ALD Pro

ИНСТРУКЦИИ

НАСТРОЙКА ЖУРНАЛИРОВАНИЯ СОБЫТИЙ

Версия 2.4.1

Содержание

Область применения

Данная инструкция в полном объеме актуальна для домена, в котором на контроллерах домена установлена операционная система (ОС) Astra Linux 1.7.4 или выше, а также установлен ALD Pro версией выше 2.0.0.

Термины и определения

Таблица 2.1. Термины и определения.

Термин	Эквивалент	Определение
Контроллер домена	КД	Сервер, который контролирует определенную область компьютерной сети, а также управляет доступом к различным ресурсам внутри этой области.
Логи	Журналы событий	Записи о различных событиях, происходящих в системе и пр.
Хронологическийпорядок		Упорядоченное по дате и времени расположение (хранение) событий.
Журналированиесобытий		Автоматическая запись информации о событиях, происходящих с некоторым объектом. Ведется в хронологическом порядке. Записывается в локальные файлы, базу данных и т.д. Используется для последующей обработки.
Сервер аудита		Компьютер из состава домена ALD Pro, на котором развернута подсистема аудита
Security Informationand Event Management	SIEM	Инструменты для сбора, анализа, интерпретации и управления информацией об активности в информационной системе, чтобы обнаруживать и предотвращать угрозы безопасности.
Служба каталога		Средство иерархического представления ресурсов и информации об этих ресурсах.
Uniform ResourceLocator	URL	Уникальный адрес ресурса, в котором должны быть специфицированы как минимум протокол и доменное имя ресурса. Также опционально могут быть заполнены и другие части адреса: путь и параметры.
Lightweight DirectoryAccess Protocol	LDAP	Протокол прикладного уровня для доступа к службе каталогов, разработанный как облегчённый вариант протокола DAP. LDAP — относительно простой протокол, использующий TCP/IP и позволяющий производить операции аутентификации (*bind*), поиска (*search*) и сравнения (*compare*), а также операции добавления, изменения или удаления записей.
SSH	Secure SHell	Сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений.
Samba		Пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных операционных системах по протоколу SMB/CIFS.
DNS	Domain Name System	Система доменных имён — это иерархическая децентрализованная система именования для ресурсов, подключённых к глобальной сети, которая ведёт список доменных имён вместе с их числовыми IP-адресами или местонахождениями.
Kerberos		Сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними. Kerberos выполняет аутентификацию в качестве службы аутентификации доверенной третьей стороны, используя криптографический ключ. Kerberos построен на криптографии симметричных ключей и требует наличия центра распределения ключей. Расширения Kerberos могут обеспечить использование криптографии с открытым ключом на определённых этапах аутентификации.
Тэг	TAG (tag)	Произвольная строка, используемая для фильтрации информации в журналах
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.
Источник	source	Именованная коллекция сконфигурированных исходных драйверов.
Internet Protocol	IP	Маршрутизируемый протокол сетевого уровня стека TCP/IP. Именно IP стал тем протоколом, который объединил отдельные компьютерные сети во всемирную сеть Интернет. Неотъемлемой частью протокола является адресация сети.
IP-адрес		Уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP.
DoS атака	denial-of-service attack	Атака типа «отказ в обслуживании» — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён. Отказ системы может быть только первым шагом к овладению системой (если в нештатной ситуации ПО выдаёт какую-либо критическую информацию — например, версию, часть программного кода и т. д.).
ACL	access control list	Список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей). Списки контроля доступа являются основой систем с избирательным управлением доступа (DAC).
DAC	discretionary access control	Управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа. Также используются названия:- дискреционное управление доступом;- контролируемое управление доступом;- разграничительное управление доступом.

Описание

Подсистема аудита ALD Pro реализует централизованный сбор событий служб контроллеров домена в коллекторе, которым выступает сервер аудита, и собранные данные могут в дальнейшем передаваться в систему управления информационной безопасностью и событиями безопасности (SIEM) для дальнейшего анализа.

Журнал событий в ALD Pro для версии 2.0.0 и выше основан на open source решении Syslog-ng и позволяет собирать информацию на сервере журнала событий о следующих событиях безопасности:

1. логи авторизации Fly;
2. логи удаленного подключения;
3. логи состояния подключения к сети.

Подробности о работе с журналом событий из портала управления ALD Pro версией 2.0.0 и выше можно найти в разделе «Журнал событий» Справочного центра.

В ALD Pro не предусмотрено расширение списка регистрируемых событий средствами графического интерфейса портала управления. Данная инструкция содержит необходимую информацию о действиях администратора и настройках, которые которые необходимо сделать на каждом контроллере домена и сервере аудита под управлением ALD Pro. После выполнения этой настройки будет включено журналирование событий и осуществлен сбор журналов на сервере аудита, что позволяет значительно увеличить количество регистрируемых и собираемых на сервере аудита событий безопасности. Кроме того, собираемую на сервере аудите информацию о событиях безопасности можно отправить в стороннюю SIEM (см. скрипт для отправки в разделе 7.1).

Перечень событий безопасности, которые собираются в журналах событий на контроллерах домена и информация о которых перенаправляется на сервер аудита с помощью данной инструкции, приведен в таблице 3.1.

Таблица 3.1. Перечень событий безопасности, настройка журналирования которых рассматривается в настоящей инструкции.

	Наименование события	Эквивалент события в Active Directory (при наличии)	Примечание
1	Подключение к рабочему столу Fly	4624_An_account_was_successfully_logged_on	См. раздел 5.1
2	Ввод некорректных данных аутентификации при подключении к рабочему столуFly	4625_An_account_failed_to_log_on	См. раздел 5.1
3	Отключение сессии рабочего стола Fly		См. раздел 5.1
4	Вход (подключение) по SSH	4624_An_account_was_successfully_logged_on	См. раздел 5.1
5	Ввод некорректных данных аутентификации при подключении поSSH	4625_An_account_failed_to_log_on	См. раздел 5.1
6	Завершение сессии SSH		См. раздел 5.1
7	Чтение информации из службы каталога	1644_ldap_query	См. раздел 5.2
8	Создание нового пользователя (группы) в LDAP	4720_A_user_account_was_created	См. раздел 5.2
9	Изменение пользователя (группы)	4738_A_user_account_was_changed	См. раздел 5.2
10	Удаление пользователя (группы)		См. раздел 5.2
11	Ввод в домен нового компьютера	4741_A_computer_account_was_created	См. раздел 5.2
12	Изменение параметров компьютера в домене	4742_A_computer_account_was_changed	См. раздел 5.2
13	Удаление компьютера из домена		См. раздел 5.2
14	Запрос объекта службы каталога (для CRUD операций)	4661_The_handle_to_an_object_was_requested	См. раздел 5.2
15	Создание новой реплики путем продвижения сервера до контроллера домена	4928_Active_Directory_replica_source_naming_context_established	См. раздел 5.2
16	Удаление контроллера домена, в процессе чего удаляется реплика	4929_Active_Directory_replica_source_naming_context_removed	См. раздел 5.2
17	Добавление и удаление ролей	5136_A_directory_service_object_was_modified	См. раздел 5.2
18	Доступ к файлам в службе Samba	5145_A_network_share_object_was_checked	См. раздел 5.3
19	Ошибка при попытке переноса зоны DNS	6001_dns_server_successfully_completed_transfer_of_zone_version	См. раздел 5.4
20	Успешный перенос зоны DNS	6001_dns_server_successfully_completed_transfer_of_zone_version	См. раздел 5.4
21	Запрос билета подлинности службы Kerberos	4768_A_Kerberos_authentication_ticket_was_requested	См. раздел 5.5
22	Запрос билета TGS службы Kerberos	4769_Kerberos_service_ticket_requested	См. раздел 5.5
23	Сбой при предварительной проверке подлинности Kerberos	4771_Kerberos_pre_authentication_failed	См. раздел 5.5
24	Создание и запуск нового процесса пользователем	4688_A_new_process_has_been_created	См. раздел 5.6
25	Подключение к каталогу LDAP	5156_WFP_has_permitted_connection	См. раздел 5.7

Системные требования

1. Для корректной работы всех описанных ниже сценариев необходимо, чтобы на всех контроллерах домена и серверах аудита была установлена операционная система Astra Linux 1.7.4 или выше. В операционной системе Astra Linux версий **до** версии 1.7.4 используются другие версии пакета службы каталога и включение расширенных атрибутов с помощью команды «`dsconf`» с опцией `config replace nsslapd-auditlog-display-attrs=*` невозможно (выполнение завершается ошибкой). Остальные пункты инструкции выполняются без изменений. Расширенные атрибуты журнала аудита службы каталога - это атрибуты, начинающиеся с символа «#».

2. Для применения настоящей инструкции предварительно необходимо:

- выполнить установку ALD Pro версии 2.0.0 (или выше);
- настроить домен под управлением данного продукта (настроить согласно «Руководству администратора ALD Pro»);
- развернуть подсистему аудита в домене.

Настройка журналирования событий безопасности на КД и сбор данных журналов на сервере аудита

5.1. Настройка журналирования событий из интерфейса портала управления

На портале управления ALD Pro версии 2.0.0 и выше есть возможность включить правила для настройки сборов журналов событий на сервере аудита из состава домена с помощью syslog-ng. Для этого в разделе портала управления «Журнал событий → Настройка сбора журналов событий → Новое правило» необходимо заполнить обязательные поля «Имя правила» (произвольная строка для администратора), «Сервер сбора логов» (выбрать из списка компьютер с развернутой подсистемой аудита) и «Тип логов» (выбрать из списка тип события, информация о котором будет собираться).

Для поля «Тип логов» доступны следующие значения:

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

Более подробно настройка журналирования и сборов событий на сервере аудита из интерфейса портала управления изложена в Справочном центре портала управления ALD Pro в разделе «Журнал событий».

5.2. Настройка журналирования событий службы каталога

5.2.1. Настройка журналирования событий службы каталога на контроллере домена

Все описания настройки журналов в разделах 5.2.1, 5.3.1, 5.4.1, 5.5.1, 5.6.1, 5.7.1 (для каждого КД или сервера общего доступа к файлам из состава домена) и 5.2.2, 5.3.2, 5.4.2, 5.5.2, 5.6.2, 5.7.2 (для сервера аудита) написаны как полностью независимые блоки (то есть каждый раздел 5.2.x, где x - [1,2], можно настраивать полностью самостоятельно), поэтому внутри каждого из разделов идет пункт о перезапуске сервиса `syslog-ng`.

Однако если инструкция применяется целиком, то можно последовательно выполнить все пункты 5.x.1 (где x - [2-7]) для КД и затем перезапустить сервис `syslog-ng` на данном КД или сервере общего доступа к файлам один раз. Затем повторить для следующего КД и т.д.

Затем можно последовательно выполнить все пункты 5.x.2 (где x - [2-7] или какой-то другой набор настроек, которые должны совпадать с настройками соответствующих пунктов на КД) для сервера аудита и перезапустить сервис `syslog-ng` один раз на сервере аудита.

Можно обратиться к разделу 8, где указаны последовательно все команды для полной настройки КД и сервера общего доступа к файлам, а также сервера аудита для сбора всех журналов по данной инструкции.

Во всех командах и примерах далее в документе:

- `ldap://alddc1.ald.lan` - URL в LDAP контроллера домена ALD Pro, на котором требуется включить расширенный аудит;
- `ALDPRO-LAN` - наименование домена ALD Pro, на котором происходит настройка правил;
- `ПАРОЛЬ_АДМИНИСТРАТОРА` - вместо данной строки должен использоваться реальный пароль администратора (пользователя с правами на конфигурацию служб) конкретного КД;
- `100.100.100.100` - IP-адрес компьютера (возможно использование и доменного имени компьютера, но предпочтительно использовать IP-адрес), с развернутой подсистемой аудита.

Перед выполнением команд по конфигурации службы каталога можно выключить запись истории команд в командной строке, чтобы пароль администратора или другого привилегированного пользователя не сохранялся в истории, или же использовать другие

способы (например, не использовать ключ «-w», тогда после ввода каждой команды потребуется ввод пароля администратора, помимо этого, можно использовать переменные среды в командах ниже, куда предварительно необходимо внести нужную информацию).

Ниже приведен минимальный алгоритм включения и настройки файлов журналов службы каталога для выполнения настоящей инструкции. Более подробная информация про назначение журналов службы каталога 389 DS, настройку отображения файлов журналов, а также настройку ротации файлов журналов приведена в разделе 6.1 настоящей инструкции.

Расширенный аудит на сервере службы каталога включается вручную, после чего станет доступен файл журнала аудита `/var/log/dirsrv/slapd-ALDPRO-LAN/audit`.

Команда для включения расширенного аудита на контроллере домена:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-auditlog-logging-enabled=on
```

Расширенный аудит ошибок включается вручную, записи добавляются в общий файл расширенного аудита, который должен быть включён предыдущей командой.

Команда для включения расширенного аудита ошибок на контроллере домена:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-auditfaillog-logging-enabled=on
```

Для включения записи в журнал аудита **основных** расширенных атрибутов операций необходимо добавить в конфигурационный файл службы каталога специальную запись с помощью команды ниже (работает для версии Astr Linux SE 1.7.4 или выше, см. раздел 4 настоящей инструкции). Данная команда должна быть введена без пробелов и переносов строк.

Команда для включения записи в журнал аудита службы каталогов расширенных атрибутов операции:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-auditlog-display-attrs=loginShell,krbExtraData,
↪krbLastPwdChange,krbPasswordExpiration,
x-ald-user-mac,uid,displayName,initials,gecos,sn,homeDirectory,mail,
↪krbPrincipalName,krbCanonicalName,givenName,rbtamiddlename,street,l,st,
↪postalCode,c,employeeNumber,telephoneNumber,title,rbtadp,rbtaou,
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
entyusn,modifyTimestamp,modifiersName,objectClass,ipaNTSecutityIdentifier,cn,
 ↪creatorsName,createTimestamp,modifyTimestamp,nsUniqueId,ipaUniqueId,
 ↪parentid,entryid,uidNumber,gidNumber,entryUUID,dsEntryDN,entrydn
```

Расширенный аудит безопасности включается вручную, после чего станет доступен файл журнала аудита событий безопасности `/var/log/dirsrv/slapd-ALDPRO-LAN/security`.

Команда для включения аудита безопасности на контроллере домена:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-securitylog-logging-enabled=on
```

Примечание: Администратору необходимо настроить ротацию журналов на контроллерах домена и сервере аудита (смотри раздел 6 настоящей инструкции), поскольку размеры журналов будут достаточно большими и возможно полное заполнение ими дискового пространства!

После выполнения необходимых настроек службы каталога для журналирования событий с необходимым в каждом конкретном случае уровнем детальности, требуется провести настройку службы `syslog-ng` для перенаправления с её помощью информации на сервер аудита из логов службы каталога.

Для предварительной настройки службы `syslog-ng` на контроллере домена необходимо:

1. Создать дополнительный каталог `/etc/syslog-ng/siem`;
2. В файле конфигурации `/etc/syslog-ng/syslog-ng.conf` добавить строку для подключения конфигураций службы:

```
@include "/etc/syslog-ng/siem/*.conf"
```

Для выполнения настройки службы `syslog-ng` для пересылки журналов службы каталога на контроллере домена необходимо выполнить следующую последовательность действий (создать набор путей журналов):

1. Настроить единую точку пересылки журналов на сервер аудита в службе `syslog-ng` .
2. Настроить перенаправление журнала доступа службы каталога в точку пересылки

журналов в службе `syslog-ng` .

3. Настроить перенаправление журнала аудита службы каталога в точку пересылки журналов в службе `syslog-ng` .

4. Настроить перенаправление журнала ошибок службы каталога в точку пересылки журналов в службе `syslog-ng` .

5. Настроить перенаправление журнала событий безопасности службы каталога в точку пересылки журналов в службе `syslog-ng` .

Для настройки точки пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/destination.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию (ip-адрес сервера аудита из состава домена):

```
destination d_audit {
    network("100.100.100.100" transport("tcp") port(514) flags(syslog-
↪protocol) template("${ISODATE} ${HOST} ${MESSAGE} ${TAGS}\n"));
};
```

Где `100.100.100.100` - IP-адрес компьютера с развернутой *подсистемой аудита*.

Примечание: При настройке пересылки различных журналов в один и тот же пункт назначения (destination) в службе syslog-ng возникает ошибка дубликатов. Для устранения данной ошибки можно воспользоваться директивой @define allow-config-dups 1, которую необходимо добавить в начало конфигурационного файла /etc/syslog-ng/syslog-ng.conf. Однако данную директиву необходимо применять с осторожностью, поскольку, если дубликаты пунктов назначения содержат различные настройки, то во всех случаях будет использоваться последний встреченный syslog-ng вариант. Что может привести к нежелательному поведению для тех источников, которые были настроены с помощью первого из дубликатов. Администратору рекомендуется разобраться с настройкой пунктов назначения и не использовать директиву @define allow-config-dups 1 без детального понимания ее необходимости.

Для настройки фильтрации записей в журнале доступа к службе каталога на КД и последующего перенаправления отфильтрованных записей в точку пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации

`/etc/syslog-ng/siem/output-dirsrv-access.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
source s_access_dirsrv {
    file("/var/log/dirsrv/slapd-ALDPRO-LAN/access" follow-freq(1) flags(no-
 ↪parse));
};

filter f_access_dirsrv {
    match("MOD" value("MESSAGE")) or match("DEL" value("MESSAGE")) or match(
 ↪"ADD" value("MESSAGE")) or match("SRCH" value("MESSAGE")) or match(
 ↪"connection from" value("MESSAGE")) or match("RESULT" value("MESSAGE"));
};

log {
    source(s_access_dirsrv);
    filter(f_access_dirsrv);
    rewrite
    {
            set-tag("tag-dirsrv-access");
    };
    destination(d_audit);
};
```

Для настройки перенаправления журнала аудита к службе каталога в точку пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-dirsrv-audit.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
source s_audit_dirsrv {
    file("/var/log/dirsrv/slapd-ALDPRO-LAN/audit" follow-freq(1) flags(no-
 ↪parse) );
};

log {
    source(s_audit_dirsrv);
    rewrite
    {
            set-tag("tag-dirsrv-audit");
    };
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    destination(d_audit);
};
```

Поскольку информация в журнал аудита (и в журнал ошибок аудита) службы каталога попадает в формате `ключ: значение\n` и к одному событию может быть достаточно большое количество таких пар, то для объединения всех таких записей от одного события в одну строку (flags(no-multi-line)) можно использовать следующий файл конфигурации (`/etc/syslog-ng/siem/output-dirsrv-audit.conf`):

```
source s_audit_dirsrv {
    file("/var/log/dirsrv/slapd-ALDPRO-LAN/audit"  multi-line-mode(prefix-
↪suffix) multi-line-prefix("time: [0-9]+") multi-line-suffix("\n$") flags(no-
↪multi-line) follow-freq(1));
};

log {
    source(s_audit_dirsrv);
    rewrite
    {
        subst("^", "time: ", value("MESSAGE"));
        set-tag("tag-dirsrv-audit");
    };
    destination(d_audit);
};
```

Для настройки перенаправления журнала ошибок службы каталога в точку пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-dirsrv-error.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
source s_errors_dirsrv {
    file("/var/log/dirsrv/slapd-ALDPRO-LAN/errors" follow-freq(1) flags(no-
↪parse));
};

log {
    source(s_errors_dirsrv);
    rewrite
    {
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
            set-tag("tag-dirsrv-error");
    };
    destination(d_audit);
};
```

Для настройки перенаправления журнала событий безопасности службы каталога в точку пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-dirsrv-security.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
source s_security_dirsrv {
    file("/var/log/dirsrv/slapd-ALDPRO-LAN/security" follow-freq(1) flags(no-
↪parse));
};

log {
    source(s_security_dirsrv);
    rewrite
    {
            set-tag("tag-dirsrv-security");
    };
    destination(d_audit);
};
```

Функция `subst` в данной инструкции используется в файлах конфигурации двумя способами:

- заменяет первый указанный параметр (в нашем случае это строка с наименованием тэга и источника) вторым параметром (в нашем случае это пустая строка) внутри значения, указанного третьим параметром (в нашем случае это текст сообщения соответствующего журнала событий службы каталога);
- заменяет первый указанный параметр (в нашем случае это регулярное выражение, следовательно заменяется строка, которая соответствует этому регулярному выражению) вторым параметром (в нашем случае это пустая строка), затем идет указание типа регулярного выражения (в нашем случае это `type``("``pcre»), где `pcre - perl compartible regular expression`), внутри значения, указанного четвертым параметром (в нашем случае это текст сообщения соответствующего журнала событий службы каталога).

Более подробную информацию по конфигурации службы `syslog-ng` можно посмотреть в справке операционной системы Astra Linux с помощью команды «`man syslog-ng.conf`».

Во всех примерах в данном разделе и ниже в настоящем документе наименования папок и файлов могут задаваться администратором самостоятельно и находиться в других каталогах операционной системы в соответствии с настройками службы `syslog-ng` . Значение параметра `set-tag` для каждого типа лога может быть любым, но именно это значение необходимо использовать при настройки перенаправления событий в соответствующий журнал на сервере аудита из состава домена (смотри раздел 5.2.2).

После выполнения действий необходимо перезапустить службу `syslog-ng` на контроллере домена с помощью следующей команды:

```
systemctl restart syslog-ng
```

5.2.2. Настройка журналирования событий службы каталога на сервере аудита

После выполнения необходимых настроек на контроллере домена, требуется провести настройку службы `syslog-ng` на сервере аудита из состава домена для сбора с помощью нее информации с контроллера домена.

Для предварительной настройки службы `syslog-ng` на сервере аудита необходимо:

1. Создать дополнительный каталог `/etc/syslog-ng/siem`;
2. В файле конфигурации `/etc/syslog-ng/syslog-ng.conf` добавить строку для подключения конфигураций службы:

```
@include "/etc/syslog-ng/siem/*.conf"
```

Для настройки службы `syslog-ng` на сервере аудита необходимо выполнить следующую последовательность действий (каждый пункт из списка ниже сопоставляется с соответствующим пунктом раздела 5.1.1):

1. Настроить точку сбора журналов в службе `syslog-ng` .
2. Настроить перенаправление по тегу журнала доступа службы каталога в журнал службы `syslog-ng` .

3. Настроить перенаправление по тегу журнала аудита службы каталога в журнал службы `syslog-ng` .

4. Настроить перенаправление по тегу журнала ошибок службы каталога в журнал службы `syslog-ng` .

5. Настроить перенаправление по тегу журнала событий безопасности службы каталога в журнал службы `syslog-ng` .

Перед выполнением следующего пункта необходимо убедиться, что источник «`source s_net`» не был создан предварительно (например при настройке сбора журналов на сервере аудита из портала управления). Для этого необходимо осуществить поиск подстроки «`source s_net`» по всем каталогам в файлах «*.conf», в которых служба `syslog-ng` читает файлы конфигурации (пути к каталогам начинаются с символа «@» и чаще всего находятся в файле `/etc/syslog-ng/syslog-ng.conf`). Если такой источник был найден и совпадает с приведенным ниже, то следующий пункт по созданию файла `/etc/syslog-ng/siem/source.conf` не выполняется. Если же источник «`s_net`» не был найден, то тогда для настройки точки сбора журналов службы каталогов в службе `syslog-ng` на сервер аудита необходимо создать файл конфигурации `/etc/syslog-ng/siem/source.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
source s_net {
    network(
        transport("tcp")
        port(514)
        flags(syslog-protocol)
        log_iw_size(65536)
        max_connections(1000)
    );
};
```

Для настройки перенаправления по тэгу журнала доступа к службе каталога в журнал службы `syslog-ng` необходимо создать файл конфигурации этого журнала `/etc/syslog-ng/siem/input-dirsrv-access.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_access_dirsrv_file {
    file("/var/log/aldpro/access_dirsrv.log" template("${MESSAGE}\n"));
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
filter f_dirsrv_access {
    message("tag-dirsrv-access");
};

log {
    source(s_net);
    filter(f_dirsrv_access);
    rewrite {
        subst(" tag-dirsrv-access,.source.s_access_dirsrv", "", value(
↪"MESSAGE"));
    };
    destination(d_access_dirsrv_file);
};
```

Для настройки перенаправления по тэгу журнала аудита службы каталога в журнал службы `syslog-ng` необходимо создать файл конфигурации этого журнала `/etc/syslog-ng/siem/input-dirsrv-audit.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_audit_dirsrv_file {
    file("/var/log/aldpro/audit_dirsrv.log" template("${MESSAGE}\n"));
};

filter f_dirsrv_audit {
    message("tag-dirsrv-audit");
};

log {
    source(s_net);
    filter(f_dirsrv_audit);
    rewrite {
        subst(" tag-dirsrv-audit,.source.s_audit_dirsrv", "", value("MESSAGE
↪"));
    };
    destination(d_audit_dirsrv_file);
};
```

Для настройки перенаправления по тэгу журнала ошибок в службе каталога в журнал

службы `syslog-ng` необходимо создать файл конфигурации этого журнала `/etc/syslog-ng/siem/input-dirsrv-error.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_error_dirsrv_file {
    file("/var/log/aldpro/error_dirsrv.log" template("${MESSAGE}\n"));
};

filter f_dirsrv_error {
    message("tag-dirsrv-error");
};

log {
    source(s_net);
    filter(f_dirsrv_error);
    rewrite {
        subst(" tag-dirsrv-error,.source.s_errors_dirsrv", "", value("MESSAGE
↪"));
    };
    destination(d_error_dirsrv_file);
};
```

Для настройки перенаправления по тэгу журнала событий безопасности в службе каталога в журнал службы `syslog-ng` необходимо создать файл конфигурации этого журнала `/etc/syslog-ng/siem/input-dirsrv-security.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_security_dirsrv_file {
    file("/var/log/aldpro/security_dirsrv.log" template("${MESSAGE}\n"));
};

filter f_dirsrv_security {
    message("tag-dirsrv-security");
};

log {
    source(s_net);
    filter(f_dirsrv_security);
    rewrite {
        subst(" tag-dirsrv-security,.source.s_security_dirsrv", "", value(
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
 ↪"MESSAGE"));
    };
    destination(d_security_dirsrv_file);
};
```

Во всех примерах в данном разделе и ниже в документе наименования папок и файлов задаются администратором самостоятельно и находиться в других каталогах операционной системы в соответствии с необходимыми администратору настройками. Также значение параметра `message` внутри фильтра (filter) должно совпадать с соответствующим параметром `set-tag` для каждого типа лога (смотри раздел 5.2.1).

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

5.3. Настройка журналирования событий доступа к файлам в службе Samba

5.3.1. Настройка журналирования событий доступа к файлам в службе Samba на сервере общего доступа к файлам

Для включения записи событий доступа к файлам в службе Samba в файле конфигурации `/etc/samba/smb.conf` в секцию «global» добавить следующие строки:

```
vfs objects = full_audit
full_audit:prefix = %u|%I|%S
full_audit:success = connect, create_file, linkat, mkdirat, open, read,
 ↪renameat, unlinkat, write
full_audit:failure = connect, create_file, linkat, mkdirat, open, read,
 ↪renameat, unlinkat, write
full_audit:facility = local5
full_audit:priority = notice
```

Если в файле конфигурации `/etc/samba/smb.conf` в секции «global» присутствует следующая строка: `log level = N`, где N - это уровень журналирования событий в

службе, то к данной строке дописываем через пробел строку « vfs:1». Если такой строки нет, то записываем:

```
log level = 1 vfs:1
```

После этого необходимо перезапустить службу `samba` и службу `winbind` с помощью следующей команды:

```
systemctl restart smbd winbind
```

Для предварительной настройки службы `syslog-ng` на сервере общего доступа к файлам необходимо:

1. Создать дополнительный каталог `/etc/syslog-ng/siem`;
2. В файле конфигурации `/etc/syslog-ng/syslog-ng.conf` добавить строку для подключения конфигураций службы:

```
@include "/etc/syslog-ng/siem/*.conf"
```

Для настройки службы `syslog-ng` на сервере общего доступа к файлам необходимо выполнить следующую последовательность действий:

1. Настроить единую точку пересылки журналов на сервер аудита в службе `syslog-ng` .
2. Настроить перенаправление журнала службы Samba в точку пересылки журналов в службе `syslog-ng` .

Для настройки точки пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/destination.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_audit {
    network("100.100.100.100" transport("tcp") port(514) flags(syslog-
↪protocol) template("${ISODATE} ${HOST} ${PROGRAM} ${MESSAGE} ${TAGS}\n"));
};
```

Где 100.100.100.100 - IP-адрес компьютера, с развернутой подсистемой аудита.

Для настройки перенаправления записей о доступе к файловым ресурсам службы `Samba` из системного журнала в точку пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-samba.conf` с правами на

чтение всем пользователям и внести в этот файл следующую информацию:

```
filter f_smbd {
    program('smbd_audit');
};

log {
    source(s_src);
    filter(f_smbd);
    destination(d_audit);
};
```

Примечание: Источник source(s_src) описан в файле /etc/syslog-ng/syslog-ng.conf.

После выполнения настроек необходимо перезапустить службу `syslog-ng` на сервере общего доступа к файлам с помощью следующей команды:

```
systemctl restart syslog-ng
```

5.3.2. Настройка журналирования событий доступа к файлам в службе Samba на сервере аудита

Далее приведена настройка файлов конфигурации службы `syslog-ng` на сервере аудита. Если предварительная настройка службы `syslog-ng`, а также если настройка точки сбора журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/source.conf`) не выполнялись, то необходимо произвести настройки в соответствии с описанием в разделе 5.2.2 настоящей инструкции. Затем необходимо создать набор файлов конфигурации для фильтрации событий службы samba.

Для настройки журнала службы samba в службе `syslog-ng` на сервере аудита необходимо создать файл `/etc/syslog-ng/siem/input-samba.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_samba {
    file("/var/log/aldpro/samba.log" template("${MESSAGE}\n"));
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
filter f_samba {
    message("smbd_audit");
};

log {
    source(s_net);
    filter(f_samba);
    rewrite {
        subst(" .source.s_src", "", value("MESSAGE"));
    };
    destination(d_samba);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

5.4. Настройка журналирования событий переноса зоны DNS

5.4.1. Настройка журналирования событий переноса зоны DNS на контроллере домена

Настройка журналирования событий переноса зоны DNS на контроллере домена выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки пересылки журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/destination.conf`) в соответствии с описанием в разделе 5.2.1 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий переноса зоны DNS.

Для настройки журналирования событий переноса зоны на контроллере домена необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-dns-zone.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
filter f_dnszone {
    message('AXFR') or message('IXFR');
};

log {
    source(s_src);
    filter(f_dnszone);
    destination(d_audit);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на контроллере домена с помощью следующей команды:

```
systemctl restart syslog-ng
```

5.4.2. Настройка журналирования событий переноса зоны DNS на сервере аудита

Настройка журналирования событий переноса зоны DNS на сервере аудита выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки сбора журналов в службе `syslog-ng` (создание файла конфигурации /etc/syslog-ng/siem/source.conf) в соответствии с описанием в разделе 5.2.2 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий переноса зоны DNS.

Для настройки журналирования событий переноса зоны на сервере аудита необходимо создать файл конфигурации `/etc/syslog-ng/siem/input-dns-zone.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
destination d_dnszone {
    file("/var/log/aldpro/dnszone.log" template("${MESSAGE}\n"));
};

filter f_dnszone {
    message('AXFR') or message('IXFR');
};

log {
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    source(s_net);
    filter(f_dnszone);
    rewrite {
        subst(" .source.s_src", "", value("MESSAGE"));
    };
    destination(d_dnszone);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

5.5. Настройка журналирования событий Kerberos

5.5.1. Настройка журналирования событий Kerberos на контроллере домена

На первом этапе необходимо настроить службу `Kerberos`. Для этого необходимо:

1. В файле `/lib/systemd/system/krb5-kdc.service` в параметр `ReadWriteDirectories` добавить `/var/log`;
2. Перечитать файл: `systemctl daemon-reload`;
3. Перезапустить службу: `systemctl restart krb5-kdc.service`.

Настройка журналирования событий `Kerberos` на контроллере домена выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки пересылки журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/destination.conf`) в соответствии с описанием в разделе 5.2.1 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий `Kerberos`.

Для настройки журналирования событий Kerberos на контроллере домена необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-krb-audit.conf` с

правами на чтение для всех пользователей и внести в него следующую информацию:

```
source s_krb_audit {
    file("/var/log/krb5kdc.log" follow-freq(1) flags(no-parse) );
};

filter f_krb_audit {
    match("AS_REQ" value("MESSAGE")) or match("TGS_REQ" value("MESSAGE"));
};

log {
    source(s_krb_audit);
    filter(f_krb_audit);
    rewrite
    {
        set-tag("tag-krb-audit");
    };
    destination(d_audit);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на контроллере домена с помощью следующей команды:

```
systemctl restart syslog-ng
```

5.5.2. Настройка журналирования событий Kerberos на сервере аудита

Настройка журналирования событий Kerberos на сервере аудита выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки сбора журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/source.conf`) в соответствии с описанием в разделе 5.2.2 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий Kerberos.

Для настройки журналирования событий `Kerberos` на контроллере домена необходимо создать файл конфигурации `/etc/syslog-ng/siem/input-krb-audit.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
destination d_krb_audit_file {
    file("/var/log/aldpro/krb_audit.log" template("${MESSAGE}\n"));
};

filter f_krb_audit {
    message("tag-krb-audit");
};

log {
    source(s_net);
    filter(f_krb_audit);
    rewrite {
        subst(" tag-krb-audit,.source.s_krb_audit", "", value("MESSAGE"));
    };
    destination(d_krb_audit_file);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

5.6. Настройка журналирования событий создания и запуска нового процесса пользователем

5.6.1. Настройка журналирования событий создания и запуска нового процесса пользователем на контроллере домена

Для настройки журналирования событий создания и запуска нового процесса пользователем на контроллере домена необходимо создать файл `/etc/audit/rules.d/siem.rules` со следующим содержимым (или добавить в этот файл следующие строки, если он уже создан):

```
-a always,exit -F arch=b32 -S execve -F auid>=1000
-a always,exit -F arch=b64 -S execve -F auid>=1000
```

Внести в файл /etc/audit/audit.conf следующее изменение (для установки максимального размера файла `/var/log/audit/audit.log` в мегабайтах):

```
max_log_file = 500
```

И перезапустить службу `auditd` следующей командой:

```
systemctl restart auditd
```

Настройка журналирования событий создания и запуска нового процесса пользователем на контроллере домена выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки пересылки журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/destination.conf`) в соответствии с описанием в разделе 5.2.1 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий создания и запуска нового процесса пользователем.

Для настройки журналирования событий создания и запуска нового процесса пользователем на контроллере домена необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-user-proc.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
source s_user_proc {
    file("/var/log/audit/audit.log" flags(no-parse) persist-name("user_proc
↪") follow-freq(1));
};

filter f_user_proc {
        match("syscall=59" value("MESSAGE"));
};

log {
    source(s_user_proc);
    filter(f_user_proc);
    destination(d_audit);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на контроллере домена с помощью следующей команды:

```
systemctl restart syslog-ng
```

5.6.2. Настройка журналирования событий создания и запуска нового процесса пользователем на сервере аудита

Настройка журналирования событий создания и запуска нового процесса пользователем на сервере аудита выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки сбора журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/source.conf`) в соответствии с описанием в разделе 5.2.2 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий создания и запуска нового процесса пользователем.

Для настройки журналирования событий создания и запуска нового процесса пользователем на сервере аудита необходимо создать файл конфигурации `/etc/syslog-ng/siem/input-user-proc.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
destination d_user_proc {
    file("/var/log/aldpro/userproc.log" template("${MESSAGE}\n"));
};

filter f_user_proc {
        match("syscall=59" value("MESSAGE"));
};

log {
    source(s_net);
    filter(f_user_proc);
    rewrite {
        subst(" .source.s_user_proc", "", value("MESSAGE"));
    };
    destination(d_user_proc);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

5.7. Настройка журналирования события подключения к каталогу LDAP

5.7.1. Настройка журналирования события подключения к каталогу LDAP на контроллере домена

Для настройки журналирования событий подключения к каталогу LDAP на контроллере домена необходимо создать файл `/etc/audit/rules.d/siem.rules` со следующим содержимым (или добавить в этот файл следующие строки, если он уже создан):

```
-a always,exit -S accept -S accept4 -F exe=/usr/sbin/ns-slapd -k ldapconnect
-a exit,always -F exit=-EACCES -F exe=/usr/sbin/ns-slapd -k ldapconnect
```

Где `ldapconnect` - строка, которая является ключом для фильтрации сообщений и может задаваться администратором произвольно (но затем эта строка используется в файлах конфигурации).

После внесения изменений необходимо перезапустить службу `auditd` следующей командой:

```
systemctl restart auditd
```

Настройка журналирования событий подключения к каталогу LDAP на контроллере домена выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки пересылки журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/destination.conf`) в соответствии с описанием в разделе 5.2.1 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий подключения к каталогу LDAP.

Для настройки журналирования событий подключения к каталогу LDAP на контроллере домена необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-ldapconnect.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
source s_ldap {
    file("/var/log/audit/audit.log" flags(no-parse) persist-name("ldap_conn
↪") follow-freq(1));
};

filter f_ldapconnect {
    message('ldapconnect');
};

log {
    source(s_ldap);
    filter(f_ldapconnect);
    destination(d_audit);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на контроллере домена с помощью следующей команды:

```
systemctl restart syslog-ng
```

5.7.2. Настройка журналирования события подключения к каталогу LDAP на сервере аудита

Настройка журналирования событий подключения к каталогу LDAP на сервере аудита выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки сбора журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/source.conf`) в соответствии с описанием в разделе 5.2.2 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий подключения к каталогу LDAP.

Для настройки журналирования событий подключения к каталогу LDAP на сервере аудита необходимо создать файл конфигурации `/etc/syslog-ng/siem/input-ldapconnect.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
destination d_ldapconnect {
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    file("/var/log/aldpro/ldapconnect.log" template("${MESSAGE}\n"));
};

filter f_ldapconnect {
    message("ldapconnect");
};

log {
    source(s_net);
    filter(f_ldapconnect);
    rewrite {
        subst(" .source.s_ldap", "", value("MESSAGE"));
        subst(' key="ldapconnect"', "", value("MESSAGE"));
    };
    destination(d_ldapconnect);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

Ротация журналов

6.1. Настройка режимов ведения и ротации журналов событий службы каталога на контроллерах домена

Вся конфигурационная информация службы каталога находится в файле `dse.ldif`, в главной ветке хранения информации о конфигурации `cn=config`, как это показано на следующем рисунке:

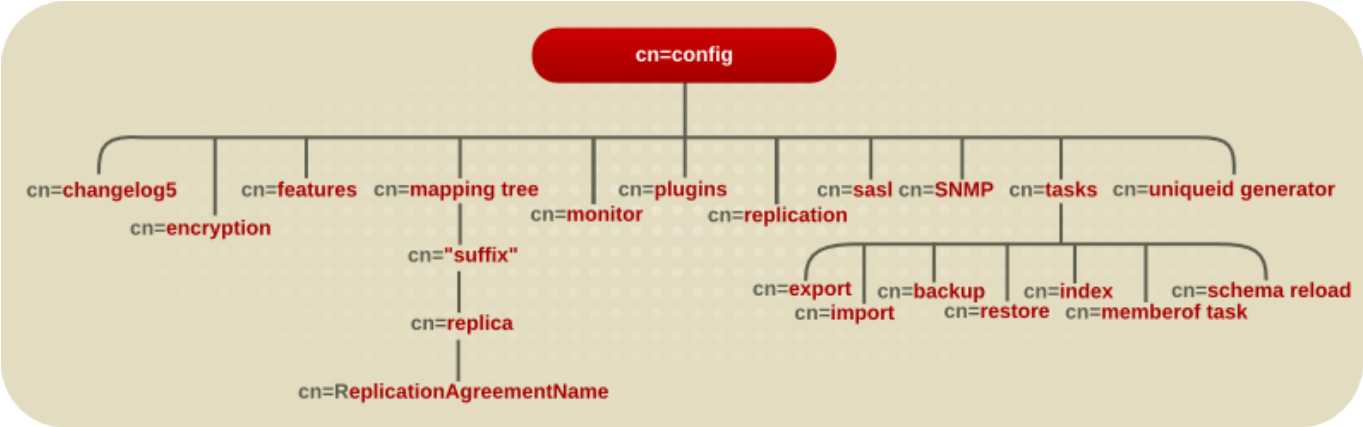

Рисунок 6.1 – Ветка службы каталога, показывающая записи для хранения различных данных о конфигурации.

Важно: Перед внесением любых изменений в конфигурацию подсистемы журналирования службы каталога администратору **настоятельно рекомендуется** ознакомиться с данным разделом в полном объёме!

Служба каталога 389 Directory Server может осуществлять запись о событиях журналы следующих типов:

- `access log` - журнал доступа, который содержит информацию о клиентских подключениях и попытках подключения к экземпляру сервера каталогов; данный тип журнала включен по умолчанию;
- `error log` - журнал ошибок, который содержит подробные сообщения об ошибках и неудачных операциях, а также о событиях, с которыми служба каталога сталкивается во время работы; при установке определенных уровней журналирования для данного

типа журнала в него записываются сообщения о транзакциях и операциях сервера каталогов или общая информацию о процессах сервера каталогов и задачах LDAP, например сообщения о запуске сервера, входах в систему и поиске в каталоге, а также информация о соединении; данный тип журнала включен по умолчанию;

- `audit log` - журнал аудита, который записывает **успешные** изменения, внесенные в каждую базу данных службы каталога, а также в конфигурацию сервера; данный тип журнала **не включен по умолчанию**;
- `audit fail log` - журнал ошибок аудита, который записывает только события о **неудачных** попытках изменений в базе данных или конфигурации сервера, этот тип журнала имеет идентичный формат с типом журнала аудита; данный тип журнала **не включен по умолчанию**;
- `security log` - журнал событий безопасности, который записывает ряд событий об ошибках авторизации/аутентификации, блокировки учетных записей, событий DoS и TCP атак и прочее; данный тип журнала **не включен по умолчанию**.

Каждый из типов журналов имеет свой формат (кроме журналов аудита и ошибок аудита, которые имеют идентичный формат).

Примечание: Если серверу службы каталога не удается выполнить запись в журнал ошибок, сервер отправляет сообщение об ошибке в службу системного журнала (чаще всего это служба `syslog`) и завершает работу.

Чтобы посмотреть пути для сохранения файлов журналов данного экземпляра службы каталога на конкретном КД можно выполнить команду:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config get nsslapd-accesslog nsslapd-errorlog nsslapd-auditlog nsslapd-
↪auditfaillog nsslapd-securitylog
```

Пример результата (для всех файлов использованы значения по умолчанию):

```
nsslapd-accesslog: /var/log/dirsrv/slapd-ALDPRO-LAN/access
nsslapd-errorlog: /var/log/dirsrv/slapd-ALDPRO-LAN/errors
nsslapd-auditlog: /var/log/dirsrv/slapd-ALDPRO-LAN/audit
nsslapd-auditfaillog: /var/log/dirsrv/slapd-ALDPRO-LAN/audit
nsslapd-securitylog: /var/log/dirsrv/slapd-ALDPRO-LAN/security
```

Для изменения конфигурация включения файлов журналов на каждом контроллере

домена необходимо выполнить команды для каждого файла журнала, при этом необходимо использовать опцию replace. Для изменения режима ведения различных типов журналов (включения записи в журнал или прекращения записи) необходимо использовать параметры, приведенные в таблице 6.1. Для включения ведения журналов определенного типа необходимо использовать опцию on.

Таблица 6.1. Параметры изменения режима ведения всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	`nsslapd-accesslog-logging-enabled`	on	on/off
error log	`nsslapd-errorlog-logging-enabled`	on	on/off
audit log	`nsslapd-auditlog-logging-enabled`	off	on/off
audit fail log	`nsslapd-auditfaillog-logging-enabled`	off	on/off
security log	`nsslapd-securitylog-logging-enabled`	off	on/off

Пример включения ведения файла `security` на конкретном экземпляре сервера каталога:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-securitylog-logging-enabled=on
```

Если ведение журнала определенного типа включено, то для изменения пути для сохранения файла используется команда dsconf с опцией `config replace` и параметрами `nsslapd-accesslog`, `nsslapd-errorlog`, `nsslapd-auditlog`, `nsslapd-auditfaillog`, `nsslapd-securitylog`.

Пример изменения пути и наименования для сохранения журнала безопасности службы каталога на конкретном экземпляре сервера каталога:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-securitylog=/var/log/dirsrv_security.log
```

Журнал доступа, и журнал ошибок могут записывать разные объемы информации в зависимости от установленного уровня журналирования. Администратор службы каталога может установить следующие параметры конфигурации для управления уровнями

журналирования:

1. ля журнала доступа: `nsslapd-accesslog-level` (необходимо установить значение on, по умолчанию `off`)
2. для журнала ошибок: `nsslapd-errorlog-level` (необходимо установить значение on, по умолчанию `off`)

Изменение уровня журналирования для журнала доступа, установленного по умолчанию, может привести к очень быстрому росту файла журнала. В документации, описывающей службу каталога, не рекомендуется изменять значения по умолчанию без предварительного контакта со службой технической поддержки.

Значения параметров для установки уровня журналирования в журнала доступа к службе каталога:

- 0 — журналирование доступа к каталогу не ведется
- 4 — журналирование только внутренних операций доступа к каталогу
- 256 — журналирование всех подключений, операций и результатов доступа к конкретной записи каталога (это значение по умолчанию)
- 512 — журналирование доступа не только к самой записи каталога, но и к связанным с ней записям.

Эти значения можно складывать, чтобы получить необходимые администратору типы записей при ведении журнала доступа, например 516 (4 + 512) для получения журналирования внутренних операций доступа к каталогу, а также журналирование доступа к записи и связанных с ней записям.

Для установки уровня журналирования используется команда `dsconf` с опцией `config replace`.

Пример установки максимального уровня журналирования для журнала доступа (крайне не рекомендуется к применению).

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-accesslog-level=772
```

После установки уровня журналирования значением 256 или выше для журнала доступа можно также добавить запись статистики по каждой операции поиска. Во время некоторых операций поиска, особенно с такими фильтрами, как (`cn=user*`), время, затрачиваемое сервером на получение данных, обработку результата и выдачу ответа (`etime`), может

быть очень продолжительным. Поэтому расширение журнала доступа информацией, связанной с индексами, используемыми во время операции поиска, помогает диагностировать проблемы с операциями чтения в службе каталога.

Чтобы включить сбор статистики и запись ее в журнал доступа (информация о количестве поисков в индексе - операций чтения базы данных и общая продолжительность поиска в индексе для каждой операции поиска, с минимальным воздействием на сервер) необходимо использовать атрибут `nsslapd-statlog-level`.

Пример включения записи информации о статистике использования индексов при операциях чтения службы каталога.

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-statlog-level=1
```

Пример включения записи информации о статистике использования индексов при операциях чтения службы каталога.

```
ldapsearch -D "cn=Directory Manager" -H ldap://alddc1.ald.lan -b "dc=ald,
↪dc=lan" -s sub -x "cn=user*"
```

Фрагмент журнала доступа после включения опции записи статистики и выполнения операции поиска с фильтром «cn=user*»:

```
[30/Nov/2023:11:34:11.834135997 +0300] conn=1 op=73 SRCH base="dc=ald,dc=lan
↪" scope=2 filter="(cn=user)"* attrs=ALL
[30/Nov/2023:11:34:11.835750508 +0300] conn=1 op=73 STAT read index:
↪attribute=objectclass key(eq)=referral --> count 0
[30/Nov/2023:11:34:11.836648697 +0300] conn=1 op=73 STAT read index:
↪attribute=cn key(sub)=er_ --> count 25
[30/Nov/2023:11:34:11.837538489 +0300] conn=1 op=73 STAT read index:
↪attribute=cn key(sub)=ser --> count 25
[30/Nov/2023:11:34:11.838814948 +0300] conn=1 op=73 STAT read index:
↪attribute=cn key(sub)=use --> count 25
[30/Nov/2023:11:34:11.841241531 +0300] conn=1 op=73 STAT read index:
↪attribute=cn key(sub)=^us --> count 25
[30/Nov/2023:11:34:11.842230318 +0300] conn=1 op=73 STAT read index:
↪duration 0.000010276
[30/Nov/2023:11:34:11.843185322 +0300] conn=1 op=73 RESULT err=0 tag=101
↪nentries=24 wtime=0.000078414 optime=0.001614101 etime=0.001690742
```

Изменение уровня журналирования для журнала ошибок, установленного по умолчанию, может привести к очень быстрому росту файла журнала, а также серьезно снизить производительность сервера службы каталога. В документации на службу каталога не рекомендуется изменять значения по умолчанию без предварительного контакта со службой технической поддержки.

Принимаемые значения параметров для установки уровня журналирования в журнале ошибок:

- 1 —записывает событие о том, когда сервер службы каталога выполняет функции (входит и выходит из каждой функции);
- 2 —записывает отладочную информацию для пакетов, обрабатываемых сервером службы каталога;
- 4 —записывает событие о том, когда сервер службы каталога выполняет функции (входит и выходит из каждой функции) с дополнительными сообщениями для отладки;
- 8 —записывает текущий статус подключения, включая методы подключения, используемые для привязки SASL;
- 16 —записывает информацию о количестве пакетов, отправленных и полученных сервером;
- 32 —записывает событие о всех функциях, вызываемые операцией поиска в каталоге;
- 64 —записывает ошибок построчно информацию из всех файлов конфигурации (`*.conf`), которые использовал сервер при запуске, по умолчанию сервер службы каталога обрабатывает только файл `slapd-collations.conf`;
- 128 —записывает подробную информацию об обработке списка управления доступом (ACL);
- 2048 —записывает отладочную информацию о разборе схемы базы данных (при внутренних операциях сервера службы каталога);
- 4096 —записывает отладочную информацию для служебных потоков сервера службы каталога;
- 8192 —записывает подробную информацию о каждой операции, связанной с репликацией, включая обновления и ошибки, данная информация может быть полезна для отладки проблем репликации;
- 16384 —записывает критические ошибки и другие сообщения, которые сервер каталогов всегда записывает в журнал ошибок, например сообщения о запуске сервера, нужно учитывать, что журнал **ошибок содержит эти сообщения**

независимо от настройки уровня журнала;

- 32768 —записывает отладочную информацию для кэша записей базы данных;
- 65536 —записывает событие о том, когда подключаемый модуль сервера вызывает функцию `slapi-log-error()`, этот уровень журнала можно использовать для отладки подключаемого модуля сервера службы каталога.

Эти значения можно складывать, чтобы получить необходимые администратору типы записей при ведении журнала ошибок.

Важно: Включение высокого уровня ведения журнала ошибок может значительно снизить производительность сервера. Поэтому следует включать высокие уровни ведения журнала отладки, такие как репликация (8192), только для устранения неполадок!

Для установки уровня журналирования для журнала ошибок службы каталога необходимо использовать команду dsconf с опцией config replace.

Пример установки уровня журналирования для журнала ошибок.

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-errorlog-level=96
```

Примечание: Для корректного функционирования службы каталога (устранения проблем с занимаемым журналами местом на диске) требуется настроить ротацию журналов. Для этого необходимо настроить политики **создания** и **удаления** для всех типов файлов журналов. Политика создания журнала задается при запуске нового файла журнала, а политика удаления журнала задается при удалении старого файла журнала.

Для определения политики создания журналов службы каталога необходимо задать (изменить при необходимости) следующие параметры:

1. Режим доступа к вновь создаваемым файлам журналов.
2. Максимальное количество журналов.
3. Максимальный размер файла для каждого журнала.
4. Максимальное время записи в файл для каждого журнала.

Для задания режима доступа к вновь создаваемым файлам журналов администратор может использовать нумерованные права доступа к файлам UNIX. Это трехзначные числа, где первый разряд определяет разрешения владельца файла, второй разряд определяет разрешения группы, а в третьем разряде определены разрешения всех остальных пользователей данного компьютера. При этом в каждом разряде которых стоит число от нуля до семи, причем каждое из чисел означает следующее:

- 0 — Всё запрещено
- 1 — Разрешено только выполнять
- 2 — Разрешено только писать
- 3 — Разрешено писать и выполнять
- 4 — Разрешено только читать
- 5 — Разрешено читать и выполнять
- 6 — Разрешено читать и писать
- 7 — Разрешено читать, писать и выполнять

При этом, вновь заданный с помощью соответствующей команды режим доступа к конкретному типу журнала влияет только на вновь создаваемые файлы во время ротации. Параметры службы каталога, которые определяют режим доступа к файлам журналов, приведены в таблице 6.2.

Таблица 6.2. Параметры режима доступа к файлам всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	`nsslapd-accesslog-mode`	600	000/777
error log	`nsslapd-errorlog-mode`	600	000/777
audit log	`nsslapd-auditlog-mode`	600	000/777
audit fail log	`nsslapd-auditfaillog-mode`	600	000/777
security log	`nsslapd-securitylog-mode`	600	000/777

Для задания максимального количества журналов службы каталога определенного типа необходимо использовать параметры службы каталога, которые приведены в таблице 6.3.

Таблица 6.3. Параметры максимального количества файлов для всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	`nsslapd-accesslog-maxlogsperdir`	10	Натуральные числа от 1 до ((2^32) - 1) включительно.
error log	`nsslapd-errorlog-maxlogsperdir`	1	Натуральные числа от 1 до ((2^32) - 1) включительно.
audit log	`nsslapd-errorlog-maxlogsperdir`	1	Натуральные числа от 1 до ((2^32) - 1) включительно.
audit fail log	`nsslapd-auditfaillog-maxlogsperdir`	1	Натуральные числа от 1 до ((2^32) - 1) включительно.
security log	`nsslapd-securitylog-maxlogsperdir`	10	Натуральные числа от 1 до ((2^32) - 1) включительно.

Однако, задание **только** атрибута `*-maxlogsperdir` **не** позволит реализовать полноценную ротацию журналов, необходимо также задать параметры максимального времени записи в журналы.

Для задания максимального времени записи в файл журнала службы каталога определенного типа необходимо использовать **совместно** параметры службы каталога, указанные в таблицах 6.4 и 6.5. Значение в таблице 6.4 задает количество диапазонов времени, через которые будет осуществляться ротация журнала определенного типа, а значение в таблице 6.5 задает сам диапазона времени ротации (`minute` - минута, `hour` - час, `day` - день, `week` - неделя, `month` - месяц).

Таблица 6.4. Параметры максимального количества диапазонов времени записи в файлы для всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	nsslapd-accesslog-logrotationtime	1	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
error log	nsslapd-errorlog-logrotationtime	1	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
audit log	nsslapd-auditlog-logrotationtime	1	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
audit fail log	nsslapd-auditfaillog-logrotationtime	1	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
security log	nsslapd-securitylog-logrotationtime	1	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.

Таблица 6.5. Параметры, задающие диапазон времени, для записи в файлы всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	nsslapd-accesslog-logrotationtimeunit	day	Диапазон времени:minute/hour/day/week/month
error log	nsslapd-errorlog-logrotationtimeunit	week	Диапазон времени:minute/hour/day/week/month
audit log	nsslapd-auditlog-logrotationtimeunit	week	Диапазон времени:minute/hour/day/week/month
audit fail log	nsslapd-auditfaillog-logrotationtimeunit	week	Диапазон времени:minute/hour/day/week/month
security log	nsslapd-securitylog-logrotationtimeunit	month	Диапазон времени:minute/hour/day/week/month

Помимо этого, необходимо учитывать тот факт, что при достаточно высокой нагрузке на сервер каталога, размер журнала доступа (access) будет расти достаточно быстро, поэтому значения по умолчанию для параметров nsslapd-accesslog-logrotationtime и nsslapd-accesslog-logrotationtimeunit необходимо изменить в соответствии с потребностями администратора с учетом свободного места на дисковой подсистеме каждого контроллера домена. Также необходимо проанализировать скорость роста остальных файлов журнала

службы каталога и, при необходимости, поменять значения по умолчанию для параметров максимального времени записи в соответствующие файлы журналов.

Помимо задания ротации журналов по времени существует параметр задания ротации журналов по занимаемому им месту на диске. Для задания максимального размера каждого журнала службы каталога определенного типа в мегабайтах необходимо использовать параметры самого службы каталога, указанные в таблице 6.6. Если значение параметра равно «-1», то это означает, что размер файла не задан и журнал будет расти в объеме до тех пор, пока не заполнит все пространство на жестком диске.

Таблица 6.6. Параметры, задающие максимальный размер файла для всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	`nsslapd-accesslog-maxlogsize`	`100`	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
error log	`nsslapd-errorlog-maxlogsize`	`100`	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
audit log	`nsslapd-auditlog-maxlogsize`	`100`	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
audit fail log	`nsslapd-auditfaillog-maxlogsize`	`100`	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
security log	`nsslapd-securitylog-maxlogsize`	`100`	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.

Важно:

1. Для реализации ротации журналов администратор должен изменить параметр `*-maxlogsperdir` для тех типов файлов журналов службы каталога, у которых значение этого параметра равно единице (поскольку в этом случае, параметры службы каталога `*-logrotationtime`, `*-logrotationtimeunit` и `*-maxlogsize` игнорируются и сервер службы каталога **не осуществляет ротацию** тех типов журналов, у которых значение параметра `*-maxlogsperdir` равно единице).

2. При этом, если значение атрибута `*-logrotationtime` равно «-1» для какого-то типа файла журнала, то сервер службы каталога также **не будет осуществлять**

ротацию журналов этого типа по времени и атрибут `*-maxlogsperdir` для этого типа журнала будет проигнорирован. Фактически, установка значения «`*-logrotationtime=-1`» для определенного типа журнала означает, что время для проведения ротации этого типа журнала не задано. Однако ротация этого журнала по объему занимаемого им места на диске будет происходить (если параметр `*-maxlogsize` для этого типа журнала **не равен «-1»**).

Например, для изменения конфигурации ротации журнала ошибок службы каталога можно использовать следующую команду:

Пример включения ведения файла `security` на конкретном экземпляре сервера каталога:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-errorlog-mode=644 nsslapd-errorlog-
↪maxlogsperdir=5 nsslapd-errorlog-maxlogsize=500 nsslapd-errorlog-
↪logrotationtime=7 nsslapd-errorlog-logrotationtimeunit=day
```

Эта команда для файла журнала ошибок (в примере выше это файл error) службы каталога на данном экземпляре 389 Directory Server выполнит следующие действия:

- установит режим доступа для файла журнала ошибок равный «644» (означающий, что владелец файла имеет права на чтение и запись, а группа и остальные пользователи — только на чтение);
- установит максимальное количество файлов журнала ошибок в каталоге хранения журналов равное 5;
- установит режим ротации журнала таким образом, что файл будет ротироваться (текущий журнал становится архивным) либо по достижению размера в 500 Мб, либо один раз в 7 дней.

Также для задания времени ротации файлов журналов службы каталога определенного типа необходимо использовать **совместно** параметры службы каталога, указанные в таблицах 6.7, 6.8 и 6.9. Значение в таблице 6.8 задает конкретное значение часа, когда будет осуществляться ротация журнала определенного типа, а значение в таблице 6.9 задает значение минуты в этом часе, когда будет осуществляться ротация журнала определенного типа. Для использования параметров ротации журналов из таблиц 6.8 и 6.9, необходимо предварительно включить параметр (задать значение on для параметра журнала определенного типа) из таблицы 6.7, который определяет, будут ли читаться параметры таблиц 6.8 и 6.9, после чего задать значения часов и минут для журнала

необходимого типа. Задание механизма ротации всех типов журналов службы каталога таким способом значительно облегчит последующий анализ журналов или инцидентов (поскольку все журналы могут ротироваться в одно и то же время, затем можно их архивировать и отправлять в какое-то хранилище, где затем в случае необходимости проведения поиска конкретных записей журналов можно будет достаточно быстро найти всю записанную информацию по дате и времени журналов).

Таблица 6.7. Параметры, задающие возможность для проведения ротации в конкретное время для всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	`nsslapd-accesslog-logrotationsync-enabled`	off	on/off
error log	`nsslapd-errorlog-logrotationsync-enabled`	off	on/off
audit log	`nsslapd-auditlog-logrotationsync-enabled`	off	on/off
audit fail log	`nsslapd-auditfaillog-logrotationsync-enabled`	off	on/off
security log	`nsslapd-securitylog-logrotationsync-enabled`	off	on/off

Таблица 6.8. Параметры, задающие конкретное значение часа при настройке ротации файлов для всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	`nsslapd-accesslog-logrotationsynchour`	0	Целые числа от 0 до 23 включительно.
error log	`nsslapd-errorlog-logrotationsynchour`	0	Целые числа от 0 до 23 включительно.
audit log	`nsslapd-auditlog-logrotationsynchour`	0	Целые числа от 0 до 23 включительно.
audit fail log	`nsslapd-auditfaillog-logrotationsynchour`	0	Целые числа от 0 до 23 включительно.
security log	`nsslapd-securitylog-logrotationsynchour`	0	Целые числа от 0 до 23 включительно.

Таблица 6.9. Параметры, задающие значение минуты в часе (см. предыдущую таблицу)

при настройке ротации файлов всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	nsslapd-accesslog-logrotationsyncmin	0	Целые числа от 0 до 59 включительно.
error log	nsslapd-errorlog-logrotationsyncmin	0	Целые числа от 0 до 59 включительно.
audit log	nsslapd-auditlog-logrotationsyncmin	0	Целые числа от 0 до 59 включительно.
audit fail log	nsslapd-auditfaillog-logrotationsyncmin	0	Целые числа от 0 до 59 включительно.
security log	nsslapd-securitylog-logrotationsyncmin	0	Целые числа от 0 до 59 включительно.

Пример включения ротации журнала `access` в 11 часов 11 минут на конкретном экземпляре сервера каталога:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-auditlog-logrotationsync-enabled=on nsslapd-
↪accesslog-logrotationsynchour=11 nsslapd-accesslog-logrotationsyncmin=11
```

Аналогично вышеприведенным примерам и используя данные таблиц 6.1-6.9 можно настроить политики создания новых файлов при ротации всех журналов для текущего экземпляра службы каталога.

Для определение политики **удаления** журналов службы каталога при ротации журналов необходимо задать (изменить при необходимости) параметры для каждого типа журналов, приведенные в таблицах 6.10 и 6.11:

Таблица 6.10. Параметры, задающие значение минимального свободного места на диске при настройке ротации файлов для всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	nsslapd-accesslog-logminfreediskspace	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
error log	nsslapd-errorlog-logminfreediskspace	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
audit log	nsslapd-auditlog-logminfreediskspace	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
audit fail log	nsslapd-auditfaillog-logminfreediskspace	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
security log	nsslapd-securitylog-logminfreediskspace	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.

Таблица 6.11. Параметры, задающие значение максимального занимаемого места на диске при настройке ротации файлов всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	nsslapd-accesslog-logmaxdiskspace	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
error log	nsslapd-errorlog-logmaxdiskspace	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
audit log	nsslapd-auditlog-logmaxdiskspace	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
audit fail log	nsslapd-auditfaillog-logmaxdiskspace	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
security log	nsslapd-securitylog-logmaxdiskspace	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.

При задании одной из вышеуказанных опций будет происходить удаление соответствующих файлов службы каталога во время ротации журналов.

При задании опции `logminfreediskspace` произойдет следующее: при достижении указанного в параметре значения свободного места на диске, где хранится соответствующий файл журнала, самый старый архивный файл этого журнала

автоматически удаляется.

При задании опции `logmaxdiskspace` произойдет следующее: при достижении указанного в параметре значения суммарного места на диске для определенного типа журналов (например, всех журналов `audit`, включая архивные), самый старый архивный файл этого журнала автоматически удаляется.

Примечание: Важно обратить внимание, что в зависимости от значений, установленных в `nsslapd-accesslog-logminfreediskspace` и `nsslapd-accesslog-maxlogsize`, фактическое количество журналов может быть меньше того, которое настроил администратор в параметре `nsslapd-accesslog-maxlogsperdir`. Например, если для параметра `nsslapd-accesslog-maxlogsperdir` используется значение по умолчанию (10 файлов), а администратор установил `nsslapd-accesslog-logminfreediskspace=500` и `nsslapd-accesslog-maxlogsize=100`, сервер каталогов сохранит только 5 файлов доступа.

Также можно определить **временную** политику **удаления** журналов службы каталога. Для этого необходимо **совместно** задать параметры для каждого типа журналов, приведенные в таблицах 6.12 и 6.13:

Таблица 6.12. Параметры, задающие значение минимального свободного места на диске при настройке ротации файлов для всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	`nsslapd-accesslog-logmaxdiskspace`	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
error log	`nsslapd-errorlog-logmaxdiskspace`	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
audit log	`nsslapd-auditlog-logmaxdiskspace`	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
audit fail log	`nsslapd-auditfaillog-logmaxdiskspace`	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.
security log	`nsslapd-securitylog-logmaxdiskspace`	100	«-1» или натуральные числа от 1 до ((2^32) - 1) включительно.

Таблица 6.13. Параметры, задающие значение максимального занимаемого места на диске при настройке ротации файлов всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	`nsslapd-accesslog-logexpirationtimeunit`	`month`	Диапазон времени:day/week/month
error log	`nsslapd-errorlog-logexpirationtimeunit`	`month`	Диапазон времени:day/week/month
audit log	`nsslapd-auditlog-logexpirationtimeunit`	`week`	Диапазон времени:day/week/month
audit fail log	`nsslapd-auditfaillog-logexpirationtimeunit`	`week`	Диапазон времени:day/week/month
security log	`nsslapd-securitylog-logexpirationtimeunit`	`month`	Диапазон времени:day/week/month

Если у параметров `*-logexpirationtime` или `*-logexpirationtimeunit` установлены значения минус единица или ноль (или любое другое значение, которое не входит в диапазон возможных значений для этого параметра, в том числе и строковое), то это означает, что соответствующий тип журнала службы каталога никогда не удаляется.

Пример настройки для автоматического удаления самого старого журнала `access`, если суммарный размер всех журналов этого типа превышает 500 Мб на жестком диске на конкретном экземпляре сервера каталога:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-accesslog-logmaxdiskspace=500
```

Также существуют параметры для задания сжатия журналов службы каталога после проведения ротации, что позволяет существенно (в десять и более раз) уменьшить занимаемое архивными журналами место на жестком диске. Для задания режима сжатия файлов журнала службы каталога определенного типа необходимо использовать параметры службы каталога, указанные в таблице 6.14.

Таблица 6.14. Параметры сжатия файлов для всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	`nsslapd-accesslog-compress`	off	on/off
error log	`nsslapd-errorlog-compress`	off	on/off
audit log	`nsslapd-auditlog-compress`	off	on/off
audit fail log	`nsslapd-auditfaillog-compress`	off	on/off
security log	`nsslapd-securitylog-compress`	on	on/off

Несмотря на то, что ряд параметров применяется без перезагрузки сервера службы каталога, тем не менее, после выполнения всех необходимых настроек журналов службы следует перезапустить службу каталога с помощью следующей команды:

```
dsctl INSTANCE_NAME restart
```

Где INSTANCE_NAME - имя экземпляра службы каталога.

6.2. Настройка ротации журналов событий службы аудита и службы kerberos на контроллере домена

> События службы `kerberos` можно как перенаправить в системный журнал (по умолчанию в ОС Astra Linux SE 1.7.4 - `/var/log/syslog`), так и записать их в свой собственный файл. Каким образом будет проводиться запись в журнал указано в файле конфигурации службы - `/etc/krb5.conf` в секции `logging`. Настройка корректной записи в свой журнал по указанному в секции `logging` пути по умолчанию приведена в пункте 5.5.1 настоящей инструкции. Однако в этом случае необходимо настраивать ротацию этого журнала с помощью утилиты `logrotate`.

Утилита `logrotate` — это утилита, выполняющая ротацию и сжатие файлов журналов. При правильной настройке этой утилиты для работы с файлом конкретного журнала, его размеры никогда не увеличатся до такой степени, что будут угрожать стабильности системы.

По умолчанию утилита `logrotate` предустановлена в ОС Astra Linux 1.7 и выше. Она уже

настроена для своевременной обработки журналов некоторых имеющихся в системе и используемых пользователями приложений, в том числе `syslog`.

Конфигурация самой утилиты `logrotate` находится в следующем каталоге:

- `/etc/logrotate.conf` — основной файл конфигурации, который, как правило, содержит некоторые параметры, предустановленные автоматически, настройки для ряда базовых журналов, не принадлежащих системным пакетам и инструкцию include для подключения конфигурации, хранящейся по адресу `/etc/logrotate.d`;
- `/etc/logrotate.d` — содержит файлы с конфигурацией; в этом каталоге утилита logrotate считывает файлы конфигурации для различных журналов и системных пакетов, при этом каждый из таких файлов — конфигурация ротации соответствующего журнала; администратор при необходимости может добавить свои файлы конфигурации в этот каталог, и они также будут обработаны утилитой `logrotate`.

Также необходимо после настройки утилиты настроить режим запуска этой утилиты в планировщике задач операционной системы (`cron`). Подробную инструкцию по настройке планировщика, по диагностике возможных проблем и прочим возможностям можно посмотреть в справке операционной системе по утилите cron.

Для службы `kerberos` необходимо провести настройку утилиты `logrotate` самостоятельно. Для настройки ротации журнала службы `kerberos` (должен сохраняться по пути `/var/log/krb5kdc.log` после проведения настройки из пункта 5.5.1 настоящей инструкции) с помощью утилиты `logrotate` необходимо выполнить следующие действия:

1. Создать файл `/etc/logrotate.d/kerberos` с правами «644», в который внести и сохранить следующую информацию:

```
/var/log/krb5kdc.log {
    daily
    rotate 5
    minsize 1G
    compress
    missingok
    notifempty}
```

2. Для применения изменений и запуска утилиты в текущий момент времени необходимо выполнить команду:

```
logrotate /etc/logrotate.conf
```

3. Для запуска утилиты `logrotate` по расписанию необходимо настроить планировщик операционной системы таким образом, чтобы он запускал утилиту не реже самого минимального интервала времени для ротации всех журналов, которые есть в конфигурационных файлов утилиты `logrotate`: в данном случае (рассматривается только один журнал службы `kerberos`) это будет один раз в день, тогда необходимо выполнить следующую команду с правами пользователя `root` или другого привилегированного пользователя, который может запускать утилиту `logrotate`:

```
crontab -e
```

Для запуска утилиты `logrotate` ежедневно в 0 часов 5 минут в появившемся в результате выполнения предыдущей команды файле необходимо ввести в пустой строке следующие данные, после чего сохранить файл (требуются соответствующие привилегии):

```
5 0 * * * /usr/sbin/logrotate /etc/logrotate.conf
```

После выполнения настройки (внесения изменений в файл `crontab`) можно перезапустить сервис `cron` с помощью следующей команды (хотя это и не обязательно, `cron` должен читать изменения по дате их сохранения):

```
systemctl restart cron
```

В первой строке файла конфигурации утилиты `logrotate` указан путь к файлу, к которому будут применять различные директивы, которые перечислены ниже в этом конфигурационном файле. Указанные в примере директивы описывают следующее поведение утилиты:

- `daily` — ротацию выполнять один раз в сутки (для сервисов, которые записывают в свои журналы достаточно мало информации, можно использовать опцию monthly — один раз в месяц или `weekly` — один раз в неделю, а для сервисов, которые записывают в журналы **очень** много информации можно использовать опцию `hourly`, которая говорит о том, что ротация будет выполняться один раз в час);
- `rotate 5` — позволяет в автоматическом режиме хранить последние 5 журналов;
- `minsize` — журнал будет ротироваться, когда его размер больше указанного, но не ранее, чем наступает соответствующий временной интервал ротации (`hourly`, `daily`, `weekly`, `monthly`, `yearly`), для указания размеров файла журнала можно использовать большие буквы «G» — гигабайт, «M» — мегабайт;

- compress — используется для сжатия архивных журналов (стандартно используется утилита gzip);
- missingok — не оставляет сообщение об ошибке в работе в системном журнале, если ротируемый журнал пуст;
- notifempty — запрещает ротировать файл, если он пустой.

Дополнительную информацию о работе утилит logrotate и cron, а также обо всех допустимых параметрах настройки ротации журналов и способах запуска команд по расписанию можно посмотреть в справке операционной системы по данным утилитам.

После настройки ротации журнала службы kerberos необходимо провести настройку журнала службы аудита. Настройка журнала службы аудита производится путем редактирования файла конфигурации /etc/audit/auditd.conf. Этот файл, в числе, прочих содержит следующие параметры:

- log_file — файл, в котором будут храниться журналы подсистемы аудита;
- log_format— формат, в котором будет сохранены журналы;
- freq — максимальное число записей протокола аудита, которые могут храниться в буфере;
- flush — режим синхронизации буфера с диском: - none — ничего не делать, - incremental — переносить данные из буфера на диск с частотой, указанной в значении параметра freq, - data — синхронизировать немедленно, - sync — синхронизировать как данные, так и метаданные файла при записи на диск;
- max_log_file — максимальный размер файла лога в мегабайтах;
- max_log_file_action — действие при превышении максимального размера файла лога;
- space_left — минимум свободного пространства в мегабайтах, по достижении которого должно быть осуществлено действие, указанное в следующем параметре;
- **space_left_admin — указывает, что делать, когда на диске недостаточно свободного места:**
  - ignore — ничего не делать,
  - syslog — отправлять в журнал syslog,
  - email — отправлять уведомление по почте,
  - suspend — прекратить запись логов на диск,
  - single — перейти в однопользовательский режим,
  - halt — выключить машину;

- `disk_full_action` — действие, которое нужно осуществить при переполнении диска (этот параметр может принимать те же значения, что и `space_left_admin`).

В разделе 5.6.1 приведена настройка журнала аудита, при которой все параметры, кроме `max_log_file`, остаются неизменными. По аналогии с данным примером можно провести требуемые администратору изменения конфигурации журналирования событий аудита. После всех изменений файла конфигурации необходимо перезапустить сервис `auditd` с помощью команды:

```
systemctl restart auditd
```

6.3. Настройка ротации журналов событий на сервере аудита

Настройку ротации журналов, которые перенаправляются с контроллеров домена на сервер аудита из состава домена ALD Pro согласно настоящей инструкции, необходимо проводить с помощью утилиты `logrotate`. Основные сведения о работе данной утилиты приведены в разделе 6.2 настоящей инструкции.

Ниже приведены файлы конфигурации для утилиты `logrotate`, обеспечивающие ротацию всех журналов, которые создаются в папке `/var/log/aldpro/` на сервера аудита, согласно настоящей инструкции.``

1. Файл конфигурации `/etc/logrotate.d/access_dirsrv` для ротации журнала доступа к службе каталога, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/access_dirsrv.log {
    hourly
    rotate 10
    minsize 1G
    compress
    missingok
    notifempty
}
```

2. Файл конфигурации `/etc/logrotate.d/audit_dirsrv` для ротации журнала аудита службы каталога, который необходимо создать с правами «644», внести в

него следующую информацию и сохранить:

```
/var/log/aldpro/audit_dirsrv.log {
    hourly
    rotate 10
    minsize 100M
    compress
    missingok
    notifempty
}
```

3. Файл конфигурации `/etc/logrotate.d/error_dirsrv` для ротации журнала ошибок службы каталога, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/error_dirsrv.log {
    hourly
    rotate 5
    minsize 100M
    compress
    missingok
    notifempty
}
```

4. Файл конфигурации `/etc/logrotate.d/security_dirsrv` для ротации журнала событий безопасности службы каталога, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/security_dirsrv.log {
    hourly
    rotate 5
    minsize 100M
    compress
    missingok
    notifempty
}
```

5. Файл конфигурации `/etc/logrotate.d/samba` для ротации журнала событий службы `samba`, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/samba.log {
    hourly
    rotate 5
    minsize 10M
    compress
    missingok
    notifempty
}
```

6. Файл конфигурации `/etc/logrotate.d/dns_audit` для ротации журнала событий трансфера зоны `dns`, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/dnszone.log {
    hourly
    rotate 5
    minsize 1M
    compress
    missingok
    notifempty
}
```

7. Файл конфигурации `/etc/logrotate.d/kerberos_audit` для ротации журнала событий получения билетов службы `kerberos`, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/krb_audit.log {
    hourly
    rotate 10
    minsize 1G
    compress
    missingok
    notifempty
}
```

8. Файл конфигурации `/etc/logrotate.d/user_proc` для ротации журнала событий запуска новых процессов пользователями домена, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/userproc.log {
    hourly
    rotate 10
    minsize 1G
    compress
    missingok
    notifempty
}
```

9. Файл конфигурации `/etc/logrotate.d/ldap_audit` для ротации журнала событий подключения к каталогу `ldap`, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/ldapconnect.log {
    hourly
    rotate 10
    minsize 1G
    compress
    missingok
    notifempty
}
```

После создания описанных выше файлов конфигурации необходимо добавить ежечасный запуск утилиты `logrotate` в конфигурационный файл утилиты `cron`. Для этого необходимо скопировать файл `/etc/cron.daily/logrotate` в каталог `/etc/cron.hourly` и выполнить команду под пользователем root или другим привилегированным пользователем, который может запускать утилиту logrotate:

```
crontab -e
```

Затем в открывшемся файле конфигурации утилиты cron добавить новую строку (запуск утилиты `/usr/sbin/logrotate` от имени пользователя каждый час каждого дня в 0 минут) и сохранить сделанные изменения:

```
0 * * * * /usr/sbin/logrotate /etc/logrotate.conf
```

Отправка журналов в стороннюю SIEM

7.1. Настройка отправки журналов событий с сервера аудита в стороннюю SIEM

Собираемые журналы можно перенаправлять с помощью инструментов `syslog-ng` как с клиентов домена или контроллеров домена, так и с сервера аудита в сторонние SIEM. В настоящей инструкции не рассматривается настройка отправки журналов событий с клиентов или контроллеров домена, поскольку приведенный ниже файл конфигурации позволяет администратору самостоятельно модифицировать его и реализовать необходимую настройку отправки журналов событий по той схеме, которая отвечает требованиям безопасности в конкретной реализации системы.

Ниже приведен пример файла конфигурации отправки всех файлов, создаваемых в разделах 5.x.2 (где x - [2-7]) настоящей инструкции, в стороннюю SIEM, которая установлена на компьютере с IP-адресом «8.8.8.8» и настроена на «прослушивание» следующих портов по заданным протоколам :

1. протокол tcp, порт 5154;
2. протокол tcp, порт 5155;
3. протокол tcp, порт 5156;
4. протокол tcp, порт 5157;
5. протокол udp, порт 5173.

Для настройки `syslog-ng` по отправке файлов журналов с сервера аудита в стороннюю SIEM необходимо на сервере аудита (при условии модификации файла конфигурации `/etc/syslog-ng/syslog-ng.conf` в соответствии с разделом 5.2.2) создать файл `/etc/syslog-ng/siem/siem_rules.conf` с правами на чтение всем пользователям (644), куда вставить приведенный ниже текст файла конфигурации (параметр `follow-freq(10)` определяет интервала опроса (в секундах) для каждого конкретного файла службой `syslog-ng`, в данном случае 1 раз в 10 секунд, этот параметр можно корректировать по необходимости, минимальное значение единица, если задано нулевое значение, то служба `syslog-ng` будет использовать значение по умолчанию):

```
#destinations
destination siem_dirsrv {
    network("8.8.8.8" transport("tcp") port(5154) flags(syslog-protocol)
 ↪template("${MESSAGE}\n"));
};

destination siem_krb5kdc {
    network("8.8.8.8" transport("tcp") port(5155) flags(syslog-protocol)
 ↪template("${MESSAGE}\n"));
};

destination siem_samba {
    network("8.8.8.8" transport("tcp") port(5156) flags(syslog-protocol)
 ↪template("${MESSAGE}\n"));
};

destination siem_bind {
    network("8.8.8.8" transport("tcp") port(5157) flags(syslog-protocol)
 ↪template("${MESSAGE}\n"));
};

destination siem_audit {
    network("8.8.8.8" transport("udp") port(5154) flags(syslog-protocol)
 ↪template("${MESSAGE}\n"));
};

#sources
source aldpro_access {
    file(
        "/var/log/aldpro/access_dirsrv.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_audit {
    file(
        "/var/log/aldpro/audit_dirsrv.log"
        follow-freq(10)
        flags(no-parse)
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    );
};

source aldpro_security {
    file(
        "/var/log/aldpro/security_dirsrv.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_errors {
    file(
        "/var/log/aldpro/errors_dirsrv.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_krb5kdc {
    file(
        "/var/log/aldpro/krb_audit.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_samba {
    file(
        "/var/log/aldpro/samba.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_bind {
    file(
        "/var/log/aldpro/dnszone.log"
        follow-freq(10)
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
        flags(no-parse)
    );
};

source aldpro_ldap {
    file(
        "/var/log/aldpro/ldapconnect.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_userproc {
    file(
        "/var/log/aldpro/userproc.log"
        follow-freq(10)
        flags(no-parse)
    );
};


#logs
log {
    source(aldpro_access);
    destination(siem_dirsrv);
};

log {
    source(aldpro_audit);
    destination(siem_dirsrv);
};

log {
    source(aldpro_security);
    destination(siem_dirsrv);
};

log {
    source(aldpro_errors);
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    destination(siem_dirsrv);
};

log {
    source(aldpro_krb5kdc);
    destination(siem_krb5kdc);
};

log {
    source(aldpro_samba);
    destination(siem_samba);
};

log {
    source(aldpro_bind);
    destination(siem_bind);
};

log {
    source(aldpro_ldap);
    destination(siem_audit);
};

log {
    source(aldpro_userproc);
    destination(siem_audit);
};
```

Затем необходимо заменить настройки пунктов назначения для файлов журналов (раздел `#destinations`) на актуальные в системе, и в случае коррекции наименований и отправки данных на меньшее или большее количество точек отправки, необходимо изменить в разделе `#logs` соответствующие записи.

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

Настройка журналирования на КД, сервере общего доступа к файлам и сервере аудита (только команды).

Информация в данном разделе приведена максимально коротко и ёмко, для более глубокого понимания и индивидуальной настройки системы журналирования за помощью необходимо обращаться к соответствующему разделу инструкции, где приведена детальная информация.

После настройки, описанной в данном разделе:

1. будет осуществляться полное журналирование всех событий безопасности и перенаправление ряда журналов с КД и сервера общего доступа к файлам на сервер аудита из состава изделия;

2. НЕ будет настроена ротация журналов служб на КД, на сервере общего доступа к файлам и на сервере аудита;

3. НЕ будет осуществлено перенаправление информации с сервера аудита в стороннюю SIEM.

Для настройки ротации журналов на КД необходимо обратиться к разделам 6.1 и 6.2 настоящей инструкции. Для настройки ротации журналов на сервере аудита необходимо обратиться к разделу 6.3 настоящей инструкции. Для настройки перенаправления информации журналов с сервера аудита (или сразу с КД) в стороннюю SIEM необходимо обратиться к разделу 7.1.

1. Настройка всех КД в домене (изменение конфигурации 389 DS, настройка syslog-ng, перезапуск служб). **Дальнейшие действия нужно выполнить на каждом контроллере в домене!**

а) настроить 389 DS, службы Kerberos и auditd

```
# настройка 389 DS
# ldap://alddc1.ald.lan - необходимо по очереди заменить на адрес каждого
 ↪конкретного КД в домене, "ПАРОЛЬ_АДМИНИСТРАТОРА" - необходимо вписать
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
 ↪реальный пароль администратора
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-auditlog-logging-enabled=on
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-auditfaillog-logging-enabled=on
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-securitylog-logging-enabled=on

# следующая команда без пробелов в одну строку
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-auditlog-display-attrs=loginShell,
krbExtraData,krbLastPwdChange,krbPasswordExpiration,x-ald-user-mac,uid,
 ↪displayName,initials,gecos,sn,homeDirectory,mail,krbPrincipalName,
krbCanonicalName,givenName,rbtamiddlename,street,l,st,postalCode,c,
 ↪employeeNumber,telephoneNumber,title,rbtadp,rbtaou,entyusn,modifiersName,
objectClass,ipaNTSecutityIdentifier,cn,creatorsName,createTimestamp,
 ↪modifyTimestamp,nsUniqueId,ipaUniqueId,parentid,entryid,uidNumber,gidNumber,
 ↪
entryUUID,dsEntryDN,entrydn

# настройка службы Kerberos
# в файле /lib/systemd/system/krb5-kdc.service в параметр
 ↪ReadWriteDirectories добавить /var/log и прочитать новую конфигурацию
 ↪службы
systemctl daemon-reload

# настройка службы auditd
# создаем файл /etc/audit/rules.d/siem.rules
touch /etc/audit/rules.d/siem.rules

# вставить в файл /etc/audit/rules.d/siem.rules следующее содержимое
-a always,exit -F arch=b32 -S execve -F auid>=1000
-a always,exit -F arch=b64 -S execve -F auid>=1000
-a always,exit -S accept -S accept4 -F exe=/usr/sbin/ns-slapd -k ldapconnect
-a exit,always -F exit=-EACCES -F exe=/usr/sbin/ns-slapd -k ldapconnect

# перезапустить службы
systemctl restart krb5-kdc.service auditd
```

б) настроить syslog-ng на КД

```
# создать каталог /etc/syslog-ng/siem для дальнейшего включения его в
 ↪конфигурацию службы syslog-ng и записи в него необходимых файлов
 ↪конфигурации этой службы
mkdir /etc/syslog-ng/siem

# вставить в файл /etc/syslog-ng/syslog-ng.conf следующую строку
@include "/etc/syslog-ng/siem/*.conf"

# создать набор файлов конфигурации syslog-ng и задать им права
touch /etc/syslog-ng/siem/destination.conf
touch /etc/syslog-ng/siem/output-dirsrv-access.conf
touch /etc/syslog-ng/siem/output-dirsrv-audit.conf
touch /etc/syslog-ng/siem/output-dirsrv-error.conf
touch /etc/syslog-ng/siem/output-dirsrv-security.conf
touch /etc/syslog-ng/siem/output-dns-zone.conf
touch /etc/syslog-ng/siem/output-krb-audit.conf
touch /etc/syslog-ng/siem/output-user-proc.conf
touch /etc/syslog-ng/siem/output-ldapconnect.conf
chmod 744 /etc/syslog-ng/siem/*

# вставить в файл /etc/syslog-ng/siem/destination.conf следующее содержимое
 ↪(IP-адрес заменить на реальный адрес сервера аудита из состава домена)
destination d_audit {network("100.100.100.100" transport("tcp") port(514)
 ↪flags(syslog-protocol) template("${ISODATE} ${HOST} ${MESSAGE} ${TAGS} \n
 ↪"));};

# вставить в файл /etc/syslog-ng/siem/output-dirsrv-access.conf следующее
 ↪содержимое
source s_access_dirsrv {file("/var/log/dirsrv/slapd-ALDPRO-LAN/access" follow-
 ↪freq(1) flags(no-parse));};
filter f_access_dirsrv {match("MOD" value("MESSAGE")) or match("DEL" value(
 ↪"MESSAGE")) or match("ADD" value("MESSAGE")) or match("SRCH" value("MESSAGE
 ↪")) or match("connection from" value("MESSAGE")) or match("RESULT" value(
 ↪"MESSAGE"));};
log {
    source(s_access_dirsrv);
    filter(f_access_dirsrv);
    rewrite {set-tag("tag-dirsrv-access");};
    destination(d_audit);
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# вставить в файл /etc/syslog-ng/siem/output-dirsrv-audit.conf следующее
 ↪содержимое (если НЕТ необходимости в передаче данных о событии в одну
 ↪строку)
source s_audit_dirsrv {file("/var/log/dirsrv/slapd-ALDPRO-LAN/audit" follow-
 ↪freq(1) flags(no-parse) );};
log {
    source(s_audit_dirsrv);
    rewrite { set-tag("tag-dirsrv-audit"); };
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-dirsrv-audit.conf следующее
 ↪содержимое (если ЕСТЬ необходимость в передаче данных о событии в одну
 ↪строку)
source s_audit_dirsrv {file("/var/log/dirsrv/slapd-ALDPRO-LAN/audit" multi-
 ↪line-mode(prefix-suffix) multi-line-prefix("time: [0-9]+") multi-line-
 ↪suffix("\n$") flags(no-multi-line) follow-freq(1));};
log {
    source(s_audit_dirsrv);
    rewrite { subst("^", "time: ", value("MESSAGE")); set-tag("tag-dirsrv-
 ↪audit"); };
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-dirsrv-error.conf следующее
 ↪содержимое
source s_errors_dirsrv {file("/var/log/dirsrv/slapd-ALDPRO-LAN/errors" follow-
 ↪freq(1) flags(no-parse));};
log {
    source(s_errors_dirsrv);
    rewrite {set-tag("tag-dirsrv-error");};
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-dirsrv-error.conf следующее
 ↪содержимое
source s_security_dirsrv {file("/var/log/dirsrv/slapd-ALDPRO-LAN/security"
 ↪follow-freq(1) flags(no-parse));};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
log {
    source(s_security_dirsrv);
    rewrite {set-tag("tag-dirsrv-security"); };
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-dns-zone.conf следующее
 ↪содержимое
filter f_dnszone{message('AXFR') or message('IXFR');};
log {
    source(s_src);
    filter(f_dnszone);
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-krb-audit.conf следующее
 ↪содержимое
source s_krb_audit {file("/var/log/krb5kdc.log" follow-freq(1) flags(no-
 ↪parse) );};
filter f_krb_audit {match("AS_REQ" value("MESSAGE")) or match("TGS_REQ"
 ↪value("MESSAGE"));};
log {
    source(s_krb_audit);
    filter(f_krb_audit);
    rewrite {set-tag("tag-krb-audit");};
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-user-proc.conf следующее
 ↪содержимое
source s_user_proc {file("/var/log/audit/audit.log" flags(no-parse) persist-
 ↪name("user_proc") follow-freq(1));};
filter f_user_proc {match("syscall=59" value("MESSAGE"));};
log {
    source(s_user_proc);
    filter(f_user_proc);
    destination(d_audit);
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# вставить в файл /etc/syslog-ng/siem/output-ldapconnect.conf следующее
 ↪содержимое
source s_ldap {file("/var/log/audit/audit.log" flags(no-parse) persist-name(
 ↪"ldap_conn") follow-freq(1));};
filter f_ldapconnect {message('ldapconnect');};
log {
    source(s_ldap);
    filter(f_ldapconnect);
    destination(d_audit);
};

# перезапустить сервис syslog-ng
systemctl restart syslog-ng
```

2. Настройка сервера общего доступа к файлам для журналирования операций с общими файловыми ресурсами с помощью пакета программ Samba.

```
# в файле конфигурации /etc/samba/smb.conf  в секцию "global" добавить
 ↪следующие строки
vfs objects = full_audit
full_audit:prefix = %u|%I|%S
full_audit:success = connect, create_file, linkat, mkdirat, open, read,
 ↪renameat, unlinkat, write
full_audit:failure = connect, create_file, linkat, mkdirat, open, read,
 ↪renameat, unlinkat, write
full_audit:facility = local5
full_audit:priority = notice

# Если в файле конфигурации /etc/samba/smb.conf в секции "global"
 ↪присутствует следующая строка "log level = N" где N - это уровень
 ↪журналирования событий в службе, то к данной строке дописываем через
 ↪пробел строку " vfs:1". Если такой строки нет, то записываем
log level = 1 vfs:1

# создать каталог /etc/syslog-ng/siem для дальнейшего включения его в
 ↪конфигурацию службы syslog-ng и записи в него необходимых файлов
 ↪конфигурации этой службы
mkdir /etc/syslog-ng/siem
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# вставить в файл /etc/syslog-ng/syslog-ng.conf следующую строку
@include "/etc/syslog-ng/siem/*.conf"

# создать набор файлов конфигурации syslog-ng и задать им права
touch /etc/syslog-ng/siem/destination.conf
touch /etc/syslog-ng/siem/output-samba.conf
chmod 744 /etc/syslog-ng/siem/*

# вставить в файл /etc/syslog-ng/siem/destination.conf следующее содержимое
 ↪(IP-адрес заменить на реальный адрес сервера аудита из состава домена)
destination d_audit {network("100.100.100.100" transport("tcp") port(514)
 ↪flags(syslog-protocol) template("${ISODATE} ${HOST} ${PROGRAM} ${MESSAGE} $
 ↪{TAGS} \n"));};

# вставить в файл /etc/syslog-ng/siem/output-samba.conf следующее содержимое
filter f_samba{program('smbd_audit');};
log {
    source(s_src);
    filter(f_samba);
    destination(d_audit);
};

# перезапустить службы
systemctl restart smbd winbind syslog-ng
```

3. Настройка сервера аудита из состава домена для журналирования событий с КД и с сервера общего доступа к файлам.

```
# создать каталог /etc/syslog-ng/siem для дальнейшего включения его в
 ↪конфигурацию службы syslog-ng и записи в него необходимых файлов
 ↪конфигурации этой службы
mkdir /etc/syslog-ng/siem

# вставить в файл /etc/syslog-ng/syslog-ng.conf следующую строку
@include "/etc/syslog-ng/siem/*.conf"

# создать набор файлов конфигурации syslog-ng и задать им права
touch /etc/syslog-ng/siem/destination.conf
touch /etc/syslog-ng/siem/input-dirsrv-access.conf
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
touch /etc/syslog-ng/siem/input-dirsrv-audit.conf
touch /etc/syslog-ng/siem/input-dirsrv-error.conf
touch /etc/syslog-ng/siem/input-dirsrv-security.conf
touch /etc/syslog-ng/siem/input-samba.conf
touch /etc/syslog-ng/siem/input-dns-zone.conf
touch /etc/syslog-ng/siem/input-krb-audit.conf
touch /etc/syslog-ng/siem/input-user-proc.conf
touch /etc/syslog-ng/siem/input-ldapconnect.conf
chmod 744 /etc/syslog-ng/siem/*

# если такого источника на сервере аудита нет (осуществить поиск подстроки "s_
 ↪net" во всех файлах конфигурации syslog-ng), то создать файл /etc/syslog-ng/
 ↪siem/source.conf и вставить в него следующее содержимое
source s_net {
    network(
        transport("tcp")
        port(514)
        flags(syslog-protocol)
        log_iw_size(65536)
        max_connections(1000)
    );
};

# все файлы журналов сохраняются в каталог /var/log/aldpro
# вставить в файл /etc/syslog-ng/siem/input-dirsrv-access.conf следующее
 ↪содержимое
destination d_access_dirsrv_file {file("/var/log/aldpro/access_dirsrv.log"
 ↪template("${MESSAGE}\n"));};
filter f_dirsrv_access {message("tag-dirsrv-access");};
log {
    source(s_net);
    filter(f_dirsrv_access);
    rewrite { subst(" tag-dirsrv-access,.source.s_access_dirsrv", "", value(
 ↪"MESSAGE")); };
    destination(d_access_dirsrv_file);
};

# вставить в файл /etc/syslog-ng/siem/input-dirsrv-audit.conf следующее
 ↪содержимое
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
destination d_audit_dirsrv_file {file("/var/log/aldpro/audit_dirsrv.log"
 ↪template("${MESSAGE}\n"));};
filter f_dirsrv_audit { message("tag-dirsrv-audit");};
log {
    source(s_net);
    filter(f_dirsrv_audit);
    rewrite { subst(" tag-dirsrv-audit,.source.s_audit_dirsrv", "", value(
 ↪"MESSAGE")); };
    destination(d_audit_dirsrv_file);
};

# вставить в файл /etc/syslog-ng/siem/input-dirsrv-error.conf следующее
 ↪содержимое
destination d_error_dirsrv_file {file("/var/log/aldpro/error_dirsrv.log"
 ↪template("${MESSAGE}\n"));};
filter f_dirsrv_error {message("tag-dirsrv-error");};
log {
    source(s_net);
    filter(f_dirsrv_error);
    rewrite { subst(" tag-dirsrv-error,.source.s_errors_dirsrv", "", value(
 ↪"MESSAGE")); };
    destination(d_error_dirsrv_file);
};

# вставить в файл /etc/syslog-ng/siem/input-dirsrv-security.conf следующее
 ↪содержимое
destination d_security_dirsrv_file {file("/var/log/aldpro/security_dirsrv.log
 ↪" template("${MESSAGE}\n"));};
filter f_dirsrv_security {message("tag-dirsrv-security");};
log {
    source(s_net);
    filter(f_dirsrv_security);
    rewrite { subst(" tag-dirsrv-security,.source.s_security_dirsrv", "",
 ↪value("MESSAGE")); };
    destination(d_security_dirsrv_file);
};  destination d_samba {
    file("/var/log/aldpro/samba.log" template("${MESSAGE}\n"));
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# вставить в файл /etc/syslog-ng/siem/input-samba.conf следующее содержимое
destination d_samba {file("/var/log/aldpro/samba.log" template("${MESSAGE}\n
 ↪"));};
filter f_samba {message("smbd_audit");};
log {
    source(s_net);
    filter(f_samba);
    rewrite { subst(" .source.s_src", "", value("MESSAGE")); };
    destination(d_samba);
};

# вставить в файл /etc/syslog-ng/siem/input-dns-zone.conf следующее
 ↪содержимое
destination d_dnszone {file("/var/log/aldpro/dnszone.log" template("${MESSAGE}
 ↪\n"));};
filter f_dnszone {message('AXFR') or message('IXFR');};
log {
    source(s_net);
    filter(f_dnszone);
    rewrite {subst(" .source.s_src", "", value("MESSAGE"));};
    destination(d_dnszone);
};

# вставить в файл /etc/syslog-ng/siem/input-krb-audit.conf следующее
 ↪содержимое
destination d_krb_audit_file {file("/var/log/aldpro/krb_audit.log" template("
 ↪${MESSAGE}\n"));};
filter f_krb_audit {message("tag-krb-audit");};
log {
    source(s_net);
    filter(f_krb_audit);
    rewrite { subst(" tag-krb-audit,.source.s_krb_audit", "", value("MESSAGE
 ↪")); };
    destination(d_krb_audit_file);
};

# вставить в файл /etc/syslog-ng/siem/input-user-proc.conf следующее
 ↪содержимое
destination d_user_proc {file("/var/log/aldpro/userproc.log" template("$
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
 ↪{MESSAGE}\n"));};
filter f_user_proc {match("syscall=59" value("MESSAGE"));};
log {
    source(s_net);
    filter(f_user_proc);
    rewrite { subst(" .source.s_user_proc", "", value("MESSAGE")); };
    destination(d_user_proc);
};

# вставить в файл /etc/syslog-ng/siem/input-ldapconnect.conf следующее
 ↪содержимое
destination d_ldapconnect {file("/var/log/aldpro/ldapconnect.log" template("$
 ↪{MESSAGE}\n"));};
filter f_ldapconnect {message("ldapconnect");};
log {
    source(s_net);
    filter(f_ldapconnect);
    rewrite {
        subst(" .source.s_ldap", "", value("MESSAGE"));
        subst(' key="ldapconnect"', "", value("MESSAGE"));
    };
    destination(d_ldapconnect);
};

# перезапустить сервис syslog-ng
systemctl restart syslog-ng
```