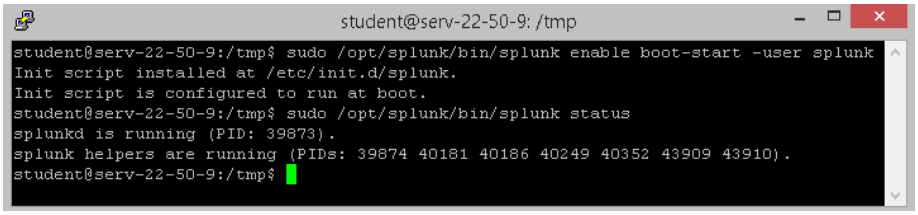

Рис. 12.12. Скрипт автозапуску splunk.

Після enable boot-start ініціалізаційний скрипт зберігається у ***/etc/systemd/system/Splunkd.service***
Щоб переконатися, у відсутності прихованих помилок перевіряємо логи Splunk

sudo -u splunk tail -n 200 /opt/splunk/var/log/splunk/splunkd.log
sudo -u splunk tail -n 100 /opt/splunk/var/log/splunk/web_service.log

Під час першого запуску Splunk може згенерувати попередження про недостатній вільний простір на кореневому розділі (/). Для коректної роботи Splunk рекомендує мінімум 5 ГБ вільного місця, але у лабораторному середовищі це не завжди можливо.

Зараз команда df -h показує ***/dev/mapper/vg0-lv--root 14G 8.6G 4.1G 69% /.***

Оскільки доступно лише ≈4 ГБ, Splunk виводить попередження приблизно такого змісту
WARN DiskMon - minFreeSpace=5000MB. Free disk space under '/': 4100MB.

Це лише попередження — Splunk продовжує працювати, але нагадує, що місця менше від рекомендованого. У лабораторному середовищі Splunk не генерує великих обсягів даних, тому можна зменшити мінімальний поріг вільного місця, щоб вимкнути попередження DiskMon і забезпечити стабільний запуск.

Налаштуємо мінімальний поріг вільного місця (minFreeSpace) у конфігураційному файлі ***/opt/splunk/etc/system/local/server.conf***. Якщо файлу ***/opt/splunk/etc/system/local/server.conf*** не існує — його потрібно створити вручну. Додаємо у файл секцію, що встановлює новий поріг — 1000 МБ (1 ГБ), достатній для лабораторних робіт.

[diskUsage]
minFreeSpace = 1000

Перезапускаємо Splunk:

sudo -u splunk /opt/splunk/bin/splunk restart

Після перезапуску попередження про недостатній простір більше не буде з'являєтись, а Splunk буде працювати стабільно та прогнозовано в рамках лабораторного середовища.

Для відокремлення локальних журналів у власний індекс (наприклад, local_logs) створюємо індекс для лабораторії. На запит Splunk username вводимо логін та пароль користувача admin, створеного при першому запуску (рис.12.11) та виконуємо перевірку цілісності та переліку індексів:

sudo -u splunk /opt/splunk/bin/splunk add index local_logs

sudo -u splunk /opt/splunk/bin/splunk list index

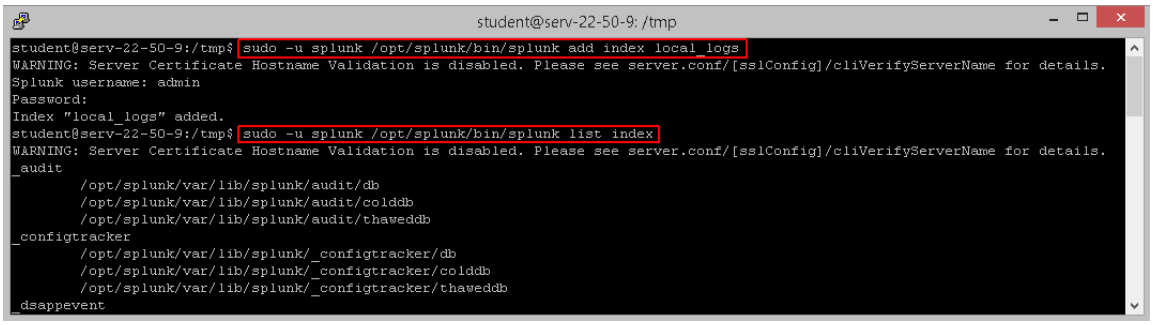

Рис. 12.13. Створення індексу локальних логів splunk.

Щоб Splunk почав індексувати /var/log та конкретні журнали необхідно додати моніторинг локальних логів. Але користувач splunk, від імені якого запускаються команди, не має прав читати системні журнали.

Група adm має право читати журнали у /var/log завдяки ACL та системним дозволам, тому включення користувача splunk до цієї групи є стандартною практикою в Linux. Додаємо користувача splunk до групи adm, яка має доступ до /var/log/* та перезапускаємось:

sudo usermod -aG adm splunk

sudo -u splunk /opt/splunk/bin/splunk restart

Додаємо моніторинг локальних логів (файлів).

sudo -u splunk /opt/splunk/bin/splunk add monitor /var/log/syslog -index local_logs -sourcetype syslog

sudo -u splunk /opt/splunk/bin/splunk add monitor /var/log/auth.log -index local_logs -sourcetype linux_secure

Щоб увімкнути моніторинг всього каталогу виконується команда:

sudo -u splunk /opt/splunk/bin/splunk add monitor /var/log -index local_logs -sourcetype syslog

Вказаний варіант виставляє однаковий sourcetype для всіх файлів із каталогу /var/log. У виробничих системах рекомендується або не вказувати sourcetype, або задавати окремо для кожного файлу.

Індексація локальних логів, базова візуалізація та доступ з віддаленої машини

Щоб підключатися до Splunk Web із фізичного ПК, на віртуальній машині (VirtualBox) налаштовуємо Port Forwarding. Пункт виконується у меню **[Oracle VirtualBox Manager] – [File] – [Tools] – [Network Manager] – [Nat Network] – [Properties] – [Port Forfarding] – [IPv4]**. Назва правила NAT – “Serv-G-N-9 Splunk”, де G – група, а N – варіант, що Ви виконуєте, протокол – “TCP”.

У якості Guest IP задаємо IP-адресу сервера, яку ми отримали за допомогою команди ***ip a*** , Port – 8000 – порт «за замовчуванням» для SSH доступу. У якості Host IP задаємо IP-адресу нашого фізичного ПК , що використовується для налаштованого раніше правила “Serv-G-N-9 SSH”.

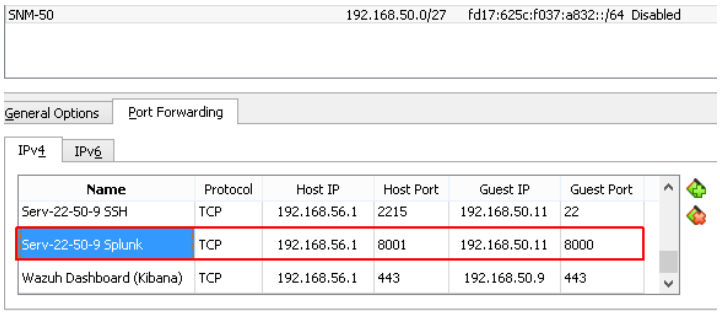

Рис. 12.15. Налаштування правила переадресації портів для Splunk до серверу Serv-22-50-9.

У результаті, конфігурація Port Forwarding для забезпечення доступу з фізичного хосту до WEB-інтерфейсу Splunk ВМ Serv-G-N-9 (Ubuntu Server) має вигляд, зображений на рис. 12.15. У якості порту переадресації обрано 8001, бо порт 8000 вже був зайнятий в одній з попередніх робіт для підключення до SERV-G-N-3 Graphite.

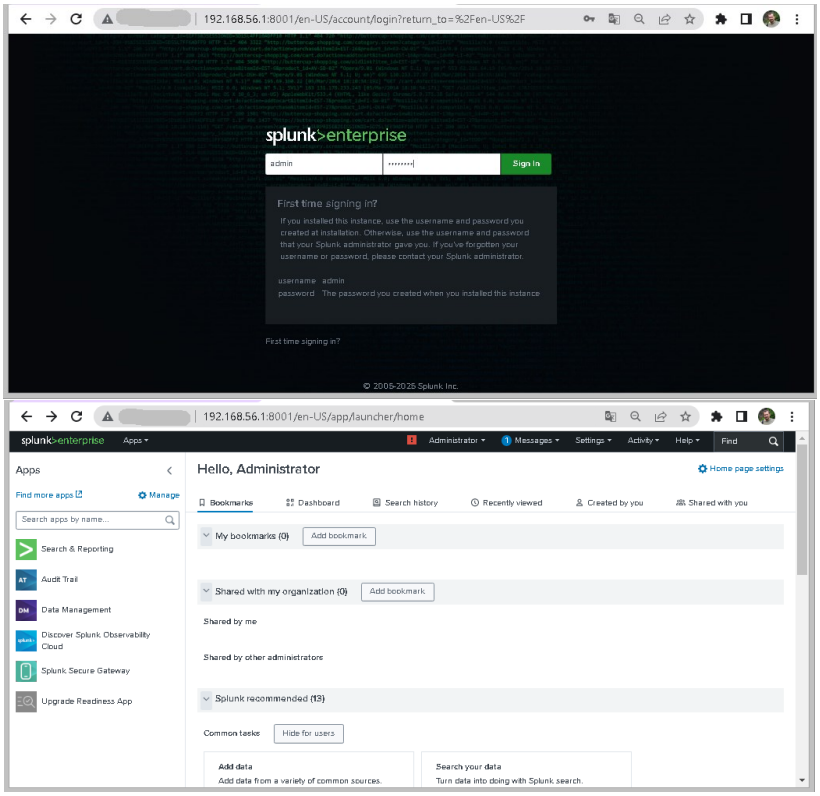

Рис. 12.16. Логін та стартовий екран веб-інтерфейсу Splunk.

Перевіримо надходження подій у Splunk. Обираємо меню Search & Reporting та виконуємо пошук для перевірки подій набравши у пошуковому рядку ***index=local_logs | stats count by sourcetype.*** Цей запит Показує кількість отриманих подій у індексі local_logs, згрупованих за їхнім типом джерела (sourcetype).

Переконуємося, що події з'явилися та sourcetype відповідає очікуваному.

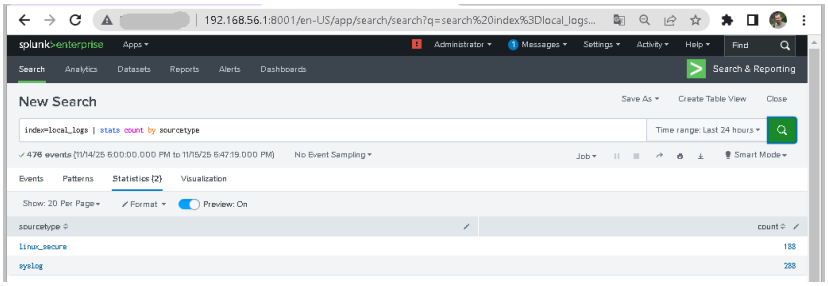

Рис. 12.17. Результат пошуку index=local_logs | stats count by sourcetype

Створимо Saved Search та Dashboard. У рядку пошуку набираємо

index=local_logs sourcetype=syslog | timechart count by host span=1h

Використаний запит будує погодинну статистику кількості syslog-подій від кожного хосту, що допомагає відстежувати активність систем у часі. Зберігаємо його по кнопці Save As.

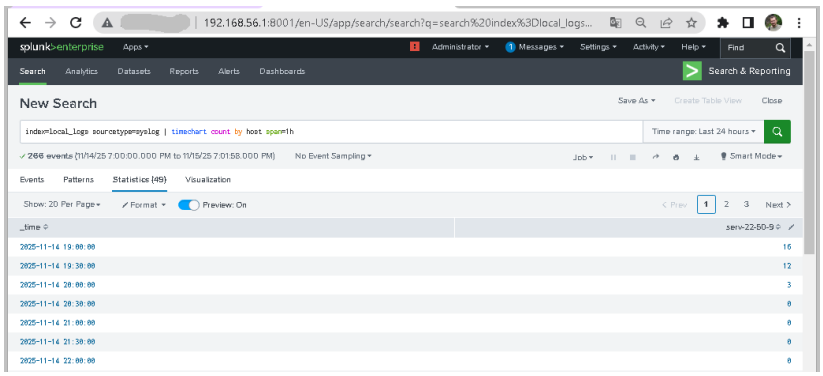

Рис. 12.18. Результат пошуку index=local_logs sourcetype=syslog | timechart count by host span=1h

Створюємо Dashboard з уменем syslog_hourly_count та переглядаємо його у відповідному меню.

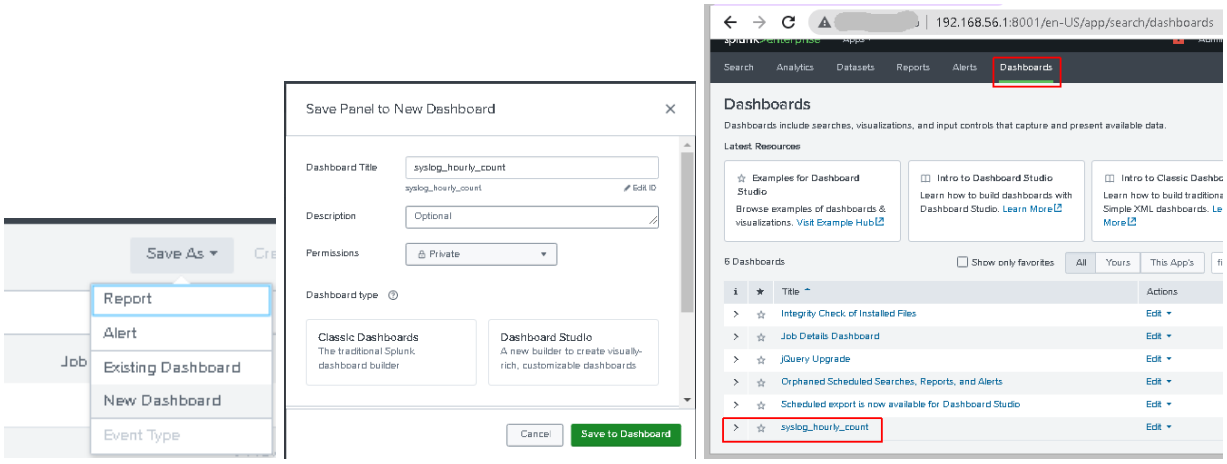

Рис. 12.19. Збереження та перегляд Dashboard

Таким чином ми встановили та налаштували Splunk Free на сервері Ubuntu, створили окремого користувача для безпечного запуску, активували автозапуск сервісу, оптимізували конфігурацію під обмежені ресурси лабораторного середовища та налаштували базовий збір системних логів.

Завдання до лабораторної роботи

1. Розгорнути Ubuntu Server (маска імені Serv-G-N-9) з аплайнсу та підготувати його до встановлення Splunk (оновлення системи, перевірка ресурсів, підготовка робочого середовища).
2. Встановити Splunk Free на Ubuntu та виконати перший запуск з прийняттям ліцензії й створенням адміністративного користувача.
3. Створити окремого сервісного користувача splunk, передати йому права на каталог Splunk та налаштувати автозапуск сервісу.
4. Виконати базові CLI-налаштування Splunk, включно зі зміною порогу дискового моніторингу для лабораторного середовища.
5. Створити індекс local_logs, налаштувати доступ Splunk до системних логів та додати моніторинг /var/log/syslog та /var/log/auth.log.
6. Виконати базові пошукові запити у Splunk, візуалізувати дані та забезпечити доступ до Splunk Web з віддаленої машини.

Корисні посилання

- Free. Trial. Splunk Enterprise 10.0.1
https://www.splunk.com/en_us/download/splunk-enterprise.html

- Free. Trial. Splunk Cloud Platform trial
https://www.splunk.com/en_us/download/splunk-cloud.html

- Github. Devops-school. Splunk-Download
https://gist.github.com/devops-school/3247238bfdf8a4cbaf6039a1a38ba516

- Free Splunk License—Here's How To Do It
https://kinneygroup.com/blog/splunk-free-license/

- Installing Splunk Enterprise on Ubuntu: Step-by-Step Guide
https://medium.com/@dannyopara/installing-splunk-enterprise-on-ubuntu-step-by-step-guide-b545982038c3

- Instructions for installing Splunk on an Ubuntu server
https://community.splunk.com/t5/Installation/Instructions-for-installing-Splunk-on-an-Ubuntu-server-12-04-1/m-p/106993

- Instructions for installing Splunk on an Ubuntu server
https://www.fosstechnix.com/how-to-install-splunk-on-ubuntu-24-04-lts/