Интеграция SIEM со службой каталога ALD Pro на базе FreeIPA

06/10/2025

Содержание

Система управления информацией о безопасности и событиями (Security Information and Event Management, SIEM) позволяет организациям обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб. Нашей командой совместно с разработчиками ведущих SIEM-систем был проанализирован технологический стек компонентов службы каталога ALD Pro на базе FreeIPA для правильной настройки функций аудита с учётом многолетнего опыта работы партнеров со службой каталога MS AD. На основе этой информации коллегами из Positive Technologies (MaxPatrol) и Лаборатории Касперского (Kaspersky Unified Monitoring and Analysis Platform, KUMA) были разработаны комплекты экспертизы для нормализации событий и автоматического выявления возможных инцидентов безопасности (корреляции). Интеграция службы каталога с SIEM-системой значительно повышает безопасность ИТ-инфраструктуры.

Инструкции по интеграции с MaxPatrol и KUMA разработаны вендорами этих продуктов, которые также оказывают поддержку по проведению пилотного тестирования и внедрению своих программных продуктов. Со своей стороны хотим предоставить вам информацию о настройке аудита на стороне ALD Pro для получения наиболее важных событий безопасности.

1 Настройка аудита

Для эксплуатации продукта ALD Pro на предприятиях крупного бизнеса требуется обеспечить интеграцию с SIEM-системами, которые позволяют выявлять потенциальные инциденты безопасности для их последующего расследования.

Продукт ALD Pro построен на базе службы каталога FreeIPA, поэтому взаимодействие с каталогом возможно по следующим протоколам:

- LDAP v3 (389 Directory Server),
- Kerberos V5, kpasswd, kadmin (MIT KDC),
- REST API (FreeIPA, ALD Pro).

Каждый компонент системы логирует информацию в свои файлы, поэтому перечень файлов будет зависеть от того, какие события потребуется анализировать.

2 Файлы журналов технологических компонентов

2.1 Журналы 389 Directory Server

2.1.1 Аудит доступа

Аудит доступа включен по умолчанию, данные находятся в файле /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access. Приведем пример событий из этого журнала:

```
[16/Aug/2024:14:02:46.884502086 +0300] conn=19435 fd=168 slot=168 SSL connection from
10.0.1.11 to 10.0.1.11
[16/Aug/2024:14:02:46.888295154 +0300] conn=19435 TLS1.3 128-bit AES-GCM
[16/Aug/2024:14:02:46.890129938 +0300] conn=9 op=75696 SRCH base="dc=ald,dc=company,d
c=lan" scope=2 filter="(&(|(objectClass=krbprincipalaux)(objectClass=krbprincipal)
(objectClass=ipakrb
principal))(|(ipaKrbPrincipalAlias=HTTP/dc-1.ald.company.lan@ALD.COMPANY.LAN)
(krbPrincipalName:caseIgnoreIA5Match:=HTTP/dc-1.ald.company.lan@ALD.COMPANY.LAN)))"
attrs="krbPrincipalName k
rbCanonicalName krbUPEnabled krbPrincipalKey krbTicketPolicyReference
krbPrincipalExpiration krbPasswordExpiration krbPwdPolicyReference krbPrincipalType
krbPwdHistory krbLastPwdChange k
rbPrincipalAliases krbLastSuccessfulAuth krbLastFailedAuth krbLoginFailedCount
krbPrincipalAuthInd krbExtraData krbLastAdminUnlock krbObjectReferences
krbTicketFlags krbMaxTicketLife krb
MaxRenewableAge nsAccountLock passwordHistory ipaKrbAuthzData ipaUserAuthType
ipatokenRadiusConfigLink krbAuthIndMaxTicke..."
```

Результат подключения клиента к серверу фиксируется в событиях следующего вида:

```
[16/Aug/2024:14:03:13.633920599 +0300] conn=19479 op=-1 fd=168 Disconnect - Bad Ber
Tag or uncleanly closed connection - B1
```

При этом используются следующие коды подключения:

- A1 — клиент прерывает соединение;
- B1 — обнаружен поврежденный тег BER. Если теги BER, которые инкапсулируют данные, отправляемые по сети, повреждены при получении, в журнал доступа записывается код соединения B1;
- B2 — тег BER длиннее значения атрибута nsslapd-maxbersize.;
- B3 — обнаружен поврежденный тег BER;
- B4 — серверу не удалось сбросить ответ данных обратно клиенту;
- P2 — обнаружено закрытое или поврежденное соединение;
- T1 — клиент не получает результат в течение указанного периода ожидания;
- T2 — сервер закрыл соединение после превышения периода ioblocktimeout;

- U1 — соединение закрыто сервером после того, как клиент отправил запрос на отмену аутентификации (привязки).

Результат выполнения операции фиксируется событиями следующего вида:

```
[16/Aug/2024:14:03:13.634500807 +0300] conn=19480 op=0 RESULT err=0 tag=97 nentries=0
 wtime=0.000143026 optime=0.000057379 etime=0.000199902 dn="cn=Directory Manager"
```

При этом используются следующие теги для категоризации операций:

- tag=97 Результат операции привязки клиента;
- tag=100 Фактическая искомая запись;
- tag=101 Результат операции поиска;
- tag=103 Результат операции изменения;
- tag=105 Результат операции добавления;
- tag=107 Результат операции удаления;
- tag=109 Результат операции moddn;
- tag=111 Результат операции сравнения;
- tag=115 Ссылка поиска, когда запись, по которой выполнялся поиск, содержит ссылку на требуемую запись;
- tag=120 Результат расширенной операции;
- tag=121 Результат промежуточной операции.

Атрибут err события указывает на результат выполнения операции:

```
[16/Aug/2024:14:52:22.099411645 +0300] conn=6 op=110060 RESULT err=32 tag=101
 nentries=0 wtime=0.000008673 optime=0.000252093 etime=0.000259653
```

При этом используются следующие числовые коды:

- 0 0x00 LDAP_SUCCESS
- 1 0x01 LDAP_OPERATIONS_ERROR
- 2 0x02 LDAP_PROTOCOL_ERROR
- 3 0x03 LDAP_TIMELIMIT_EXCEEDED
- 4 0x04 LDAP_SIZELIMIT_EXCEEDED
- 5 0x05 LDAP_COMPARE_FALSE
- 6 0x06 LDAP_COMPARE_TRUE
- 7 0x07 LDAP_AUTH_METHOD_NOT_SUPPORTED
- LDAP_STRONG_AUTH_NOT_SUPPORTED
- 8 0x08 LDAP_STRONG_AUTH_REQUIRED
- 9 0x09 LDAP_PARTIAL_RESULTS
- 10 0x0a LDAP_REFERRAL [a]
- 11 0x0b LDAP_ADMINLIMIT_EXCEEDED
- 12 0x0c LDAP_UNAVAILABLE_CRITICAL_EXTENSION
- 13 0x0d LDAP_CONFIDENTIALITY_REQUIRED
- 14 0x0e LDAP_SASL_BIND_IN_PROGRESS
- 16 0x10 LDAP_NO_SUCH_ATTRIBUTE
- 17 0x11 LDAP_UNDEFINED_TYPE
- 18 0x12 LDAP_INAPPROPRIATE_MATCHING

- 19 0x13 LDAP_CONSTRAINT_VIOLATION
- 20 0x14 LDAP_TYPE_OR_VALUE_EXISTS
- 21 0x15 LDAP_INVALID_SYNTAX
- 32 0x20 LDAP_NO_SUCH_OBJECT
- 33 0x21 LDAP_ALIAS_PROBLEM
- 34 0x22 LDAP_INVALID_DN_SYNTAX
- 35 0x23 LDAP_IS_LEAF [b]
- 36 0x24 LDAP_ALIAS_DEREF_PROBLEM
- 48 0x30 LDAP_INAPPROPRIATE_AUTH
- 49 0x31 LDAP_INVALID_CREDENTIALS
- 50 0x32 LDAP_INSUFFICIENT_ACCESS
- 51 0x33 LDAP_BUSY
- 52 0x34 LDAP_UNAVAILABLE
- 53 0x35 LDAP_UNWILLING_TO_PERFORM
- 54 0x36 LDAP_LOOP_DETECT
- 60 0x3c LDAP_SORT_CONTROL_MISSING
- 61 0x3d LDAP_INDEX_RANGE_ERROR
- 64 0x40 LDAP_NAMING_VIOLATION
- 65 0x41 LDAP_OBJECT_CLASS_VIOLATION
- 66 0x42 LDAP_NOT_ALLOWED_ON_NONLEAF
- 67 0x43 LDAP_NOT_ALLOWED_ON_RDN
- 68 0x44 LDAP_ALREADY_EXISTS
- 69 0x45 LDAP_NO_OBJECT_CLASS_MODS
- 70 0x46 LDAP_RESULTS_TOO_LARGE [c]
- 71 0x47 LDAP_AFFECTS_MULTIPLE_DSAS
- 76 0x4C LDAP_VIRTUAL_LIST_VIEW_ERROR
- 80 0x50 LDAP_OTHER
- 81 0x51 LDAP_SERVER_DOWN
- 82 0x52 LDAP_LOCAL_ERROR
- 83 0x53 LDAP_ENCODING_ERROR
- 84 0x54 LDAP_DECODING_ERROR
- 85 0x55 LDAP_TIMEOUT
- 86 0x56 LDAP_AUTH_UNKNOWN
- 87 0x57 LDAP_FILTER_ERROR
- 88 0x58 LDAP_USER_CANCELLED
- 89 0x59 LDAP_PARAM_ERROR
- 90 0x5A LDAP_NO_MEMORY
- 91 0x5B LDAP_CONNECT_ERROR
- 92 0x5C LDAP_NOT_SUPPORTED
- 93 0x5D LDAP_CONTROL_NOT_FOUND
- 94 0x5E LDAP_MORE_RESULTS_TO_RETURN
- 95 0x5F LDAP_MORE_RESULTS_TO_RETURN
- 96 0x60 LDAP_CLIENT_LOOP
- 97 0x61 LDAP_REFERRAL_LIMIT_EXCEEDED
- 118 0x76 LDAP_CANCELLED

2.1.2 Расширенный аудит доступа

Журнал доступа содержит краткую информацию по событиям, чего явно недостаточно для эффективного выявления инцидентов безопасности. Поэтому для интеграции с SIEM-системой

потребуется включить расширенный аудит доступа, для чего нужно выполнить команду dsconf со следующими параметрами:

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

После этого станет доступен файл /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit, в котором будут появляться события аудита в формате LDIF, например:

```
time: 20230914154158
dn: uid=fedya,cn=users,cn=accounts,dc=ald,dc=lan
result: 0
changetype: modify
delete: sn
sn: fedya1234
-
add: sn
sn: fedya
-
replace: internalModifiersName
internalModifiersName: cn=ldbm database,cn=plugins,cn=config-
replace: modifiersname
modifiersname: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20230914124158Z
-
replace: entryusn
entryusn: 79170
-
```

Может потребоваться включить в события дополнительные атрибуты записей, данная функция доступна на ALSE 1.7.4+ Тогда нужно выполнить следующую команду, указав вместо «*» желаемые атрибуты:

```
dsconf -D "cn=Directory Manager" ldap://alddc1.ald.lan config replace nsslapd-
auditlog-display-attrs=*
```

Символ «*» позволяет включить в события все атрибуты записей, но это приведет к деградации, поэтому недопустимо в продуктивных средах.

2.1.3 Аудит ошибок

Аудит ошибок (errors) включен по умолчанию, данные находятся в файле /var/log/dirsrv/slapd-ALD-COMPANY-LAN/errors. Приведем пример событий из этого журнала:

```
[16/Aug/2024:09:26:21.939753519 +0300] - ERR - attr_syntax_create - Error: the
EQUALITY matching rule [caseIgnoreIA5Match] is not compatible with the syntax [1.3.6.
1.4.1.1466.115.121.1.15] for the attribute [proxyAddresses]
```

```
[16/Aug/2024:09:26:21.956445447 +0300] - ERR - attr_syntax_create - Error: the SUBSTR
matching rule [caseIgnoreIA5SubstringsMatch] is not compatible with the syntax [1.3.6
.1.4.1.1466.115.121.1.15] for the attribute [proxyAddresses]
[16/Aug/2024:09:26:21.986762434 +0300] - ERR - attr_syntax_create - Error: the
EQUALITY matching rule [caseIgnoreIA5Match] is not compatible with the syntax [1.3.6.
1.4.1.1466.115.121.1.15] for the attribute [user-custom-attr]
```

В данном журнале фиксируются не только ошибки, но и вполне успешные операции, например, в части работы механизма репликации, создания индексов и др.

2.1.4 Расширенный аудит ошибок

Расширенный аудит ошибок требуется включать вручную, записи будут добавляться в общий файл расширенного аудита audit. Для этого нужно выполнить команду dsconf со следующими параметрами:

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

2.1.5 Расширенный аудит безопасности

Аудит безопасности требуется включать вручную, после чего станет доступен файл /var/log/dirsrv/slapd-ALD-COMPANY-LAN/security. Для этого выполните команду:

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

Указанные изменения могут быть выполнены на лету, перезагружать службу каталога после внесения изменений не требуется.

2.1.6 Передача событий в syslog

Служба каталога 389 Directory Server позволяет перенаправить события из файлов access, errors и audit (исключая security) в /var/log/syslog, для этого нужно поменять значение атрибута nsslapd-logging-backend с dirsrv-log на syslog и перезагрузить dirsrv:

```
dsconf -D "cn=Directory Manager" ldap://alddc1.ald.lan config replace nsslapd-
logging-backend=syslog

systemctl restart dirsrv@ALD-LAN.service
```

2.2 Журналы MIT KDC

События аутентификации фиксируются в журнале **/var/log/auth.log**, куда по умолчанию пишут события службы Kerberos, Apache, SSH и др.

Вообще по умолчанию у KDC есть собственный файл /var/log/krb5kdc.log, но служба не имеет прав на запись в папку /var/log. Для исправления этой ошибки требуется в файле krb5-kdc.service добавить этот каталог в список ReadWriteDirectories. После внесения изменений нужно сделать перезагрузку конфигурации всех юнитов с помощью команды daemon-reload и перезагрузить KDC:

```
cat /lib/systemd/system/krb5-kdc.service
...
ReadWriteDirectories=-/var/tmp /tmp /var/lib/krb5kdc -/var/run /run /var/log
..


systemctl daemon-reload

systemctl restart krb5-kdc
```

2.3 Журналы Samba

Служба Samba (SMB) по умолчанию ведет только системные журналы, необходимые для отладки ее работы. Для включения аудита необходимо внести дополнительные параметры в секцию global в файле /etc/samba/smb.conf и перезагрузить службу smbd. События аудита можно будет извлечь из файла /var/log/messages:

```
cat /etc/samba/smb.conf
[global]
...
log level = 1 vfs:1
full_audit:prefix = %u|%I|%S
#full_audit:success = connect, open, mkdir, rmdir, unlink, write, rename
full_audit:success = connect mkdirat pread pwrite renameat unlinkat create_file
#full_audit:failure = connect, open, mkdir, rmdir, unlink, write, rename
full_audit:failure = none
full_audit:facility = local5
full_audit:priority = notice
vfs objects = full_audit
....

systemctl restart smbd
```

2.4 Журналы DNS

За **DNS** в ALD Pro отвечает **служба named-pkcs11**, которая логирует свои события в /var/log/syslog, но сами DNS-записи находятся в LDAP-каталоге, поэтому соответствующие события можно будет извлечь из аудита 389 Directory Server.

2.5 Журналы аудита операционной системы

Для аудита запускаемых процессов пользователями и новых подключений к системе необходимо использовать **auditd**, который логирует в /var/log/audit/audit.log. Для работы подсистемы требуется дополнительная настройка правил.

3 Примеры событий

3.1 Событие 4768 A Kerberos authentication ticket was requested

Факт выдачи TGT-билета фиксируется в файле /var/log/auth.log на контроллере домена. Далее мы приводим два события, созданные при аутентификации хоста srvsssd.ald.lan в домене ALD.LAN. Первая попытка заканчивается требованием выполнить предварительную аутентификацию (NEEDED_PREAUTH):

```
авг 09 18:05:44 alddc1.ald.lan krb5kdc[19850](info): AS_REQ (8 etypes {aes256-cts-
hmac-sha1-96(18), aes128-cts-hmac-sha1-96(17), aes256-cts-hmac-sha384-192(20),
aes128-cts-hmac-sha256-128(19), DEPRECATED:des3-cbc-sha1(16), DEPRECATED:arcfour-
hmac(23), camellia128-cts-cmac(25), camellia256-cts-cmac(26)}) 192.168.100.125:
NEEDED_PREAUTH: host/srvsssd.ald.lan@ALD.LAN for krbtgt/ALD.LAN@ALD.LAN, Additional
pre-authentication required
```

Второе событие указывает на то, что TGT-билет был успешно выдан (ISSUE) хосту:

```
авг 09 18:05:44 alddc1.ald.lan krb5kdc[19850](info): AS_REQ (8 etypes {aes256-cts-
hmac-sha1-96(18), aes128-cts-hmac-sha1-96(17), aes256-cts-hmac-sha384-192(20),
aes128-cts-hmac-sha256-128(19), DEPRECATED:des3-cbc-sha1(16), DEPRECATED:arcfour-
hmac(23), camellia128-cts-cmac(25), camellia256-cts-cmac(26)}) 192.168.100.125:
ISSUE: authtime 1691593544, etypes {rep=aes256-cts-hmac-sha1-96(18), tkt=aes256-cts-
hmac-sha1-96(18), ses=aes256-cts-hmac-sha1-96(18)}, host/srvsssd.ald.lan@ALD.LAN for
 krbtgt/ALD.LAN@ALD.LAN
```

3.2 Событие 4769 Kerberos service ticket requested

Факт выдачи TGS-билета фиксируется в файле /var/log/auth.log. Далее мы приводим событие, созданное в процессе посещения веб-сайта на сервере cons.ald.company.lan с аутентификацией по Kerberos пользователем admin@ALD.COMPANY.LAN с компьютера 192.168.130.11. В результате был выпущен билет (TGS) на сервис HTTP/cons.ald.company.lan@ALD.COMPANY.LAN.

```
Aug 15 11:49:08 dc-1 krb5kdc[1751]: TGS_REQ (8 etypes {aes256-cts-hmac-sha1-96(18),
aes128-cts-hmac-sha1-96(17), aes256-cts-hmac-sha384-192(20), aes128-cts-hmac-sha256-1
28(19), DEPRECATED:des3-cbc-sha1(16), DEPRECATED:arcfour-hmac(23), camellia128-cts-
cmac(25), camellia256-cts-cmac(26)}) 192.168.130.11: ISSUE: authtime 1723711740,
etypes {rep=aes256-cts-hmac-sha1-96(18), tkt=aes256-cts-hmac-sha1-96(18), ses=aes256-
cts-hmac-sha1-96(18)}, admin@ALD.COMPANY.LAN for HTTP/cons.ald.company.lan@ALD.COMPAN
Y.LAN
```

3.3 Событие 4771 Kerberos pre authentication failed

Факт неудачной Kerberos-аутентификации фиксируется в файле /var/log/auth.log на контроллере домена. В приведенном далее примере пользователь admin использовал неправильный пароль, и ему было отказано в предоставлении TGT-билета.

Первая попытка заканчивается требованием выполнить предварительную аутентификацию (NEEDED_PREAUTH), что является нормальным поведением и предусмотрено протоколом:

```
Aug 16 15:13:01 dc-1 krb5kdc[2610]: AS_REQ (8 etypes {aes256-cts-hmac-sha1-96(18),
aes128-cts-hmac-sha1-96(17), aes256-cts-hmac-sha384-192(20), aes128-cts-hmac-sha256-1
28(19), DEPRECATED:des3-cbc-sha1(16), DEPRECATED:arcfour-hmac(23), camellia128-cts-
cmac(25), camellia256-cts-cmac(26)}) 10.0.1.11: NEEDED_PREAUTH: admin@ALD.COMPANY.LAN
for krbtgt/ALD.COMPANY.LAN@ALD.COMPANY.LAN, Additional pre-authentication required
```

Второе событие указывает на то, что пользователю было отказано (PREAUTH_FAILED) в выдаче TGT-билета, т.к. он не прошел предварительную аутентификацию:

```
Aug 16 15:13:01 dc-1 krb5kdc[2611]: AS_REQ (8 etypes {aes256-cts-hmac-sha1-96(18),
aes128-cts-hmac-sha1-96(17), aes256-cts-hmac-sha384-192(20), aes128-cts-hmac-sha256-1
28(19), DEPRECATED:des3-cbc-sha1(16), DEPRECATED:arcfour-hmac(23), camellia128-cts-
cmac(25), camellia256-cts-cmac(26)}) 10.0.1.11: PREAUTH_FAILED: admin@ALD.COMPANY.LAN
for krbtgt/ALD.COMPANY.LAN@ALD.COMPANY.LAN, Preauthentication failed
```

3.4 Событие 4624 An account was successfully logged on

Факт успешной аутентификации на сервере можно найти в журнале /var/log/auth.log.

Пример подключения к рабочему столу Fly:

```
Aug 10 13:40:22 alddc1 fly-dm[741]: :0[741]: pam_unix(fly-dm:auth): authentication
failure; logname= uid=0 euid=0 tty=/dev/tty7 ruser= rhost= user=admin@ald.lan
Aug 10 13:40:23 alddc1 fly-dm[741]: :0[741]: pam_sss(fly-dm:auth): authentication
success; logname= uid=0 euid=0 tty=/dev/tty7 ruser= rhost= user=admin@ald.lan
Aug 10 13:40:25 alddc1 fly-dm[741]: :0[741]: pam_kiosk2(fly-dm:session): No admin@ald.
lan profile found, trying common profile
Aug 10 13:40:25 alddc1 fly-dm[741]: :0[741]: pam_kiosk2(fly-dm:session): No common
profile found, further processing stopped
Aug 10 13:40:25 alddc1 fly-dm[741]: :0[741]: pam_unix(fly-dm:session): session opened
for user admin@ald.lan by (uid=0)
Aug 10 13:40:25 alddc1 systemd-logind[726]: New session 474 of user admin.
```

Пример отключения сессии рабочего стола:

```
Aug 10 13:41:44 alddc1 polkitd(authority=local)[525]: Unregistered Authentication
Agent for unix-session:474 (system bus name :1.13358, object path /org/kde/
PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8)
```

```
Aug 10 13:41:44 alddc1 fly-dm[741]: :0[741]: pam_unix(fly-dm:session): session closed
for user admin@ald.lan
Aug 10 13:41:44 alddc1 systemd-logind[726]: Removed session 474.
```

Пример подключения к удаленному рабочему столу Fly с другого сервера через веб-интерфейс ALD Pro, вкладка "Удаленный доступ", подключиться можно только к активной сессии:

```
Oct 10 11:37:15 alddc1 fly-wmpam[30795]: pam_unix(fly-wm:auth): authentication
failure; logname= uid=14000000 euid=0 tty=/dev/tty7 ruser= rhost= user=admin
Oct 10 11:37:15 alddc1 fly-wmpam[30795]: pam_sss(fly-wm:auth): authentication
success; logname= uid=14000000 euid=0 tty=/dev/tty7 ruser= rhost= user=admin
```

Пример подключения по SSH:

```
Aug 10 13:36:43 alddc1 sshd[31725]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.100.110 user=admin
Aug 10 13:36:43 alddc1 sshd[31725]: pam_sss(sshd:auth): authentication success;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.100.110 user=admin
Aug 10 13:36:43 alddc1 sshd[31723]: Accepted keyboard-interactive/pam for admin from
192.168.100.110 port 58828 ssh2
Aug 10 13:36:43 alddc1 sshd[31723]: pam_kiosk2(sshd:session): No admin profile found,
trying common profile
Aug 10 13:36:43 alddc1 sshd[31723]: pam_kiosk2(sshd:session): No common profile
found, further processing stopped
Aug 10 13:36:43 alddc1 sshd[31723]: pam_unix(sshd:session): session opened for user
admin by (uid=0)
Aug 10 13:36:43 alddc1 systemd-logind[726]: New session 473 of user admin.
```

Пример отключения сессии SSH:

```
Aug 10 13:43:51 alddc1 sshd[31728]: Received disconnect from 192.168.100.110 port
58828:11: disconnected by user
Aug 10 13:43:51 alddc1 sshd[31728]: Disconnected from user admin 192.168.100.110 port
58828
Aug 10 13:43:51 alddc1 sshd[31723]: pam_unix(sshd:session): session closed for user
admin
```

3.5 Событие 4625 An account failed to log on

Факт неудачной аутентификации при подключении к контроллеру домена фиксируется в журнале /var/log/auth.log.

Пример ввода неверного пароля при подключении к рабочему столу:

```
Aug 10 13:47:59 alddc1 fly-dm[2576]: :0[2576]: pam_unix(fly-dm:auth): authentication
failure; logname= uid=0 euid=0 tty=/dev/tty7 ruser= rhost= user=admin@ald.lan
```

```
Aug 10 13:47:59 alddc1 fly-dm[2576]: :0[2576]: pam_sss(fly-dm:auth): authentication
failure; logname= uid=0 euid=0 tty=/dev/tty7 ruser= rhost= user=admin@ald.lan
Aug 10 13:47:59 alddc1 fly-dm[2576]: :0[2576]: pam_sss(fly-dm:auth): received for
 user admin@ald.lan: 7 (Сбой при проверке подлинности)
```

Пример ввода неверного пароля при подключении по SSH:

```
Aug 10 13:51:59 alddc1 sshd[6544]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.100.110 user=admin
Aug 10 13:51:59 alddc1 sshd[6544]: pam_sss(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.100.110 user=admin
Aug 10 13:51:59 alddc1 sshd[6544]: pam_sss(sshd:auth): received for user admin: 7
 (Authentication failure)
Aug 10 13:52:01 alddc1 sshd[6542]: error: PAM: Authentication failure for admin from
192.168.100.110
```

Пример с несуществующим пользователем при подключении по SSH:

```
Aug 10 13:53:23 alddc1 sshd[7210]: Invalid user xyz from 192.168.100.110 port 58834
Aug 10 13:53:23 alddc1 sshd[7210]: Postponed keyboard-interactive for invalid user
xyz from 192.168.100.110 port 58834 ssh2 [preauth]
Aug 10 13:53:25 alddc1 sshd[7213]: pam_unix(sshd:auth): check pass; user unknown
Aug 10 13:53:25 alddc1 sshd[7213]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.100.110
Aug 10 13:53:25 alddc1 sshd[7213]: pam_sss(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.100.110 user=xyz
Aug 10 13:53:25 alddc1 sshd[7213]: pam_sss(sshd:auth): received for user xyz: 10
 (User not known to the underlying authentication module)
Aug 10 13:53:27 alddc1 sshd[7210]: error: PAM: Authentication failure for illegal
user xyz from 192.168.100.110
Aug 10 13:53:27 alddc1 sshd[7210]: Failed keyboard-interactive/pam for invalid user
xyz from 192.168.100.110 port 58834 ssh2
```

3.6 Событие 4720 A user account was created

Создание нового пользователя можно увидеть в /var/log/dirsrv/slapd-ALD-LAN/access.

В следующем примере мы создаем нового пользователя "kazan" в домене ald.lan:

```
[03/Aug/2023:16:00:34.934156788 +0300] conn=757 fd=155 slot=155 connection from
192.168.100.120 to 192.168.100.120
[03/Aug/2023:16:00:34.938442409 +0300] conn=757 op=0 BIND dn="" method=sasl version=3
 mech=GSS-SPNEGO
[03/Aug/2023:16:00:34.939850435 +0300] conn=757 op=0 RESULT err=0 tag=97 nentries=0
 wtime=0.000120634 optime=0.001410210 etime=0.001530124 dn="uid=admin,cn=users,cn=acc
ounts,dc=ald,dc=lan"
[03/Aug/2023:16:00:34.941065359 +0300] conn=757 op=1 SRCH base="cn=ipaconfig,cn=etc,d
c=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs=ALL
[03/Aug/2023:16:00:34.941367788 +0300] conn=757 op=1 RESULT err=0 tag=101 nentries=1
 wtime=0.000084803 optime=0.000303040 etime=0.000386853
```

```
[03/Aug/2023:16:00:34.942062060 +0300] conn=757 op=2 SRCH base="uid=kazan,cn=deleted
users,cn=accounts,cn=provisioning,dc=ald,dc=lan" scope=0 filter="(objectClass=*)"
 attrs=""
[03/Aug/2023:16:00:34.942474051 +0300] conn=757 op=2 RESULT err=32 tag=101 nentries=0
 wtime=0.000079578 optime=0.000411581 etime=0.000489852
[03/Aug/2023:16:00:34.942932594 +0300] conn=757 op=3 SRCH base="cn=UPG
Definition,cn=Definitions,cn=Managed Entries,cn=etc,dc=ald,dc=lan" scope=0 filter="(o
bjectClass=*)" attrs="* aci"
[03/Aug/2023:16:00:34.943298785 +0300] conn=757 op=3 RESULT err=0 tag=101 nentries=1
 wtime=0.000162308 optime=0.000367144 etime=0.000528400
[03/Aug/2023:16:00:34.943646144 +0300] conn=757 op=4 SRCH base="cn=kazan,cn=groups,cn
=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs=""
[03/Aug/2023:16:00:34.943760601 +0300] conn=757 op=4 RESULT err=32 tag=101 nentries=0
 wtime=0.000045272 optime=0.000115172 etime=0.000159521
[03/Aug/2023:16:00:34.946474742 +0300] conn=757 op=5 ADD dn="uid=kazan,cn=users,cn=ac
counts,dc=ald,dc=lan"
[03/Aug/2023:16:00:35.003586430 +0300] conn=757 op=5 RESULT err=0 tag=105 nentries=0
 wtime=0.000152986 optime=0.057113724 etime=0.057264684 csn=64cba4f7000000040000
[03/Aug/2023:16:00:35.004265004 +0300] conn=757 op=6 SRCH base="uid=kazan,cn=users,cn
=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="x-ald-user-cap
ipaUserAuthType mail krbPrincipalName givenName x-ald-user-mac uidNumber
ipatokenRadiusUserName ipatokenRadiusConfigLink ipaCertMapData homeDirectory
memberofindirect ou x-ald-aud-mask title * sn loginShell ipaNTProfilePath
nsAccountLock ipaNTLogonScript telephoneNumber ipaNTHomeDirectoryDrive rbtadp
krbCanonicalName usercertificate;binary memberOf uid ipaNTHomeDirectory x-ald-user-
caps krbPrincipalExpiration x-ald-aud-type gidNumber userClass aci"
[03/Aug/2023:16:00:35.005283195 +0300] conn=757 op=6 RESULT err=0 tag=101 nentries=1
 wtime=0.000079512 optime=0.001019873 etime=0.001098204
[03/Aug/2023:16:00:35.006255026 +0300] conn=757 op=7 SRCH base="dc=ald,dc=lan" scope=2
 filter="(|(member=uid=kazan,cn=users,cn=accounts,dc=ald,dc=lan)
(memberUser=uid=kazan,cn=users,cn=accounts,dc=ald,dc=lan)
(memberHost=uid=kazan,cn=users,cn=accounts,dc=ald,dc=lan))" attrs=""
[03/Aug/2023:16:00:35.006492609 +0300] conn=757 op=7 RESULT err=0 tag=101 nentries=0
 wtime=0.000079415 optime=0.000238559 etime=0.000316538 notes=P details="Paged
Search" pr_idx=0 pr_cookie=-1
[03/Aug/2023:16:00:35.006901527 +0300] conn=757 op=8 SRCH base="uid=kazan,cn=users,cn
=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs=""
[03/Aug/2023:16:00:35.007136509 +0300] conn=757 op=8 RESULT err=0 tag=101 nentries=1
 wtime=0.000072523 optime=0.000235599 etime=0.000306865
[03/Aug/2023:16:00:35.007345093 +0300] conn=757 op=9 MOD dn="cn=ipausers,cn=groups,cn
=accounts,dc=ald,dc=lan"
[03/Aug/2023:16:00:35.022278849 +0300] conn=757 op=9 RESULT err=0 tag=103 nentries=0
 wtime=0.000055017 optime=0.014935025 etime=0.014988987 csn=64cba4f8000000040000
[03/Aug/2023:16:00:35.022724728 +0300] conn=757 op=10 SRCH base="uid=kazan,cn=users,c
n=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="* aci"
[03/Aug/2023:16:00:35.024048030 +0300] conn=757 op=10 RESULT err=0 tag=101 nentries=1
 wtime=0.000081113 optime=0.001324138 etime=0.001404173
[03/Aug/2023:16:00:35.025685027 +0300] conn=757 op=11 SRCH base="uid=kazan,cn=users,c
n=accounts,dc=ald,dc=lan" scope=0 filter="(userPassword=*)" attrs="userPassword"
[03/Aug/2023:16:00:35.025907983 +0300] conn=757 op=11 RESULT err=0 tag=101 nentries=1
 wtime=0.000055757 optime=0.000224052 etime=0.000277495
[03/Aug/2023:16:00:35.026367200 +0300] conn=757 op=12 SRCH base="uid=kazan,cn=users,c
n=accounts,dc=ald,dc=lan" scope=0 filter="(krbPrincipalKey=*)" attrs="krbPrincipalKey
"
[03/Aug/2023:16:00:35.026621675 +0300] conn=757 op=12 RESULT err=0 tag=101 nentries=1
 wtime=0.000057654 optime=0.000255353 etime=0.000311796
[03/Aug/2023:16:00:35.027893433 +0300] conn=757 op=13 UNBIND
[03/Aug/2023:16:00:35.027906355 +0300] conn=757 op=13 fd=155 Disconnect - Cleanly
Closed Connection - U1
```

В представленных событиях access мы видим следующее:

- conn=757 – номер подключения;
- connection from 192.168.100.120 to 192.168.100.120 – источник подключения, в нашем примере мы делали изменения локально на контроллере домена ALD Pro;
- SRCH base="uid=kazan,cn=deleted users,cn=accounts,cn=provisioning,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="" – тип запроса SRCH. Бывают так же запросы MOD, ADD, DEL и т.д.;
- RESULT err=32 tag=101 nentries=0 wtime=0.000079578 optime=0.000411581 etime=0.000489852 – после каждого запроса идет результат, в нашем случае с кодом выполнения “err=32”, что означает “объект не найден” (расшифровка err), далее мы видим “tag=101” (расшифровка tag, таблица 7.1), который означает, что текущее значение является результатом запроса SRCH. Также мы можем видеть время выполнение операции etime=0.000489852 в секундах и кол-во возвращаемых записей nentries=0, это можно использовать для аналога события EventID 1644;
- ADD dn="uid=kazan,cn=users,cn=accounts,dc=ald,dc=lan" – тип запроса ADD, в нашем случае добавили нового пользователя kazan;
- MOD dn="cn=ipausers,cn=groups,cn=accounts,dc=ald,dc=lan" – тип запроса MOD, изменили группу ipausers, добавив туда нового пользователя.

Расширенную информацию можно получить из /var/log/dirsrv/slapd-ALD-LAN/audit:

```
time: 20230803160035
dn: uid=kazan,cn=users,cn=accounts,dc=ald,dc=lan
#givenName: kazan
#sn: kazan123
#uid: kazan
#cn: kazan kazan123
#displayName: kazan kazan123
#initials: kk
#gecos: kazan kazan123
#krbPrincipalName: kazan@ALD.LAN
#nsAccountLock: FALSE
#proxyAddresses: SMTP:kazan@ald.lan
#rbtadp: ou=IT,ou=ald.lan,cn=orgunits,cn=accounts,dc=ald,dc=lan
#objectClass: top
#objectClass: person
#objectClass: organizationalperson
#objectClass: inetorgperson
#objectClass: inetuser
#objectClass: posixaccount
#objectClass: krbprincipalaux
#objectClass: krbticketpolicyaux
#objectClass: ipaobject
#objectClass: ipasshuser
#objectClass: x-ald-user
#objectClass: x-ald-user-parsec14
#objectClass: x-ald-audit-policy
#objectClass: ruPostMailAccount
#objectClass: rbtaCustomUserAttrs
#objectClass: rbtaUserMeta
#objectClass: rbta-unit
#objectClass: rbta-address
#objectClass: rbta-inetorgperson-ext
#objectClass: ipaSshGroupOfPubKeys
#loginShell: /bin/bash
#homeDirectory: /home/kazan
```

```
#mail: kazan@ald.lan
#xaldusermacmax: 0
#xaldusermacmin: 0
#x-ald-user-mac: 0:0x0:0:0x0
#krbCanonicalName: kazan@ALD.LAN
#userPassword: ****************************
#creatorsName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
#modifiersName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
#createTimestamp: 20230803130034Z
#modifyTimestamp: 20230803130034Z
#nsUniqueId: ba785801-31fd11ee-96e796b2-300f2d85
#ipaUniqueID: bc3bd89c-31fd-11ee-b409-5254001c2f55
#parentid: 36
#entryid: 2164
#krbPrincipalKey: 0□0□□0□□□ □ □ □ ؍h□ 0 □ □ |RQ[GRg^mo4]PRuv□I0G□ □@ >
#uidNumber: 14000010
#gidNumber: 14000010
#entryUUID: 88989397-3f53-4d35-9957-4ed6b1621c21
#entryusn: 19299
#dsEntryDN: uid=kazan,cn=users,cn=accounts,dc=ald,dc=lan
#entrydn: uid=kazan,cn=users,cn=accounts,dc=ald,dc=lan
result: 0
changetype: add
givenName: kazan
sn: kazan123
uid: kazan
cn: kazan kazan123
displayName: kazan kazan123
initials: kk
gecos: kazan kazan123
krbPrincipalName: kazan@ALD.LAN
nsAccountLock: FALSE
proxyAddresses: SMTP:kazan@ald.lan
rbtadp: ou=IT,ou=ald.lan,cn=orgunits,cn=accounts,dc=ald,dc=lan
objectClass: top
objectClass: person
objectClass: organizationalperson
objectClass: inetorgperson
objectClass: inetuser
objectClass: posixaccount
objectClass: krbprincipalaux
objectClass: krbticketpolicyaux
objectClass: ipaobject
objectClass: ipasshuser
objectClass: x-ald-user
objectClass: x-ald-user-parsec14
objectClass: x-ald-audit-policy
objectClass: ruPostMailAccount
objectClass: rbtaCustomUserAttrs
objectClass: rbtaUserMeta
objectClass: rbta-unit
objectClass: rbta-address
objectClass: rbta-inetorgperson-ext
objectClass: ipaSshGroupOfPubKeys
uidNumber: -1
loginShell: /bin/bash
homeDirectory: /home/kazan
gidNumber: -1
mail: kazan@ald.lan
```

```
xaldusermacmax: 0
xaldusermacmin: 0
x-ald-user-mac: 0:0x0:0:0x0
krbCanonicalName: kazan@ALD.LAN
userPassword:: e1BCS0RGMi1TSEE1MTJ9MTAwMDAkVWo3ZzlGTzlwU3QzMHJjZGJwZGtpTENNTzI
0Q0MxMG4kcmdLaFduUDNMdUM3TUtZVVFhM3V6cTR5Uit4V3FlTnFaQ0RGNEl4c2hnZk1kcDl1ZlFv
RlJYOUpHbTl4UVpRd1ZWOEJrNVFWdTM1MWI2Zm1LaEgxQWc9PQ==
creatorsName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
modifiersName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
createTimestamp: 20230803130034Z
modifyTimestamp: 20230803130034Z
ipaUniqueID: bc3bd89c-31fd-11ee-b409-5254001c2f55
```

В представленном событии audit мы видим следующее:

- dn: uid=kazan,cn=users,cn=accounts,dc=ald,dc=lan – изменяемый объект;
- #givenName: kazan – строки, начинающиеся на “#”, являются дополнительными атрибутами изменяемого объекта, которые нужно включать. По умолчанию их нет. Для их активации также необходимо обновить пакет 389-ds-base. В нашем примере мы включили отображение всех атрибутов, но в своей инфраструктуре вы можете настроить отображение атрибутов в соответствии с потребностями вашей организации, чтобы снизить нагрузку на систему со стороны аудита;
- creatorsName, modifiersName – имя учетной записи, кто запросил изменение.

3.7 Событие 4738 A user account was changed

В данном примере у пользователя uid=fedya была изменена фамилия с sn: fedya1234 на sn: fedya.

В логах access нам будет интересна только строка, по которой мы видим, что было сделано изменение у пользователя uid=fedya.

```
[14/Sep/2023:15:41:58.443157909 +0300] conn=8658 op=5 MOD dn="uid=fedya,cn=users,cn=a
ccounts,dc=ald,dc=lan"
```

Полный лог из /var/log/dirsrv/slapd-ALD-LAN/access:

```
[14/Sep/2023:15:41:58.427662084 +0300] conn=8658 fd=157 slot=157 connection from
192.168.100.120 to 192.168.100.120
[14/Sep/2023:15:41:58.434497814 +0300] conn=8658 op=0 BIND dn="" method=sasl version=3
 mech=GSS-SPNEGO
[14/Sep/2023:15:41:58.435694581 +0300] conn=8658 (Internal) op=0(1)(1) SRCH base="dc=
ald,dc=lan" scope=2 filter="(krbPrincipalName=admin@ALD.LAN)" attrs=ALL
[14/Sep/2023:15:41:58.435823151 +0300] conn=8658 (Internal) op=0(1)(1) ENTRY dn="uid=
admin,cn=users,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.435830641 +0300] conn=8658 (Internal) op=0(1)(1)STAT read
index: attribute=objectclass key(eq)=referral --> count 0
[14/Sep/2023:15:41:58.435832400 +0300] conn=8658 (Internal) op=0(1)(1)STAT read
index: attribute=krbPrincipalName key(eq)=admin@ALD.LAN --> count 1
[14/Sep/2023:15:41:58.435833819 +0300] conn=8658 (Internal) op=0(1)(1)STAT read
index: duration 0.000003519
```

```
[14/Sep/2023:15:41:58.435835160 +0300] conn=8658 (Internal) op=0(1)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000011318 optime=0.000136683 etime=0.000147216
[14/Sep/2023:15:41:58.435957231 +0300] conn=8658 (Internal) op=0(2)(1) SRCH base="uid
=admin,cn=users,cn=accounts,dc=ald,dc=lan" scope=0 filter="(|(objectclass=*)
(objectclass=ldapsubentry))" attrs="nsLookThroughLimit nsIDListScanLimit
nsPagedLookThroughLimit nsPagedIDListScanLimit nsRangeSearchLookThroughLimit
nsSizeLimit nsTimeLimit nsPagedSizeLimit nsIdleTimeout"
[14/Sep/2023:15:41:58.436037322 +0300] conn=8658 (Internal) op=0(2)(1) ENTRY dn="uid=
admin,cn=users,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.436042329 +0300] conn=8658 (Internal) op=0(2)(1)STAT read
index: duration 0.000000000
[14/Sep/2023:15:41:58.436043891 +0300] conn=8658 (Internal) op=0(2)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000005085 optime=0.000085497 etime=0.000090040
[14/Sep/2023:15:41:58.436310984 +0300] conn=8658 (Internal) op=0(5)(1) SRCH base="uid
=admin,cn=users,cn=accounts,dc=ald,dc=lan" scope=0 filter="(|(objectclass=*)
(objectclass=ldapsubentry))" attrs=ALL
[14/Sep/2023:15:41:58.436374672 +0300] conn=8658 (Internal) op=0(5)(1) ENTRY dn="uid=
admin,cn=users,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.436379508 +0300] conn=8658 (Internal) op=0(5)(1)STAT read
index: duration 0.000000000
[14/Sep/2023:15:41:58.436380911 +0300] conn=8658 (Internal) op=0(5)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000003233 optime=0.000068473 etime=0.000071163
[14/Sep/2023:15:41:58.436489527 +0300] conn=8658 op=0 RESULT err=0 tag=97 nentries=0
 wtime=0.000152216 optime=0.001994385 etime=0.002145552 dn="uid=admin,cn=users,cn=acc
ounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.438153975 +0300] conn=8658 op=1 SRCH base="cn=ipaconfig,cn=etc,
dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs=ALL
[14/Sep/2023:15:41:58.438533995 +0300] conn=8658 op=1 ENTRY dn="cn=ipaConfig,cn=etc,d
c=ald,dc=lan"
[14/Sep/2023:15:41:58.438561151 +0300] conn=8658 op=1 STAT read index: duration
0.000000000
[14/Sep/2023:15:41:58.438563288 +0300] conn=8658 op=1 RESULT err=0 tag=101 nentries=1
 wtime=0.000080720 optime=0.000407742 etime=0.000487481
[14/Sep/2023:15:41:58.439221974 +0300] conn=8658 op=2 SRCH base="uid=fedya,cn=users,c
n=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="distinguishedName"
[14/Sep/2023:15:41:58.439445407 +0300] conn=8658 op=2 ENTRY dn="uid=fedya,cn=users,cn
=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.439471382 +0300] conn=8658 op=2 STAT read index: duration
0.000000000
[14/Sep/2023:15:41:58.439473739 +0300] conn=8658 op=2 RESULT err=0 tag=101 nentries=1
 wtime=0.000074722 optime=0.000250241 etime=0.000323916
[14/Sep/2023:15:41:58.439838478 +0300] conn=8658 op=3 SRCH base="uid=fedya,cn=users,c
n=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="objectClass"
[14/Sep/2023:15:41:58.440075210 +0300] conn=8658 op=3 ENTRY dn="uid=fedya,cn=users,cn
=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.440101035 +0300] conn=8658 op=3 STAT read index: duration
0.000000000
[14/Sep/2023:15:41:58.440103286 +0300] conn=8658 op=3 RESULT err=0 tag=101 nentries=1
 wtime=0.000080263 optime=0.000263882 etime=0.000343179
[14/Sep/2023:15:41:58.442152925 +0300] conn=8658 op=4 SRCH base="uid=fedya,cn=users,c
n=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="c telephoneNumber
objectClass krbPasswordExpiration employeeNumber jpegPhoto title ipaSshPubKey
usercertificate;binary postalCode l uidNumber st mobile sn street"
[14/Sep/2023:15:41:58.442398962 +0300] conn=8658 op=4 ENTRY dn="uid=fedya,cn=users,cn
=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.442424652 +0300] conn=8658 op=4 STAT read index: duration
0.000000000
[14/Sep/2023:15:41:58.442426922 +0300] conn=8658 op=4 RESULT err=0 tag=101 nentries=1
 wtime=0.000088038 optime=0.000272842 etime=0.000359871
```

```
[14/Sep/2023:15:41:58.443157909 +0300] conn=8658 op=5 MOD dn="uid=fedya,cn=users,cn=a
ccounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.443172892 +0300] conn=8658 (Internal) op=5(1)(1) SRCH base="uid
=fedya,cn=users,cn=accounts,dc=ald,dc=lan" scope=0 filter="(|(objectclass=*)
(objectclass=ldapsubentry))" attrs=ALL
[14/Sep/2023:15:41:58.443239719 +0300] conn=8658 (Internal) op=5(1)(1) ENTRY dn="uid=
fedya,cn=users,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.443246184 +0300] conn=8658 (Internal) op=5(1)(1)STAT read
index: duration 0.000000000
[14/Sep/2023:15:41:58.443247867 +0300] conn=8658 (Internal) op=5(1)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000008447 optime=0.000073188 etime=0.000080916
[14/Sep/2023:15:41:58.447416728 +0300] conn=8658 op=5 RESULT err=0 tag=103 nentries=0
 wtime=0.000087388 optime=0.004259792 etime=0.004344256 csn=6502ffb1000000040000
[14/Sep/2023:15:41:58.447872369 +0300] conn=8658 op=6 SRCH base="uid=fedya,cn=users,c
n=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="ipaNTProfilePath
ipatokenRadiusUserName memberofindirect ipatokenRadiusConfigLink
usercertificate;binary * ipaNTHomeDirectoryDrive uidNumber loginShell homeDirectory
krbPrincipalName ou rbtadp ipaUserAuthType krbCanonicalName title ipaNTHomeDirectory
mail krbPrincipalExpiration x-ald-user-mac x-ald-user-cap userClass ipaNTLogonScript
gidNumber telephoneNumber x-ald-user-caps givenName memberOf nsAccountLock
ipaCertMapData x-ald-aud-mask x-ald-aud-type sn uid aci"
[14/Sep/2023:15:41:58.449110659 +0300] conn=8658 op=6 ENTRY dn="uid=fedya,cn=users,cn
=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.449148238 +0300] conn=8658 op=6 STAT read index: duration
0.000000000
[14/Sep/2023:15:41:58.449151755 +0300] conn=8658 op=6 RESULT err=0 tag=101 nentries=1
 wtime=0.000114332 optime=0.001277399 etime=0.001390537
[14/Sep/2023:15:41:58.450105700 +0300] conn=8658 op=7 SRCH base="dc=ald,dc=lan"
 scope=2 filter="(|(member=uid=fedya,cn=users,cn=accounts,dc=ald,dc=lan)
(memberUser=uid=fedya,cn=users,cn=accounts,dc=ald,dc=lan)
(memberHost=uid=fedya,cn=users,cn=accounts,dc=ald,dc=lan))" attrs=""
[14/Sep/2023:15:41:58.450437287 +0300] conn=8658 op=7 ENTRY dn="cn=ipausers,cn=groups
,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.450498871 +0300] conn=8658 op=7 RESULT err=0 tag=101 nentries=1
 wtime=0.000100984 optime=0.000394070 etime=0.000493507 notes=P details="Paged
Search" pr_idx=0 pr_cookie=-1
[14/Sep/2023:15:41:58.451041060 +0300] conn=8658 op=8 SRCH base="uid=fedya,cn=users,c
n=accounts,dc=ald,dc=lan" scope=0 filter="(userPassword=*)" attrs="userPassword"
[14/Sep/2023:15:41:58.451304953 +0300] conn=8658 op=8 ENTRY dn="uid=fedya,cn=users,cn
=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.451332876 +0300] conn=8658 op=8 STAT read index: duration
0.000000000
[14/Sep/2023:15:41:58.451335316 +0300] conn=8658 op=8 RESULT err=0 tag=101 nentries=1
 wtime=0.000075945 optime=0.000292875 etime=0.000367745
[14/Sep/2023:15:41:58.451816643 +0300] conn=8658 op=9 SRCH base="uid=fedya,cn=users,c
n=accounts,dc=ald,dc=lan" scope=0 filter="(krbPrincipalKey=*)" attrs="krbPrincipalKey
"
[14/Sep/2023:15:41:58.452078782 +0300] conn=8658 op=9 ENTRY dn="uid=fedya,cn=users,cn
=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.452113605 +0300] conn=8658 op=9 STAT read index: duration
0.000000000
[14/Sep/2023:15:41:58.452116650 +0300] conn=8658 op=9 RESULT err=0 tag=101 nentries=1
 wtime=0.000069018 optime=0.000296392 etime=0.000364129
[14/Sep/2023:15:41:58.455393723 +0300] conn=8658 op=10 UNBIND
[14/Sep/2023:15:41:58.455411993 +0300] conn=8658 op=10 fd=157 Disconnect - Cleanly
Closed Connection - U1
[14/Sep/2023:15:41:58.479901390 +0300] conn=8658 (Internal) op=5(9)(1) SRCH base="cn=
anonymous-limits,cn=etc,dc=ald,dc=lan" scope=0 filter="(|(objectclass=*)
(objectclass=ldapsubentry))" attrs="nsLookThroughLimit nsIDListScanLimit
```

```
nsPagedLookThroughLimit nsPagedIDListScanLimit nsRangeSearchLookThroughLimit
nsSizeLimit nsTimeLimit nsPagedSizeLimit nsIdleTimeout"
[14/Sep/2023:15:41:58.479959198 +0300] conn=8658 (Internal) op=5(9)(1) ENTRY dn="cn=a
nonymous-limits,cn=etc,dc=ald,dc=lan"
[14/Sep/2023:15:41:58.479968874 +0300] conn=8658 (Internal) op=5(9)(1)STAT read
index: duration 0.000000000
[14/Sep/2023:15:41:58.479971628 +0300] conn=8658 (Internal) op=5(9)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000020043 optime=0.000068513 etime=0.000087481
```

Расширенную информацию можно будет получить из /var/log/dirsrv/slapd-ALD-LAN/audit.

В представленном событии audit мы видим следующее:

- учетная запись пользователя fedya

```
dn: uid=fedya,cn=users,cn=accounts,dc=ald,dc=lan
```

- была изменена

```
changetype: modify
```

- был удален атрибут sn с значением fedya1234

```
delete: sn
sn: fedya1234
```

- и добавлен новый атрибут sn с значением fedya

```
add: sn
sn: fedya
```

Полный лог:

```
time: 20230914154158
dn: uid=fedya,cn=users,cn=accounts,dc=ald,dc=lan
#entryusn: 79170
#modifyTimestamp: 20230914124158Z
#modifiersName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
#internalModifiersName: cn=ldbm database,cn=plugins,cn=config
#sn: fedya
#gidNumber: 14000009
#uidNumber: 14000009
#krbPrincipalKey: 0ﻩ^C^B^A^A^A^C^B^A^A^A^C^B^A^A^A
```

```
#krbCanonicalName: fedya@ALD.LAN
#x-ald-user-mac: 0:0x0:0:0x0
#xaldusermacmin: 0
#xaldusermacmax: 0
#mail: fedya@ald.lan
#homeDirectory: /home/fedya
#loginShell: /bin/bash
#objectClass: top
#objectClass: person
#objectClass: organizationalperson
#objectClass: inetorgperson
#objectClass: inetuser
#objectClass: posixaccount
#objectClass: krbprincipalaux
#objectClass: krbticketpolicyaux
#objectClass: ipaobject
#objectClass: ipasshuser
#objectClass: x-ald-user
#objectClass: x-ald-user-parsec14
#objectClass: x-ald-audit-policy
#objectClass: ruPostMailAccount
#objectClass: rbtaCustomUserAttrs
#objectClass: rbtaUserMeta
#objectClass: rbta-unit
#objectClass: rbta-address
#objectClass: rbta-inetorgperson-ext
#objectClass: ipaSshGroupOfPubKeys
#objectClass: mepOriginEntry
#objectClass: ipantuserattrs
#rbtadp: ou=ald.lan,cn=orgunits,cn=accounts,dc=ald,dc=lan
#proxyAddresses: SMTP:fedya@ald.lan
#nsAccountLock: FALSE
#krbPrincipalName: fedya@ALD.LAN
#gecos: fedya fedya
#initials: ff
#displayName: fedya fedya
#cn: fedya fedya
#uid: fedya
#givenName: fedya
#krbPasswordExpiration: 20230801125933Z
#krbLastPwdChange: 20230801125933Z
#krbExtraData:
#mepManagedEntry: cn=fedya,cn=groups,cn=accounts,dc=ald,dc=lan
#memberOf: cn=ipausers,cn=groups,cn=accounts,dc=ald,dc=lan
#memberOf: cn=Organization units,cn=roles,cn=accounts,dc=ald,dc=lan
#memberOf: cn=Organization units,cn=privileges,cn=pbac,dc=ald,dc=lan
#memberOf: cn=Organization units - Read -
Relations,cn=permissions,cn=pbac,dc=ald,dc=lan
#memberOf: cn=Organization units - Read - OU,cn=permissions,cn=pbac,dc=ald,dc=lan
#ipaNTSecurityIdentifier: S-1-5-21-50723194-4244010569-790930296-1009
#rbtamiddlename: 1234
#nsUniqueId: 2ecec201-306b11ee-96e796b2-300f2d85
#dsEntryDN: uid=fedya,cn=users,cn=accounts,dc=ald,dc=lan
#entrydn: uid=fedya,cn=users,cn=accounts,dc=ald,dc=lan
result: 0
changetype: modify
delete: sn
sn: fedya1234
-
```

```
add: sn
sn: fedya
-
replace: internalModifiersName
internalModifiersName: cn=ldbm database,cn=plugins,cn=config
-
replace: modifiersname
modifiersname: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20230914124158Z
-
replace: entryusn
entryusn: 79170
-
```

3.8 Событие 4740 A user account was locked out

Блокировка пользователя в ALD Pro происходит в карточке пользователя на вкладке "Основное" путем клика на кнопку "Заблокировать УЗ".

В данном примере рассматривается результат записи в журналах доступа и аудита 389DS при выполнении блокировки УЗ пользователя через интерфейс ALD Pro.

В представленных логах access мы видим следующее: каждая строка начинается с даты, затем в каждой строке идет conn=1748008 – номер подключения, и далее для каждого нового подключения:

- connection from 10.166.1.177 to 10.166.1.177 – источник подключения, в нашем примере мы делали изменения локально на контроллере домена ALD Pro (через портал);
- TLS1.3 128-bit AES-GCM - протокол для устанавливаемого подключения и тип используемого шифрования;
- далее идут парные операции (op=0 ... op=N в рамках данного подключения): в первой записи парной операции идет указание на номер операции (например, op=0) и на тип операции (например, BIND), а во второй записи (которая может разделяться другими записями, то есть идти не подряд) идет указание на этот же номер операции (op=0) и на ответ (RESULT), в рамках которого будет указание на тип ошибки (err=) и на тип ответа (tag=), далее идут теги с количеством возвращаемых записей (nentries=0), время (в секундах) ожидания в очереди на выполнение запроса (wtime=), время (в секундах) выполнения операции клиента (optime=) и время в секундах между получением запроса сервером каталогов и отправкой результата обратно клиенту (etime=);
- в результате (RESULT) второй операции (op=2) написана УЗ, от имени которой было установлено соединение dn="uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"

```
[14/Aug/2024:19:07:22.136379679 +0300] conn=1748008 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000173241 optime=0.004159978 etime=0.004328601 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

- четвертая операция (op=4) - операция поиска (SRCH) с параметрами base="uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" scope=0 filter="(objectClass=*)" attrs="nsAccountLock". В результате (RESULT) выполнения четвертой операции (op=4) в рамках подключения 1748008 (conn=1748008) мы видим, что тип ошибки равен 0 (err=0), тип ответа

(tag=101) указывает на то, что это ответ на операцию поиска, количество возвращенных сервером записей =1 (nentries=1);

- для операции поиска "err=0" указывает, что были возвращены все соответствующие результаты поиска. Возможно, существовали совпадающие записи (или атрибуты в совпадающих записях), которые не были возвращены, потому что клиенту не был разрешен доступ к ним, или потому что они иным образом находились за пределами ограничений поиска;
- пятая операция (op=5) - операция изменения (MOD) УЗ пользователя с dn="uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan";
- в результате (RESULT) выполнения девятой операции (op=5) в рамках подключения 1748008 (conn=1748008) мы видим, что тип ошибки равен 0 (err=0), это указывает, что изменения запроса были применены к целевой записи, тип ответа (tag=103) указывает на то, что это ответ на операцию изменения, количество возвращенных сервером записей =0 (nentries=0).

Однако из представленного ниже фрагмента журнала access невозможно понять, какие именно изменения записи были выполнены. Для этого необходимо дополнительно анализировать журнал audit.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access (символ троеточия обозначает пропуск данных, не относящихся к текущему подключению или необходимой операции. Важно помнить, что на загруженном сервере могут быть 1000+ записей в секунду в журнале access, которые будут относиться к различным подключениям):

```
[14/Aug/2024:19:07:22.071725350 +0300] conn=1748008 fd=177 slot=177 SSL connection
from 10.166.1.177 to 10.166.1.177
[14/Aug/2024:19:07:22.084179953 +0300] conn=1748008 TLS1.3 128-bit AES-GCM
[14/Aug/2024:19:07:22.103133091 +0300] conn=1748008 op=0 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:07:22.121107904 +0300] conn=1748008 op=0 RESULT err=14 tag=97
 nentries=0 wtime=0.030546659 optime=0.017987655 etime=0.048530432, SASL bind in
progress
[14/Aug/2024:19:07:22.128716455 +0300] conn=1748008 op=1 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:07:22.131437831 +0300] conn=1748008 op=1 RESULT err=14 tag=97
 nentries=0 wtime=0.000187480 optime=0.002735432 etime=0.002918837, SASL bind in
progress
[14/Aug/2024:19:07:22.132228437 +0300] conn=1748008 op=2 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:07:22.136379679 +0300] conn=1748008 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000173241 optime=0.004159978 etime=0.004328601 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
...
[14/Aug/2024:19:08:45.571718001 +0300] conn=1748008 op=4 SRCH base="uid=test,cn=users
,cn=accounts,dc=ald,dc=company,dc=lan" scope=0 filter="(objectClass=*)" attrs="nsAcco
untLock"
[14/Aug/2024:19:08:45.572754586 +0300] conn=1748008 op=4 RESULT err=0 tag=101
 nentries=1 wtime=0.000293106 optime=0.001006501 etime=0.001295577
...
[14/Aug/2024:19:08:45.574330066 +0300] conn=1748008 op=5 MOD dn="uid=test,cn=users,cn
=accounts,dc=ald,dc=company,dc=lan"
[14/Aug/2024:19:08:45.599361787 +0300] conn=1748008 op=5 RESULT err=0 tag=103
 nentries=0 wtime=0.000268694 optime=0.025042345 etime=0.025302142
 csn=66bcd68d000000040000
```

В представленных логах audit мы видим следующее:

- пользователь с УЗ "uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" (строка "modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan") успешно (строка "result: 0") изменил (строка "changetype: modify") объект "dn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" (строка "dn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan") 19:08:45 14.08.2024 (строка "time: 20240814190845"), что с точностью до секунд совпадает с записью в журнале access, которая приведена выше;
- после строки "changetype: modify" приведены все изменения, которые были сделаны в записи объекта "dn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan". Было сделано 5 изменений:

1. Следующие 2 строки означают удаление атрибута "nsAccountLock" (атрибут блокировки записи), у которого было значение "FALSE":

```
delete: nsAccountLock
nsAccountLock: FALSE
```

2. Следующие 2 строки означают добавление атрибута "nsAccountLock" (атрибут блокировки записи) со значением "TRUE":

```
add: nsAccountLock
nsAccountLock: TRUE
```

3. Следующие 2 строки означают замену значения атрибута "modifiersname" (строка, содержащая dn УЗ, от имени которой произведено изменение в БД) значением "uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan":

```
replace: modifiersname
modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
```

4. Следующие 2 строки означают замену значения атрибута "modifytimestamp" (строка, определена в RFC 1274 - синтаксис GeneralizedTime, ГГГГММДДччммссZ - всемирное координированное время, - содержит дату и время самого последнего изменения текущей записи с точностью до секунд) значением "20240814160845Z":

```
replace: modifytimestamp
modifytimestamp: 20240814160845Z
```

5. Следующие 2 строки означают замену значения атрибута "entryusn" (порядковый номер обновления записи) значением "1047199":

```
replace: entryusn
entryusn: 1047199
```

- строки, начинающиеся на “#”, являются дополнительными атрибутами изменяемого объекта, которые нужно включать, по умолчанию их нет.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit:

```
time: 20240814190845
dn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
```

```
#loginShell: /bin/bash
#krbExtraData:
#krbLastPwdChange: 20240814160732Z
#krbPasswordExpiration: 20240814160732Z
#x-ald-user-mac: 0:0x0:0:0x0
#uid: test
#displayName: test testov
#initials: tt
#gecos: test testov
#sn: testov
#homeDirectory: /home/test
#mail: test@ald.company.lan
#krbPrincipalName: test@ALD.COMPANY.LAN
#krbCanonicalName: test@ald.company.lan
#givenName: test
#rbtamiddlename: testovich
#l: Москва
#rbtadp: ou=Тестовое,ou=Пользователи и
компьютеры,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan
#rbtaou: Тестовое
#entryusn: 1047199
#modifyTimestamp: 20240814160845Z
#modifiersName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#objectClass: top
#objectClass: person
#objectClass: organizationalperson
#objectClass: inetorgperson
#objectClass: inetuser
#objectClass: posixaccount
#objectClass: krbprincipalaux
#objectClass: krbticketpolicyaux
#objectClass: ipaobject
#objectClass: ipasshuser
#objectClass: x-ald-user
#objectClass: x-ald-user-parsec14
#objectClass: x-ald-audit-policy
#objectClass: rbta-unit
#objectClass: rbta-address
#objectClass: rbtaCustomUserAttrs
#objectClass: rbta-inetorgperson-ext
#objectClass: ruPostMailAccount
#objectClass: rbtaUserMeta
#objectClass: ipaSshGroupOfPubKeys
#objectClass: mepOriginEntry
#objectClass: ipantuserattrs
#ipaNTSecurityIdentifier: S-1-5-21-1041372395-3838146183-17441569-1375
#creatorsName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#cn: test testov
#createTimestamp: 20240814160733Z
#nsUniqueId: 346d2f01-5a5711ef-a67ccb9d-af0c8f85
#ipaUniqueId: 50fc6172-5a57-11ef-a8e1-02000aa601b1
#parentid: 3
#entryid: 5107
#uidNumber: 815000375
#gidNumber: 815000375
#entryUUID: 674f72bc-7bf6-4b39-89c3-42f0c9ece145
#dsEntryDN: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#entrydn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
result: 0
```

```
changetype: modify
delete: nsAccountLock
nsAccountLock: FALSE
-
add: nsAccountLock
nsAccountLock: TRUE
-
replace: modifiersname
modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20240814160845Z
-
replace: entryusn
entryusn: 1047199
-
```

3.9 Событие 4767 A user account was unlocked

Блокировка пользователя в ALD Pro происходит в карточке пользователя на вкладке "Основное" путем клика на кнопку "Заблокировать УЗ".

В данном примере рассматривается результат записи в журналах доступа и аудита 389DS при выполнении блокировки УЗ пользователя через интерфейс ALD Pro.

В представленных логах access мы видим следующее: каждая строка начинается с даты, затем в каждой строке идет conn=1748070 – номер подключения. Для каждого нового подключения:

- connection from 10.166.1.177 to 10.166.1.177 – источник подключения, в нашем примере мы делали изменения локально на контроллере домена ALD Pro (через портал);
- далее идут парные операции (op=0 ... op=N в рамках данного подключения): в первой записи парной операции идет указание на номер операции (например, op=0) и на тип операции (например, BIND), а во второй записи (которая может разделяться другими записями, то есть идти не подряд) идет указание на этот же номер операции (op=0) и на ответ (RESULT), в рамках которого будет указание на тип ошибки (err=) и на тип ответа (tag=), далее идут теги с количеством возвращаемых записей (nentries=0), время (в секундах) ожидания в очереди на выполнение запроса (wtime=), время (в секундах) выполнения операции клиента (optime=) и время в секундах между получением запроса сервером каталогов и отправкой результата обратно клиенту (etime=);
- в результате (RESULT) нулевой операции (op=0) написана УЗ, от имени которой было установлено соединение dn="uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"

```
[14/Aug/2024:19:08:59.679080403 +0300] conn=1748070 op=0 RESULT err=0 tag=97
 nentries=0 wtime=0.000423929 optime=0.015435394 etime=0.015856476 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

- третья операция (op=3) - операция поиска (SRCH) с параметрами base="uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" scope=0 filter="(objectClass=*)" attrs="nsAccountLock". В результате (RESULT) выполнения третьей операции (op=3) в рамках подключения 1748070 (conn=1748070) мы видим, что тип ошибки равен 0 (err=0), тип ответа (tag=101) указывает на то, что это ответ на операцию поиска, количество возвращенных сервером записей =1 (nentries=1);

- для операции поиска "err=0" указывает, что были возвращены все соответствующие результаты поиска. Возможно, существовали совпадающие записи (или атрибуты в совпадающих записях), которые не были возвращены, потому что клиенту не был разрешен доступ к ним, или потому что они иным образом находились за пределами ограничений поиска;
- четвертая операция (op=4) - операция изменения (MOD) УЗ пользователя с dn="uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan";
- в результате (RESULT) выполнения девятой операции (op=4) в рамках подключения 1748070 (conn=1748070) мы видим, что тип ошибки равен 0 (err=0). Это указывает, что изменения запроса были применены к целевой записи, тип ответа (tag=103) указывает на то, что это ответ на операцию изменения, количество возвращенных сервером записей =0 (nentries=0).

Однако, из представленного ниже фрагмента журнала access невозможно понять, какие именно изменения записи были выполнены. Для этого необходимо дополнительно анализировать журнал audit.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access (символ троеточия обозначает пропуск данных, не относящихся к текущему подключению или необходимой операции. Важно помнить, что на загруженном сервере могут быть 1000+ записей в секунду в журнале access, которые будут относиться к различным подключениям):

```
[14/Aug/2024:19:08:59.619609590 +0300] conn=1748070 fd=177 slot=177 connection from
10.166.1.177 to 10.166.1.177
...
[14/Aug/2024:19:08:59.663652659 +0300] conn=1748070 op=0 BIND dn="" method=sasl
version=3 mech=GSS-SPNEGO
[14/Aug/2024:19:08:59.679080403 +0300] conn=1748070 op=0 RESULT err=0 tag=97
 nentries=0 wtime=0.000423929 optime=0.015435394 etime=0.015856476 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
[14/Aug/2024:19:08:59.682536423 +0300] conn=1748070 op=1 SRCH base="cn=ipaconfig,cn=e
tc,dc=ald,dc=company,dc=lan" scope=0 filter="(objectClass=*)" attrs=ALL
[14/Aug/2024:19:08:59.683744086 +0300] conn=1748070 op=1 RESULT err=0 tag=101
 nentries=1 wtime=0.000206580 optime=0.001208819 etime=0.001411862
[14/Aug/2024:19:08:59.686298993 +0300] conn=1748070 op=2 SRCH base="uid=test,cn=users
,cn=accounts,dc=ald,dc=company,dc=lan" scope=0 filter="(objectClass=*)" attrs="distin
guishedName"
[14/Aug/2024:19:08:59.687502730 +0300] conn=1748070 op=2 RESULT err=0 tag=101
 nentries=1 wtime=0.000199056 optime=0.001206969 etime=0.001401374
[14/Aug/2024:19:08:59.688837479 +0300] conn=1748070 op=3 SRCH base="uid=test,cn=users
,cn=accounts,dc=ald,dc=company,dc=lan" scope=0 filter="(objectClass=*)" attrs="nsAcco
untLock"
[14/Aug/2024:19:08:59.690298414 +0300] conn=1748070 op=3 RESULT err=0 tag=101
 nentries=1 wtime=0.000216149 optime=0.001464339 etime=0.001678262
[14/Aug/2024:19:08:59.692629150 +0300] conn=1748070 op=4 MOD dn="uid=test,cn=users,cn
=accounts,dc=ald,dc=company,dc=lan"
[14/Aug/2024:19:08:59.714130971 +0300] conn=1748070 op=4 RESULT err=0 tag=103
 nentries=0 wtime=0.000234758 optime=0.021508293 etime=0.021736614
 csn=66bcd69b000000040000
```

В представленных логах audit мы видим следующее:

- пользователь с УЗ "uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" (строка "modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan") успешно (строка "result: 0") изменил (строка "changetype: modify") объект "dn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" (строка "dn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan") 19:08:59 14.08.2024 (строка "time:

20240814190859"), что с точностью до секунд совпадает с записью в журнале access, которая приведена выше;

- после строки "changetype: modify" приведены все изменения, которые были сделаны в записи объекта "dn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan". Было сделано 5 изменений:

1. Следующие 2 строки означают удаление атрибута "nsAccountLock" (атрибут блокировки записи), у которого было значение "TRUE":

```
delete: nsAccountLock
nsAccountLock: TRUE
```

2. Следующие 2 строки означают добавление атрибута "nsAccountLock" (атрибут блокировки записи) со значением "FALSE":

```
add: nsAccountLock
nsAccountLock: FALSE
```

3. Следующие 2 строки означают замену значения атрибута "modifiersname" (строка, содержащая dn УЗ, от имени которой произведено изменение в БД) значением "uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan":

```
replace: modifiersname
modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
```

4. Следующие 2 строки означают замену значения атрибута "modifytimestamp" (строка, определена в RFC 1274 - синтаксис GeneralizedTime, ГГГГММДДччммссZ - всемирное координированное время - содержит дату и время самого последнего изменения текущей записи с точностью до секунд) значением "20240814160859Z":

```
replace: modifytimestamp
modifytimestamp: 20240814160859Z
```

5. Следующие 2 строки означают замену значения атрибута "entryusn" (порядковый номер обновления записи) значением "1047203":

```
replace: entryusn
entryusn: 1047203
```

- строки, начинающиеся на “#”, являются дополнительными атрибутами изменяемого объекта, которые нужно включать. По умолчанию их нет.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit:

```
time: 20240814190859
dn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#loginShell: /bin/bash
#krbExtraData:
#krbLastPwdChange: 20240814160732Z
#krbPasswordExpiration: 20240814160732Z
#x-ald-user-mac: 0:0x0:0:0x0
#uid: test
```

```
#displayName: test testov
#initials: tt
#gecos: test testov
#sn: testov
#homeDirectory: /home/test
#mail: test@ald.company.lan
#krbPrincipalName: test@ALD.COMPANY.LAN
#krbCanonicalName: test@ald.company.lan
#givenName: test
#rbtamiddlename: testovich
#l: Москва
#rbtadp: ou=Тестовое,ou=Пользователи и
компьютеры,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan
#rbtaou: Тестовое
#entryusn: 1047203
#modifyTimestamp: 20240814160859Z
#modifiersName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#objectClass: top
#objectClass: person
#objectClass: organizationalperson
#objectClass: inetorgperson
#objectClass: inetuser
#objectClass: posixaccount
#objectClass: krbprincipalaux
#objectClass: krbticketpolicyaux
#objectClass: ipaobject
#objectClass: ipasshuser
#objectClass: x-ald-user
#objectClass: x-ald-user-parsec14
#objectClass: x-ald-audit-policy
#objectClass: rbta-unit
#objectClass: rbta-address
#objectClass: rbtaCustomUserAttrs
#objectClass: rbta-inetorgperson-ext
#objectClass: ruPostMailAccount
#objectClass: rbtaUserMeta
#objectClass: ipaSshGroupOfPubKeys
#objectClass: mepOriginEntry
#objectClass: ipantuserattrs
#ipaNTSecurityIdentifier: S-1-5-21-1041372395-3838146183-17441569-1375
#creatorsName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#cn: test testov
#createTimestamp: 20240814160733Z
#nsUniqueId: 346d2f01-5a5711ef-a67ccb9d-af0c8f85
#ipaUniqueId: 50fc6172-5a57-11ef-a8e1-02000aa601b1
#parentid: 3
#entryid: 5107
#uidNumber: 815000375
#gidNumber: 815000375
#entryUUID: 674f72bc-7bf6-4b39-89c3-42f0c9ece145
#dsEntryDN: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#entrydn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
result: 0
changetype: modify
delete: nsAccountLock
nsAccountLock: TRUE
-
add: nsAccountLock
nsAccountLock: FALSE
```

```
-
replace: modifiersname
modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20240814160859Z
-
replace: entryusn
entryusn: 1047203
-
```

3.10 Событие 4726 A user account was deleted

Полное удаление пользователя в ALD Pro происходит в 2 этапа:

1. Перенос пользователя в корзину (удаление учетной записи (УЗ) пользователя из ветки БД, хранящей записи о пользователях (cn=users,cn=accounts), также происходит удаление пользователя из всех групп пользователей, в которые он входит, затем создается запись о пользователе в ветке БД, отвечающей за корзину).
2. Удаление пользователя из корзины.

В данном примере рассматривается ТОЛЬКО событие удаления учетной записи пользователя из ветки БД, хранящей записи о пользователях.

В представленных логах access мы видим следующее: каждая строка начинается с даты, затем в каждой строке идет conn=1748081 – номер подключения, и далее для каждого нового подключения:

- connection from 10.166.1.177 to 10.166.1.177 – источник подключения, в нашем примере мы делали изменения локально на контроллере домена ALD Pro (через портал);
- TLS1.3 128-bit AES-GCM - протокол для устанавливаемого подключения и тип используемого шифрования;
- далее идут парные операции (op=0 ... op=N в рамках данного подключения): в первой записи парной операции идет указание на номер операции (например, op=0) и на тип операции (например, BIND), а во второй записи (которая может разделяться другими записями, то есть идти не подряд) идет указание на этот же номер операции (op=0) и на ответ (RESULT), в рамках которого будет указание на тип ошибки (err=) и на тип ответа (tag=), далее идут теги с количеством возвращаемых записей (nentries=0), время (в секундах) ожидания в очереди на выполнение запроса (wtime=), время (в секундах) выполнения операции клиента (optime=) и время в секундах между получением запроса сервером каталогов и отправкой результата обратно клиенту (etime=);
- в результате (RESULT) второй операции (op=2) написана УЗ, от имени которой было установлено соединение dn="uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan":

```
[14/Aug/2024:19:09:11.136379679 +0300] conn=1748081 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000173241 optime=0.004159978 etime=0.004328601 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

- девятая операция (op=9) - операция удаления (DEL) УЗ пользователя с dn="uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan";
- в результате (RESULT) выполнения девятой операции (op=9) в рамках подключения 1748081 (conn=1748081) мы видим, что тип ошибки равен 0 (err=0). Для операции удаления это

указывает, что целевая запись была удалена, затем тип ответа (tag=97) указывает на то, что это ответ на операцию удаления.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access (символ троеточия обозначает пропуск данных, не относящихся к текущему подключению или необходимой операции. Важно помнить, что на загруженном сервере могут быть 1000+ записей в секунду в журнале access, которые будут относиться к различным подключениям):

```
[14/Aug/2024:19:09:11.071725350 +0300] conn=1748081 fd=177 slot=177 SSL connection
from 10.166.1.177 to 10.166.1.177
[14/Aug/2024:19:09:11.084179953 +0300] conn=1748081 TLS1.3 128-bit AES-GCM
[14/Aug/2024:19:09:11.103133091 +0300] conn=1748081 op=0 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:09:11.121107904 +0300] conn=1748081 op=0 RESULT err=14 tag=97
 nentries=0 wtime=0.030546659 optime=0.017987655 etime=0.048530432, SASL bind in
progress
[14/Aug/2024:19:09:11.128716455 +0300] conn=1748081 op=1 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:09:11.131437831 +0300] conn=1748081 op=1 RESULT err=14 tag=97
 nentries=0 wtime=0.000187480 optime=0.002735432 etime=0.002918837, SASL bind in
progress
[14/Aug/2024:19:09:11.132228437 +0300] conn=1748081 op=2 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:09:11.136379679 +0300] conn=1748081 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000173241 optime=0.004159978 etime=0.004328601 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
...
[14/Aug/2024:19:09:40.861179236 +0300] conn=1748081 op=9 DEL dn="uid=test,cn=users,cn
=accounts,dc=ald,dc=company,dc=lan"
[14/Aug/2024:19:09:40.933662499 +0300] conn=1748081 op=9 RESULT err=0 tag=107
 nentries=0 wtime=0.000204590 optime=0.072495768 etime=0.072695760
 csn=66bcd6c4000000040000
```

В представленных логах audit мы видим следующее:

- пользователь с УЗ "uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" (строка "modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan") успешно (строка "result: 0") удалил (строка "changetype: delete") объект "dn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" (строка "dn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan") 19:09:40 14.08.2024 (строка "time: 20240814190940"), что с точностью до секунд совпадает с записью в журнале access, которая приведена выше;
- строки, начинающиеся на “#”, являются дополнительными атрибутами изменяемого объекта, которые нужно включать. По умолчанию их нет.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit:

```
time: 20240814190940
dn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#loginShell: /bin/bash
#krbExtraData:
#krbLastPwdChange: 20240814160732Z
#krbPasswordExpiration: 20240814160732Z
#x-ald-user-mac: 0:0x0:0:0x0
#uid: test
#displayName: test testov
```

```
#initials: tt
#gecos: test testov
#sn: testov
#homeDirectory: /home/test
#mail: test@ald.company.lan
#krbPrincipalName: test@ALD.COMPANY.LAN
#krbCanonicalName: test@ald.company.lan
#givenName: test
#rbtamiddlename: testovich
#l: Москва
#rbtadp: ou=Тестовое,ou=Пользователи и
компьютеры,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan
#rbtaou: Тестовое
#entryusn: 1047203
#modifyTimestamp: 20240814160859Z
#modifiersName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#objectClass: top
#objectClass: person
#objectClass: organizationalperson
#objectClass: inetorgperson
#objectClass: inetuser
#objectClass: posixaccount
#objectClass: krbprincipalaux
#objectClass: krbticketpolicyaux
#objectClass: ipaobject
#objectClass: ipasshuser
#objectClass: x-ald-user
#objectClass: x-ald-user-parsec14
#objectClass: x-ald-audit-policy
#objectClass: rbta-unit
#objectClass: rbta-address
#objectClass: rbtaCustomUserAttrs
#objectClass: rbta-inetorgperson-ext
#objectClass: ruPostMailAccount
#objectClass: rbtaUserMeta
#objectClass: ipaSshGroupOfPubKeys
#objectClass: mepOriginEntry
#objectClass: ipantuserattrs
#ipaNTSecurityIdentifier: S-1-5-21-1041372395-3838146183-17441569-1375
#creatorsName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#cn: test testov
#createTimestamp: 20240814160733Z
#nsUniqueId: 346d2f01-5a5711ef-a67ccb9d-af0c8f85
#ipaUniqueId: 50fc6172-5a57-11ef-a8e1-02000aa601b1
#parentid: 3
#entryid: 5107
#uidNumber: 815000375
#gidNumber: 815000375
#entryUUID: 674f72bc-7bf6-4b39-89c3-42f0c9ece145
#dsEntryDN: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#entrydn: uid=test,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
result: 0
changetype: delete
modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
```

3.11 Событие 4727 A security-enabled global group was created

В представленных логах access мы видим следующее: каждая строка начинается с даты, затем в каждой строке идет conn=1748150 – номер подключения, и далее для каждого нового подключения:

- connection from 10.166.1.177 to 10.166.1.177 – источник подключения, в нашем примере мы делали изменения локально на контроллере домена ALD Pro (через портал);
- TLS1.3 128-bit AES-GCM - протокол для устанавливаемого подключения и тип используемого шифрования;
- далее идут парные операции (op=0 ... op=N в рамках данного подключения): в первой записи парной операции идет указание на номер операции (например, op=0) и на тип операции (например, BIND), а во второй записи (которая может разделяться другими записями, то есть идти не подряд) идет указание на этот же номер операции (op=0) и на ответ (RESULT), в рамках которого будет указание на тип ошибки (err=) и на тип ответа (tag=), далее идут теги с количеством возвращаемых записей (nentries=0), время (в секундах) ожидания в очереди на выполнение запроса (wtime=), время (в секундах) выполнения операции клиента (optime=) и время в секундах между получением запроса сервером каталогов и отправкой результата обратно клиенту (etime=);
- в результате (RESULT) второй операции (op=2) написана УЗ, от имени которой было установлено соединение dn="uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"

```
[14/Aug/2024:19:15:13.157142060 +0300] conn=1748150 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000062971 optime=0.001866303 etime=0.001927801 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

- пятая операция (op=5) - операция добавления (ADD) УЗ группы пользователей с dn="cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan";
- в результате (RESULT) выполнения пятой операции (op=5) в рамках подключения 1748150 (conn=1748150) мы видим, что тип ошибки равен 0 (err=0), для операции добавления это указывает, что целевая запись была успешно создана, затем тип ответа (tag=105) указывает на то, что это ответ на операцию добавления.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access:

```
[14/Aug/2024:19:15:13.123876592 +0300] conn=1748150 fd=176 slot=176 SSL connection
from 10.166.1.177 to 10.166.1.177
[14/Aug/2024:19:15:13.133007480 +0300] conn=1748150 TLS1.3 128-bit AES-GCM
[14/Aug/2024:19:15:13.139564609 +0300] conn=1748150 op=0 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:15:13.146545333 +0300] conn=1748150 op=0 RESULT err=14 tag=97
 nentries=0 wtime=0.014668332 optime=0.006998207 etime=0.021663680, SASL bind in
progress
[14/Aug/2024:19:15:13.152143246 +0300] conn=1748150 op=1 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:15:13.153227759 +0300] conn=1748150 op=1 RESULT err=14 tag=97
 nentries=0 wtime=0.000124327 optime=0.001097072 etime=0.001220223, SASL bind in
progress
[14/Aug/2024:19:15:13.155278384 +0300] conn=1748150 op=2 BIND dn="" method=sasl
version=3 mech=GSSAPI
```

```
[14/Aug/2024:19:15:13.157142060 +0300] conn=1748150 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000062971 optime=0.001866303 etime=0.001927801 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
[14/Aug/2024:19:15:13.406338644 +0300] conn=1748150 op=3 SRCH base="uid=test_group,cn
=users,cn=accounts,dc=ald,dc=company,dc=lan" scope=2 filter="(objectClass=*)" attrs="
uid"
[14/Aug/2024:19:15:13.407796240 +0300] conn=1748150 op=3 RESULT err=32 tag=101
 nentries=0 wtime=0.000531121 optime=0.001464164 etime=0.001990001
[14/Aug/2024:19:15:13.409732540 +0300] conn=1748150 op=4 SRCH base="ou=ald.company.la
n,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan" scope=0 filter="(objectClass=*)"
 attrs="ou manager displayName description objectClass"
[14/Aug/2024:19:15:13.410931850 +0300] conn=1748150 op=4 RESULT err=0 tag=101
 nentries=1 wtime=0.000488832 optime=0.001212257 etime=0.001695934
[14/Aug/2024:19:15:13.413276832 +0300] conn=1748150 op=5 ADD dn="cn=test_group,cn=gro
ups,cn=accounts,dc=ald,dc=company,dc=lan"
[14/Aug/2024:19:15:13.469626524 +0300] conn=1748150 op=5 RESULT err=0 tag=105
 nentries=0 wtime=0.000602135 optime=0.056376250 etime=0.056972144
 csn=66bcd811000000040000
```

В представленных логах audit мы видим следующее:

- пользователь с УЗ "uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" (строка "creatorsName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan", которая появляется при операциях добавления и строка "modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan", которая появляется при всех записях модификации данных, в том числе и при добавлении) успешно (строка "result: 0") создал (строка "changetype: add") объект "dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan" (строка "dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan") 19:15:13 14.08.2024 (строка "time: 20240814191513"), что с точностью до секунд совпадает с записью в журнале access, которая приведена выше;
- по cn=groups,cn=accounts мы можем определить, что создана группа пользователей, которой присвоен "objectClass: ipausergroup", а также другие классы;
- строки, начинающиеся на “#”, являются дополнительными атрибутами изменяемого объекта, которые нужно включать. По умолчанию их нет.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit:

```
time: 20240814191513
dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
#rbtadp: ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan
#rbtaou: ald.company.lan
#entryusn: 1047238
#modifyTimestamp: 20240814161513Z
#modifiersName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#objectClass: groupofnames
#objectClass: ipaobject
#objectClass: ipausergroup
#objectClass: nestedgroup
#objectClass: posixgroup
#objectClass: rbta-unit
#objectClass: top
#objectClass: x-ald-audit-policy
#creatorsName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#cn: test_group
```

```
#createTimestamp: 20240814161513Z
#nsUniqueId: 51eec881-5a5811ef-a67ccb9d-af0c8f85
#ipaUniqueId: 62de672c-5a58-11ef-b47f-02000aa601b1
#parentid: 4
#entryid: 5110
#gidNumber: 815000376
#entryUUID: f323a072-7c9a-40f0-9752-b16fcaa38d21
#dsEntryDN: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
#entrydn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
result: 0
changetype: add
cn: test_group
description: Group for tests
rbtadp: ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan
rbtaou: ald.company.lan
gidNumber: -1
objectClass: groupofnames
objectClass: ipaobject
objectClass: ipausergroup
objectClass: nestedgroup
objectClass: posixgroup
objectClass: rbta-unit
objectClass: top
objectClass: x-ald-audit-policy
creatorsName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
modifiersName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
createTimestamp: 20240814161513Z
modifyTimestamp: 20240814161513Z
ipaUniqueID: 62de672c-5a58-11ef-b47f-02000aa601b1
```

3.12 Событие 4728 A member was added to a security-enabled global group

В представленных логах access мы видим следующее: каждая строка начинается с даты, затем в каждой строке идет conn=1748272 – номер подключения, и далее для каждого нового подключения:

- connection from 10.166.1.177 to 10.166.1.177 – источник подключения, в нашем примере мы делали изменения локально на контроллере домена ALD Pro (через портал);
- TLS1.3 128-bit AES-GCM - протокол для устанавливаемого подключения и тип используемого шифрования;
- далее идут парные операции (op=0 ... op=N в рамках данного подключения): в первой записи парной операции идет указание на номер операции (например, op=0) и на тип операции (например, BIND), а во второй записи (которая может разделяться другими записями, то есть идти не подряд) идет указание на этот же номер операции (op=0) и на ответ (RESULT), в рамках которого будет указание на тип ошибки (err=) и на тип ответа (tag=), далее идут теги с количеством возвращаемых записей (nentries=0), время (в секундах) ожидания в очереди на выполнение запроса (wtime=), время (в секундах) выполнения операции клиента (optime=) и время (в секундах) между получением запроса сервером каталогов и отправкой результата обратно клиенту (etime=);
- в результате (RESULT) второй операции (op=2) написана УЗ, от имени которой было установлено соединение dn="uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"

```
[14/Aug/2024:19:15:49.614713822 +0300] conn=1748272 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000147285 optime=0.005463644 etime=0.005606508 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

- третья операция (op=3) - операция изменения (MOD) УЗ группы пользователей с dn="cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan";
- в результате (RESULT) выполнения третьей операции (op=3) в рамках подключения 1748272 (conn=1748272) мы видим, что тип ошибки равен 0 (err=0), для операции изменения это указывает, что целевая запись была успешно изменена, затем тип ответа (tag=103) указывает на то, что это ответ на операцию изменения.

Однако, из представленного ниже фрагмента журнала access невозможно понять, какие именно изменения УЗ группы пользователей были выполнены. Для этого необходимо дополнительно анализировать журнал audit.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access (символ троеточия обозначает пропуск данных, не относящихся к текущему подключению или необходимой операции. Важно помнить, что на загруженном сервере могут быть 1000+ записей в секунду в журнале access, которые будут относиться к различным подключениям):

```
[14/Aug/2024:19:15:49.557839474 +0300] conn=1748272 fd=178 slot=178 SSL connection
from 10.166.1.177 to 10.166.1.177
[14/Aug/2024:19:15:49.571383036 +0300] conn=1748272 TLS1.3 128-bit AES-GCM
[14/Aug/2024:19:15:49.579855838 +0300] conn=1748272 op=0 BIND dn="" method=sasl
version=3 mech=GSSAPI
...
[14/Aug/2024:19:15:49.597992396 +0300] conn=1748272 op=0 RESULT err=14 tag=97
 nentries=0 wtime=0.020865562 optime=0.018150285 etime=0.039011307, SASL bind in
progress
...
[14/Aug/2024:19:15:49.605909268 +0300] conn=1748272 op=1 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:15:49.608538129 +0300] conn=1748272 op=1 RESULT err=14 tag=97
 nentries=0 wtime=0.000138629 optime=0.002637121 etime=0.002771652, SASL bind in
progress
[14/Aug/2024:19:15:49.609255793 +0300] conn=1748272 op=2 BIND dn="" method=sasl
version=3 mech=GSSAPI
...
[14/Aug/2024:19:15:49.614713822 +0300] conn=1748272 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000147285 optime=0.005463644 etime=0.005606508 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
...
[14/Aug/2024:19:15:49.615703104 +0300] conn=1748272 op=3 MOD dn="cn=test_group,cn=gro
ups,cn=accounts,dc=ald,dc=company,dc=lan"
...
[14/Aug/2024:19:15:49.677329214 +0300] conn=1748272 op=3 RESULT err=0 tag=103
 nentries=0 wtime=0.000286815 optime=0.061633789 etime=0.061916081
 csn=66bcd835000000040000
```

В представленных логах audit мы видим следующее:

- пользователь с УЗ "uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" (строка "modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan") успешно (строка "result: 0") изменил (строка "changetype: modify") объект "dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan" (строка "dn:

cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan") 19:15:49 14.08.2024 (строка "time: 20240814191549"), что с точностью до секунд совпадает с записью в журнале access, которая приведена выше;

- после строки "changetype: modify" приведены все изменения, которые были сделаны в записи объекта "dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan". Было сделано 4 изменения:

1. Следующие 2 строки означают добавление в группу пользователей (add: member) УЗ пользователя uid=test_user,cn=users,cn=accounts,dc=ald,dc=company,dc=lan (member: uid=test_user,cn=users,cn=accounts,dc=ald,dc=company,dc=lan):

```
add: member
member: uid=test_user,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
```

2. Следующие 2 строки означают замену значения атрибута "modifiersname" (строка, содержащая dn УЗ, от имени которой произведено изменение в БД) значением "uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan":

```
replace: modifiersname
modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
```

3. Следующие 2 строки означают замену значения атрибута "modifytimestamp" (строка, определена в RFC 1274 - синтаксис GeneralizedTime, ГГГГММДДччммссZ - всемирное координированное время - содержит дату и время самого последнего изменения текущей записи с точностью до секунд) значением "20240814161549Z":

```
replace: modifytimestamp
modifytimestamp: 20240814161549Z
```

4. Следующие 2 строки означают замену значения атрибута "entryusn" (порядковый номер обновления записи) значением "1047243":

```
replace: entryusn
entryusn: 1047243
```

- строки, начинающиеся на “#”, являются дополнительными атрибутами изменяемого объекта, которые нужно включать, по умолчанию их нет.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit:

```
time: 20240814191549
dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
#rbtadp: ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan
#rbtaou: ald.company.lan
#entryusn: 1047243
#modifyTimestamp: 20240814161549Z
#modifiersName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#objectClass: groupofnames
#objectClass: ipaobject
#objectClass: ipausergroup
#objectClass: nestedgroup
#objectClass: posixgroup
#objectClass: rbta-unit
```

```
#objectClass: top
#objectClass: x-ald-audit-policy
#objectClass: ipantgroupattrs
#ipaNTSecurityIdentifier: S-1-5-21-1041372395-3838146183-17441569-1376#creatorsName:
uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#cn: test_group
#createTimestamp: 20240814161513Z
#nsUniqueId: 51eec881-5a5811ef-a67ccb9d-af0c8f85
#ipaUniqueId: 62de672c-5a58-11ef-b47f-02000aa601b1
#parentid: 4
#entryid: 5110
#gidNumber: 815000376
#entryUUID: f323a072-7c9a-40f0-9752-b16fcaa38d21
#dsEntryDN: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
#entrydn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
result: 0
changetype: modify
add: member
member: uid=test_user,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
-
replace: modifiersname
modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20240814161549Z
-
replace: entryusn
entryusn: 1047243
-
```

3.13 Событие 4729 A member was removed from a security-enabled global group

В представленных логах access мы видим следующее: каждая строка начинается с даты, затем в каждой строке идет conn=1748394 – номер подключения, и далее для каждого нового подключения:

- connection from 10.166.1.177 to 10.166.1.177 – источник подключения, в нашем примере мы делали изменения локально на контроллере домена ALD Pro (через портал);
- TLS1.3 128-bit AES-GCM - протокол для устанавливаемого подключения и тип используемого шифрования;
- далее идут парные операции (op=0 ... op=N в рамках данного подключения): в первой записи парной операции идет указание на номер операции (например, op=0) и на тип операции (например, BIND), а во второй записи (которая может разделяться другими записями, то есть идти не подряд) идет указание на этот же номер операции (op=0) и на ответ (RESULT), в рамках которого будет указание на тип ошибки (err=) и на тип ответа (tag=), далее идут теги с количеством возвращаемых записей (nentries=0), время (в секундах) ожидания в очереди на выполнение запроса (wtime=), время (в секундах) выполнения операции клиента (optime=) и время (в секундах) между получением запроса сервером каталогов и отправкой результата обратно клиенту (etime=);
- в результате (RESULT) второй операции (op=2) написана УЗ, от имени которой было установлено соединение dn="uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan":

```
[14/Aug/2024:19:16:11.836416624 +0300] conn=1748394 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000062824 optime=0.001450992 etime=0.001512302 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

- третья операция (op=3) - операция изменения (MOD) УЗ группы пользователей с dn="cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan";
- в результате (RESULT) выполнения третьей операции (op=3) в рамках подключения 1748394 (conn=1748394) мы видим, что тип ошибки равен 0 (err=0), для операции изменения это указывает, что целевая запись была успешно изменена, затем тип ответа (tag=103) указывает на то, что это ответ на операцию изменения.

Однако из представленного ниже фрагмента журнала access невозможно понять, какие именно изменения УЗ группы пользователей были выполнены. Для этого необходимо дополнительно анализировать журнал audit.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access (символ троеточия обозначает пропуск данных, не относящихся к текущему подключению или необходимой операции. Важно помнить, что на загруженном сервере могут быть 1000+ записей в секунду в журнале access, которые будут относиться к различным подключениям):

```
[14/Aug/2024:19:16:11.790034125 +0300] conn=1748394 fd=172 slot=172 SSL connection
from 10.166.1.177 to 10.166.1.177
...
[14/Aug/2024:19:16:11.801174328 +0300] conn=1748394 TLS1.3 128-bit AES-GCM
[14/Aug/2024:19:16:11.808680296 +0300] conn=1748394 op=0 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:16:11.825763873 +0300] conn=1748394 op=0 RESULT err=14 tag=97
 nentries=0 wtime=0.017994924 optime=0.017092700 etime=0.035083770, SASL bind in
progress
[14/Aug/2024:19:16:11.832229033 +0300] conn=1748394 op=1 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:16:11.834512612 +0300] conn=1748394 op=1 RESULT err=14 tag=97
 nentries=0 wtime=0.000206872 optime=0.002292895 etime=0.002496257, SASL bind in
progress
[14/Aug/2024:19:16:11.834968200 +0300] conn=1748394 op=2 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:16:11.836416624 +0300] conn=1748394 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000062824 optime=0.001450992 etime=0.001512302 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
...
[14/Aug/2024:19:16:11.862835068 +0300] conn=1748394 op=3 MOD dn="cn=test_group,cn=gro
ups,cn=accounts,dc=ald,dc=company,dc=lan"
...
[14/Aug/2024:19:16:11.931222870 +0300] conn=1748394 op=3 RESULT err=0 tag=103
 nentries=0 wtime=0.000270055 optime=0.068389269 etime=0.068653085
 csn=66bcd84b000000040000
```

В представленных логах audit мы видим следующее:

- пользователь с УЗ "uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" (строка "modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan") успешно (строка "result: 0") изменил (строка "changetype: modify") объект "dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan" (строка "dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan") 19:16:11 14.08.2024 (строка

"time: 20240814191611"), что с точностью до секунд совпадает с записью в журнале access, которая приведена выше;

- после строки "changetype: modify" приведены все изменения, которые были сделаны в записи объекта "dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan". Было сделано 4 изменения:

  1. Следующие 2 строки означают удаление из группы пользователей (delete: member) УЗ пользователя uid=test_user,cn=users,cn=accounts,dc=ald,dc=company,dc=lan (member: uid=test_user,cn=users,cn=accounts,dc=ald,dc=company,dc=lan):

```
delete: member

member: uid=test_user,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
```

  2. Следующие 2 строки означают замену значения атрибута "modifiersname" (строка, содержащая dn УЗ, от имени которой произведено изменение в БД) значением "uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan":

```
replace: modifiersname
modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
```

  3. Следующие 2 строки означают замену значения атрибута "modifytimestamp" (строка, определена в RFC 1274 - синтаксис GeneralizedTime, ГГГГММДДччммссZ - всемирное координированное время - содержит дату и время самого последнего изменения текущей записи с точностью до секунд) значением "20240814161611Z":

```
replace: modifytimestamp
modifytimestamp: 20240814161611Z
```

  4. Следующие 2 строки означают замену значения атрибута "entryusn" (порядковый номер обновления записи) значением "1047248":

```
replace: entryusn
entryusn: 1047248
```

- строки, начинающиеся на “#”, являются дополнительными атрибутами изменяемого объекта, которые нужно включать, по умолчанию их нет.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit:

```
time: 20240814191611
dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
#rbtadp: ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan
#rbtaou: ald.company.lan
#entryusn: 1047248
#modifyTimestamp: 20240814161611Z
#modifiersName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#objectClass: groupofnames
#objectClass: ipaobject
#objectClass: ipausergroup
#objectClass: nestedgroup
#objectClass: posixgroup
#objectClass: rbta-unit
```

```
#objectClass: top
#objectClass: x-ald-audit-policy
#objectClass: ipantgroupattrs
#ipaNTSecurityIdentifier: S-1-5-21-1041372395-3838146183-17441569-1376
#creatorsName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#cn: test_group
#createTimestamp: 20240814161513Z
#nsUniqueId: 51eec881-5a5811ef-a67ccb9d-af0c8f85
#ipaUniqueId: 62de672c-5a58-11ef-b47f-02000aa601b1
#parentid: 4
#entryid: 5110
#gidNumber: 815000376
#entryUUID: f323a072-7c9a-40f0-9752-b16fcaa38d21
#dsEntryDN: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
#entrydn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
result: 0
changetype: modify
delete: member
member: uid=test_user,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
-
replace: modifiersname
modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20240814161611Z
-
replace: entryusn
entryusn: 1047248
-
```

3.14 Событие 4730 A security-enabled global group was deleted

В представленных логах access мы видим следующее: каждая строка начинается с даты, затем в каждой строке идет conn=1748507 – номер подключения, и далее для каждого нового подключения:

- connection from 10.166.1.177 to 10.166.1.177 – источник подключения, в нашем примере мы делали изменения локально на контроллере домена ALD Pro (через портал);
- TLS1.3 128-bit AES-GCM - протокол для устанавливаемого подключения и тип используемого шифрования;
- Далее идут парные операции (op=0 ... op=N в рамках данного подключения), в первой записи парной операции идет указание на номер операции (например, op=0) и на тип операции (например, BIND), а во второй записи (которая может разделяться другими записями, то есть идти не подряд) идет указание на этот же номер операции (op=0) и на ответ (RESULT), в рамках которого будет указание на тип ошибки (err=) и на тип ответа (tag=), далее идут теги с количеством возвращаемых записей (nentries=0), время (в секундах) ожидания в очереди на выполнение запроса (wtime=), время (в секундах) выполнения операции клиента (optime=) и время (в секундах) между получением запроса сервером каталогов и отправкой результата обратно клиенту (etime=);
- в результате (RESULT) второй операции (op=2) написана УЗ, от имени которой было установлено соединение dn="uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan":

```
[14/Aug/2024:19:16:30.855634101 +0300] conn=1748507 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000181151 optime=0.004042657 etime=0.004219986 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

- четвертая операция (op=4) - операция поиска (SRCH) с параметрами base="cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan" scope=2 filter="(objectClass=*)" attrs=ALL". В данном случае в БД ищется объект для последующего удаления (см. описание пятой операции ниже). В результате (RESULT) выполнения четвертой операции (op=4) в рамках подключения 1748507 (conn=1748507) мы видим, что тип ошибки равен 0 (err=0), тип ответа (tag=101) указывает не то, что это ответ на операцию поиска, количество возвращенных сервером записей =1 (nentries=1);
- для операции поиска "err=0" указывает, что были возвращены все соответствующие результаты поиска. Возможно, существовали совпадающие записи (или атрибуты в совпадающих записях), которые не были возвращены, потому что клиенту не был разрешен доступ к ним, или потому что они иным образом находились за пределами ограничений поиска;
- пятая операция (op=5) - операция удаления (DEL) УЗ группы пользователей с dn="cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan";
- в результате (RESULT) выполнения пятой операции (op=5) в рамках подключения 1748507 (conn=1748507) мы видим, что тип ошибки равен 0 (err=0). Для операции удаления это указывает, что целевая запись была успешно удалена, затем тип ответа (tag=107) указывает не то, что это ответ на операцию удаления.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access:

```
[14/Aug/2024:19:16:30.800533744 +0300] conn=1748507 fd=172 slot=172 SSL connection
from 10.166.1.177 to 10.166.1.177
...
[14/Aug/2024:19:16:30.811054608 +0300] conn=1748507 TLS1.3 128-bit AES-GCM
...
[14/Aug/2024:19:16:30.820562169 +0300] conn=1748507 op=0 BIND dn="" method=sasl
version=3 mech=GSSAPI
...
[14/Aug/2024:19:16:30.838157479 +0300] conn=1748507 op=0 RESULT err=14 tag=97
 nentries=0 wtime=0.019545562 optime=0.017606611 etime=0.037149914, SASL bind in
progress
[14/Aug/2024:19:16:30.846925916 +0300] conn=1748507 op=1 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:16:30.849481680 +0300] conn=1748507 op=1 RESULT err=14 tag=97
 nentries=0 wtime=0.000224176 optime=0.002571416 etime=0.002792053, SASL bind in
progress
[14/Aug/2024:19:16:30.851601249 +0300] conn=1748507 op=2 BIND dn="" method=sasl
version=3 mech=GSSAPI
[14/Aug/2024:19:16:30.855634101 +0300] conn=1748507 op=2 RESULT err=0 tag=97
 nentries=0 wtime=0.000181151 optime=0.004042657 etime=0.004219986 dn="uid=ga_astra_a
dmin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
[14/Aug/2024:19:16:30.856626562 +0300] conn=1748507 op=3 EXT oid="1.3.6.1.4.1.4203.1.
11.3" name="whoami-plugin"
[14/Aug/2024:19:16:30.856906512 +0300] conn=1748507 op=3 RESULT err=0 tag=120
 nentries=0 wtime=0.000281743 optime=0.000289138 etime=0.000566129
[14/Aug/2024:19:16:30.857537738 +0300] conn=1748507 op=4 SRCH base="cn=test_group,cn=
groups,cn=accounts,dc=ald,dc=company,dc=lan" scope=2 filter="(objectClass=*)"
 attrs=ALL
```

```
[14/Aug/2024:19:16:30.871868744 +0300] conn=1748507 op=4 RESULT err=0 tag=101
 nentries=1 wtime=0.000244088 optime=0.014333163 etime=0.014573476 notes=U details="P
artially Unindexed Filter" - entryLevelRights: vadn
[14/Aug/2024:19:16:30.872858706 +0300] conn=1748507 op=5 DEL dn="cn=test_group,cn=gro
ups,cn=accounts,dc=ald,dc=company,dc=lan"
...
[14/Aug/2024:19:16:30.891692564 +0300] conn=1748507 op=5 RESULT err=0 tag=107
 nentries=0 wtime=0.000308450 optime=0.018843446 etime=0.019146505
 csn=66bcd85e000000040000
```

В представленных логах audit мы видим следующее:

- пользователь с УЗ "uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" (строка "modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan") успешно (строка "result: 0") удалил (строка "changetype: delete") объект "dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan" (строка "dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan") 19:16:30 14.08.2024 (строка "time: 20240814191630"), что с точностью до секунд совпадает с записью в журнале access, которая приведена выше;
- по cn=groups,cn=accounts мы можем определить, что удалена группа пользователей, которой был присвоен "objectClass: ipausergroup", а также другие классы;
- строки, начинающиеся на “#”, являются дополнительными атрибутами изменяемого объекта, которые нужно включать, по умолчанию их нет.

Фрагмент журнала /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit:

```
time: 20240814191630
dn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
#rbtadp: ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan
#rbtaou: ald.company.lan
#entryusn: 1047248
#modifyTimestamp: 20240814161611Z
#modifiersName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#objectClass: groupofnames
#objectClass: ipaobject
#objectClass: ipausergroup
#objectClass: nestedgroup
#objectClass: posixgroup
#objectClass: rbta-unit
#objectClass: top
#objectClass: x-ald-audit-policy
#objectClass: ipantgroupattrs
#ipaNTSecurityIdentifier: S-1-5-21-1041372395-3838146183-17441569-1376
#creatorsName: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
#cn: test_group
#createTimestamp: 20240814161513Z
#nsUniqueId: 51eec881-5a5811ef-a67ccb9d-af0c8f85
#ipaUniqueId: 62de672c-5a58-11ef-b47f-02000aa601b1
#parentid: 4
#entryid: 5110
#gidNumber: 815000376
#entryUUID: f323a072-7c9a-40f0-9752-b16fcaa38d21
#dsEntryDN: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
#entrydn: cn=test_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
result: 0
```

```
changetype: delete
modifiersname: uid=ga_astra_admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
```

3.15 Событие 4741 A computer account was created

В данном примере мы вводим в домен новый сервер alddc3.ald.lan.

В логах access нам будет интересна следующая строка:

```
[13/Sep/2023:14:20:55.320129565 +0300] conn=752 op=8 ADD dn="fqdn=alddc3.ald.lan,cn=c
omputers,cn=accounts,dc=ald,dc=lan"
```

Полный лог из /var/log/dirsrv/slapd-ALD-LAN/access:

```
[13/Sep/2023:14:20:55.222547920 +0300] conn=752 fd=151 slot=151 connection from
192.168.100.120 to 192.168.100.120
[13/Sep/2023:14:20:55.226180040 +0300] conn=752 op=0 BIND dn="" method=sasl version=3
 mech=GSS-SPNEGO
[13/Sep/2023:14:20:55.227013192 +0300] conn=752 (Internal) op=0(1)(1) SRCH base="dc=a
ld,dc=lan" scope=2 filter="(krbPrincipalName=admin@ALD.LAN)" attrs=ALL
[13/Sep/2023:14:20:55.227098606 +0300] conn=752 (Internal) op=0(1)(1) ENTRY dn="uid=a
dmin,cn=users,cn=accounts,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.227104424 +0300] conn=752 (Internal) op=0(1)(1)STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.227105899 +0300] conn=752 (Internal) op=0(1)(1)STAT read index:
attribute=krbPrincipalName key(eq)=admin@ALD.LAN --> count 1
[13/Sep/2023:14:20:55.227107074 +0300] conn=752 (Internal) op=0(1)(1)STAT read index:
duration 0.000002359
[13/Sep/2023:14:20:55.227108209 +0300] conn=752 (Internal) op=0(1)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000008377 optime=0.000091539 etime=0.000099294
[13/Sep/2023:14:20:55.227273579 +0300] conn=752 (Internal) op=0(2)(1) SRCH base="uid=
admin,cn=users,cn=accounts,dc=ald,dc=lan" scope=0 filter="(|(objectclass=*)
(objectclass=ldapsubentry))" attrs="nsLookThroughLimit nsIDListScanLimit
nsPagedLookThroughLimit nsPagedIDListScanLimit nsRangeSearchLookThroughLimit
nsSizeLimit nsTimeLimit nsPagedSizeLimit nsIdleTimeout"
[13/Sep/2023:14:20:55.227319601 +0300] conn=752 (Internal) op=0(2)(1) ENTRY dn="uid=a
dmin,cn=users,cn=accounts,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.227323579 +0300] conn=752 (Internal) op=0(2)(1)STAT read index:
duration 0.000000000
[13/Sep/2023:14:20:55.227324774 +0300] conn=752 (Internal) op=0(2)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000004444 optime=0.000050417 etime=0.000054462
[13/Sep/2023:14:20:55.227522469 +0300] conn=752 (Internal) op=0(5)(1) SRCH base="uid=
admin,cn=users,cn=accounts,dc=ald,dc=lan" scope=0 filter="(|(objectclass=*)
(objectclass=ldapsubentry))" attrs=ALL
[13/Sep/2023:14:20:55.227560267 +0300] conn=752 (Internal) op=0(5)(1) ENTRY dn="uid=a
dmin,cn=users,cn=accounts,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.227563754 +0300] conn=752 (Internal) op=0(5)(1)STAT read index:
duration 0.000000000
[13/Sep/2023:14:20:55.227564869 +0300] conn=752 (Internal) op=0(5)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000002564 optime=0.000041237 etime=0.000043405
[13/Sep/2023:14:20:55.227649759 +0300] conn=752 op=0 RESULT err=0 tag=97 nentries=0
 wtime=0.000105128 optime=0.001471426 etime=0.001575793 dn="uid=admin,cn=users,cn=acc
ounts,dc=ald,dc=lan"
```

```
[13/Sep/2023:14:20:55.233015654 +0300] conn=752 op=1 SRCH base="cn=ipaconfig,cn=etc,d
c=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs=ALL
[13/Sep/2023:14:20:55.233320970 +0300] conn=752 op=1 ENTRY dn="cn=ipaConfig,cn=etc,dc
=ald,dc=lan"
[13/Sep/2023:14:20:55.233347997 +0300] conn=752 op=1 STAT read index: duration
0.000000000
[13/Sep/2023:14:20:55.233350660 +0300] conn=752 op=1 RESULT err=0 tag=101 nentries=1
 wtime=0.000072154 optime=0.000333358 etime=0.000404475
[13/Sep/2023:14:20:55.233615565 +0300] conn=752 op=2 SRCH base="cn=schema" scope=0
 filter="(objectClass=*)" attrs="attributeTypes objectClasses"
[13/Sep/2023:14:20:55.276950292 +0300] conn=752 op=2 ENTRY dn="cn=schema"
[13/Sep/2023:14:20:55.277100409 +0300] conn=752 op=2 STAT read index: duration
0.000000000
[13/Sep/2023:14:20:55.277103749 +0300] conn=752 op=2 RESULT err=0 tag=101 nentries=1
 wtime=0.000048648 optime=0.043483780 etime=0.043530386
[13/Sep/2023:14:20:55.315274932 +0300] conn=752 op=3 SRCH base="fqdn=alddc3.ald.lan,c
n=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs=""
[13/Sep/2023:14:20:55.315530024 +0300] conn=752 op=3 STAT read index: duration
0.000000000
[13/Sep/2023:14:20:55.315534373 +0300] conn=752 op=3 RESULT err=32 tag=101 nentries=0
 wtime=0.000143401 optime=0.000255861 etime=0.000397774
[13/Sep/2023:14:20:55.315861611 +0300] conn=752 op=4 SRCH base="cn=computers,cn=accou
nts,dc=ald,dc=lan" scope=2 filter="(&(serverHostName=alddc3.ald.lan)
(&(objectClass=ipaobject)(objectClass=nshost)(objectClass=ipahost)
(objectClass=pkiuser)(objectClass=ipaservice)(objectClass=rbta-address)
(objectClass=rbta-unit)))" attrs=""
[13/Sep/2023:14:20:55.316386248 +0300] conn=752 op=4 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.316390405 +0300] conn=752 op=4 STAT read index:
attribute=serverHostName key(eq)=alddc3.ald.lan --> count 0
[13/Sep/2023:14:20:55.316392065 +0300] conn=752 op=4 STAT read index: duration
0.000005737
[13/Sep/2023:14:20:55.316393920 +0300] conn=752 op=4 RESULT err=0 tag=101 nentries=0
 wtime=0.000073044 optime=0.000524347 etime=0.000595553
[13/Sep/2023:14:20:55.316734389 +0300] conn=752 op=5 SRCH base="fqdn=alddc3.ald.lan,c
n=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="fqdn
userCertificate rbtadp nsHardwarePlatform krbPrincipalName krbPrincipalAuthInd
ipaAllowedToPerform macAddress krbCanonicalName nsOsVersion * memberofindirect
description memberOf userClass managedBy l ipaAssignedIDView nsHostLocation aci"
[13/Sep/2023:14:20:55.316866566 +0300] conn=752 op=5 STAT read index: duration
0.000000000
[13/Sep/2023:14:20:55.316870122 +0300] conn=752 op=5 RESULT err=32 tag=101 nentries=0
 wtime=0.000077169 optime=0.000132471 etime=0.000208572
[13/Sep/2023:14:20:55.318039265 +0300] conn=752 op=6 SRCH base="fqdn=alddc3.ald.lan,c
n=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs=""
[13/Sep/2023:14:20:55.318168752 +0300] conn=752 op=6 STAT read index: duration
0.000000000
[13/Sep/2023:14:20:55.318172109 +0300] conn=752 op=6 RESULT err=32 tag=101 nentries=0
 wtime=0.000052347 optime=0.000129040 etime=0.000180385
[13/Sep/2023:14:20:55.318445434 +0300] conn=752 op=7 SRCH base="cn=computers,cn=accou
nts,dc=ald,dc=lan" scope=2 filter="(&(serverHostName=alddc3.ald.lan)
(&(objectClass=ipaobject)(objectClass=nshost)(objectClass=ipahost)
(objectClass=pkiuser)(objectClass=ipaservice)(objectClass=rbta-address)
(objectClass=rbta-unit)))" attrs=""
[13/Sep/2023:14:20:55.318524512 +0300] conn=752 op=7 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.318527384 +0300] conn=752 op=7 STAT read index:
attribute=serverHostName key(eq)=alddc3.ald.lan --> count 0
```

```
[13/Sep/2023:14:20:55.318528744 +0300] conn=752 op=7 STAT read index: duration
0.000003319
[13/Sep/2023:14:20:55.318530347 +0300] conn=752 op=7 RESULT err=0 tag=101 nentries=0
 wtime=0.000060060 optime=0.000078759 etime=0.000137685
[13/Sep/2023:14:20:55.320129565 +0300] conn=752 op=8 ADD dn="fqdn=alddc3.ald.lan,cn=c
omputers,cn=accounts,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.332339646 +0300] conn=752 op=8 RESULT err=0 tag=105 nentries=0
 wtime=0.000098345 optime=0.012211737 etime=0.012308528 csn=65019b27000000040000
[13/Sep/2023:14:20:55.332749019 +0300] conn=752 op=9 SRCH base="fqdn=alddc3.ald.lan,c
n=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="fqdn
userCertificate objectClass rbtadp nsHardwarePlatform krbPrincipalName
krbPrincipalAuthInd ipaAllowedToPerform macAddress krbCanonicalName nsOsVersion
memberofindirect description memberOf userClass managedBy ipaUniqueID l
ipaAssignedIDView nsHostLocation"
[13/Sep/2023:14:20:55.332993028 +0300] conn=752 op=9 ENTRY dn="fqdn=alddc3.ald.lan,cn
=computers,cn=accounts,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.333013236 +0300] conn=752 op=9 STAT read index: duration
0.000000000
[13/Sep/2023:14:20:55.333015028 +0300] conn=752 op=9 RESULT err=0 tag=101 nentries=1
 wtime=0.000124798 optime=0.000265120 etime=0.000388948
[13/Sep/2023:14:20:55.333524283 +0300] conn=752 op=10 SRCH base="dc=ald,dc=lan"
 scope=2 filter="(|
(member=fqdn=alddc3.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan)
(memberUser=fqdn=alddc3.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan)
(memberHost=fqdn=alddc3.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan))" attrs=""
[13/Sep/2023:14:20:55.333738896 +0300] conn=752 op=10 RESULT err=0 tag=101 nentries=0
 wtime=0.000182716 optime=0.000215595 etime=0.000397298 notes=P details="Paged
Search" pr_idx=0 pr_cookie=-1
[13/Sep/2023:14:20:55.333954803 +0300] conn=752 op=11 SRCH base="cn=dns,dc=ald,dc=lan
" scope=0 filter="(objectClass=*)" attrs=ALL
[13/Sep/2023:14:20:55.334144778 +0300] conn=752 op=11 ENTRY dn="cn=dns,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.334169773 +0300] conn=752 op=11 STAT read index: duration
0.000000000
[13/Sep/2023:14:20:55.334171601 +0300] conn=752 op=11 RESULT err=0 tag=101 nentries=1
 wtime=0.000039631 optime=0.000214667 etime=0.000253456
[13/Sep/2023:14:20:55.334568930 +0300] conn=752 op=12 SRCH base="fqdn=alddc3.ald.lan,
cn=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(userPassword=*)" attrs="user
Password"
[13/Sep/2023:14:20:55.334765370 +0300] conn=752 op=12 STAT read index: duration
0.000000000
[13/Sep/2023:14:20:55.334768285 +0300] conn=752 op=12 RESULT err=0 tag=101 nentries=0
 wtime=0.000063401 optime=0.000196585 etime=0.000259016
[13/Sep/2023:14:20:55.335022847 +0300] conn=752 op=13 SRCH base="fqdn=alddc3.ald.lan,
cn=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(krbPrincipalKey=*)" attrs="k
rbPrincipalKey"
[13/Sep/2023:14:20:55.335128141 +0300] conn=752 op=13 STAT read index: duration
0.000000000
[13/Sep/2023:14:20:55.335131495 +0300] conn=752 op=13 RESULT err=0 tag=101 nentries=0
 wtime=0.000050669 optime=0.000105038 etime=0.000154674
[13/Sep/2023:14:20:55.336081090 +0300] conn=752 op=14 SRCH base="cn=ipaconfig,cn=etc,
dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="ipaSearchRecordsLimit
ipaSearchTimeLimit ipaDomainResolutionOrder ipaSELinuxUserMapOrder
ipaDefaultEmailDomain ipaUserSearchFields ipaMaxHostnameLength ipaHomesRootDir
ipaMaxUsernameLength ipaConfigString ipaDefaultPrimaryGroup ipaSELinuxUserMapDefault
ipaMigrationEnabled ipaUserAuthType ipaGroupSearchFields ipaCertificateSubjectBase
ipaPwdExpAdvNotify ipaDefaultLoginShell ipaKrbAuthzData"
[13/Sep/2023:14:20:55.336346473 +0300] conn=752 op=14 ENTRY dn="cn=ipaConfig,cn=etc,d
c=ald,dc=lan"
```

```
[13/Sep/2023:14:20:55.336365403 +0300] conn=752 op=14 STAT read index: duration
0.000000000
[13/Sep/2023:14:20:55.336367038 +0300] conn=752 op=14 RESULT err=0 tag=101 nentries=1
 wtime=0.000065116 optime=0.000285364 etime=0.000349730
[13/Sep/2023:14:20:55.336928832 +0300] conn=752 op=15 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=2 filter="(cn=CA)" attrs="ipaConfigString cn"
[13/Sep/2023:14:20:55.337768302 +0300] conn=752 op=15 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.337774212 +0300] conn=752 op=15 STAT read index: attribute=cn
key(eq)=ca --> count 1
[13/Sep/2023:14:20:55.337780265 +0300] conn=752 op=15 STAT read index: duration
0.000027300
[13/Sep/2023:14:20:55.337782698 +0300] conn=752 op=15 RESULT err=0 tag=101 nentries=0
 wtime=0.000050993 optime=0.000838560 etime=0.000887994
[13/Sep/2023:14:20:55.338102461 +0300] conn=752 op=16 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=1 filter="(objectClass=ipaConfigObject)" attrs="cn"
[13/Sep/2023:14:20:55.338384117 +0300] conn=752 op=16 ENTRY dn="cn=alddc1.ald.lan,cn=
masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.338786536 +0300] conn=752 op=16 ENTRY dn="cn=alddc2.ald.lan,cn=
masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.338812013 +0300] conn=752 op=16 STAT read index:
attribute=parentid key(eq)=887 --> count 2
[13/Sep/2023:14:20:55.338814646 +0300] conn=752 op=16 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.338816250 +0300] conn=752 op=16 STAT read index:
attribute=objectClass key(eq)=ipaconfigobject --> count 23
[13/Sep/2023:14:20:55.338817793 +0300] conn=752 op=16 STAT read index: duration
0.000005344
[13/Sep/2023:14:20:55.338819604 +0300] conn=752 op=16 RESULT err=0 tag=101 nentries=2
 wtime=0.000062008 optime=0.000710267 etime=0.000771078
[13/Sep/2023:14:20:55.339165624 +0300] conn=752 op=17 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=2 filter="(&(cn=CA)(ipaConfigString=caRenewalMaster))"
 attrs=ALL
[13/Sep/2023:14:20:55.339301926 +0300] conn=752 op=17 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.339305630 +0300] conn=752 op=17 STAT read index:
attribute=ipaConfigString key(eq)=carenewalmaster --> count 0
[13/Sep/2023:14:20:55.339307130 +0300] conn=752 op=17 STAT read index: duration
0.000005149
[13/Sep/2023:14:20:55.339308912 +0300] conn=752 op=17 RESULT err=0 tag=101 nentries=0
 wtime=0.000063557 optime=0.000136330 etime=0.000198526
[13/Sep/2023:14:20:55.339510610 +0300] conn=752 op=18 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=2 filter="(cn=KRA)" attrs="ipaConfigString cn"
[13/Sep/2023:14:20:55.339617817 +0300] conn=752 op=18 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.339621073 +0300] conn=752 op=18 STAT read index: attribute=cn
key(eq)=kra --> count 0
[13/Sep/2023:14:20:55.339622769 +0300] conn=752 op=18 STAT read index: duration
0.000005514
[13/Sep/2023:14:20:55.339624570 +0300] conn=752 op=18 RESULT err=0 tag=101 nentries=0
 wtime=0.000059332 optime=0.000107266 etime=0.000165289
[13/Sep/2023:14:20:55.339793722 +0300] conn=752 op=19 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=1 filter="(objectClass=ipaConfigObject)" attrs="cn"
[13/Sep/2023:14:20:55.339932422 +0300] conn=752 op=19 ENTRY dn="cn=alddc1.ald.lan,cn=
masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.339987340 +0300] conn=752 op=19 ENTRY dn="cn=alddc2.ald.lan,cn=
masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.340004476 +0300] conn=752 op=19 STAT read index:
attribute=parentid key(eq)=887 --> count 2
```

```
[13/Sep/2023:14:20:55.340006193 +0300] conn=752 op=19 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.340007246 +0300] conn=752 op=19 STAT read index:
attribute=objectClass key(eq)=ipaconfigobject --> count 23
[13/Sep/2023:14:20:55.340008241 +0300] conn=752 op=19 STAT read index: duration
0.000003912
[13/Sep/2023:14:20:55.340009416 +0300] conn=752 op=19 RESULT err=0 tag=101 nentries=2
 wtime=0.000061406 optime=0.000211749 etime=0.000272249
[13/Sep/2023:14:20:55.340305629 +0300] conn=752 op=20 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=2 filter="(|(cn=HTTP)(cn=KDC)(cn=KPASSWD))" attrs="ipaConfi
gString cn"
[13/Sep/2023:14:20:55.340478756 +0300] conn=752 op=20 ENTRY dn="cn=KDC,cn=alddc1.ald.
lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.340585708 +0300] conn=752 op=20 ENTRY dn="cn=KPASSWD,cn=alddc1.
ald.lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.340668806 +0300] conn=752 op=20 ENTRY dn="cn=HTTP,cn=alddc1.ald
.lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.340929323 +0300] conn=752 op=20 ENTRY dn="cn=KDC,cn=alddc2.ald.
lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.341152205 +0300] conn=752 op=20 ENTRY dn="cn=KPASSWD,cn=alddc2.
ald.lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.341354702 +0300] conn=752 op=20 ENTRY dn="cn=HTTP,cn=alddc2.ald
.lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.341381275 +0300] conn=752 op=20 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.341384042 +0300] conn=752 op=20 STAT read index: attribute=cn
key(eq)=kpasswd --> count 2
[13/Sep/2023:14:20:55.341385673 +0300] conn=752 op=20 STAT read index: attribute=cn
key(eq)=kdc --> count 2
[13/Sep/2023:14:20:55.341387362 +0300] conn=752 op=20 STAT read index: attribute=cn
key(eq)=http --> count 2
[13/Sep/2023:14:20:55.341389066 +0300] conn=752 op=20 STAT read index: duration
0.000002409
[13/Sep/2023:14:20:55.341390818 +0300] conn=752 op=20 RESULT err=0 tag=101 nentries=6
 wtime=0.000057366 optime=0.001075210 etime=0.001131357
[13/Sep/2023:14:20:55.341840024 +0300] conn=752 op=21 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=1 filter="(objectClass=ipaConfigObject)" attrs="cn"
[13/Sep/2023:14:20:55.341993759 +0300] conn=752 op=21 ENTRY dn="cn=alddc1.ald.lan,cn=
masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.342079524 +0300] conn=752 op=21 ENTRY dn="cn=alddc2.ald.lan,cn=
masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.342096153 +0300] conn=752 op=21 STAT read index:
attribute=parentid key(eq)=887 --> count 2
[13/Sep/2023:14:20:55.342097764 +0300] conn=752 op=21 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.342098734 +0300] conn=752 op=21 STAT read index:
attribute=objectClass key(eq)=ipaconfigobject --> count 23
[13/Sep/2023:14:20:55.342099786 +0300] conn=752 op=21 STAT read index: duration
0.000003823
[13/Sep/2023:14:20:55.342100983 +0300] conn=752 op=21 RESULT err=0 tag=101 nentries=2
 wtime=0.000052285 optime=0.000256421 etime=0.000307834
[13/Sep/2023:14:20:55.342386106 +0300] conn=752 op=22 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=2 filter="(&(cn=KDC)(ipaConfigString=pkinitEnabled))"
 attrs=ALL
[13/Sep/2023:14:20:55.342594265 +0300] conn=752 op=22 ENTRY dn="cn=KDC,cn=alddc1.ald.
lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.342716237 +0300] conn=752 op=22 ENTRY dn="cn=KDC,cn=alddc2.ald.
lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
```

```
[13/Sep/2023:14:20:55.342734738 +0300] conn=752 op=22 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.342736655 +0300] conn=752 op=22 STAT read index:
attribute=ipaConfigString key(eq)=pkinitenabled --> count 2
[13/Sep/2023:14:20:55.342737758 +0300] conn=752 op=22 STAT read index: duration
0.000004109
[13/Sep/2023:14:20:55.342738972 +0300] conn=752 op=22 RESULT err=0 tag=101 nentries=2
 wtime=0.000045996 optime=0.000349074 etime=0.000394139
[13/Sep/2023:14:20:55.342966257 +0300] conn=752 op=23 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=2 filter="(|(cn=HTTP)(cn=KDC)(cn=KPASSWD))" attrs="ipaConfi
gString cn"
[13/Sep/2023:14:20:55.343155738 +0300] conn=752 op=23 ENTRY dn="cn=KDC,cn=alddc1.ald.
lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.343330632 +0300] conn=752 op=23 ENTRY dn="cn=KPASSWD,cn=alddc1.
ald.lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.343456301 +0300] conn=752 op=23 ENTRY dn="cn=HTTP,cn=alddc1.ald
.lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.343612283 +0300] conn=752 op=23 ENTRY dn="cn=KDC,cn=alddc2.ald.
lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.343784714 +0300] conn=752 op=23 ENTRY dn="cn=KPASSWD,cn=alddc2.
ald.lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.343913191 +0300] conn=752 op=23 ENTRY dn="cn=HTTP,cn=alddc2.ald
.lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.343939801 +0300] conn=752 op=23 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.343942757 +0300] conn=752 op=23 STAT read index: attribute=cn
key(eq)=kpasswd --> count 2
[13/Sep/2023:14:20:55.343944264 +0300] conn=752 op=23 STAT read index: attribute=cn
key(eq)=kdc --> count 2
[13/Sep/2023:14:20:55.343945835 +0300] conn=752 op=23 STAT read index: attribute=cn
key(eq)=http --> count 2
[13/Sep/2023:14:20:55.343947312 +0300] conn=752 op=23 STAT read index: duration
0.000002577
[13/Sep/2023:14:20:55.343948989 +0300] conn=752 op=23 RESULT err=0 tag=101 nentries=6
 wtime=0.000046790 optime=0.000973185 etime=0.001018659
[13/Sep/2023:14:20:55.344410954 +0300] conn=752 op=24 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=1 filter="(objectClass=ipaConfigObject)" attrs="cn"
[13/Sep/2023:14:20:55.344583609 +0300] conn=752 op=24 ENTRY dn="cn=alddc1.ald.lan,cn=
masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.344672729 +0300] conn=752 op=24 ENTRY dn="cn=alddc2.ald.lan,cn=
masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.344689504 +0300] conn=752 op=24 STAT read index:
attribute=parentid key(eq)=887 --> count 2
[13/Sep/2023:14:20:55.344691486 +0300] conn=752 op=24 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.344692495 +0300] conn=752 op=24 STAT read index:
attribute=objectClass key(eq)=ipaconfigobject --> count 23
[13/Sep/2023:14:20:55.344693539 +0300] conn=752 op=24 STAT read index: duration
0.000005115
[13/Sep/2023:14:20:55.344694616 +0300] conn=752 op=24 RESULT err=0 tag=101 nentries=2
 wtime=0.000048803 optime=0.000279371 etime=0.000327371
[13/Sep/2023:14:20:55.345078345 +0300] conn=752 op=25 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=2 filter="(|(cn=DNS)(cn=DNSKeySync))" attrs="ipaConfigStrin
g cn"
[13/Sep/2023:14:20:55.345257748 +0300] conn=752 op=25 ENTRY dn="cn=DNS,cn=alddc1.ald.
lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.345345480 +0300] conn=752 op=25 ENTRY dn="cn=DNSKeySync,cn=aldd
c1.ald.lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
```

```
[13/Sep/2023:14:20:55.345502026 +0300] conn=752 op=25 ENTRY dn="cn=DNS,cn=alddc2.ald.
lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.345636752 +0300] conn=752 op=25 ENTRY dn="cn=DNSKeySync,cn=aldd
c2.ald.lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.345654618 +0300] conn=752 op=25 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.345656149 +0300] conn=752 op=25 STAT read index: attribute=cn
key(eq)=dnskeysync --> count 2
[13/Sep/2023:14:20:55.345657011 +0300] conn=752 op=25 STAT read index: attribute=cn
key(eq)=dns --> count 3
[13/Sep/2023:14:20:55.345657982 +0300] conn=752 op=25 STAT read index: duration
0.000002734
[13/Sep/2023:14:20:55.345659104 +0300] conn=752 op=25 RESULT err=0 tag=101 nentries=4
 wtime=0.000055549 optime=0.000576635 etime=0.000631317
[13/Sep/2023:14:20:55.346021322 +0300] conn=752 op=26 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=1 filter="(objectClass=ipaConfigObject)" attrs="cn"
[13/Sep/2023:14:20:55.346181960 +0300] conn=752 op=26 ENTRY dn="cn=alddc1.ald.lan,cn=
masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.346306201 +0300] conn=752 op=26 ENTRY dn="cn=alddc2.ald.lan,cn=
masters,cn=ipa,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.346324794 +0300] conn=752 op=26 STAT read index:
attribute=parentid key(eq)=887 --> count 2
[13/Sep/2023:14:20:55.346326495 +0300] conn=752 op=26 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.346327504 +0300] conn=752 op=26 STAT read index:
attribute=objectClass key(eq)=ipaconfigobject --> count 23
[13/Sep/2023:14:20:55.346328559 +0300] conn=752 op=26 STAT read index: duration
0.000003403
[13/Sep/2023:14:20:55.346329770 +0300] conn=752 op=26 RESULT err=0 tag=101 nentries=2
 wtime=0.000045374 optime=0.000303843 etime=0.000348397
[13/Sep/2023:14:20:55.346560442 +0300] conn=752 op=27 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=2 filter="(&(cn=DNSSEC)(ipaConfigString=dnssecKeyMaster))"
 attrs=ALL
[13/Sep/2023:14:20:55.346629705 +0300] conn=752 op=27 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[13/Sep/2023:14:20:55.346631831 +0300] conn=752 op=27 STAT read index:
attribute=ipaConfigString key(eq)=dnsseckeymaster --> count 0
[13/Sep/2023:14:20:55.346632745 +0300] conn=752 op=27 STAT read index: duration
0.000002191
[13/Sep/2023:14:20:55.346633956 +0300] conn=752 op=27 RESULT err=0 tag=101 nentries=0
 wtime=0.000051611 optime=0.000069493 etime=0.000120328
[13/Sep/2023:14:20:55.347475589 +0300] conn=752 op=28 UNBIND
[13/Sep/2023:14:20:55.347485861 +0300] conn=752 op=28 fd=151 Disconnect - Cleanly
Closed Connection - U1
[13/Sep/2023:14:20:55.355527748 +0300] conn=752 (Internal) op=13(1)(1) SRCH base="cn=
anonymous-limits,cn=etc,dc=ald,dc=lan" scope=0 filter="(|(objectclass=*)
(objectclass=ldapsubentry))" attrs="nsLookThroughLimit nsIDListScanLimit
nsPagedLookThroughLimit nsPagedIDListScanLimit nsRangeSearchLookThroughLimit
nsSizeLimit nsTimeLimit nsPagedSizeLimit nsIdleTimeout"
[13/Sep/2023:14:20:55.355584911 +0300] conn=752 (Internal) op=13(1)(1) ENTRY dn="cn=a
nonymous-limits,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.355593724 +0300] conn=752 (Internal) op=13(1)(1)STAT read
index: duration 0.000000000
[13/Sep/2023:14:20:55.355595320 +0300] conn=752 (Internal) op=13(1)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000022582 optime=0.000067365 etime=0.000088964
[13/Sep/2023:14:20:55.357712878 +0300] conn=752 (Internal) op=15(1)(1) SRCH base="cn=
anonymous-limits,cn=etc,dc=ald,dc=lan" scope=0 filter="(|(objectclass=*)
(objectclass=ldapsubentry))" attrs="nsLookThroughLimit nsIDListScanLimit
```

```
nsPagedLookThroughLimit nsPagedIDListScanLimit nsRangeSearchLookThroughLimit
nsSizeLimit nsTimeLimit nsPagedSizeLimit nsIdleTimeout"
[13/Sep/2023:14:20:55.357768876 +0300] conn=752 (Internal) op=15(1)(1) ENTRY dn="cn=a
nonymous-limits,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.357777233 +0300] conn=752 (Internal) op=15(1)(1)STAT read
index: duration 0.000000000
[13/Sep/2023:14:20:55.357778854 +0300] conn=752 (Internal) op=15(1)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000021879 optime=0.000066114 etime=0.000087078
[13/Sep/2023:14:20:55.359532030 +0300] conn=752 (Internal) op=14(1)(1) SRCH base="cn=
anonymous-limits,cn=etc,dc=ald,dc=lan" scope=0 filter="(|(objectclass=*)
(objectclass=ldapsubentry))" attrs="nsLookThroughLimit nsIDListScanLimit
nsPagedLookThroughLimit nsPagedIDListScanLimit nsRangeSearchLookThroughLimit
nsSizeLimit nsTimeLimit nsPagedSizeLimit nsIdleTimeout"
[13/Sep/2023:14:20:55.359579258 +0300] conn=752 (Internal) op=14(1)(1) ENTRY dn="cn=a
nonymous-limits,cn=etc,dc=ald,dc=lan"
[13/Sep/2023:14:20:55.359588921 +0300] conn=752 (Internal) op=14(1)(1)STAT read
index: duration 0.000000000
[13/Sep/2023:14:20:55.359591321 +0300] conn=752 (Internal) op=14(1)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000014852 optime=0.000056868 etime=0.000070659
```

В логах audit мы можем увидеть аналогичную информацию:

- был создан новый компьютер alddc3.ald.lan

```
changetype: add
fqdn: alddc3.ald.lan
nsHardwarePlatform: x86_64
nsOsVersion: 5.15.0-70-generic
```

- и что его создал admin

```
modifiersName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
```

Полная информация из /var/log/dirsrv/slapd-ALD-LAN/audit

```
time: 20230913142055
dn: fqdn=alddc3.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan
#fqdn: alddc3.ald.lan
#nsHardwarePlatform: x86_64
#nsOsVersion: 5.15.0-70-generic
#rbtadp: ou=ald.lan,cn=orgunits,cn=accounts,dc=ald,dc=lan
#objectClass: ipaobject
#objectClass: nshost
#objectClass: ipahost
#objectClass: pkiuser
#objectClass: ipaservice
#objectClass: rbta-address
#objectClass: rbta-unit
#objectClass: krbprincipalaux
#objectClass: krbprincipal
#objectClass: ieee802device
#objectClass: ipasshhost
```

```
#objectClass: top
#objectClass: ipaSshGroupOfPubKeys
#cn: alddc3.ald.lan
#serverHostName: alddc3
#krbPrincipalName: host/alddc3.ald.lan@ALD.LAN
#krbCanonicalName: host/alddc3.ald.lan@ALD.LAN
#managedBy: fqdn=alddc3.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan
#internalCreatorsName: cn=ldbm database,cn=plugins,cn=config
#internalModifiersName: cn=ldbm database,cn=plugins,cn=config
#creatorsName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
#modifiersName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
#createTimestamp: 20230913112055Z
#modifyTimestamp: 20230913112055Z
#nsUniqueId: 8a25cf81-522711ee-ae1996b2-300f2d85
#ipaUniqueID: 9b07257e-5227-11ee-8d34-5254001c2f55
#parentid: 39
#entryid: 2204
#entryUUID: d1b22b67-b1ff-4d3c-ad84-9dd9370af508
#entryusn: 74925
#dsEntryDN: fqdn=alddc3.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan
#entrydn: fqdn=alddc3.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan
result: 0
changetype: add
fqdn: alddc3.ald.lan
nsHardwarePlatform: x86_64
nsOsVersion: 5.15.0-70-generic
rbtadp: ou=ald.lan,cn=orgunits,cn=accounts,dc=ald,dc=lan
objectClass: ipaobject
objectClass: nshost
objectClass: ipahost
objectClass: pkiuser
objectClass: ipaservice
objectClass: rbta-address
objectClass: rbta-unit
objectClass: krbprincipalaux
objectClass: krbprincipal
objectClass: ieee802device
objectClass: ipasshhost
objectClass: top
objectClass: ipaSshGroupOfPubKeys
cn: alddc3.ald.lan
serverHostName: alddc3
krbPrincipalName: host/alddc3.ald.lan@ALD.LAN
krbCanonicalName: host/alddc3.ald.lan@ALD.LAN
managedBy: fqdn=alddc3.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan
internalCreatorsName: cn=ldbm database,cn=plugins,cn=config
internalModifiersName: cn=ldbm database,cn=plugins,cn=config
creatorsName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
modifiersName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
createTimestamp: 20230913112055Z
modifyTimestamp: 20230913112055Z
ipaUniqueID: 9b07257e-5227-11ee-8d34-5254001c2f55
time: 20230913142058
dn: idnsName=alddc3,idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
#aRecord: 192.168.100.122
#dNSTTL: 1200
#objectClass: idnsRecord
#objectClass: top
#idnsName: alddc3
```

```
#internalCreatorsName: cn=ldbm database,cn=plugins,cn=config
#internalModifiersName: cn=ldbm database,cn=plugins,cn=config
#creatorsName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=accounts,dc
=ald,dc=lan
#modifiersName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=accounts,d
c=ald,dc=lan
#createTimestamp: 20230913112058Z
#modifyTimestamp: 20230913112058Z
#nsUniqueId: 8a25cf82-522711ee-ae1996b2-300f2d85
#parentid: 49
#entryid: 2205
#entryUUID: 4e3d458d-636c-4388-b719-646d2f97a9f7
#entryusn: 74931
#dsEntryDN: idnsName=alddc3,idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
#entrydn: idnsname=alddc3,idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
result: 0
changetype: add
aRecord: 192.168.100.122
dNSTTL: 1200
objectClass: idnsRecord
objectClass: top
idnsName: alddc3
internalCreatorsName: cn=ldbm database,cn=plugins,cn=config
internalModifiersName: cn=ldbm database,cn=plugins,cn=config
creatorsName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=accou
nts,dc=ald,dc=lan
modifiersName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=acco
unts,dc=ald,dc=lan
createTimestamp: 20230913112058Z
modifyTimestamp: 20230913112058Z
time: 20230913142058
dn: idnsName=alddc3,idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
#aRecord: 192.168.100.122
#dNSTTL: 1200
#objectClass: idnsRecord
#objectClass: top
#idnsName: alddc3
#internalCreatorsName: cn=ldbm database,cn=plugins,cn=config
#internalModifiersName: cn=ldbm database,cn=plugins,cn=config
#creatorsName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=accounts,dc
=ald,dc=lan
#modifiersName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=accounts,d
c=ald,dc=lan
#createTimestamp: 20230913112058Z
#modifyTimestamp: 20230913112058Z
#nsUniqueId: 8a25cf82-522711ee-ae1996b2-300f2d85
#parentid: 49
#entryid: 2205
#entryUUID: 4e3d458d-636c-4388-b719-646d2f97a9f7
#entryusn: 74931
#dsEntryDN: idnsName=alddc3,idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
#entrydn: idnsname=alddc3,idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
result: 0
changetype: add
aRecord: 192.168.100.122
dNSTTL: 1200
objectClass: idnsRecord
objectClass: top
idnsName: alddc3
```

```
internalCreatorsName: cn=ldbm database,cn=plugins,cn=config
internalModifiersName: cn=ldbm database,cn=plugins,cn=config
creatorsName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=accou
nts,dc=ald,dc=lan
modifiersName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=acco
unts,dc=ald,dc=lan
createTimestamp: 20230913112058Z
modifyTimestamp: 20230913112058Z
time: 20230913142058
dn: idnsName=alddc3, idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
#entryusn: 74939
#modifyTimestamp: 20230913112058Z
#modifiersName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=accounts,d
c=ald,dc=lan
#internalModifiersName: cn=ldbm database,cn=plugins,cn=config
#dNSTTL: 1200
#sSHFPRecord: 1 1 BEBF5DC176918D078BE4F0E506C32E36A2DB25A8
#aRecord: 192.168.100.122
#objectClass: idnsRecord
#objectClass: top
#idnsName: alddc3
#internalCreatorsName: cn=ldbm database,cn=plugins,cn=config
#creatorsName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=accounts,dc
=ald,dc=lan
#createTimestamp: 20230913112058Z
#nsUniqueId: 8a25cf82-522711ee-ae1996b2-300f2d85
#parentid: 49
#entryid: 2205
#entryUUID: 4e3d458d-636c-4388-b719-646d2f97a9f7
#dsEntryDN: idnsName=alddc3,idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
#entrydn: idnsname=alddc3,idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
result: 0
changetype: modify
add: sSHFPRecord
sSHFPRecord: 1 1 BEBF5DC176918D078BE4F0E506C32E36A2DB25A8
-
replace: dNSTTL
dNSTTL: 1200
-
replace: internalModifiersName
internalModifiersName: cn=ldbm database,cn=plugins,cn=config
-
replace: modifiersname
modifiersname: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=acco
unts,dc=ald,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20230913112058Z
-
replace: entryusn
entryusn: 74939
-
time: 20230913142058
dn: idnsName=alddc3, idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
#entryusn: 74941
#modifyTimestamp: 20230913112058Z
#modifiersName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=accounts,d
c=ald,dc=lan
#internalModifiersName: cn=ldbm database,cn=plugins,cn=config
```

```
#dNSTTL: 1200
#sSHFPRecord: 1 1 BEBF5DC176918D078BE4F0E506C32E36A2DB25A8
#sSHFPRecord: 1 2 B8CC0F664D1FF1C9E1CA9C738DA4CDE279D547480F8AAE8F6552708D 434ABF6F
#aRecord: 192.168.100.122
#objectClass: idnsRecord
#objectClass: top
#idnsName: alddc3
#internalCreatorsName: cn=ldbm database,cn=plugins,cn=config
#creatorsName: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=accounts,dc
=ald,dc=lan
#createTimestamp: 20230913112058Z
#nsUniqueId: 8a25cf82-522711ee-ae1996b2-300f2d85
#parentid: 49
#entryid: 2205
#entryUUID: 4e3d458d-636c-4388-b719-646d2f97a9f7
#dsEntryDN: idnsName=alddc3,idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
#entrydn: idnsname=alddc3,idnsname=ald.lan.,cn=dns,dc=ald,dc=lan
result: 0
changetype: modify
add: sSHFPRecord
sSHFPRecord: 1 2 B8CC0F664D1FF1C9E1CA9C738DA4CDE279D547480F8AAE8F6552708D 434A
BF6F
-
replace: dNSTTL
dNSTTL: 1200
-
replace: internalModifiersName
internalModifiersName: cn=ldbm database,cn=plugins,cn=config
-
replace: modifiersname
modifiersname: krbprincipalname=dns/alddc1.ald.lan@ald.lan,cn=services,cn=acco
unts,dc=ald,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20230913112058Z
-
replace: entryusn
entryusn: 74941
-
```

3.16 Событие 4742 A computer account was changed

В данном примере компьютер srvsssd.ald.lan был добавлен в организационную структуру IT.

В логах access нам будет интересна строка, по которой видно, что запись srvsssd.ald.lan была изменена:

```
[14/Sep/2023:15:20:08.592949557 +0300] conn=7827 op=6 MOD dn="fqdn=srvsssd.ald.lan,cn
=computers,cn=accounts,dc=ald,dc=lan"
```

Полный лог из /var/log/dirsrv/slapd-ALD-LAN/access:

```
[14/Sep/2023:15:20:08.321621206 +0300] conn=7827 fd=154 slot=154 connection from
192.168.100.120 to 192.168.100.120
[14/Sep/2023:15:20:08.330974384 +0300] conn=7827 op=0 BIND dn="" method=sasl version=3
 mech=GSS-SPNEGO
[14/Sep/2023:15:20:08.332564413 +0300] conn=7827 (Internal) op=0(1)(1) SRCH base="dc=
ald,dc=lan" scope=2 filter="(krbPrincipalName=admin@ALD.LAN)" attrs=ALL
[14/Sep/2023:15:20:08.332954118 +0300] conn=7827 (Internal) op=0(1)(1) ENTRY dn="uid=
admin,cn=users,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.332969778 +0300] conn=7827 (Internal) op=0(1)(1)STAT read
index: attribute=objectclass key(eq)=referral --> count 0
[14/Sep/2023:15:20:08.332972293 +0300] conn=7827 (Internal) op=0(1)(1)STAT read
index: attribute=krbPrincipalName key(eq)=admin@ALD.LAN --> count 1
[14/Sep/2023:15:20:08.332974288 +0300] conn=7827 (Internal) op=0(1)(1)STAT read
index: duration 0.000005308
[14/Sep/2023:15:20:08.332976393 +0300] conn=7827 (Internal) op=0(1)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000015894 optime=0.000406045 etime=0.000420652
[14/Sep/2023:15:20:08.333226770 +0300] conn=7827 (Internal) op=0(2)(1) SRCH base="uid
=admin,cn=users,cn=accounts,dc=ald,dc=lan" scope=0 filter="(|(objectclass=*)
(objectclass=ldapsubentry))" attrs="nsLookThroughLimit nsIDListScanLimit
nsPagedLookThroughLimit nsPagedIDListScanLimit nsRangeSearchLookThroughLimit
nsSizeLimit nsTimeLimit nsPagedSizeLimit nsIdleTimeout"
[14/Sep/2023:15:20:08.333383332 +0300] conn=7827 (Internal) op=0(2)(1) ENTRY dn="uid=
admin,cn=users,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.333392091 +0300] conn=7827 (Internal) op=0(2)(1)STAT read
index: duration 0.000000000
[14/Sep/2023:15:20:08.333394165 +0300] conn=7827 (Internal) op=0(2)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000039314 optime=0.000166964 etime=0.000205294
[14/Sep/2023:15:20:08.333788229 +0300] conn=7827 (Internal) op=0(5)(1) SRCH base="uid
=admin,cn=users,cn=accounts,dc=ald,dc=lan" scope=0 filter="(|(objectclass=*)
(objectclass=ldapsubentry))" attrs=ALL
[14/Sep/2023:15:20:08.333882420 +0300] conn=7827 (Internal) op=0(5)(1) ENTRY dn="uid=
admin,cn=users,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.333889245 +0300] conn=7827 (Internal) op=0(5)(1)STAT read
index: duration 0.000000000
[14/Sep/2023:15:20:08.333891049 +0300] conn=7827 (Internal) op=0(5)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000004099 optime=0.000101262 etime=0.000104440
[14/Sep/2023:15:20:08.334036263 +0300] conn=7827 op=0 RESULT err=0 tag=97 nentries=0
 wtime=0.000172793 optime=0.003065303 etime=0.003236775 dn="uid=admin,cn=users,cn=acc
ounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.581540552 +0300] conn=7827 op=1 SRCH base="cn=ipaconfig,cn=etc,
dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs=ALL
[14/Sep/2023:15:20:08.582329670 +0300] conn=7827 op=1 ENTRY dn="cn=ipaConfig,cn=etc,d
c=ald,dc=lan"
[14/Sep/2023:15:20:08.582399862 +0300] conn=7827 op=1 STAT read index: duration
0.000000000
[14/Sep/2023:15:20:08.582405003 +0300] conn=7827 op=1 RESULT err=0 tag=101 nentries=1
 wtime=0.000249724 optime=0.000863760 etime=0.001111140
[14/Sep/2023:15:20:08.584003274 +0300] conn=7827 op=2 SRCH base="fqdn=srvsssd.ald.lan
,cn=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs=""
[14/Sep/2023:15:20:08.584246392 +0300] conn=7827 op=2 ENTRY dn="fqdn=srvsssd.ald.lan,
cn=computers,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.584279425 +0300] conn=7827 op=2 STAT read index: duration
0.000000000
[14/Sep/2023:15:20:08.584282382 +0300] conn=7827 op=2 RESULT err=0 tag=101 nentries=1
 wtime=0.000242519 optime=0.000277960 etime=0.000519074
[14/Sep/2023:15:20:08.585966018 +0300] conn=7827 op=3 SRCH base="cn=masters,cn=ipa,cn
=etc,dc=ald,dc=lan" scope=2 filter="(&(objectClass=ipaConfigObject)(cn=CA))"
 attrs=ALL
```

```
[14/Sep/2023:15:20:08.586272189 +0300] conn=7827 op=3 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[14/Sep/2023:15:20:08.586277206 +0300] conn=7827 op=3 STAT read index: attribute=cn
key(eq)=ca --> count 1
[14/Sep/2023:15:20:08.586278871 +0300] conn=7827 op=3 STAT read index: duration
0.000008523
[14/Sep/2023:15:20:08.586280812 +0300] conn=7827 op=3 RESULT err=0 tag=101 nentries=0
 wtime=0.000187521 optime=0.000306471 etime=0.000492351
[14/Sep/2023:15:20:08.586838062 +0300] conn=7827 op=4 SRCH base="fqdn=srvsssd.ald.lan
,cn=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="obje
ctClass"
[14/Sep/2023:15:20:08.587045336 +0300] conn=7827 op=4 ENTRY dn="fqdn=srvsssd.ald.lan,
cn=computers,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.587078621 +0300] conn=7827 op=4 STAT read index: duration
0.000000000
[14/Sep/2023:15:20:08.587081693 +0300] conn=7827 op=4 RESULT err=0 tag=101 nentries=1
 wtime=0.000176989 optime=0.000241430 etime=0.000417037
[14/Sep/2023:15:20:08.591682737 +0300] conn=7827 op=5 SRCH base="fqdn=srvsssd.ald.lan
,cn=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="c
rbtadp postalCode l macAddress st street"
[14/Sep/2023:15:20:08.591991257 +0300] conn=7827 op=5 ENTRY dn="fqdn=srvsssd.ald.lan,
cn=computers,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.592044278 +0300] conn=7827 op=5 STAT read index: duration
0.000000000
[14/Sep/2023:15:20:08.592049429 +0300] conn=7827 op=5 RESULT err=0 tag=101 nentries=1
 wtime=0.000159147 optime=0.000362357 etime=0.000517176
[14/Sep/2023:15:20:08.592949557 +0300] conn=7827 op=6 MOD dn="fqdn=srvsssd.ald.lan,cn
=computers,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.592976407 +0300] conn=7827 (Internal) op=6(1)(1) SRCH base="fqd
n=srvsssd.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(|
(objectclass=*)(objectclass=ldapsubentry))" attrs=ALL
[14/Sep/2023:15:20:08.593063028 +0300] conn=7827 (Internal) op=6(1)(1) ENTRY dn="fqdn
=srvsssd.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.593076253 +0300] conn=7827 (Internal) op=6(1)(1)STAT read
index: duration 0.000000000
[14/Sep/2023:15:20:08.593079772 +0300] conn=7827 (Internal) op=6(1)(1) RESULT err=0
 tag=48 nentries=1 wtime=0.000013559 optime=0.000099437 etime=0.000111550
[14/Sep/2023:15:20:08.601361375 +0300] conn=7827 op=6 RESULT err=0 tag=103 nentries=0
 wtime=0.000146779 optime=0.008413240 etime=0.008555851 csn=6502fa93000000040000
[14/Sep/2023:15:20:08.601956375 +0300] conn=7827 op=7 SRCH base="fqdn=srvsssd.ald.lan
,cn=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(objectClass=*)" attrs="memb
erofindirect * macAddress krbPrincipalName managedBy description userCertificate
rbtadp krbCanonicalName fqdn nsOsVersion nsHostLocation ipaAllowedToPerform l
userClass krbPrincipalAuthInd memberOf ipaAssignedIDView nsHardwarePlatform aci"
[14/Sep/2023:15:20:08.603960101 +0300] conn=7827 op=7 ENTRY dn="fqdn=srvsssd.ald.lan,
cn=computers,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.604029940 +0300] conn=7827 op=7 STAT read index: duration
0.000000000
[14/Sep/2023:15:20:08.604035734 +0300] conn=7827 op=7 RESULT err=0 tag=101 nentries=1
 wtime=0.000150546 optime=0.002075423 etime=0.002223716
[14/Sep/2023:15:20:08.605065276 +0300] conn=7827 op=8 SRCH base="dc=ald,dc=lan"
 scope=2 filter="(|
(member=fqdn=srvsssd.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan)
(memberUser=fqdn=srvsssd.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan)
(memberHost=fqdn=srvsssd.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan))" attrs=""
[14/Sep/2023:15:20:08.605681184 +0300] conn=7827 op=8 ENTRY dn="cn=it_pc,cn=hostgroup
s,cn=accounts,dc=ald,dc=lan"
```

```
[14/Sep/2023:15:20:08.605733843 +0300] conn=7827 op=8 RESULT err=0 tag=101 nentries=1
 wtime=0.000248493 optime=0.000669965 etime=0.000916460 notes=P details="Paged
Search" pr_idx=0 pr_cookie=-1
[14/Sep/2023:15:20:08.606326714 +0300] conn=7827 op=9 SRCH base="fqdn=srvsssd.ald.lan
,cn=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(userPassword=*)" attrs="use
rPassword"
[14/Sep/2023:15:20:08.606635462 +0300] conn=7827 op=9 STAT read index: duration
0.000000000
[14/Sep/2023:15:20:08.606641569 +0300] conn=7827 op=9 RESULT err=0 tag=101 nentries=0
 wtime=0.000096848 optime=0.000308393 etime=0.000403281
[14/Sep/2023:15:20:08.607068810 +0300] conn=7827 op=10 SRCH base="fqdn=srvsssd.ald.la
n,cn=computers,cn=accounts,dc=ald,dc=lan" scope=0 filter="(krbPrincipalKey=*)" attrs="
krbPrincipalKey"
[14/Sep/2023:15:20:08.607365545 +0300] conn=7827 op=10 ENTRY dn="fqdn=srvsssd.ald.lan
,cn=computers,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.607400508 +0300] conn=7827 op=10 STAT read index: duration
0.000000000
[14/Sep/2023:15:20:08.607403409 +0300] conn=7827 op=10 RESULT err=0 tag=101 nentries=1
 wtime=0.000095675 optime=0.000333418 etime=0.000427589
[14/Sep/2023:15:20:08.608021447 +0300] conn=7827 op=11 SRCH base="cn=computers,cn=acc
ounts,dc=ald,dc=lan" scope=2 filter="(managedBy=fqdn=srvsssd.ald.lan,cn=computers,cn=
accounts,dc=ald,dc=lan)" attrs="fqdn"
[14/Sep/2023:15:20:08.608292895 +0300] conn=7827 op=11 ENTRY dn="fqdn=srvsssd.ald.lan
,cn=computers,cn=accounts,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.608325266 +0300] conn=7827 op=11 STAT read index:
attribute=objectclass key(eq)=referral --> count 0
[14/Sep/2023:15:20:08.608328214 +0300] conn=7827 op=11 STAT read index:
attribute=managedBy
key(eq)=fqdn=srvsssd.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan --> count 1
[14/Sep/2023:15:20:08.608329944 +0300] conn=7827 op=11 STAT read index: duration
0.000006058
[14/Sep/2023:15:20:08.608331666 +0300] conn=7827 op=11 RESULT err=0 tag=101 nentries=1
 wtime=0.000083012 optime=0.000304194 etime=0.000385846
[14/Sep/2023:15:20:08.609619681 +0300] conn=7827 op=12 SRCH base="cn=it_pc,cn=ng,cn=a
lt,dc=ald,dc=lan" scope=0 filter="(objectClass=mepmanagedentry)" attrs=""
[14/Sep/2023:15:20:08.609862019 +0300] conn=7827 op=12 ENTRY dn="cn=it_pc,cn=ng,cn=al
t,dc=ald,dc=lan"
[14/Sep/2023:15:20:08.609911162 +0300] conn=7827 op=12 STAT read index: duration
0.000000000
[14/Sep/2023:15:20:08.609915910 +0300] conn=7827 op=12 RESULT err=0 tag=101 nentries=1
 wtime=0.000130586 optime=0.000292779 etime=0.000421501
[14/Sep/2023:15:20:08.613400422 +0300] conn=7827 op=13 UNBIND
[14/Sep/2023:15:20:08.613427865 +0300] conn=7827 op=13 fd=154 Disconnect - Cleanly
Closed Connection - U1
```

В логах audit мы сможем детально понять изменения:

- компьютер srvsssd.ald.lan

```
dn: fqdn=srvsssd.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan
```

- был добавлен в орг.структура IT пользователем admin

```
changetype: modify
delete: rbtadp
```

```
rbtadp: ou=ald.lan,cn=orgunits,cn=accounts,dc=ald,dc=lan
-
add: rbtadp
rbtadp: ou=IT,ou=ald.lan,cn=orgunits,cn=accounts,dc=ald,dc=lan
modifiersname: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
```

Полный лог из /var/log/dirsrv/slapd-ALD-LAN/audit:

```
time: 20230914152008
dn: fqdn=srvsssd.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan
#entryusn: 79118
#modifyTimestamp: 20230914122008Z
#modifiersName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
#internalModifiersName: cn=ldbm database,cn=plugins,cn=config
#rbtadp: ou=IT,ou=ald.lan,cn=orgunits,cn=accounts,dc=ald,dc=lan
#fqdn: srvsssd.ald.lan
#nsHardwarePlatform: x86_64
#nsOsVersion: 5.15.0-33-generic
#objectClass: ipaobject
#objectClass: nshost
#objectClass: ipahost
#objectClass: pkiuser
#objectClass: ipaservice
#objectClass: rbta-address
#objectClass: rbta-unit
#objectClass: krbprincipalaux
#objectClass: krbprincipal
#objectClass: ieee802device
#objectClass: ipasshhost
#objectClass: top
#objectClass: ipaSshGroupOfPubKeys
#cn: srvsssd.ald.lan
#serverHostName: srvsssd
#krbPrincipalName: host/srvsssd.ald.lan@ALD.LAN
#krbCanonicalName: host/srvsssd.ald.lan@ALD.LAN
#managedBy: fqdn=srvsssd.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan
#creatorsName: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
#createTimestamp: 20230629082300Z
#ipaUniqueID: 28ec1ea2-1656-11ee-bc70-5254001c2f55
#parentid: 39
#entryid: 765
#krbPrincipalKey: 0ﻩ^C^B^A^A^A^C^B^A^A^A^C^B^A^A^A^C^B^A^A^A^C^B^A^A^A
```

```
#memberOf: cn=it_pc,cn=ng,cn=alt,dc=ald,dc=lan
#nsUniqueId: 04e24401-165611ee-bd0f96b2-300f2d85
#dsEntryDN: fqdn=srvsssd.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan
#entrydn: fqdn=srvsssd.ald.lan,cn=computers,cn=accounts,dc=ald,dc=lan
result: 0
changetype: modify
delete: rbtadp
rbtadp: ou=ald.lan,cn=orgunits,cn=accounts,dc=ald,dc=lan
-
add: rbtadp
rbtadp: ou=IT,ou=ald.lan,cn=orgunits,cn=accounts,dc=ald,dc=lan
-
replace: internalModifiersName
internalModifiersName: cn=ldbm database,cn=plugins,cn=config
-
replace: modifiersname
modifiersname: uid=admin,cn=users,cn=accounts,dc=ald,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20230914122008Z
-
replace: entryusn
entryusn: 79118
-
```

3.17 Событие 4743 A computer account was deleted

Логи находятся на контроллере домена в двух файлах:

- /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit;
- /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access.

Мы удалили учетную запись компьютера garant1.ald.company.lan в домене ALD.COMPANY.LAN.

Рассмотрим лог из /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit.

Обратим внимание на следующие строки:

- dn: fqdn=garant1.ald.company.lan,cn=computers,cn=accounts,dc=ald,dc=company,dc=lan — объект, который был удален;
- changetype: delete — тип изменений, в данном случае мы удалили компьютер garant1.ald.company.lan;
- modifiersname: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan — имя учетной записи, кто удалил компьютер.

Полный лог:

```
time: 20240816170922
dn: fqdn=garant1.ald.company.lan,cn=computers,cn=accounts,dc=ald,dc=company,dc=lan
result: 0
changetype: delete
modifiersname: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
time: 20240816170922
dn: idnsName=garant1,idnsname=ald.company.lan.,cn=dns,dc=ald,dc=company,dc=lan
result: 0
changetype: modify
delete: aRecord
```

```
-
replace: modifiersname
modifiersname: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20240816140922Z
-
replace: entryusn
entryusn: 8872
-
time: 20240816170922
dn: idnsname=ald.company.lan.,cn=dns,dc=ald,dc=company,dc=lan
result: 0
changetype: modify
replace: idnsSOAserial
idnsSOAserial: 1723817362
-
replace: modifiersname
modifiersname: krbprincipalname=dns/dc-1.ald.company.lan@ald.company.lan,cn=services,
cn=accounts,dc=ald,dc=company,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20240816140922Z
-
replace: entryusn
entryusn: 8874
-
```

Рассмотрим лог из /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access.

Обратим внимание на следующие параметры:

- 192.168.130.10 - IP контроллера домена;
- conn=28338 – номер подключения, в рамках которого происходит операция удаления компьютера;
- DEL dn="fqdn=garant1.ald.company.lan,cn=computers,cn=accounts,dc=ald,dc=company,dc=lan" - тип запроса DEL, в нашем случае удалили компьютер:

```
[16/Aug/2024:17:09:22.351810248 +0300] conn=28338 fd=168 slot=168 connection from
192.168.130.10 to 192.168.130.10
[16/Aug/2024:17:09:22.356699958 +0300] conn=28338 op=0 BIND dn="" method=sasl
version=3 mech=GSS-SPNEGO
[16/Aug/2024:17:09:22.358025803 +0300] conn=28338 op=0 RESULT err=0 tag=97 nentries=0
 wtime=0.000107486 optime=0.001328345 etime=0.001435221 dn="uid=admin,cn=users,cn=acc
ounts,dc=ald,dc=company,dc=lan"
[16/Aug/2024:17:09:22.456088322 +0300] conn=28338 op=1 SRCH base="cn=ipaconfig,cn=etc
,dc=ald,dc=company,dc=lan" scope=0 filter="(objectClass=*)" attrs=ALL
[16/Aug/2024:17:09:22.457084361 +0300] conn=28338 op=1 RESULT err=0 tag=101 nentries=1
 wtime=0.000306909 optime=0.001002003 etime=0.001305464
[16/Aug/2024:17:09:22.459102104 +0300] conn=28338 op=2 SRCH base="fqdn=garant1.ald.co
mpany.lan,cn=computers,cn=accounts,dc=ald,dc=company,dc=lan" scope=0 filter="(objectC
lass=*)" attrs=""
[16/Aug/2024:17:09:22.459542721 +0300] conn=28338 op=2 RESULT err=0 tag=101 nentries=1
 wtime=0.000284385 optime=0.000444074 etime=0.000725737
```

```
[16/Aug/2024:17:09:22.462894288 +0300] conn=28338 op=3 SRCH base="cn=garant1.ald.comp
any.lan,cn=masters,cn=ipa,cn=etc,dc=ald,dc=company,dc=lan" scope=0 filter="(objectCla
ss=*)" attrs="objectClass"
[16/Aug/2024:17:09:22.463427965 +0300] conn=28338 op=3 RESULT err=32 tag=101
 nentries=0 wtime=0.000244761 optime=0.000537441 etime=0.000779245
[16/Aug/2024:17:09:22.465521303 +0300] conn=28338 op=4 SRCH base="cn=services,cn=acco
unts,dc=ald,dc=company,dc=lan" scope=1 filter="(&(&(objectClass=ipaService)(!(|
(krbPrincipalName=kadmin/*)(krbPrincipalName=K/M@*)(krbPrincipalName=krbtgt/*))))(&(|
(krbPrincipalName=*garant1.ald.company.lan*)(managedBy=*garant1.ald.company.lan*)
(ipaKrbAuthzData=*garant1.ald.company.lan*))(&(objectClass=krbprincipal)
(objectClass=krbprincipalaux)(objectClass=krbticketpolicyaux)(objectClass=ipaobject)
(objectClass=ipaservice)(objectClass=pkiuser))))" attrs="krbPrincipalName
ipaKrbAuthzData krbPrincipalAuthInd ipaAllowedToPerform userCertificate
krbCanonicalName"
[16/Aug/2024:17:09:22.471654201 +0300] conn=28338 op=4 RESULT err=0 tag=101 nentries=0
 wtime=0.000237238 optime=0.006133236 etime=0.006366984
[16/Aug/2024:17:09:22.473157612 +0300] conn=28338 op=5 SRCH base="cn=masters,cn=ipa,c
n=etc,dc=ald,dc=company,dc=lan" scope=2 filter="(&(objectClass=ipaConfigObject)
(cn=CA))" attrs=ALL
[16/Aug/2024:17:09:22.473614078 +0300] conn=28338 op=5 RESULT err=0 tag=101 nentries=0
 wtime=0.000206205 optime=0.000459265 etime=0.000662516
[16/Aug/2024:17:09:22.474378285 +0300] conn=28338 op=6 DEL dn="fqdn=garant1.ald.compa
ny.lan,cn=computers,cn=accounts,dc=ald,dc=company,dc=lan"
[16/Aug/2024:17:09:22.493604659 +0300] conn=28338 op=6 RESULT err=0 tag=107 nentries=0
 wtime=0.000112992 optime=0.019230612 etime=0.019338636
[16/Aug/2024:17:09:22.494921329 +0300] conn=28338 op=7 UNBIND
[16/Aug/2024:17:09:22.494970823 +0300] conn=28338 op=7 fd=168 Disconnect - Cleanly
Closed Connection - U1
```

3.18 Событие 5137 A directory service object was created

Файл логов находятся на контроллере домена в двух каталогах:

- /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit;
- /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access.

Мы создали группу пользователей "new_user_group" в домене ALD.COMPANY.LAN.

Рассмотрим лог из /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit.

Обратим внимание на следующие строки:

- dn: cn=new_user_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan — объект, который был создан;
- changetype: add — тип изменений, в данном случае мы добавили/создали новый объект.
- creatorsName: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan — имя учетной записи, кто создал объект.

Полный лог:

```
time: 20240815143028 - время создания объекта 2024 год 08 месяц 15 число 14 час 30
 минут 28 секунд.
time: 20240815143028
dn: cn=new_user_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
result: 0
changetype: add
cn: new_user_group
```

```
rbtadp: ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan
rbtaou: ald.company.lan
gidNumber: -1
objectClass: groupofnames
objectClass: ipaobject
objectClass: ipausergroup
objectClass: nestedgroup
objectClass: posixgroup
objectClass: rbta-unit
objectClass: top
objectClass: x-ald-audit-policy
creatorsName: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
modifiersName: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
createTimestamp: 20240815113028Z
modifyTimestamp: 20240815113028Z
ipaUniqueID: c5ba4bb2-5af9-11ef-8720-52540017d313
```

Рассмотрим лог из /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access.

Обратим внимание на следующие параметры:

- 192.168.130.10 - IP контроллера домена;
- conn=20182 – номер подключения;
- ADD dn="cn=new_user_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan" - тип запроса ADD, в нашем случае создали группу.

Полный лог:

```
[15/Aug/2024:14:30:28.233766942 +0300] conn=20182 fd=174 slot=174 SSL connection from
192.168.130.10 to 192.168.130.10
[15/Aug/2024:14:30:28.236780008 +0300] conn=20182 TLS1.3 128-bit AES-GCM
[15/Aug/2024:14:30:28.238460573 +0300] conn=20182 op=0 BIND dn="" method=sasl
version=3 mech=GSSAPI
[15/Aug/2024:14:30:28.240486394 +0300] conn=20182 op=0 RESULT err=14 tag=97 nentries=0
 wtime=0.004574344 optime=0.002033454 etime=0.006606540, SASL bind in progress
[15/Aug/2024:14:30:28.241553329 +0300] conn=20182 op=1 BIND dn="" method=sasl
version=3 mech=GSSAPI
[15/Aug/2024:14:30:28.242157674 +0300] conn=20182 op=1 RESULT err=14 tag=97 nentries=0
 wtime=0.000043834 optime=0.000607824 etime=0.000650927, SASL bind in progress
[15/Aug/2024:14:30:28.242391928 +0300] conn=20182 op=2 BIND dn="" method=sasl
version=3 mech=GSSAPI
[15/Aug/2024:14:30:28.243232442 +0300] conn=20182 op=2 RESULT err=0 tag=97 nentries=0
 wtime=0.000038871 optime=0.000842296 etime=0.000880413 dn="uid=admin,cn=users,cn=acc
ounts,dc=timur,dc=lan"
[15/Aug/2024:14:30:28.243635199 +0300] conn=20182 op=3 SRCH base="uid=new_user_group,
cn=users,cn=accounts,dc=ald,dc=company,dc=lan" scope=2 filter="(objectClass=*)"
 attrs="uid"
[15/Aug/2024:14:30:28.243940204 +0300] conn=20182 op=3 RESULT err=32 tag=101
 nentries=0 wtime=0.000170280 optime=0.000305992 etime=0.000475297
[15/Aug/2024:14:30:28.244337248 +0300] conn=20182 op=4 SRCH base="ou=timur.lan,cn=org
units,cn=accounts,dc=ald,dc=company,dc=lan" scope=0 filter="(objectClass=*)" attrs="o
u manager displayName description objectClass"
[15/Aug/2024:14:30:28.244558324 +0300] conn=20182 op=4 RESULT err=0 tag=101 nentries=1
 wtime=0.000062505 optime=0.000221883 etime=0.000283464
[15/Aug/2024:14:30:28.245088950 +0300] conn=20182 op=5 ADD dn="cn=new_user_group,cn=g
roups,cn=accounts,dc=ald,dc=company,dc=lan"
```

```
[15/Aug/2024:14:30:28.262368591 +0300] conn=20182 op=5 RESULT err=0 tag=105 nentries=0
 wtime=0.000097827 optime=0.017280957 etime=0.017376643
[15/Aug/2024:14:30:28.319093877 +0300] conn=20182 op=6 SRCH base="cn=new_user_group,c
n=groups,cn=accounts,dc=ald,dc=company,dc=lan" scope=2 filter="(objectClass=*)"
 attrs="cn distinguishedName gidNumber ipaUniqueID rbtadp rbtaou description
objectClass"
[15/Aug/2024:14:30:28.319907852 +0300] conn=20182 op=6 RESULT err=0 tag=101 nentries=1
 wtime=0.000206778 optime=0.000816486 etime=0.001020960 notes=U details="Partially
Unindexed Filter"
```

3.19 Событие 5136 A directory service object was modified

Рассмотрим на примере добавления пользователя "admin@ald.company.lan" в группу пользователей "new_user_group" в домене ALD.COMPANY.LAN.

Рассмотрим лог из /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit.

Обратим внимание на следующие строки:

- dn: cn=new_user_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan - объект, который был изменен.
- changetype: modify - тип изменений, в данном случае мы изменили объект;
- modifiersname: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan - имя учетной записи, кто изменил объект;
- time: 20240815150019- время создания события.

Полный лог из /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit:

```
time: 20240815150019
dn: cn=new_user_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
result: 0
changetype: modify
add: member
member: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
-
replace: modifiersname
modifiersname: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
-
replace: modifytimestamp
modifytimestamp: 20240815120019Z
-
replace: entryusn
entryusn: 8867
```

Рассмотрим лог из /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access.

Обратим внимание на следующие параметры:

- 192.168.130.10 - IP контроллера домена;
- conn=20333 – номер подключения;
- MOD dn="cn=new_user_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan" - тип запроса MOD, в нашем случае изменили (modify) группу.

Полный лог из /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access:

```
[15/Aug/2024:15:00:19.037209493 +0300] conn=20333 fd=166 slot=166 SSL connection from
192.168.130.10 to 192.168.130.10
[15/Aug/2024:15:00:19.040006566 +0300] conn=20333 TLS1.3 128-bit AES-GCM
[15/Aug/2024:15:00:19.041298736 +0300] conn=20333 op=0 BIND dn="" method=sasl
version=3 mech=GSSAPI
[15/Aug/2024:15:00:19.042457987 +0300] conn=20333 op=0 RESULT err=14 tag=97 nentries=0
 wtime=0.003943245 optime=0.001162779 etime=0.005105210, SASL bind in progress
[15/Aug/2024:15:00:19.043581369 +0300] conn=20333 op=1 BIND dn="" method=sasl
version=3 mech=GSSAPI
[15/Aug/2024:15:00:19.044184152 +0300] conn=20333 op=1 RESULT err=14 tag=97 nentries=0
 wtime=0.000035523 optime=0.000605461 etime=0.000640099, SASL bind in progress
[15/Aug/2024:15:00:19.044343707 +0300] conn=20333 op=2 BIND dn="" method=sasl
version=3 mech=GSSAPI
[15/Aug/2024:15:00:19.045161770 +0300] conn=20333 op=2 RESULT err=0 tag=97 nentries=0
 wtime=0.000024906 optime=0.000819099 etime=0.000843358 dn="uid=admin,cn=users,cn=acc
ounts,dc=ald,dc=company,dc=lan"
[15/Aug/2024:15:00:19.045409794 +0300] conn=20333 op=3 MOD dn="cn=new_user_group,cn=g
roups,cn=accounts,dc=ald,dc=company,dc=lan"
[15/Aug/2024:15:00:19.121981924 +0300] conn=20333 op=3 RESULT err=0 tag=103 nentries=0
 wtime=0.000069236 optime=0.076573681 etime=0.076639202
[15/Aug/2024:15:00:19.122356040 +0300] conn=20333 op=4 UNBIND
[15/Aug/2024:15:00:19.122373584 +0300] conn=20333 op=4 fd=166 Disconnect - Cleanly
Closed Connection - U1
```

3.20 Событие 5141 A directory service object was deleted

Файл логов находятся на контроллере домена в двух каталогах:

- /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit;
- /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access.

Мы удалили группу пользователей "new_user_group" в домене ALD.COMPANY.LAN.

Рассмотрим лог из /var/log/dirsrv/slapd-ALD-COMPANY-LAN/audit.

Обратим внимание на следующие строки:

- dn: cn=new_user_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan - объект, который был удален;
- changetype: delete - тип изменений, в данном случае мы удалили объект;
- modifiersname: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan - имя учетной записи, кто удалил объект;
- time: 20240815153100- время создания события.

```
time: 20240815153100
dn: cn=new_user_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
result: 0
changetype: delete
modifiersname: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
```

Рассмотрим лог из /var/log/dirsrv/slapd-ALD-COMPANY-LAN/access.

Обратим внимание на следующие параметры:

- 192.168.130.10 - IP контроллера домена;

- conn=20509 – номер подключения;
- DEL dn="cn=new_user_group,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan" - тип запроса DEL, в нашем случае изменили (delete) группу.

```
[15/Aug/2024:15:30:53.797194615 +0300] conn=20509 fd=166 slot=166 SSL connection from
192.168.130.10 to 192.168.130.10
[15/Aug/2024:15:30:53.800064731 +0300] conn=20509 TLS1.3 128-bit AES-GCM
[15/Aug/2024:15:30:53.801638705 +0300] conn=20509 op=0 BIND dn="" method=sasl
version=3 mech=GSSAPI
[15/Aug/2024:15:30:53.802974696 +0300] conn=20509 op=0 RESULT err=14 tag=97 nentries=0
 wtime=0.004362976 optime=0.001341484 etime=0.005703781, SASL bind in progress
[15/Aug/2024:15:30:53.804205852 +0300] conn=20509 op=1 BIND dn="" method=sasl
version=3 mech=GSSAPI
[15/Aug/2024:15:30:53.804808843 +0300] conn=20509 op=1 RESULT err=14 tag=97 nentries=0
 wtime=0.000045256 optime=0.000591075 etime=0.000635737, SASL bind in progress
[15/Aug/2024:15:30:53.805020784 +0300] conn=20509 op=2 BIND dn="" method=sasl
version=3 mech=GSSAPI
[15/Aug/2024:15:30:53.805902884 +0300] conn=20509 op=2 RESULT err=0 tag=97 nentries=0
 wtime=0.000048233 optime=0.000885030 etime=0.000932610 dn="uid=admin,cn=users,cn=acc
ounts,dc=timur,dc=lan"
[15/Aug/2024:15:30:53.806196853 +0300] conn=20509 op=3 SRCH base="cn=new_user_group,c
n=groups,dc=ald,dc=company,dc=lan" scope=2 filter="(objectClass=*)" attrs="cn
distinguishedName gidNumber ipaUniqueID rbtadp rbtaou description objectClass"
[15/Aug/2024:15:30:53.806788285 +0300] conn=20509 op=3 RESULT err=0 tag=101 nentries=1
 wtime=0.000087190 optime=0.000592302 etime=0.000678554 notes=U details="Partially
Unindexed Filter"
[15/Aug/2024:15:31:00.750535920 +0300] conn=20509 op=4 EXT oid="1.3.6.1.4.1.4203.1.11
.3" name="whoami-plugin"
[15/Aug/2024:15:31:00.750603529 +0300] conn=20509 op=4 RESULT err=0 tag=120 nentries=0
 wtime=0.000148206 optime=0.000075041 etime=0.000221796
[15/Aug/2024:15:31:00.750834595 +0300] conn=20509 op=5 SRCH base="cn=new_user_group,c
n=groups,cn=accounts,dc=ald,dc=company,dc=lan" scope=2 filter="(objectClass=*)"
 attrs=ALL
[15/Aug/2024:15:31:00.753994368 +0300] conn=20509 op=5 RESULT err=0 tag=101 nentries=1
 wtime=0.000048864 optime=0.003158796 etime=0.003204983 notes=U details="Partially
Unindexed Filter" - entryLevelRights: vadn
[15/Aug/2024:15:31:00.754447604 +0300] conn=20509 op=6 DEL dn="cn=new_user_group,cn=g
roups,cn=accounts,dc=ald,dc=company,dc=lan"
[15/Aug/2024:15:31:00.835496619 +0300] conn=20509 op=6 RESULT err=0 tag=107 nentries=0
 wtime=0.000093366 optime=0.081050193 etime=0.081136877
```

3.21 Событие 5140 A network share object was accessed

События находятся на контроллере (файловом сервере) в файле /var/log/messages.

В данном примере мы с клиента 192.168.130.11 пользователем admin подключились к общей папке share1 на контроллере домена dc-1.

Нас интересует строчка:

```
Aug 16 14:31:33 dc-1 smbd_audit[18046]: admin|192.168.130.11|share1|connect|ok|share1
```

Полный лог:

```
Aug 16 14:31:33 dc-1 smbd_audit[18046]: admin|192.168.130.11|share1|connect|ok|share1
Aug 16 14:31:33 dc-1 smbd_audit[18046]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:31:33 dc-1 smbd_audit[18046]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1
Aug 16 14:31:33 dc-1 smbd_audit[18046]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1
Aug 16 14:31:33 dc-1 smbd_audit[18046]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:31:33 dc-1 smbd_audit[18046]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:31:33 dc-1 smbd_audit[18046]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1
Aug 16 14:31:33 dc-1 smbd_audit[18046]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1
```

3.22 Событие 5142 A network share object was added

События находятся на контроллере (файловом сервере) в файле /var/log/messages

В данном примере мы с клиента 192.168.130.11 пользователем admin подключились к общей папке share1 на контроллере домена dc-1 и создали файл file1.txt.

Подключение к общей папке:

```
Aug 16 14:40:42 dc-1 smbd_audit[19202]: admin|192.168.130.11|share1|connect|ok|share1
```

Создание файла file1.txt, присутствует операция overwrite_if:

```
Aug 16 14:40:48 dc-1 smbd_audit[19202]: admin|192.168.130.11|share1|create_file|ok|
0x120116|file|overwrite_if|/share1/file1.txt
Aug 16 14:40:48 dc-1 smbd_audit[19202]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:40:48 dc-1 smbd_audit[19202]: admin|192.168.130.11|share1|create_file|ok|
0x120116|file|open|/share1/file1.txt
```

Полный лог:

```
Aug 16 14:40:42 dc-1 smbd_audit[19202]: admin|192.168.130.11|share1|connect|ok|share1
Aug 16 14:40:42 dc-1 smbd_audit[19202]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:40:48 dc-1 smbd_audit[19202]: admin|192.168.130.11|share1|create_file|ok|
0x120116|file|overwrite_if|/share1/file1.txt
Aug 16 14:40:48 dc-1 smbd_audit[19202]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:40:48 dc-1 smbd_audit[19202]: admin|192.168.130.11|share1|create_file|ok|
0x120116|file|open|/share1/file1.txt
```

Ниже представлен лог создание каталога folder1. Присутсвтует операция mkdirat:

```
Aug 16 15:13:34 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|mkdirat|ok|/
share1/folder1
Aug 16 15:13:34 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|create|/share1/folder1
Aug 16 15:13:34 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/folder1
```

3.23 Событие 5143 A network share object was modified

События находятся на контроллере (файловом сервере) в файле /var/log/messages.

В данном примере мы с клиента 192.168.130.11 пользователем admin подключились к общей папке share1 на контроллере домена dc-1 и изменили файл file1.txt.

Подключение к общей папке:

```
Aug 16 14:48:51 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|connect|ok|share1
```

Изменение файла file1.txt:

```
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120116|file|overwrite_if|/share1/.file1.txt.kate-swp
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|unlinkat|ok|/
share1/.file1.txt.kate-swp
```

В данном случае мы даже можем увидеть, что изменение было внесено через приложение Kate, так как был создан временный скрытый файл .file1.txt.kate-swp, где содержится имя файла.

Но такое поведение зависит от текстового приложения. Например, LibreOffice свое имя не вписывает во временные файлы.

Здесь важно увидеть тип операций:

- overwrite_if - создание временного файла на запись;
- unlinkat - удаление временного файла, т.е. окончание записи, где мы нажали кнопку сохранить.

Полный лог:

```
Aug 16 14:48:51 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|connect|ok|share1
Aug 16 14:48:51 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:48:51 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:48:51 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1
```

```
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:52 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120116|file|overwrite_if|/share1/.file1.txt.kate-swp
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120116|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x100|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1
Aug 16 14:48:54 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
```

```
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120116|file|open|/share1/file1.txt
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x12019f|file|open|/share1/file1.txt
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x100|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x10000|file|open|/share1/.file1.txt.kate-swp
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|unlinkat|ok|/
share1/.file1.txt.kate-swp
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:48:57 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
```

Ниже представлен лог, когда мы просто открыли файл на чтение и закрыли его без изменений. Операции overwrite_if и unlinkat отсутствуют:

```
Aug 16 14:53:08 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:53:08 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
```

```
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:53:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1
```

В логе ниже представлена информация при изменении файла file1.txt, но уже в приложении LibreOffice:

```
Aug 16 14:55:50 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:55:50 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:55:51 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:55:51 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:55:53 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:55:53 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:55:56 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:55:58 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:55:58 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x12019f|file|open|/share1/file1.txt
Aug 16 14:55:58 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:55:58 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:55:58 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1
Aug 16 14:55:58 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120116|file|overwrite_if|/share1/.~lock.file1.txt#
Aug 16 14:55:58 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.~lock.file1.txt#
Aug 16 14:55:58 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x12019f|file|open|/share1/.~lock.file1.txt#
Aug 16 14:55:58 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.~lock.file1.txt#
```

```
Aug 16 14:55:58 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x100|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x10000|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|unlinkat|ok|/
share1/.~lock.file1.txt#
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120116|file|overwrite_if|/share1/lu306001myk94.tmp
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/lu306001myk94.tmp
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x12019f|file|open|/share1/lu306001myk94.tmp
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x12019f|file|open|/share1/lu306001myk94.tmp
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x12019f|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120116|file|overwrite_if|/share1/.~lock.file1.txt#
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x12019f|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/lu306001myk94.tmp
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/lu306001myk94.tmp
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x100|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x10000|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|unlinkat|ok|/
share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x10000|file|open|/share1/lu306001myk94.tmp
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|renameat|ok|/
share1/lu306001myk94.tmp|/share1/file1.txt
```

```
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x100|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x12019f|file|open|/share1/file1.txt
Aug 16 14:56:07 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x12019f|file|open|/share1/file1.txt
Aug 16 14:56:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:56:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 14:56:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x100|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|create_file|ok|
0x10000|file|open|/share1/.~lock.file1.txt#
Aug 16 14:56:09 dc-1 smbd_audit[20268]: admin|192.168.130.11|share1|unlinkat|ok|/
share1/.~lock.file1.txt#
```

Ниже представлен лог переименования каталога folder1 в folder2:

```
Aug 16 15:17:47 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|renameat|ok|/
share1/folder1|/share1/folder2
```

Мы видим операцию renameat:

```
Aug 16 15:17:36 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/folder1
Aug 16 15:17:36 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1/folder1
Aug 16 15:17:47 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/folder1
Aug 16 15:17:47 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/folder1
Aug 16 15:17:47 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x10000|file|open|/share1/folder1
Aug 16 15:17:47 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|renameat|ok|/
share1/folder1|/share1/folder2
```

```
Aug 16 15:17:47 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/folder2
```

Ниже представлен лог переименования файла file1 в file2:

```
Aug 16 15:20:14 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|renameat|ok|/
share1/file1.txt|/share1/file2.txt
```

Мы видим операцию renameat.

```
Aug 16 15:20:06 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 15:20:06 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 15:20:06 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 15:20:06 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 15:20:14 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 15:20:14 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 15:20:14 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x10000|file|open|/share1/file1.txt
Aug 16 15:20:14 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|renameat|ok|/
share1/file1.txt|/share1/file2.txt
Aug 16 15:20:14 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file2.txt
```

3.24 Событие 5144 A network share object was deleted

События находятся на контроллере (файловом сервере) в файле /var/log/messages.

В данном примере мы с клиента 192.168.130.11 пользователем admin подключились к общей папке share1 на контроллере домена dc-1 и удалили файл file1.txt.

Подключение к общей папке:

```
Aug 16 15:11:39 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|connect|ok|share1
```

Удаление файла file1.txt:

```
Aug 16 15:11:43 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|unlinkat|ok|/
share1/file1.txt
```

Здесь важно увидеть тип операций unlinkat - удаление файла.

Полный лог:

```
Aug 16 15:11:39 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|connect|ok|share1
Aug 16 15:11:39 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|dir|open|/share1
Aug 16 15:11:39 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 15:11:39 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 15:11:39 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 15:11:39 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x120089|file|open|/share1/file1.txt
Aug 16 15:11:42 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 15:11:43 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 15:11:43 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/file1.txt
Aug 16 15:11:43 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x100|file|open|/share1/file1.txt
Aug 16 15:11:43 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x10000|file|open|/share1/file1.txt
Aug 16 15:11:43 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|unlinkat|ok|/
share1/file1.txt
```

Ниже представлен лог удаление каталога folder1. Присутствует аналогичная операция unlinkat:

```
Aug 16 15:13:56 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|unlinkat|ok|/
share1/folder1
Aug 16 15:13:54 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/folder1
Aug 16 15:13:54 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1/folder1
Aug 16 15:13:55 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/folder1
Aug 16 15:13:56 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1/folder1
Aug 16 15:13:56 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x80|file|open|/share1/folder1
Aug 16 15:13:56 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x81|dir|open|/share1/folder1
Aug 16 15:13:56 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|create_file|ok|
0x10000|dir|open|/share1/folder1
Aug 16 15:13:56 dc-1 smbd_audit[23803]: admin|192.168.130.11|share1|unlinkat|ok|/
share1/folder1
```