**Лаврінович Є.О**

**КН19**

**Лабораторна робота № 4**

**Перегляд журналів подій та системного журналу безпеки операційної системи Windows**

1. Перегляд подій у журналах подій операційної системи на ПЕОМ користувачів:

1.1. додатків:

Graphical user interface, text, application

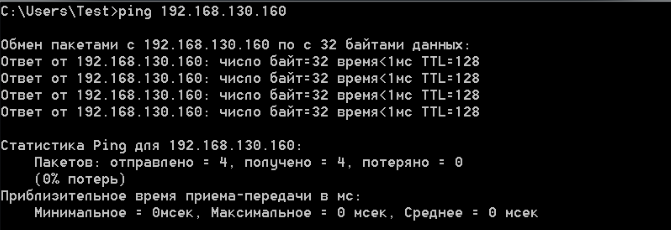
Description automatically generated

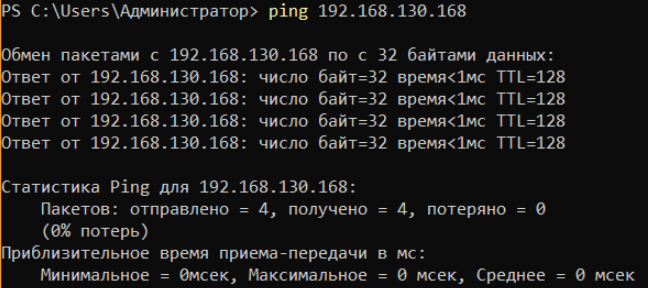
1.2. системи:

Graphical user interface, text, application, email

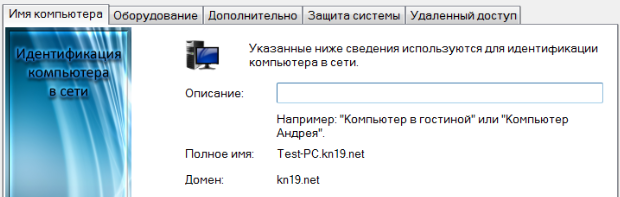
Description automatically generated

2. Перевірити за допомогою утиліти «ping» зв’язок між Windows 7 користувача та контролером домену:

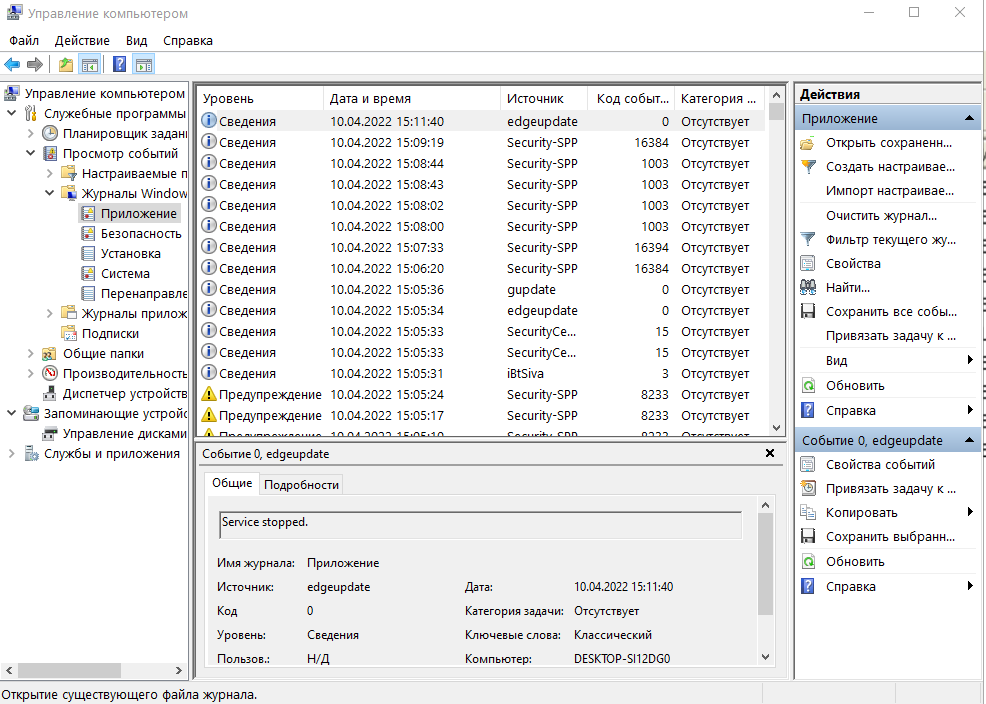




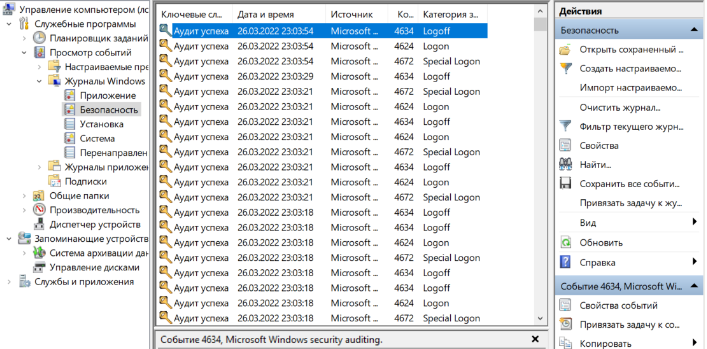
3. Виконати приєднання користувача віртуальної машини Windows 7 до контролера домену:



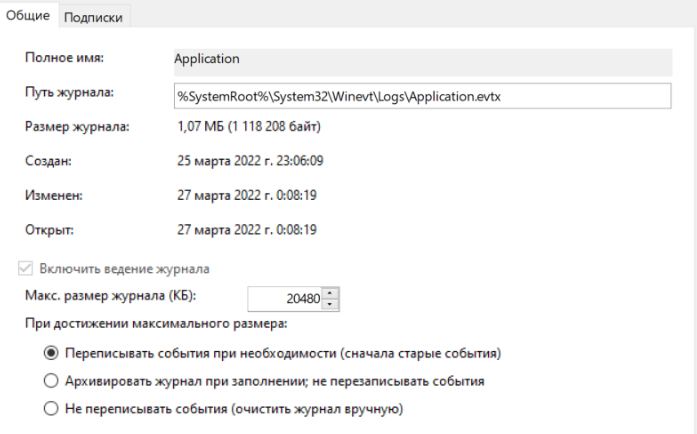
4. Переглянути події у журналах операційної системи серверу та Windows 7 користувача віртуальної машини:

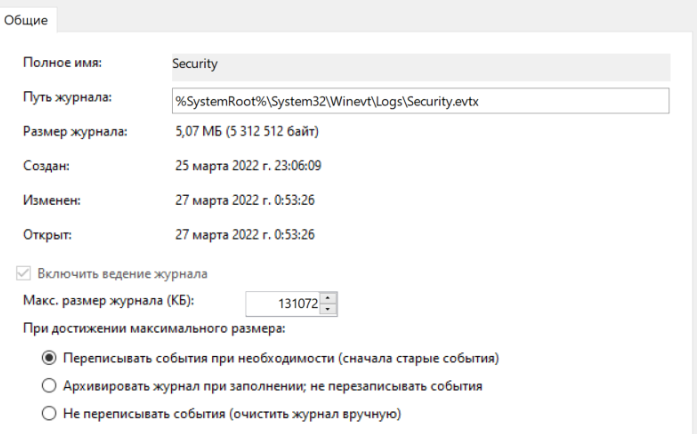


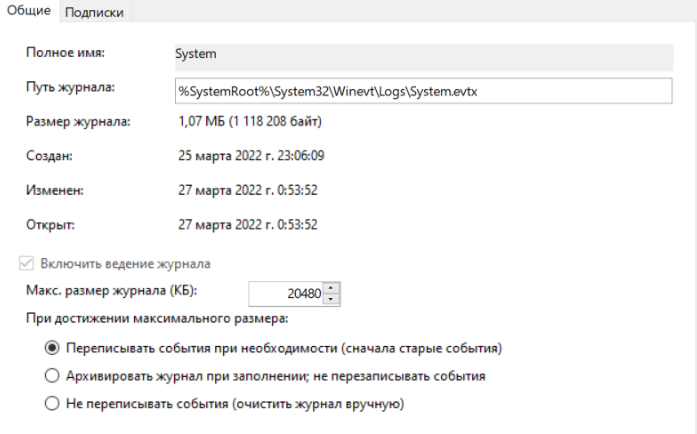
5. Перевірити події у журналі безпеки операційної системи серверу:



6. Перевірити розмір журналів подій та здійснити їх аналіз і очищення:







**Контрольні питання**

1. **Порядок встановлення та налаштування роботи контролеру домену:**

* Войдите на сервер под локальным администраторов. На сервер кроме роли Active Directory Domain Services также будет установлена служба DNS. Изменим настройки сетевого интерфейса, указав в качестве первичного DNS сервера собственный IP адрес севера или адрес 127.0.0.1.
* Затем откройте Server Manager, нажав на соответствующий значок или выполнив в консоли PowerShell команду ServerManager.exe.
* В окне Server Manager нажмите Add roles and features
* В окне мастера добавления ролей и компонентов нажмите Next.
* Далее следуйте инструкции в Wizard’e

1. **Особливості створення облікового запису користувача за допомогою контролеру домену:**

* откройте оснастку Active Directory Users and Computers, для этого откройте Диспетчер серверов и перейдите в раздел AD DS. В контекстном меню сервера выберете соответствующую оснастку.
* В окне разверните дерево вашего домена и найдите каталог с пользователями Users. Правой кнопкой мыши нажмите на каталог и выберете Создать -> Пользователь.
* Укажите данные пользователя и нажмите Finish
* Добавьте пользователя в группу Domain Admins

1. **Методика перевірки стану зв’язку між контролером домену та ПЕОМ користувача:**

* Перевірити зв'язок можно за допомогою утиліти PING.

1. **Перерахувати основні журнали операційної системи Windows, за допомогою яких здійснюється моніторинг роботи програмного забезпечення, апаратного забезпечення ПЕОМ та сервера:**

* На ПЕОМ користувачів – додатків, системи.
* На сервері – додатків, Directory Service, DNS Server, cлужба реплікації файлів, система.

1. **Визначити за допомогою технічної документації ОС Windows основні необхідні розміри журналів операційної системи Windows:**

* Для журнала безпеки:
* Типово в Windows Server 2022 Standard розмір журналу 20 МБ.
* Розмір журналу повинен перебувати в діапазоні від 20 МБ (20480 кілобайт) і 2 ТБ (2147483647 кілобайт) з кроком в один кілобайт з кроком в 1 КБ.
* Для інших журналів:
* Типово в Windows Server 2022 Standard розмір журналу 1 МБ.
* Розмір журналу повинен перебувати в діапазоні від 1 МБ (1024 кілобайт) і 2 ТБ (2147483647 кілобайт) з кроком в один кілобайт з кроком в 1 КБ.

1. **Описати основні правила перевірки та очищення системних журналів операційної системи Windows:**

* Для очищення журналу, в утиліті "Просмотр событий" відкрити розділ "Журналы Windows" і натиснути правою кнопкою мишки на потрібний журнал, після чого натиснути на "Очистить журнал…".
* Щоб перевірити розмір журналів, замість "Очистить журнал…" потрібно вибрати "Свойства".