

Журналирование в Windows

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

Российский университет дружбы народов (РУДН)

2025-12-05

Содержание I

1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС

1.0.2 Цель презентации

1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев

1.0.2 Цель презентации

1.0.1 Значение журналирования

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

1.0.2 Цель презентации

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

1.0.1 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

1.0.1 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

1.0.1 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

The screenshot shows the Windows Event Viewer application window. The title bar reads "Event Viewer". The menu bar includes "File", "Action", "View", and "Help". The left sidebar shows the "Event Viewer (Local)" tree with nodes for "Custom Views", "Windows Logs", "Applications and Services Logs", and "Subscriptions". The main pane is titled "Event Viewer (Local)" and "Overview and Summary", with a "Last refreshed: 12/5/2025 4:31:57 PM" timestamp. Below the title bar, there is an "Overview" section with a description: "To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below." Below this is a "Summary of Administrative Events" table:

| Event Type | Event ID | Source | Log | Last hour | 24 hours | 7 days |
|---------------|----------|--------|-----|-----------|----------|--------|
| Critical | - | - | - | 0 | 0 | 2 |
| Error | - | - | - | 13 | 13 | 264 |
| Warning | - | - | - | 9 | 9 | 372 |
| Information | - | - | - | 419 | 419 | 18,626 |
| Audit Success | - | - | - | 1,956 | 1,956 | 25,674 |
| Audit Failure | - | - | - | 0 | 0 | 3 |

Below the summary table is a "Recently Viewed Nodes" section with a table:

| Name | Description | Modified | Created |
|--------------------------|-------------|----------------------|-----------------------|
| Windows Logs\Security | N/A | 12/5/2025 4:32:30 PM | 11/25/2025 6:05:52 AM |
| Windows Logs\Application | N/A | 12/5/2025 4:29:20 PM | 11/25/2025 6:05:52 AM |

At the bottom is a "Log Summary" section with a table:

| Log Name | Size (Current) | Modified | Enabled | Retention Policy |
|-------------------------|----------------|-----------------------|---------|----------------------------|
| Windows PowerShell | 15.00 MB/L | 12/5/2025 4:31:19 PM | Enabled | Overwrite events as needed |
| Visual Studio | 68 KB/1.00... | 11/25/2025 6:06:11 AM | Enabled | Overwrite events as needed |
| System | 3.07 MB/2... | 12/5/2025 4:30:26 PM | Enabled | Overwrite events as needed |
| Security | 20.00 MB/L | 12/5/2025 4:31:55 PM | Enabled | Overwrite events as needed |
| OneApp_JGCC | 68 KB/1.00... | 12/5/2025 4:24:06 PM | Enabled | Overwrite events as needed |
| Microsoft Office Alerts | 68 KB/1.00... | 12/3/2025 10:11:19 PM | Enabled | Overwrite events as needed |
| Key Management Service | 68 KB/20... | 11/25/2025 6:06:11 AM | Enabled | Overwrite events as needed |
| Internet Explorer | 68 KB/1.00... | 11/25/2025 6:06:11 AM | Enabled | Overwrite events as needed |
| IntelAudioServiceLog | 68 KB/1.00... | 11/25/2025 6:06:11 AM | Enabled | Overwrite events as needed |

The right sidebar contains an "Actions" section with the following options: "Event Viewer (Local)", "Open Saved Log...", "Create Custom View...", "Import Custom View...", "Connect to Another Computer...", "View", "Refresh", and "Help".

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

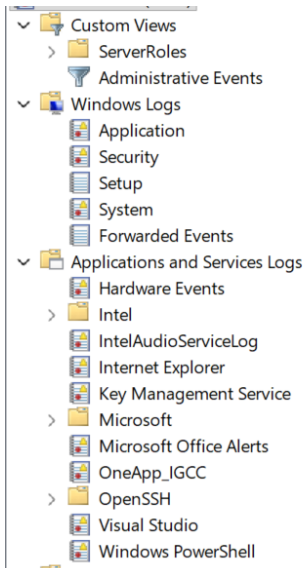
5.0.1 Основные компоненты

- 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

Application Number of events: 3,797

| Level | Date and Time | Source | Event ID | Task Category |
|-------------|----------------------|--------------|----------|----------------|
| Information | 12/5/2025 4:48:56 PM | Security-SPP | 16384 | None |
| Information | 12/5/2025 4:48:25 PM | Security-SPP | 16394 | None |
| Information | 12/5/2025 4:36:02 PM | Security-SPP | 16384 | None |
| Information | 12/5/2025 4:35:32 PM | Security-SPP | 16394 | None |
| Information | 12/5/2025 4:35:10 PM | Security-SPP | 16384 | None |
| Information | | | 1001 | None |
| Information | | | 1001 | None |
| Information | | | 1001 | None |
| Information | | | 16394 | None |
| Information | | | 16384 | None |
| Information | | | 16384 | None |
| Information | | | 15 | None |
| Information | | | 256 | Browser Events |
| Information | | | 16384 | None |
| Information | | | 256 | Browser Events |
| Information | | | 16394 | None |
| Information | | | 1001 | None |
| Information | | | 16384 | None |
| Information | | | 16394 | None |
| Information | | | 0 | None |
| Information | | | 1001 | None |
| Information | | | 1001 | None |
| Information | | | 16384 | None |
| Information | | | 8224 | None |
| Warning | | | 8233 | None |
| Information | | | 12288 | None |
| Information | | | 8233 | None |

Filter Current Log

Filter XML

Logged: Any time

Event level: ☐ Critical ☐ Warning ☐ Verbose ☐ Error ☐ Information

☒ By log Event logs: Application

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel

Actions

- Application
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To This Log...
- View
- Refresh
- Help

Event 16384, Security-SPP

Event Properties

- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

General Details

Successfully scheduled Software Protection

Log Name: Application

Source: Security-SPP

Event ID: 16384

Level: Information

User: N/A

OpCode: Info

Logged: 12/5/2025 4:48:56 PM

Task Category: None

Keywords: Classic

Computer: DESKTOP-QFC1K5Q

9 PowerShell для журналирования

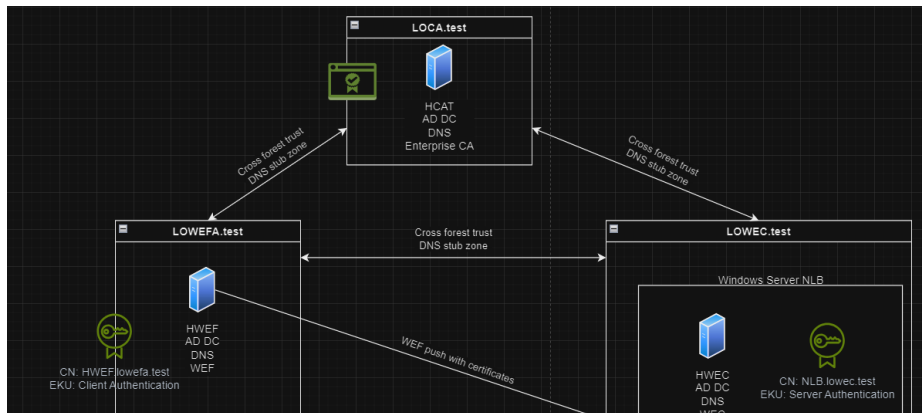
Основные команды:

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


10 Windows Event Forwarding (WEF)

Используется для:

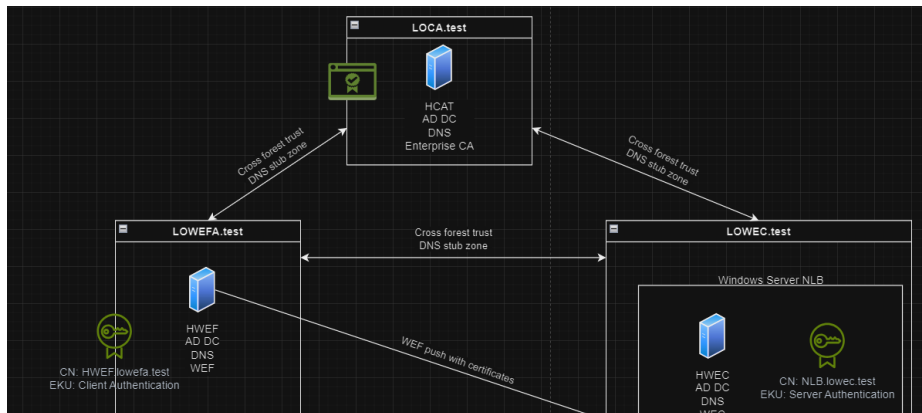
- Централизованного сбора событий



10 Windows Event Forwarding (WEF)

Используется для:

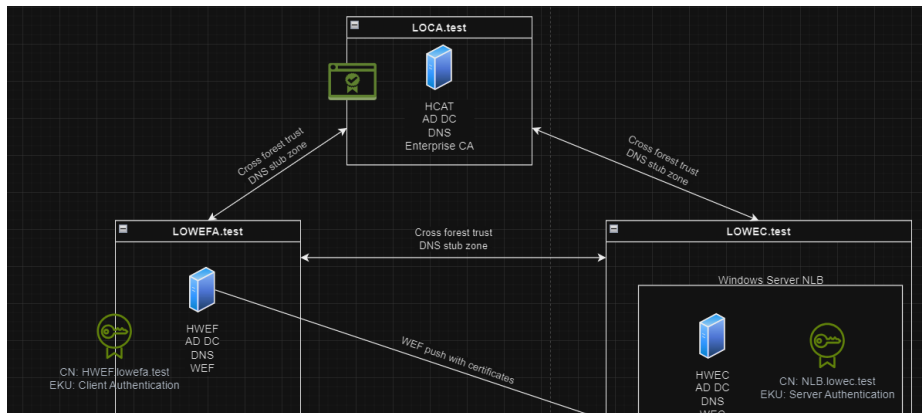
- Централизованного сбора событий
- Интеграции с SIEM



10 Windows Event Forwarding (WEF)

Используется для:

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

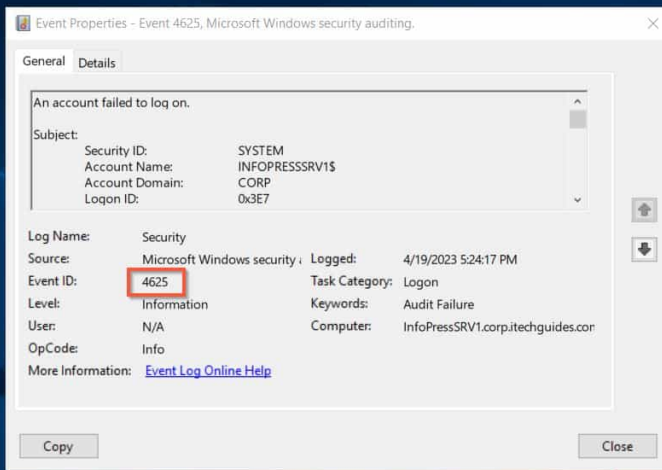


11 Журналирование безопасности

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:

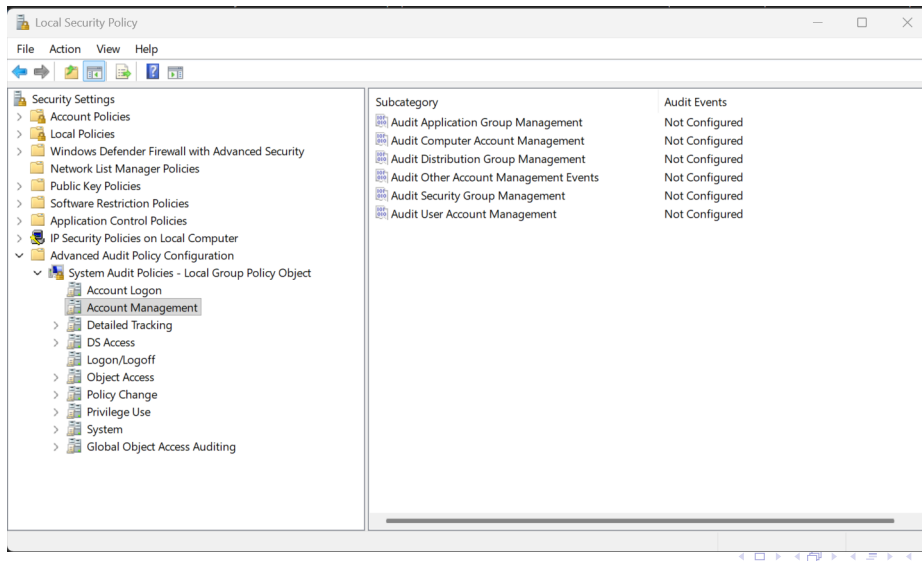
- Local Security Policy
- Advanced Audit Policy Configuration
- Sysmon

13 Расширенный аудит

Набор механизмов включает:

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

14 Настройка Audit Policies



Преимущества:

- Логирование сетевых подключений

Преимущества:

- Логирование сетевых подключений
- Отслеживание процессов

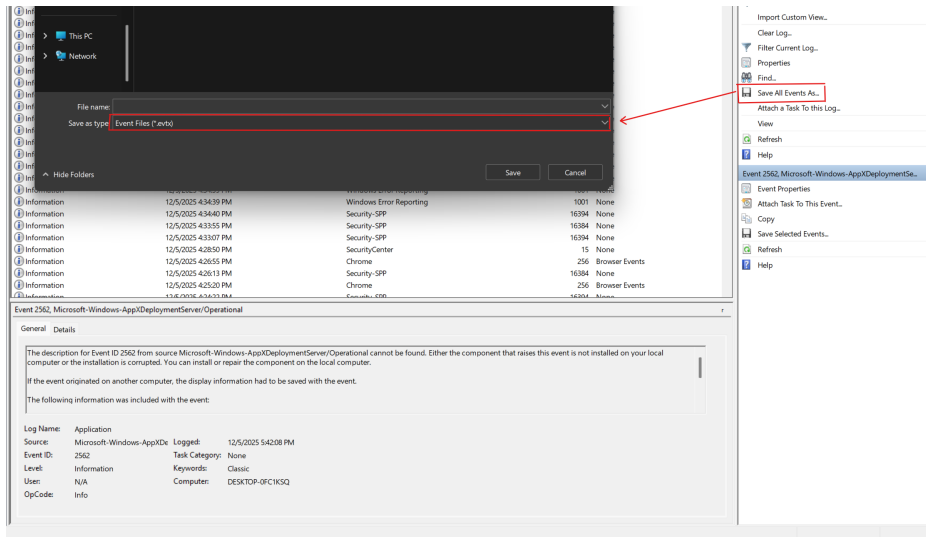
Преимущества:

- Логирование сетевых подключений
- Отслеживание процессов
- Поддержка цепочек событий

Преимущества:

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

16 Экспорт журнала событий



17 Создание Custom View

Application Number of events: 3,808 (0) New events available

| Level | Date and Time | Source | Event ID | Task Category |
|-------------|----------------------|---------------------------------|----------|----------------|
| Information | 12/5/2025 5:42:16 PM | Security-SPP | 16384 | None |
| Information | 12/5/2025 5:42:08 PM | Microsoft-Windows-AppXDeploy... | 2562 | None |
| Information | 12/5/2025 5:41:45 PM | Security-SPP | 16394 | None |
| Information | 12/5/2025 5:35:41 PM | Security-SPP | 16384 | None |
| Information | 12/5/2025 5:35:11 PM | Security-SPP | 16394 | None |
| Information | 12/5/2025 5:34:50 PM | | 16384 | None |
| Information | 12/5/2025 5:34:19 PM | | 16394 | None |
| Information | 12/5/2025 5:31:41 PM | | 6384 | None |
| Information | 12/5/2025 5:31:10 PM | | 6394 | None |
| Information | 12/5/2025 5:30:12 PM | | 6384 | None |
| Information | 12/5/2025 5:29:38 PM | | 6394 | None |
| Information | 12/5/2025 4:48:56 PM | | 6384 | None |
| Information | 12/5/2025 4:48:25 PM | | 6394 | None |
| Information | 12/5/2025 4:36:02 PM | | 6384 | None |
| Information | 12/5/2025 4:35:32 PM | | 6394 | None |
| Information | 12/5/2025 4:35:10 PM | | 6384 | None |
| Information | 12/5/2025 4:34:41 PM | | 1001 | None |
| Information | 12/5/2025 4:34:39 PM | | 1001 | None |
| Information | 12/5/2025 4:34:39 PM | | 6394 | None |
| Information | 12/5/2025 4:34:40 PM | | 6384 | None |
| Information | 12/5/2025 4:33:55 PM | | 6394 | None |
| Information | 12/5/2025 4:33:07 PM | | 15 | None |
| Information | 12/5/2025 4:28:50 PM | | 256 | Browser Events |
| Information | 12/5/2025 4:26:55 PM | | 6384 | None |
| Information | 12/5/2025 4:26:13 PM | | 256 | Browser Events |
| Information | 12/5/2025 4:25:20 PM | | 6384 | None |
| Information | 12/5/2025 4:24:22 PM | | 6394 | None |

Create Custom View

Filter XML

Logged: Any time

Event level: ☐ Critical ☐ Warning ☐ Verbose ☐ Error ☐ Information

☒ By log Event logs:

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel

Event 2562, Microsoft-Windows-AppXDeploymentServer/Operati...

General Details

The description for Event ID 2562 from source Microsoft-Win... computer or the installation is corrupted. You can install or re...

If the event originated on another computer, the display info...

The following information was included with the event:

Log Name: Application

Source: Microsoft-Windows-AppXDe Logged: 12/5/2025 5:42:08 PM

Event ID: 2562 Task Category: None

Level: Information Keywords: Classic

User: N/A Computer: DESKTOP-0FC1KSQ

Actions

Application

Open Saved Log...

Create Custom View...

Import Custom View...

Clear Log...

Filter Current Log...

Properties

Find...

Save All Events As...

Attach a Task To this Log...

View

Refresh

Help

Event 2562, Microsoft-Windows-AppXDeploymentSe...

Event Properties

Attach Task To This Event...

Copy

Save Selected Events...

Refresh

Help

- Журналирование — ключевой инструмент администратора

- Журналирование — ключевой инструмент администратора
- Позволяет обнаруживать атаки

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

- 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!