

Инструкция по настройке журнала событий актуальная

ALD Pro

Exported on 08/11/2023

Table of Contents

1	Термины и определения.....	4
2	Описание	5
3	Обоснование выбора Syslog-ng	6
4	Архитектура Syslog-ng	7
5	1 Серверы журнала событий.....	8
5.1	1.1 Минимальные требования к серверу журнала событий	8
5.2	1.2 Как развернуть сервер журнала событий	8
5.3	1.3 Что происходит при развёртывании сервера.....	8
5.4	1.4 Управление сервером журнала событий	8
5.5	1.5 Удаление сервера журнала событий	9
5.6	1.6 Что происходит при удалении сервера.....	9
6	2 Настройка сбора журналов событий.....	10
6.1	2.1 Правила сбора событий	10
6.2	2.2 Добавление нового правила сбора информации о событиях	10
6.3	2.3 Что происходит при создании правила сбор логов	11
6.4	2.3 Редактирование правила сбора информации о событиях	12
6.4.1	2.3.1 Основное	12
6.4.2	2.3.2 Конфигурационные параметры	12
6.5	2.4 Удаление правила.....	12
6.5.1	2.4.1 Как происходит удаление правила	13
6.6	2.5 Правила при работе с ALD Pro разных версий	13
7	3 Работа с логами	14
7.1	3.1 Просмотр логов на сервере	14
8	4 Использование нескольких серверов аудита.....	15

Актуально для версии 2.0.0 и выше

- [Термины и определения](#)(see page 4)
- [Описание](#)(see page 5)
- [Обоснование выбора Syslog-ng](#)(see page 6)
- [Архитектура Syslog-ng](#)(see page 7)
- [1 Серверы журнала событий](#)(see page 8)
 - [1.1 Минимальные требования к серверу журнала событий](#)(see page 8)
 - [1.2 Как развернуть сервер журнала событий](#)(see page 8)
 - [1.3 Что происходит при развёртывании сервера](#)(see page 8)
 - [1.4 Управление сервером журнала событий](#)(see page 8)
 - [1.5 Удаление сервера журнала событий](#)(see page 9)
 - [1.6 Что происходит при удалении сервера](#)(see page 9)
- [2 Настройка сбора журналов событий](#)(see page 10)
 - [2.1 Правила сбора событий](#)(see page 10)
 - [2.2 Добавление нового правила сбора информации о событиях](#)(see page 10)
 - [2.3 Что происходит при создании правила сбор логов](#)(see page 11)
 - [2.3 Редактирование правила сбора информации о событиях](#)(see page 12)
 - [2.3.1 Основное](#)(see page 12)
 - [2.3.2 Конфигурационные параметры](#)(see page 12)
 - [2.4 Удаление правила](#)(see page 12)
 - [2.4.1 Как происходит удаление правила](#)(see page 13)
 - [2.5 Правила при работе с ALD Pro разных версий](#)(see page 13)
- [3 Работа с логами](#)(see page 14)
 - [3.1 Просмотр логов на сервере](#)(see page 14)
- [4 Использование нескольких серверов аудита](#)(see page 15)

1 Термины и определения

Термин		Определение
Журналирование событий		автоматическая запись информации о событиях, происходящих с некоторым объектом. Ведется в хронологическом порядке. Записывается в локальные файлы, базу данных или т.д. Используется для последующей обработки.
Хронологический порядок		привязка к конкретной дате и времени события.
Логи		Записи о событиях, происходящих в системе и пр
Источник		Именованная коллекция сконфигурированных исходных драйверов.
Пути журналов	(Log paths)	сочетание источников, мест назначения и других объектов, таких как фильтры, синтаксические анализаторы и правила перезаписи. Приложение syslog-ng отправляет сообщения, поступающие из источников путей журнала, в определенные пункты назначения, а также выполняет фильтрацию, анализ и перезапись сообщений. Пути журналов также называются операторами журнала. Операторы могут включать другие (встроенные) операторы журнала и соединения для создания сложных путей журнала.
Security Information and Event Management	SIEM	Инструменты для сбора, анализа, интерпретации и управления информацией об активности в информационной системе, чтобы обнаруживать и предотвращать угрозы безопасности.

2 Описание

Функционал предназначен для настройки сбора логов событий компьютеров домена ALDPro в хронологическом порядке. Данные собираются на сервере журнала событий. Собранные данные могут использоваться для анализа и аудита сторонними SIEM.

Журнал событий в ALD Pro до версии 1.5.0 и ниже основан на [решении Fluentd](#). Инструкция по работе с журналом событий до ALD Pro 1.5.0 [по ссылке](#).

Журнал событий в ALD Pro после версии 1.5.0 и выше основан на [open source решении Syslog-ng](#).

Журнал событий ALD Pro позволяет собирать следующие события: логи авторизации Fly, логи удаленного подключения, логи состояния подключения к сети.

Ограничения:

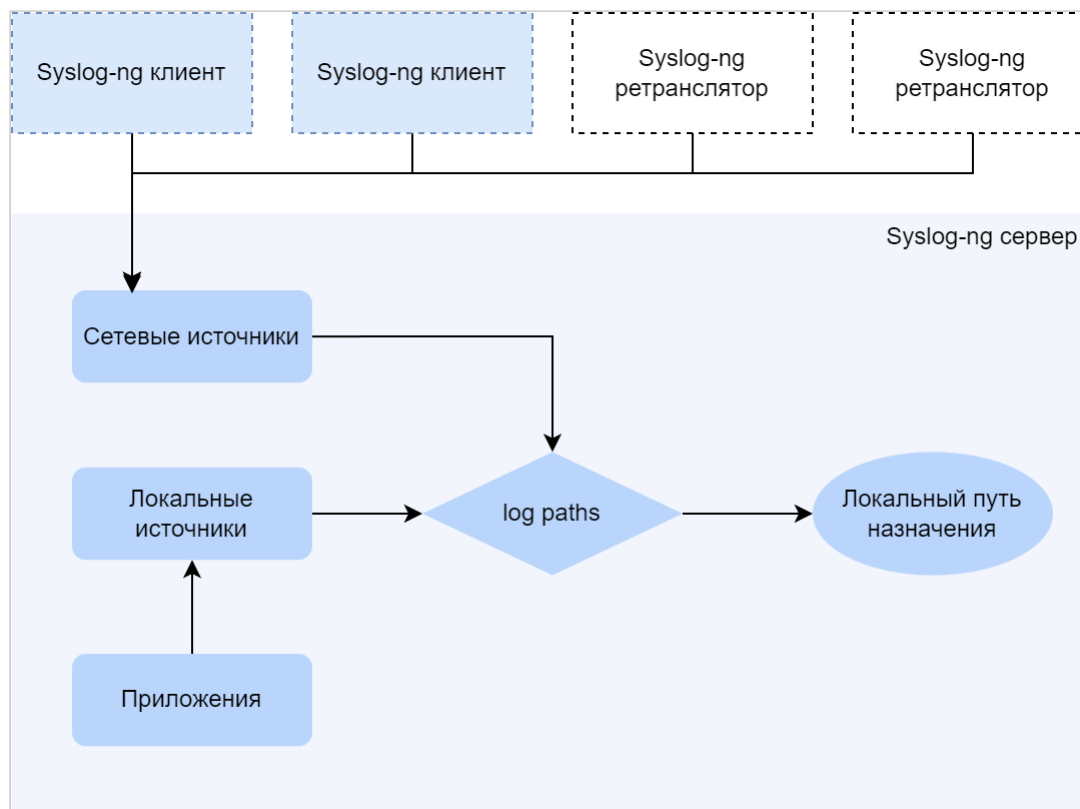
- Расширение списка регистрируемых событий из портала управления не предусмотрено.
- Функционал мониторинга, аудита и реагирования на события на портале управления не предусмотрен.

3 Обоснование выбора Syslog-ng

Syslog-ng это решение для управления журналами событий, которое поддерживает работу AstraLinux и находится в main репозитории операционной системы AstraLinux. Протокол syslog поддерживается большинством популярных SIEM.

4 Архитектура Syslog-ng

В ALD Pro Syslog-ng работает в режиме сервера. Syslog-ng действует как центральный сервер сбора журналов. Он получает сообщения от клиентов syslog-ng и ретранслирует их по сети, сохраняет их локально в файлах или передает другим приложениям, например, для анализа логов.



5 1 Серверы журнала событий

5.1 1.1 Минимальные требования к серверу журнала событий

Количество серверов - 1

Количество CPU\ядер - 2

Оперативная память - 2 Гб

Свободное дисковое пространство - 30 Гб

ОС - до Astra Linux 1.7.4 включительно

5.2 1.2 Как развернуть сервер журнала событий

Путь: Журнал событий → Серверы журнала событий → Развернуть сервер журнала событий

Будет выполнен переход на карточку нового сервера.

На карточке заполнить обязательные поля «Имя компьютера» и «Имя сайта».

Имя компьютера и Имя сайта выбираем из выпадающего списка.

Имя компьютера - какой компьютер будет использоваться в качестве сервера журналирования событий. В выпадающем списке предлагаются компьютеры, незанятые под серверы в других подсистемах и системе журнала событий ранее.

Для сохранения сервера нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов.

Разворачивание сервера может занять некоторое время, отследить выполнение можно 2 способами:

1) Через всплывающие окна в нижнем правом углу экрана. Появляются событийно.

2) Автоматизация → Задания автоматизации → Журнал заданий название задания audit_install

При успешном выполнении задания на разворачивание сервера, он появится в списке серверов на странице Журнал событий → Серверы журнала событий → Развернуть сервер журнала событий.

ALDPro позволяет разворачивать несколько серверов журнала событий. Ограничений на количество серверов в ALDPro нет.

Ограничений на количество серверов журналов событий на одном сайте нет.

5.3 1.3 Что происходит при развёртывании сервера

Агент Syslog-ng используется ОС Astra Linux и уже установлен на компьютерах.

Поэтому, при развёртывании только формируется запись в LDAP о выборе хоста в качестве сервера для журнала событий.

cn={host}, cn=log,cn=services,cn=aldpro, cn=etc,, где host - имя выбранного компьютера, base_dn - dn домена.

5.4 1.4 Управление сервером журнала событий

Путь: Журнал событий → Серверы журнала событий → {Имя компьютера}

Управление сервером журнала событий выполняется на его карточке. Для открытия карточки необходимо в списке серверов журнала событий нажать на соответствующий сервер.

На карточке сервера доступны для редактирования поля «Имя сайта».

Для сохранения изменений нажать на кнопку сохранения в правом верхнем углу.

Будет выполнен переход к списку серверов.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

5.5 1.5 Удаление сервера журнала событий

Путь: Журнал событий → Серверы журнала событий → {Имя компьютера}

Удаление сервера журнала событий осуществляется из его карточки: открыть карточку, нажав в списке серверов на соответствующий сервер, затем на карточке нажать кнопку [Удалить сервер журнала событий]. После подтверждения удаления будет выполнен переход к списку серверов журнала событий.

5.6 1.6 Что происходит при удалении сервера

При удалении сервера в интерфейсе удаляется запись в LDAP `cn=host,cn=service,cn=services,cn=aldpro,cn=etc,{base_dn}`

Раз в сутки и при перезагрузке компьютеров на компьютерах домена актуализируется состояние правил. Правила, работающие с удаленным сервером, перестают работать.

6 2 Настройка сбора журналов событий

6.1 2.1 Правила сбора событий

Путь: Журнал событий → Настройка сбора журналов событий

В подразделе на вкладке «Правила сбора событий» приводится список правил сбора информации о событиях с указанием имени правила и его состояния (включено или выключено).

В списке доступен поиск по имени правила. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

В списке доступна фильтрация по значению «Состояние», для этого необходимо нажать на значок фильтра рядом с названием столбца и отметить требуемые значения для фильтрации.

В левом нижнем углу указано количество правил, а в правом нижнем углу кнопки переключения страниц.

6.2 2.2 Добавление нового правила сбора информации о событиях

Путь: Журнал событий → Настройка сбора журналов событий → Новое правило

Для добавления нового правила необходимо нажать на кнопку [Новое правило], будет выполнен переход на карточку нового правила.

В карточке на вкладке «Основное» заполнить обязательные поля «Имя правила», «Сервер сбора логов» и «Тип логов».

В поле «Тип логов» задается тип событий, информация о которых будет собираться.

На данный момент доступны следующие значения:

- «Логи авторизации Fly» — сбор информации о входе пользователей в графический интерфейс клиентов домена;
- «Логи удаленного подключения» — сбор информации обо всех удаленных подключениях к клиентам домена по протоколу ssh;
- «Логи состояния подключения к сети» — сбор информации о состоянии подключения к сети всех клиентов домена.

Увеличение типов логов планируется на дальнейших этапах.

Внимание

С версии 2.0.0 действует ограничение: для одного сервера логов может использоваться только уникальный тип логов. Другими словами, установить 2 правила сбора логов со значениями «Логи авторизации Fly» (или др из списка) для одного сервера не получится.

Также можно заполнить поле «Описание».

Для включения или выключения правила, соответственно, установить флаг «Включено» или «Выключено».

Создание правила может занять некоторое время, отследить процесс можно 2 способами:

- 1) Через всплывающие окна в нижнем правом углу экрана. Появляются событийно.
- 2) Автоматизация → Задания автоматизации → Журнал заданий название задания add_rule.

6.3 2.3 Что происходит при создании правила сбор логов

Для просмотра и изменения конфигурационных файлов необходимы sudo права.

При создании правила сбора логов на машинах домена в /etc/syslog-ng/ создаются конфигурационные файлы, где указываются какие логи передавать на какой сервер сбора логов. В LDAP создается запись о соответствующем правиле cn={id правила}, cn-audit, {base_dn}.

output_alldpro_options.conf

Реализуется при создании первого правила сбора логов. Не привязано к серверу и типу логов.

Отвечает за настройку правила.

Настраиваются:

1. flush_lines(lines) - задает количество строк, после которых буфер сбрасывается в файл журнала. По умолчанию 1.
2. log_fifo_size(size) - определяет размер кольцевого буфера для фоновой записи журнала. По умолчанию 1000.
3. use_dns(yes/no) - указывает, должен ли syslog-ng использовать DNS для разрешения имени хоста. По умолчанию да.
4. use_fqdn(yes/no) - указывает, должны ли все сообщения журнала содержать полное доменное имя хоста. По умолчанию да.

Универсальные настройки для syslog-ng:

1. chain_hostnames(yes/no) - указывает, должны ли все логи отображаться с именами хостов.
2. keep_hostname(yes/no) - указывает, должно ли имя хоста сохраняться в сообщениях журнала.
3. log_fifo_size(size) - определяет размер кольцевого буфера для фоновой записи журнала.
4. use_dns(yes/no) - указывает, должен ли syslog-ng использовать DNS для разрешения имени хоста.
5. use_fqdn(yes/no) - указывает, должны ли все сообщения журнала содержать полное доменное имя хоста.
6. use_fqdn_dns(yes/no) - указывает, должны ли все сообщения журнала содержать полное доменное имя хоста, разрешенное через DNS.
7. use_time_recvd(yes/no) - указывает, должно ли время получения сообщения быть добавлено в сообщение журнала.
8. use_time_secs(yes/no) - указывает, должно ли время прохождения сообщения быть добавлено в сообщение журнала.
9. use_time_timezone(yes/no) - указывает, должна ли временная зона быть добавлена к сообщению журнала.
10. flush_lines(lines) - задает количество строк, после которых буфер сбрасывается в файл журнала.
11. owner(user) - определяет пользователя, которому принадлежит файл журнала.
12. group(group) - определяет группу, которой принадлежит файл журнала.
13. perm(permissions) - определяет права доступа к файлу журнала.
14. dir_create(mode) - указывает, должна ли директория для файла журнала быть создана автоматически.
15. create_dirs(yes/no) - указывает, должны ли все отсутствующие директории создаваться автоматически.
16. create_mode(mode) - задает права доступа к новым файлам журнала.
17. compress(yes/no) - указывает, должны ли файлы журнала сжиматься.
18. compress_cmd(command) - задает команду для сжатия файлов журнала.
19. compress_options(options) - задает дополнительные параметры для команды сжатия.
20. log_fifo_size(size) - определяет размер кольцевого буфера для фоновой записи журнала.

21. `flush_timeout(timeout)` - указывает, сколько времени должно пройти до сброса буфера в файл журнала.
22. `template(template)` - определяет формат сообщения журнала.

Настройка других параметров остается на усмотрение пользователя и не поддерживается ALD Pro.

output_aldpro_{тип_логов}_filter.conf

Реализуется при первом создании определённого типа правил сбора логов, не привязан к серверу. Отвечает за разграничение потоков логов по типам правил.

output_aldpro_{сервер_сбора_логов}_{тип_логов}_log.conf

Формируется при назначении определённого типа правил. Отвечает за включение правила.

output_aldpro_{сервер_сбора_логов}_destination.conf

Реализуется при первом создании правила на конкретный сервер сбора логов. Отвечает за выбор сервера сбора логов. По умолчанию используется порт 514.

6.4 2.3 Редактирование правила сбора информации о событиях

Путь: Журнал событий → Настройка сбора журналов событий → {Имя правила}

Просмотр информации о правиле доступен на его карточке. Для открытия карточки правила необходимо в списке правил нажать на соответствующее правило.

Информация о правиле представлена на вкладках:

- «Основное» — содержит основную информацию о правиле;

6.4.1 2.3.1 Основное

Путь: Журнал событий → Настройка сбора журналов событий → {Имя правила} → Основное

На этой странице к редактированию доступны:

Описание - содержит произвольные заметки о созданном правиле.

Изменение состояния правила.

Для сохранения нажмите "Сохранить". После сохранения вы останетесь на странице Основное.

6.4.2 2.3.2 Конфигурационные параметры

С версии 2.0.0 не предусмотрена возможность настройки правил сбора логов.

6.5 2.4 Удаление правила

1 способ

Для удаления правила или одновременно несколько правил необходимо в списке правил отметить требуемое правило и нажать кнопку [Удалить].

Чтоб отметить все записи — отметить пункт «Имя правила». Для снятия отметок со всех правил — нажать кнопку закрытия в правом верхнем углу.

2 способ

Также удалить правило можно из его карточки: открыть карточку, нажав в списке правил на соответствующее правило, затем на карточке на вкладке «Основное» нажать кнопку [Удалить правило]. После подтверждения удаления будет выполнен переход к списку правил.

6.5.1 2.4.1 Как происходит удаление правила

Если правило было включено, удаляется конфигурационный файл `output_aldpro_{сервер_сбора_логов}_{тип_логов}_log.conf` в `/etc/syslog-ng/` и запись в LDAP. Если правило не было включено, то удаляется только соответствующая запись в LDAP.

6.6 2.5 Правила при работе с ALD Pro разных версий

Перемещение правил при повышении версии ALD Pro до 2.0.0 и выше происходит автоматически.

Правила у которых были настроены сервера сбора логов являются работоспособными и в версии 2.0.0. **ВАЖНО!** При обновлении Системы до версии 2.0.0 все добавленные правила, у которых не настроен параметр состояния и/или сервер сбора логов, отобразятся в таблице, но будут недоступны для работы в этой версии Системы. Для корректной работы правил, их нужно удалить, развернуть и настроить.

7 3 Работа с логами

7.1 3.1 Просмотр логов на сервере

Логи сохраняются на сервере по пути `/var/log/aldpro/`. Для просмотра файлов логов необходимы `sudo` права.

Формат логов:

`{Тип_логов}_<имя правила rule1>.log`

Типы логов:

Fly - Логи авторизации Fly

Network - Логи состояния подключения к сети

Connection - Логи удаленного подключения

8 4 Использование нескольких серверов аудита

Система не имеет ограничений по количеству серверов аудита. Но поддерживается использование уникального типа логов для одного сервера логов. Т.е. создание двух правил с типом логов, например, Логи авторизации Fly на одном сервере сбора логов запрещено.