Интеграция Makves DCAP со службой каталога ALD Pro

04/07/2026

Makves DCAP — это система аудита и управления информационными активами, предназначенная для централизованного контроля действий пользователей и сервисов в корпоративной ИТ-инфраструктуре. Она обеспечивает сбор, хранение и анализ событий безопасности, а также контроль доступа к критически важным данным, помогая организациям соответствовать требованиям информационной безопасности и внутренним регламентам.

Интеграция с ALD Pro, описанная в инструкции, позволяет автоматически передавать события аудита из службы каталогов Linux в платформу Makves DCAP через протокол SYSLOG. Это обеспечивает полную прозрачность происходящего в домене, включая действия администраторов и системных сервисов, и позволяет использовать средства аналитики Makves DCAP для выявления аномалий, расследования инцидентов и повышения общей защищенности ИТ-среды.

Инструкция подготовлена разработчиками Makves DCAP.

Инструкция по настройке экспорта системных событий из службы каталога для Linux ALD Pro в систему аудита и управления информационными активами MAKVES DCAP

ALD Pro

Версия 1.0

Москва
2025

Оглавление

1 Введение

В настоящей инструкции содержатся рекомендации для организации экспорта системных событий из службы каталога Linux «ALD Pro» (далее по тексту – ALD Pro) с целью их последующей загрузки в базу данных системы аудита и управления информационными активами «Makves DCAP» (далее – платформа Makves).

Перед началом организации канала обмена информации необходимо убедиться в соблюдении следующих требований:

- В инспектируемом информационном пространстве корректно установлена и функционирует без ошибок ALD Pro.
- Сервер управления платформы Makves корректно установлен и предварительно настроен.
- Организована сетевая доступность серверов, на которых размещены платформа Makves и ALD Pro.
- Между контроллером домена и сервером управления платформы Makves настроен обмен данными по протоколу UDP, порту 514 (SYSLOG — доставка сообщений о происходящих в системе событиях).

2 Настройка сервера ALD Pro

Для возможности экспорта событий из файлов журналов необходимо выполнить ряд действий в порядке, описанном в настоящем разделе.

2.1 Включение аудита событий

Для включения аудита событий необходимо в окне терминала выполнить следующую последовательность команд:

dsconf -D "cn=Directory Manager" ldap://IP-address ***config replace nsslapd-auditlog-logging-enabled=on***

dsconf -D "cn=Directory Manager" ldap:// IP-address ***config replace nsslapd-auditfaillog-logging-enabled=on***

dsconf -D "cn=Directory Manager" ldap:// IP-address ***config replace nsslapd-auditlog-display-attrs=****

dsconf -D "cn=Directory Manager" ldap:// IP-address ***config replace nsslapd-securitylog-logging-enabled=on***

Вместо «IP-address» следует указать IP-адрес контроллера домена. Если настройка осуществляется непосредственно в окне терминала контроллера домена, то вместо «IP-address» следует указать «**localhost**».

2.2 Настройка отправки событий по протоколу SYSLOG

Настроить отправку сообщений, руководствуясь порядком действий, описанным в настоящем подразделе.

1. В окне терминала перейти в папку «syslog-ng» командой:

   cd /etc/syslog-ng

2. Создать дополнительную папку «dcap»:

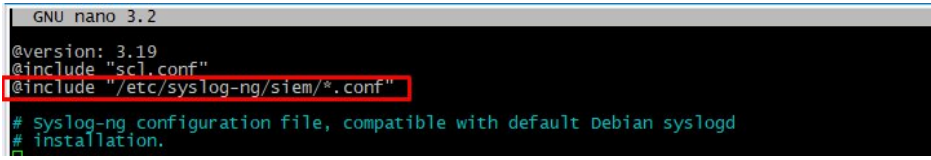
mkdir dcap

3. Открыть для редактирования конфигурационный файл «syslog-n.conf»:

   nano syslog-ng.conf

4. Добавить в конец файла следующую строку для подключения дополнительной директории конфигурации:

   @include "/etc/syslog-ng/dcap/*.conf"



5. Создать файл конфигурации для назначения (destination):
   nano /etc/syslog-ng/dcap/destinat.conf

6. Указать, куда отправлять лог
   destination d_dcap {
   network("IP" transport("udp") port(514) flags(syslog-protocol) template("${MESSAGE}\n"));
   };

   Вместо «IP» следует указать адрес сервера, куда будут отправляться события (например, IP-адрес сервера управления платформой Makves).

7. Сохранить изменения и закрыть файл.

8. Создать еще один конфигурационный файл, используя команду:
   nano /etc/syslog-ng/dcap/out-dirsrv-audit.conf
9. В созданный файл внести данные:
   source s_audit_dirsrv {
   file("/var/log/dirsrv/slapd-TEST-LOCAL***/audit" follow-freq(10)***
   flags(no-parse));
   };

   log {
   source(s_audit_dirsrv);
   destination(d_dcap);
   };

   Вместо «TEST-LOCAL» – необходимо вписать имя домена

10. Перезагрузить службу:
    systemctl restart syslog-ng
11. Проверить корректность работы службы командой:
    systemctl status syslog-ng
12. Проверить логи на наличие ошибок:
    journalctl -u syslog-ng

3 Настройка приёма событий на сервере управления платформы Makves

Для настройки приёма событий на сервере управления платформой Makves следует руководствоваться порядком, приведённым в данном разделе.

3.1 Инспекция LDAP

Агент по инспекции LDAP создаётся в следующем порядке:

- Аутентификация и авторизация выполняются методом LDAP Bind, для чего необходимо создать в ALD Pro сервисную учётную запись, которая не является POSIX-пользователем, не имеет прав на вход в домен и не отображается в портале управления, а используется только для чтения LDAP. Для этого нужно подключиться по SSH к контроллеру домена и выполнить следующие шаги:

  a. Создать файл с именем **ldap-bind.update**.
  b. Внести в файл следующее содержимое:

  dn: uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
  add:objectclass: account
  add:objectclass: simplesecurityobject
  add:uid: ldap-bind
  add:userPassword: securePassword
  add:passwordExpirationTime: 20380119031407Z
  add:nsIdleTimeout: 0

  ,где необходимо заменить **dc=ald,dc=company,dc=lan** на значения, соответствующие вашему домену, а **securePassword** — на желаемый пароль для учётной записи. При необходимости параметр **passwordExpirationTime** можно адаптировать в соответствии с политиками безопасности вашей организации.

  c. Выполнить добавление пользователя следующей командой:

  kinit admin && ipa-ldap-updater trueconf-bind.update

- Выполнить вход в консоль управления платформы Makves с учётной записью, обладающей правами администратора.
- В главном меню выбрать раздел **Настройки**, подраздел **Агенты**. Откроется таблица агентов. Создать загрузчик, используя кнопку «Создать» или выбрать в таблице уже созданный. Открыть таблицу загрузчика, кликнув на нём левой клавишей мыши. В

правом верхнем углу нажать кнопку «Создать» для создания задачи по сбору данных. В форме для создания агентов в выпадающем меню «Тип» выбрать «Инспекция LDAP».
Заполнить поля:

- Режим – выбрать «агент Makves»;
- Контроллер домена – в формате SERVER-DC.ALD.COMPANY.LAN;
- Корневая организационная единица – в формате DC=ALD,DC=COMPANY,DC=LAN;
- Имя пользователя – в формате *cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan;*
- Пароль.

- После заполнения полей нажать кнопку «Проверка». Если поля заполнены неверно, появится сообщение об ошибке.
- При корректном заполнении полей после выполнения созданной задачи в разделе **Объекты** будет отображаться информация о количестве доменов, объектов в домене, групп, пользователей и компьютеров.

3.2 Настройка приёма событий

Агент для приёма событий создаётся в следующем порядке:

- Выполнить вход в консоль управления платформы Makves с учётной записью, обладающей правами администратора.
- В главном меню выбрать раздел **Настройки**, подраздел **Агенты**. Откроется таблица агентов. Создать загрузчик, используя кнопку «Создать» или выбрать в таблице уже созданный. Открыть таблицу загрузчика, кликнув на нём левой клавишей мыши. В правом верхнем углу нажать кнопку «Создать» для создания задачи по сбору данных. В форме для создания агентов в выпадающем меню «Тип» выбрать «SYSLOG-сервер».
Заполнить поля:
  - Сетевой интерфейс – типа «192.168.1.232:514».

- Сетевой протокол – UDP.
- SYSLOG Format – ???

Установить необходимые маркеры и выбрать нужные параметры в остальных полях формы. После заполнения полей нажать кнопку «Создать».