Журналирование в Windows

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

Российский университет дружбы народов (РУДН)

2025-12-05

Содержание I

1 Введение

1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС

1.0.2 Цель презентации

1 Введение

1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев

1.0.2 Цель презентации

1 Введение

1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев
- Анализ инцидентов безопасности

1.0.2 Цель презентации

1 Введение

1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев
- Анализ инцидентов безопасности
- Мониторинг активности пользователей и служб

1.0.2 Цель презентации

1 Введение

1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев
- Анализ инцидентов безопасности
- Мониторинг активности пользователей и служб

1.0.2 Цель презентации

- Рассмотреть механизм журналирования

1 Введение

1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев
- Анализ инцидентов безопасности
- Мониторинг активности пользователей и служб

1.0.2 Цель презентации

- Рассмотреть механизм журналирования
- Изучить архитектуру Event Log

1 Введение

1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев
- Анализ инцидентов безопасности
- Мониторинг активности пользователей и служб

1.0.2 Цель презентации

- Рассмотреть механизм журналирования
- Изучить архитектуру Event Log
- Показать инструменты анализа событий

2.0.1 Категории событий Windows

- Information

2.0.1 Категории событий Windows

- Information
- Warning

2.0.1 Категории событий Windows

- Information
- Warning
- Error

2.0.1 Категории событий Windows

- Information
- Warning
- Error
- Critical

2.0.1 Категории событий Windows

- Information
- Warning
- Error
- Critical
- Audit Success

2.0.1 Категории событий Windows

- Information
- Warning
- Error
- Critical
- Audit Success
- Audit Failure

3 Основные журналы Windows

Журнал	Назначение
Application	События приложений
System	Ошибки драйверов и служб
Security	Аудит входов и изменений
Setup	Установка и конфигурация
Forwarded Events	События с других машин

4 Интерфейс Event Viewer

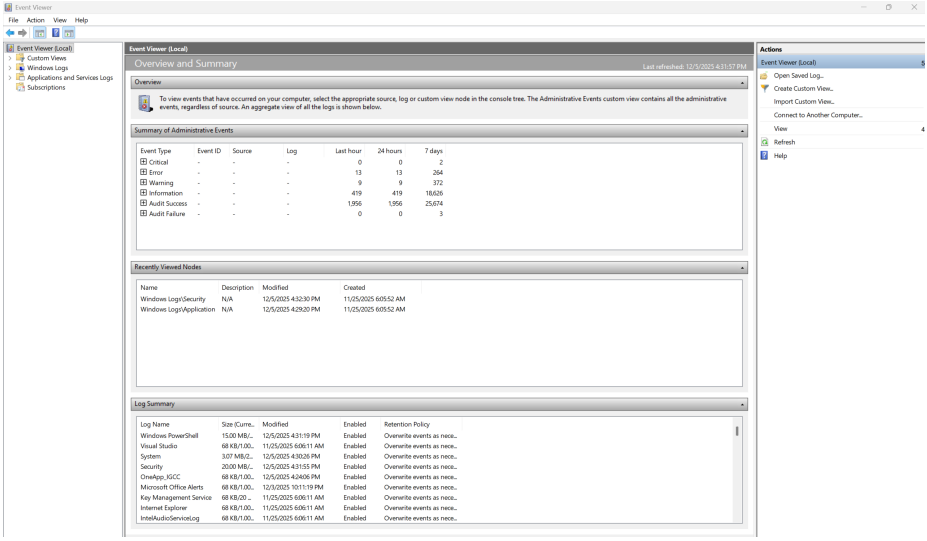


Рисунок 1: Общий вид Event Viewer

5 Архитектура журналирования Windows

5.0.1 Основные компоненты

- Event Providers

5.0.2 Типы каналов

5 Архитектура журналирования Windows

5.0.1 Основные компоненты

- Event Providers
- Event Log Service

5.0.2 Типы каналов

5 Архитектура журналирования Windows

5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels

5.0.2 Типы каналов

5 Архитектура журналирования Windows

5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels
- Event IDs

5.0.2 Типы каналов

5 Архитектура журналирования Windows

5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels
- Event IDs

5.0.2 Типы каналов

- Administrative

5 Архитектура журналирования Windows

5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels
- Event IDs

5.0.2 Типы каналов

- Administrative
- Operational

5 Архитектура журналирования Windows

5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels
- Event IDs

5.0.2 Типы каналов

- Administrative
- Operational
- Analytical

5 Архитектура журналирования Windows

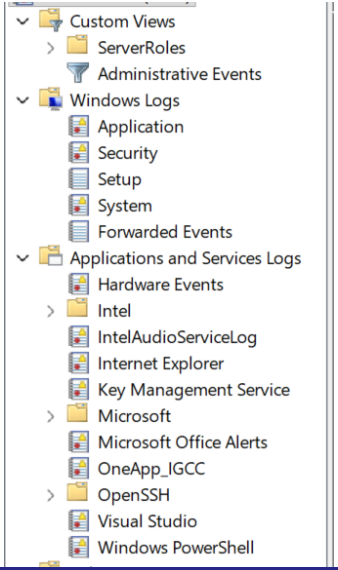
5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels
- Event IDs

5.0.2 Типы каналов

- Administrative
- Operational
- Analytical
- Debug

6 Структура каналов журналов



7 Инструменты журналирования

7.0.1 Event Viewer

- Просмотр событий

7 Инструменты журналирования

7.0.1 Event Viewer

- Просмотр событий
- Фильтрация

7 Инструменты журналирования

7.0.1 Event Viewer

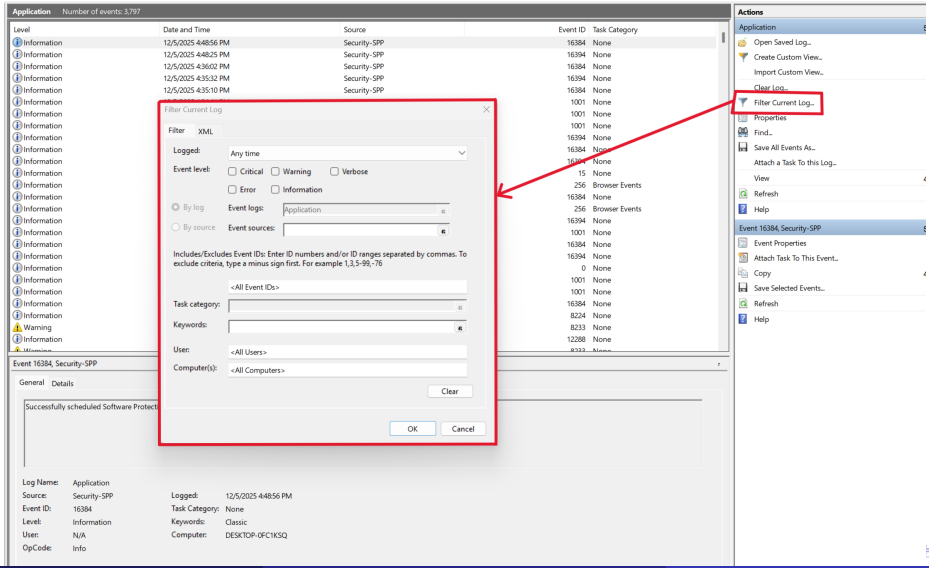
- Просмотр событий
- Фильтрация
- Экспорт журналов

7 Инструменты журналирования

7.0.1 Event Viewer

- Просмотр событий
- Фильтрация
- Экспорт журналов
- Создание Custom View

8 Фильтрация событий



9 PowerShell для журналирования

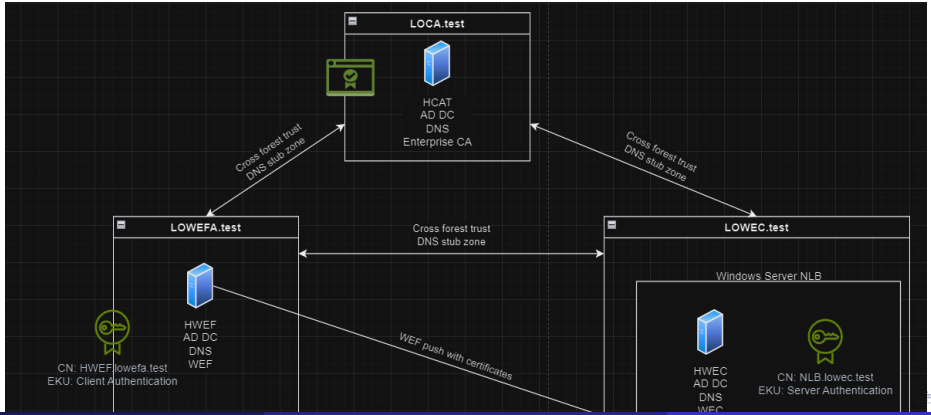
Основные команды:

```
Get-EventLog -LogName Security -Newest 20
Get-WinEvent -LogName Application
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4625}
```

10 Windows Event Forwarding (WEF)

Используется для:

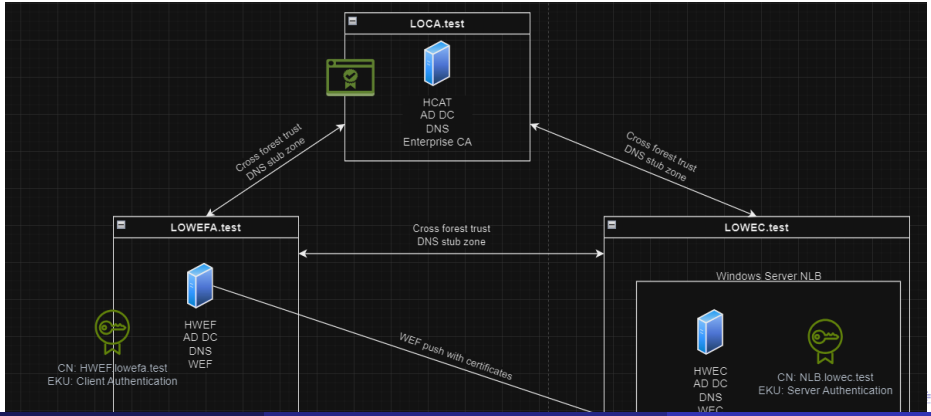
- Централизованного сбора событий



10 Windows Event Forwarding (WEF)

Используется для:

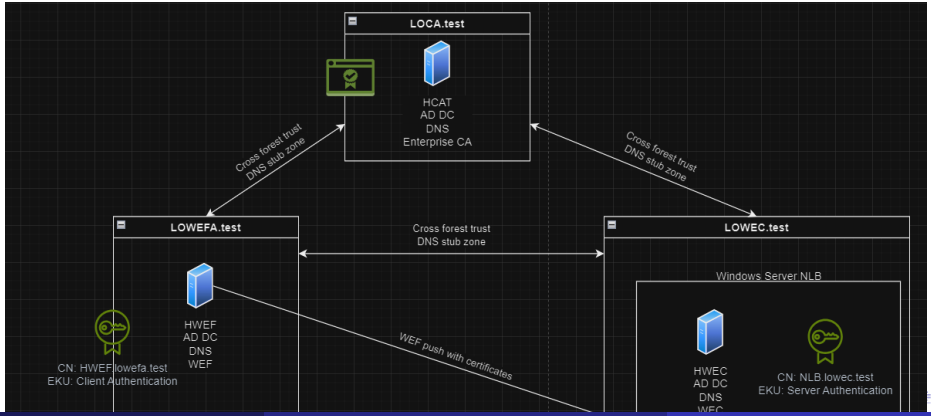
- Централизованного сбора событий
- Интеграции с SIEM



10 Windows Event Forwarding (WEF)

Используется для:

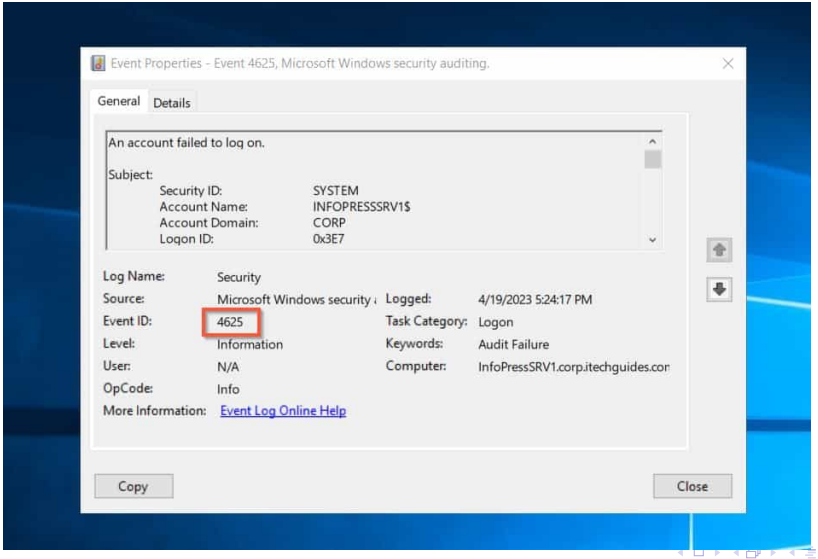
- Централизованного сбора событий
- Интеграции с SIEM
- Управления аудитом в корпоративных сетях



11.0.1 Основные события Security Log

ID	Описание
4624	Успешный вход
4625	Ошибка входа
4634	Выход
4720	Создание учётной записи
4726	Удаление учётной записи
1102	Очистка журнала

12 Пример события 4625



13 Расширенный аудит

Набор механизмов включает:

- Local Security Policy

13 Расширенный аудит

Набор механизмов включает:

- Local Security Policy
- Advanced Audit Policy Configuration

13 Расширенный аудит

Набор механизмов включает:

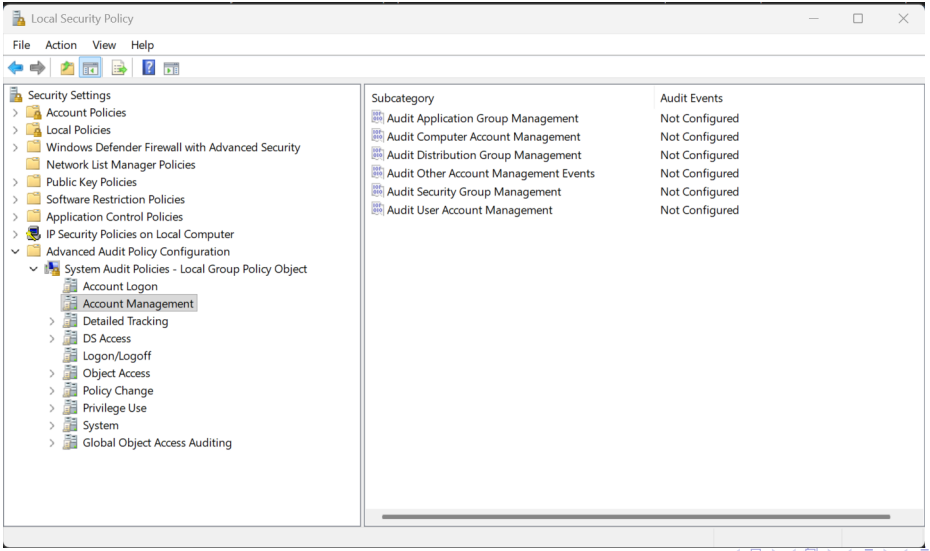
- Local Security Policy
- Advanced Audit Policy Configuration
- Sysmon

13 Расширенный аудит

Набор механизмов включает:

- Local Security Policy
- Advanced Audit Policy Configuration
- Sysmon
- Group Policy Objects

14 Настройка Audit Policies



15 Sysmon

Преимущества:

- Логирование сетевых подключений

15 Sysmon

Преимущества:

- Логирование сетевых подключений
- Отслеживание процессов

15 Sysmon

Преимущества:

- Логирование сетевых подключений
- Отслеживание процессов
- Поддержка цепочек событий

15 Sysmon

Преимущества:

- Логирование сетевых подключений
- Отслеживание процессов
- Поддержка цепочек событий
- Контроль изменений файлов

16 Экспорт журнала событий

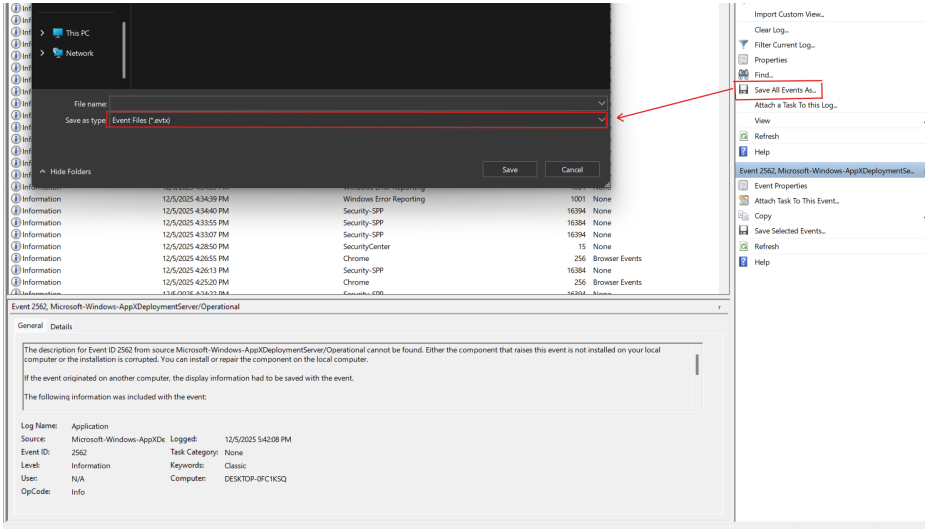
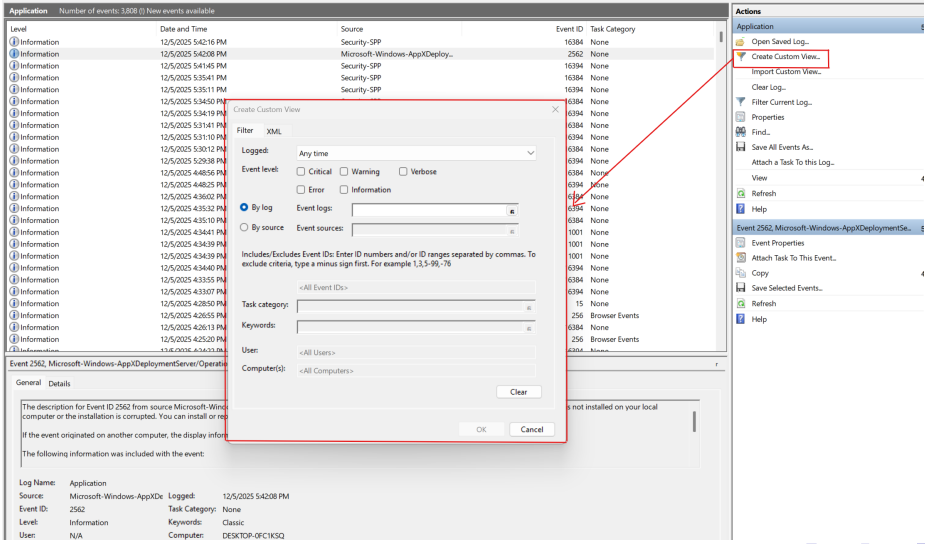


Рисунок 7: Экспорт журнала

17 Создание Custom View



18 Заключение

- Журналирование — ключевой инструмент администратора

18 Заключение

- Журналирование — ключевой инструмент администратора
- Позволяет обнаруживать атаки

18 Заключение

- Журналирование — ключевой инструмент администратора
- Позволяет обнаруживать атаки
- Обеспечивает диагностику и анализ

18 Заключение

- Журналирование — ключевой инструмент администратора
- Позволяет обнаруживать атаки
- Обеспечивает диагностику и анализ
- Укрепляет защиту инфраструктуры

18 Заключение

- Журналирование — ключевой инструмент администратора
- Позволяет обнаруживать атаки
- Обеспечивает диагностику и анализ
- Укрепляет защиту инфраструктуры
- Интегрируется с SIEM, PowerShell и Sysmon

19 Спасибо за внимание!