Реферат: Журналирование в Windows

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

Содержание

Список иллюстраций

Список таблиц

1 Введение

Журналирование является одним из наиболее важных механизмов обеспечения контроля и прозрачности функционирования операционных систем. В Windows система регистрации событий (Windows Event Logging) используется администраторами для диагностики, расследования инцидентов, анализа ошибок, мониторинга безопасности и соответствия корпоративным политикам.

От корректной настройки журналирования зависит: - выявление атак и подозрительной активности; - успешное расследование инцидентов; - стабильность работы системы; - анализ производительности и ошибок служб.

Цель данного реферата — рассмотреть архитектуру журналирования Windows, классификацию событий, ключевые инструменты администратора, особенности логирования безопасности и методы расширенной настройки аудита.

2 Основные понятия и классификация событий

Windows использует централизованную систему событий, организованную по журналам. Основные категории событий включают:

- Information — информационные сообщения
- Warning — предупреждения
- Error — ошибки
- Critical — критические сбои
- Audit Success — успешные события безопасности
- Audit Failure — неуспешные события безопасности

2.1 Основные типы журналов

Журнал	Назначение
Application	События приложений
System	События драйверов, служб и компонентов системы
Security	Аудит входов/выходов, изменений прав, активности пользователей

Журнал	Назначение
Setup	Установки и конфигурации ОС
Forwarded Events	События, полученные с других компьютеров

2.2 Пример интерфейса Event Viewer

Иллюстрация интерфейса Windows Event Viewer.

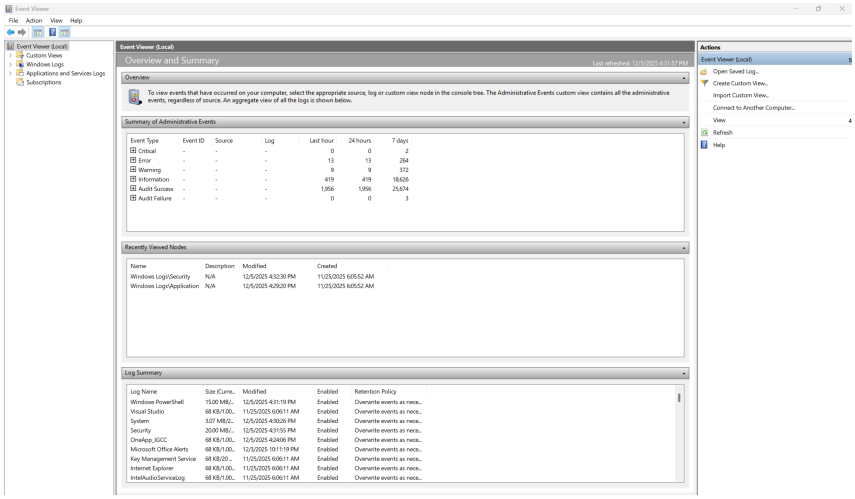

Рисунок 2.1: Общий вид Event Viewer

3 Архитектура системы журналирования Windows

Система журналирования включает:

- **Event Providers** — источники событий
- **Event Log Service** — служба записи
- **Event Channels** — каналы журналов
- **Event IDs** — уникальные идентификаторы событий

Windows оперирует системой каналов, которые могут быть: - административными (Administrative), - операционными (Operational), - аналитическими (Analytical), - отладочными (Debug).

3.1 Пример структуры каналов

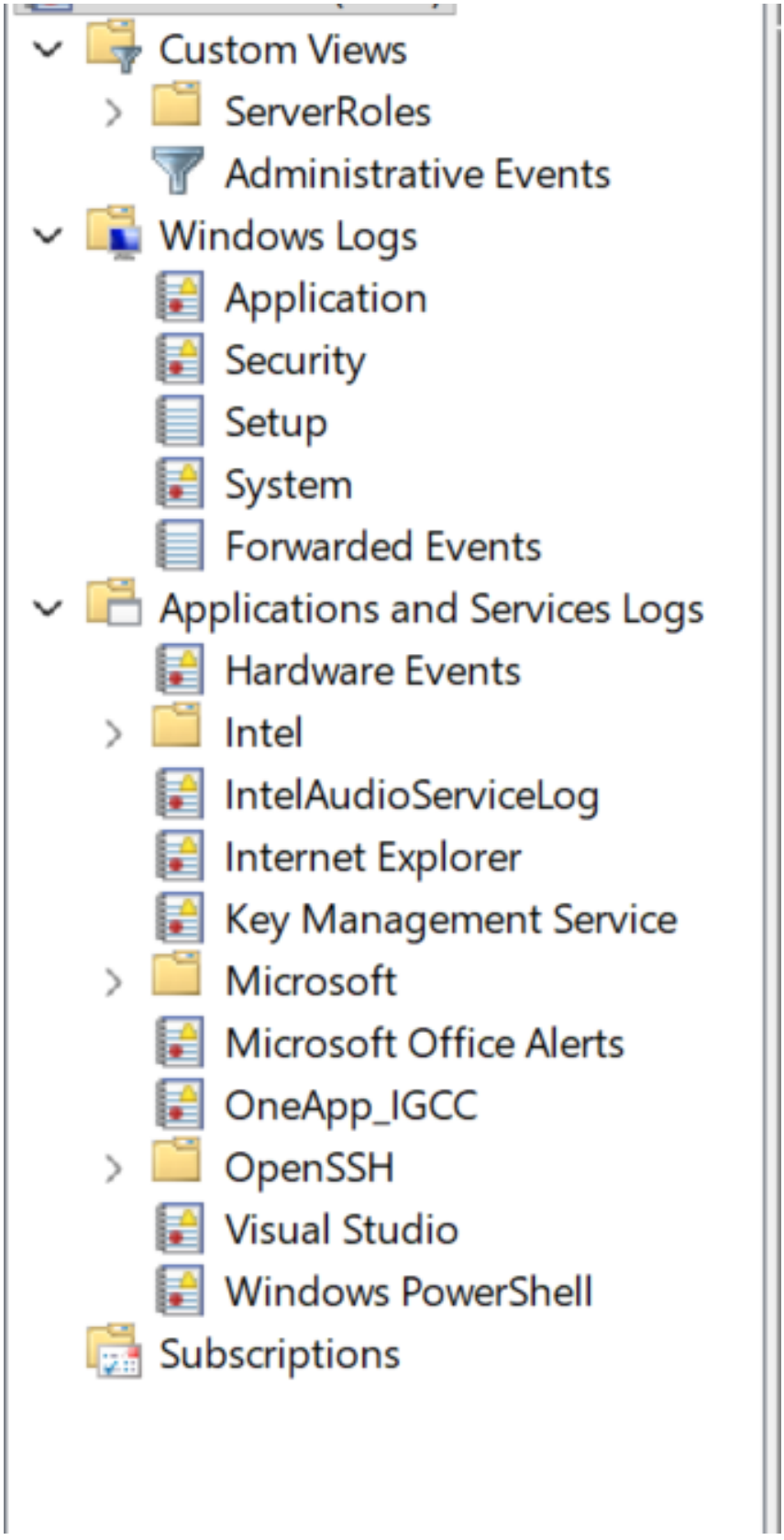

Рисунок 3.1: Структура каналов журналов

4 Инструменты журналирования Windows

4.1 Просмотр событий (Event Viewer)

Event Viewer — основной инструмент администратора для анализа журналов. Позволяет:

- фильтровать события,
- просматривать детали ошибок,
- экспортировать журналы,
- создавать пользовательские представления.

4.1.1 Пример фильтрации событий

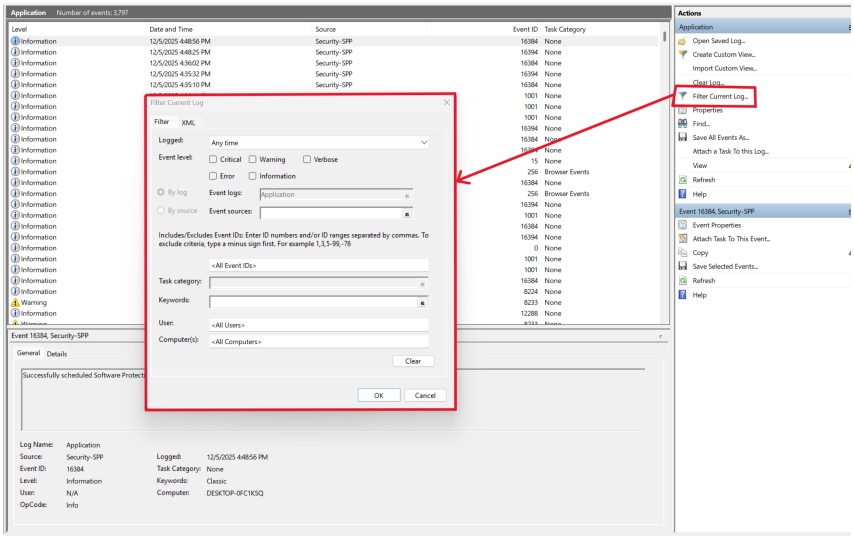

Рисунок 4.1: Фильтрация событий в Event Viewer

4.2 PowerShell для работы с журналами

Наиболее важные команды:

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

4.3 Windows Event Forwarding (WEF)

Используется для централизованного сбора событий на сервер SIEM.

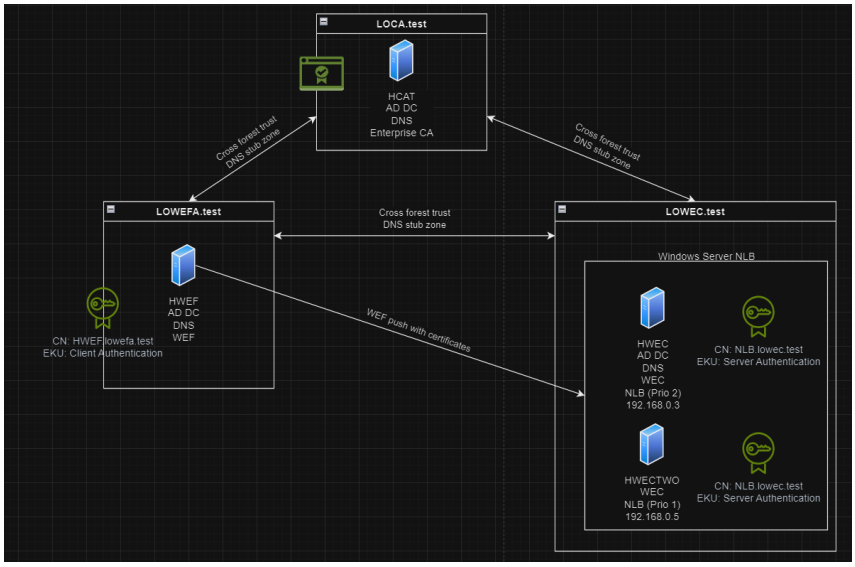

Рисунок 4.2: Схема WEF

5 Журналирование безопасности в Windows

Журнал **Security** является ключевым источником информации для анализа безопасности.

5.1 Основные события безопасности (Event IDs)

Event ID	Описание
4624	Успешный вход
4625	Неуспешный вход
4634	Выход
4720	Создание учетной записи
4726	Удаление учетной записи
1102	Очистка журнала безопасности

5.2 Пример анализа попыток подбора пароля (Brute Force)

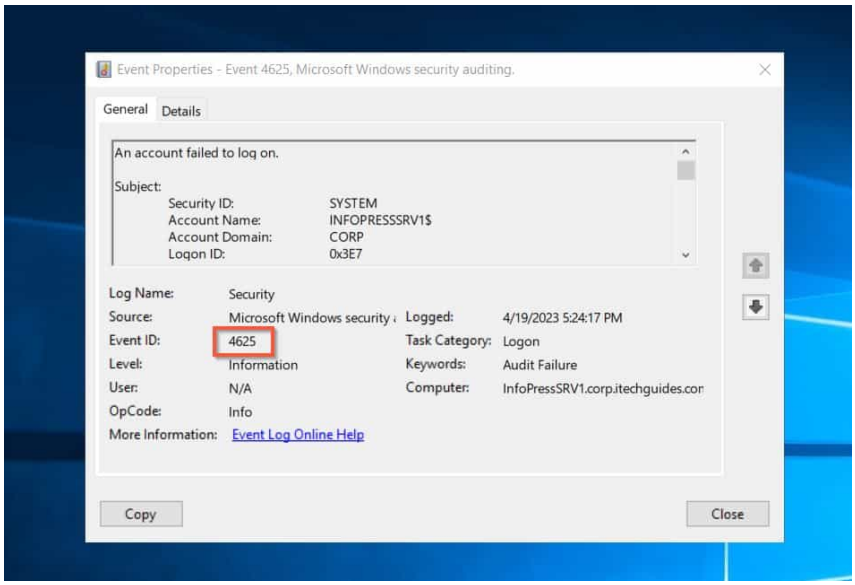

Рисунок 5.1: Пример события 4625

6 Расширенное журналирование и аудит

Windows предоставляет расширенные настройки через:

- Local Security Policy → Advanced Audit Policy Configuration
- Sysmon (Sysinternals)
- Group Policy Objects

6.1 Пример настройки Audit Policies

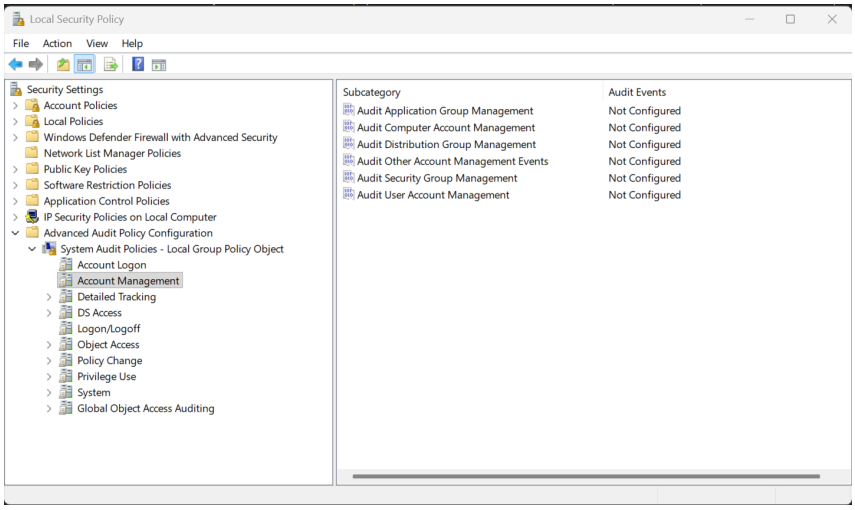

Рисунок 6.1: Audit Policy Configuration

6.2 Sysmon

Sysmon предоставляет:

- логирование сетевых подключений,

- мониторинг процессов,
- создание цепочек событий,
- контроль изменений файлов.

7 Практические примеры использования журналов

7.1 Экспорт журнала событий

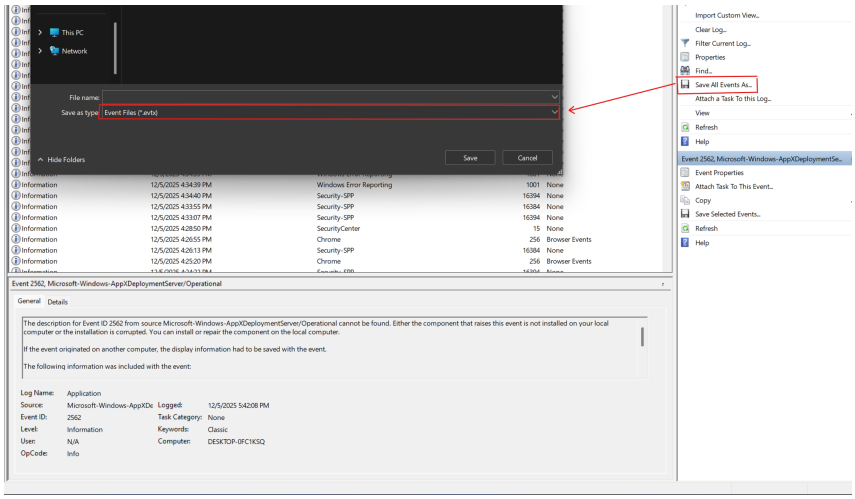

Рисунок 7.1: Экспорт журнала

7.2 Создание пользовательского фильтра

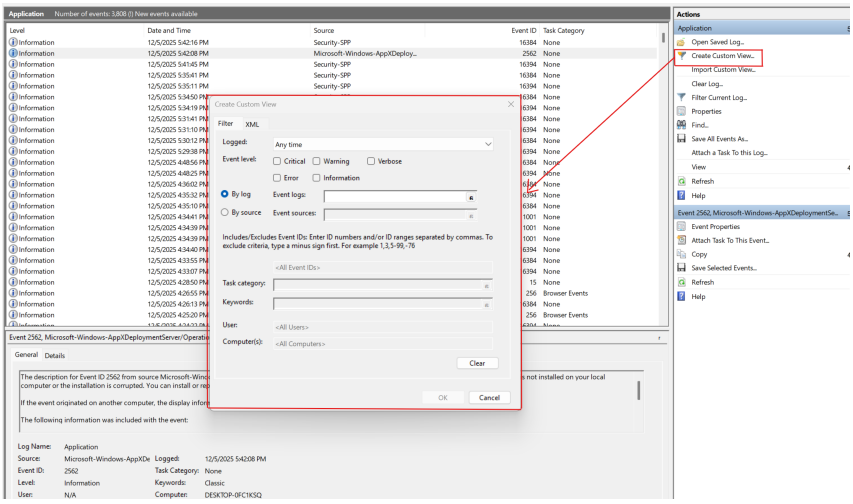

Рисунок 7.2: Custom View

8 Заключение

Журналирование в Windows является фундаментальным инструментом администратора и аналитика безопасности. Правильная настройка журналов позволяет своевременно обнаруживать атаки, анализировать ошибки и обеспечивать надежную работу инфраструктуры. Использование Event Viewer, PowerShell, Sysmon и централизованного сбора событий делает журналирование мощным механизмом обеспечения безопасности и стабильности.

9 Список литературы

- Microsoft Learn. *Windows Event Logging Architecture*. 2023. https://learn.microsoft.com/en-us/windows/win32/eventlog/event-logging
- Microsoft Learn. *Advanced Security Audit Policy*. 2024. https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy
- Microsoft Sysinternals. *Sysmon Documentation*. 2024. https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
- Microsoft Learn. *Monitoring, Logging, and Troubleshooting in Windows*. 2022. https://learn.microsoft.com/en-us/windows-server/administration/windows-logging
- MITRE ATT&CK. *Detection via Windows Event Logs*. 2023. https://attack.mitre.org