

Заворотный Константин Александрович, студент РГУ нефти и газа (НИУ) им. И.М. Губкина, г. Москва

Трегубов Демид Евгеньевич, студент РГУ нефти и газа (НИУ) им. И.М. Губкина, г. Москва

ПОСТРОЕНИЕ ОТКАЗОУСТОЙЧИВОЙ СИСТЕМЫ ЦЕНТРАЛИЗОВАННОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ FREEIPA

В статье рассматривается построение отказоустойчивой системы аутентификации на базе FreeIPA для обеспечения непрерывности бизнес-процессов. Описана архитектура высокодоступного домена с применением многомастерной репликации, распределенных служб Kerberos и избыточного DNS. Проведено моделирование отказов узлов в среде ОС ALT Linux. Проверены механизмы защиты: LDAPS, TLS, алгоритмы Kerberos AES, ролевая модель доступа и GSS-TSIG. Результаты подтверждают эффективность конфигурации в минимизации простоев и обеспечении информационной безопасности. Полученные данные применимы при проектировании доменных решений в рамках стратегии импортозамещения.

The article examines the implementation of a fault-tolerant authentication system based on FreeIPA to ensure business continuity. It describes a high-availability domain architecture using multi-master replication, distributed Kerberos services, and redundant DNS. Failure modeling was conducted in the ALT Linux OS environment. Security mechanisms including LDAPS, TLS, Kerberos AES, RBAC, and GSS-TSIG were verified. The results confirm the configuration's effectiveness in minimizing downtime and ensuring information security. The findings are applicable for designing domain solutions within import substitution strategies.

Ключевые слова: FreeIPA, централизованная аутентификация, отказоустойчивость, Kerberos, LDAP.

Key words: FreeIPA, centralized authentication, fault-tolerance, Kerberos, LDAP.

Введение

Современные корпоративные инфраструктуры становятся всё более распределёнными, а количество сервисов, пользователей и точек доступа продолжает расти. В этих условиях надёжная система централизованной аутентификации играет ключевую роль в обеспечении безопасности и доступности информационных ресурсов. Нарушение работы доменной инфраструктуры приводит к полной недоступности сервисов, остановке бизнес-процессов и риску компрометации данных. Требования регуляторов (ФЗ-152, GDPR, PCI DSS) диктуют необходимость создания отказоустойчивых и защищённых систем управления доступом.

При использовании традиционных схем сервер аутентификации становится критически важной точкой отказа: сбой оборудования, потеря сетевой связности или целевая атака на каталог могут сделать невозможной работу всех сервисов, зависящих от домена. Это повышает актуальность разработки отказоустойчивых конфигураций, основанных на открытом программном обеспечении, которое при правильной настройке способно обеспечивать функциональность, сопоставимую с коммерческими решениями. Одним из таких комплексных решений является FreeIPA, объединяющая LDAP-каталог, Kerberos, DNS, инфраструктуру сертификатов и механизмы административного контроля.

Несмотря на широкое распространение FreeIPA, вопросы её поведения в условиях отказов, корректной работы механизмов многомастерной репликации, автоматического переключения клиентов и обеспеченности требований безопасности в практических сценариях остаются недостаточно исследованными. Это делает актуальной задачу экспериментальной проверки устойчивости и надёжности доменной инфраструктуры, построенной на базе

FreeIPA, особенно при использовании отечественных дистрибутивов, таких как ALT Linux.

Целью данного исследования является оценка отказоустойчивости и защищённости высокодоступной конфигурации FreeIPA при моделировании отказов ключевых сервисов домена

Объектом исследования выступают системы централизованной аутентификации в корпоративных Linux-инфраструктурах.

Предметом исследования является высокодоступная архитектура FreeIPA, включающая многомастерную репликацию каталога, распределённые сервисы Kerberos, избыточный DNS, защищённые каналы LDAPS, криптографические механизмы аутентификации и административные политики безопасности.

Практическая значимость работы заключается в оценке показателей готовности системы к отказам и проверке защитных механизмов (TLS, Kerberos, RBAC, DNS), что позволяет использовать результаты при проектировании защищённых корпоративных доменных решений на основе открытого ПО.

Литературный обзор

Централизованная аутентификация является одним из фундаментальных механизмов обеспечения информационной безопасности, и её теоретические основы подробно описаны в ряде международных стандартов и спецификаций. Архитектура и криптографическая модель современных систем идентификации базируются на стандартах RFC 4120 (Kerberos) и RFC 4510 (LDAP).

Практические аспекты построения комплексных решений управления доступом нашли отражение в документации FreeIPA и Red Hat Identity Management (IdM). Эти источники описывают интеграцию LDAP, Kerberos, сертификатов X.509, DNS-сервисов и политик безопасности в единую административную среду. Отдельное внимание уделяется механизму

многомастерной репликации, обеспечивающему поддержку распределённых топологий и высокую степень отказоустойчивости. Руководства по Multi-Master Replication, SSSD failover и DNS SRV-механизмам приводят детальные рекомендации по построению надёжной и масштабируемой инфраструктуры.

Анализ угроз (атаки на билеты, MITM, незашифрованные соединения) обосновывает необходимость применения в Kerberos и LDAP механизмов pre-authentication, LDAPS/TLS и строгих политик доступа.

С точки зрения операционной и нормативной практики особую роль играют требования стандартов и регуляторов — ФЗ-152, GDPR, PCI DSS, рекомендаций регуляторов по защите персональных данных. Эти документы определяют необходимость обеспечения непрерывности сервисов аутентификации, применения криптографических протоколов и защиты административных операций. В среде российских Linux-дистрибутивов практические руководства ALT Linux предоставляют рекомендации по настройке FreeIPA, DNS, Kerberos, TLS и политик аутентификации с учётом требований промышленной эксплуатации.

Таким образом, доступная литература и нормативные источники формируют широкую теоретическую и методическую основу для изучения механизмов аутентификации и построения отказоустойчивых инфраструктур. Однако большинство работ охватывают протоколы, архитектуры и методики защиты, в то время как практическая оценка отказоустойчивости конкретных реализаций — особенно в открытых системах — остаётся недостаточно представленной. Это определяет необходимость проведения экспериментального исследования устойчивости FreeIPA в реальных сценариях отказов и подтверждает актуальность настоящей работы.

Методы исследования

Исследование проводилось методом экспериментального моделирования в изолированной виртуализированной среде, построенной на базе дистрибутивов ALT Linux 11 (Server и Workstation). В экспериментальной инфраструктуре были развернуты два серверных узла FreeIPA,

функционирующих в режиме многомастерной репликации, и один клиентский узел, использующий динамическое обнаружение сервисов домена через SRV-записи DNS. Логическая схема используемой топологии представлена на рисунке 1.

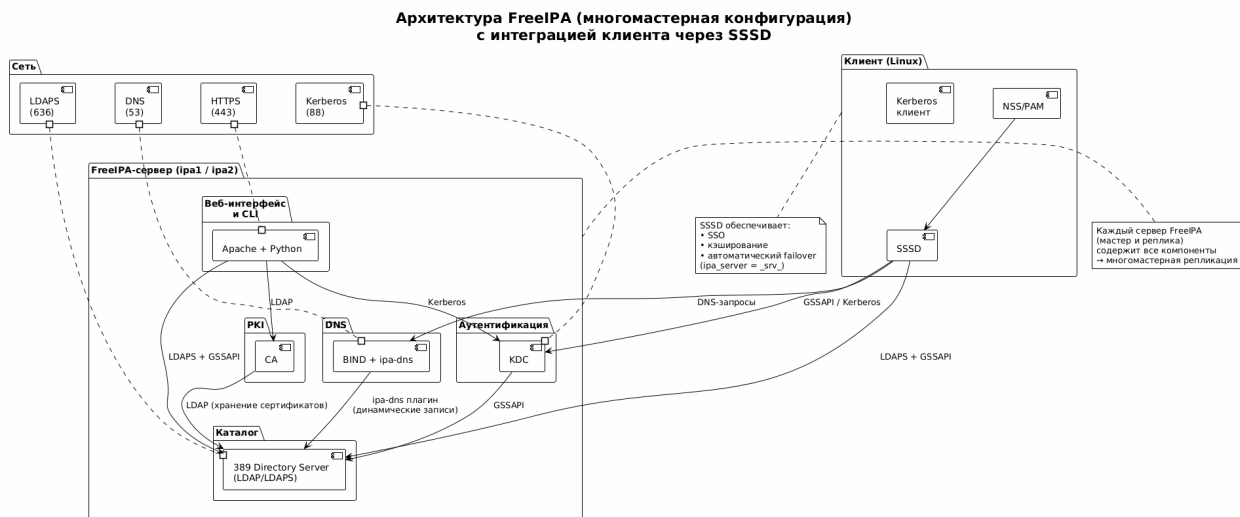


Рисунок 1 – Архитектура FreeIPA

Проверка корректности топологии выполнялась с помощью стандартных инструментов FreeIPA для просмотра репликационных сегментов.

Экспериментальная часть исследования включала моделирование нескольких типов отказов, типичных для корпоративной инфраструктуры: отключение мастер-сервера, недоступность DNS-службы, остановка KDC, временная потеря сетевой связности и проверка отказоустойчивости клиентского поведения при использовании механизма `_srv_`.

Отдельным направлением стала проверка мер безопасности (LDAPS, TLS, алгоритмы Kerberos, политики паролей, RBAC, GSS-TSIG) встроенными средствами FreeIPA и инструментами ALT Linux для оценки соответствия конфигурации установленным требованиям.

Результаты исследования

Экспериментальная оценка отказоустойчивости двухузловой системы FreeIPA показала, что механизмы многомастерной репликации, избыточности DNS и распределённых KDC обеспечивают высокую устойчивость службы

аутентификации к отказам отдельных узлов. Репликация данных каталога между мастер-сервером и репликой функционировала в обоих направлениях, что подтвердило корректность настройки и синхронизации пользовательских записей, политик доступа и сертификатов.

```
[root@ipa2 ~]# ipa user-add testuser --first=Test --last=User --password
Пароль:
Введите Пароль ещё раз для проверки:
-----
Добавлен пользователь "testuser"
-----
Имя учётной записи пользователя: testuser
Имя: Test
Фамилия: User
Полное имя: Test User
Отображаемое имя: Test User
Инициалы: TU
Домашний каталог: /home/testuser
GECOS: Test User
Оболочка входа: /bin/bash
Имя учётной записи: testuser@EXAMPLE.LOCAL
Псевдоним учётной записи: testuser@EXAMPLE.LOCAL
Окончание действия пароля пользователя: 20251116173042Z
Адрес электронной почты: testuser@example.local
UID: 162500500
ID группы: 162500500
Пароль: True
Участник групп: ipausers
Доступные ключи Kerberos: True

[root@ipa1 ~]# ipa user-show testuser
Имя учётной записи пользователя: testuser
Имя: Test
Фамилия: User
Домашний каталог: /home/testuser
Оболочка входа: /bin/bash
Имя учётной записи: testuser@EXAMPLE.LOCAL
Псевдоним учётной записи: testuser@EXAMPLE.LOCAL
Адрес электронной почты: testuser@example.local
UID: 162500500
ID группы: 162500500
Учётная запись отключена: False
Пароль: True
Участник групп: ipausers
Доступные ключи Kerberos: True
```

Рисунок 2 — Подтверждение корректной репликации данных между узлами FreeIPA.

В ходе экспериментов был проведён тест полного отключения мастер-узла. После искусственного прекращения работы сервера клиенты сохранили возможность аутентификации и продолжили получать информацию из домена без задержек.

До:

После:

```
[root@client1 ~]# kinit admin
Password for admin@EXAMPLE.LOCAL:
[root@client1 ~]# ipa user-find
-----
установлено соответствие 2 пользователей
-----
Имя учётной записи пользователя: admin
Фамилия: Administrator
Домашний каталог: /home/admin
Оболочка входа: /bin/bash
Имя учётной записи: admin@EXAMPLE.LOCAL
Псевдоним учётной записи: admin@EXAMPLE.LOCAL, root@EXAMPLE.LOCAL
UID: 162400000
ID группы: 162400000
Учётная запись отключена: False

Имя учётной записи пользователя: testuser
Имя: Test
Фамилия: User
Домашний каталог: /home/testuser
Оболочка входа: /bin/bash
Имя учётной записи: testuser@EXAMPLE.LOCAL
Псевдоним учётной записи: testuser@EXAMPLE.LOCAL
Адрес электронной почты: testuser@example.local
UID: 162500500
ID группы: 162500500
Учётная запись отключена: False
-----
Количество возвращённых записей 2

[root@client1 ~]# kinit admin
Password for admin@EXAMPLE.LOCAL:
[root@client1 ~]# ipa user-find
-----
установлено соответствие 2 пользователей
-----
Имя учётной записи пользователя: admin
Фамилия: Administrator
Домашний каталог: /home/admin
Оболочка входа: /bin/bash
Имя учётной записи: admin@EXAMPLE.LOCAL
Псевдоним учётной записи: admin@EXAMPLE.LOCAL, root@EXAMPLE.LOCAL
UID: 162400000
ID группы: 162400000
Учётная запись отключена: False

Имя учётной записи пользователя: testuser
Имя: Test
Фамилия: User
Домашний каталог: /home/testuser
Оболочка входа: /bin/bash
Имя учётной записи: testuser@EXAMPLE.LOCAL
Псевдоним учётной записи: testuser@EXAMPLE.LOCAL
Адрес электронной почты: testuser@example.local
UID: 162500500
ID группы: 162500500
Учётная запись отключена: False
-----
Количество возвращённых записей 2
```

Рисунок 3 — Работа клиента FreeIPA до и после отключения мастер-сервера.

Переключение на реплику происходило автоматически благодаря использованию SRV-записей Kerberos и LDAP, а также конфигурации клиента с динамическим поиском доступных серверов через srv-механизм SSSD.

Время восстановления обслуживания не превысило нескольких секунд, что соответствует требованиям к высокодоступным системам аутентификации.

```
[root@ipa2 ~]# dig @ipa1.example.local _kerberos._tcp.example.local SRV
; <<> DiG 9.18.41 <<> @ipa1.example.local _kerberos._tcp.example.local SRV
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 50985
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0f02d69e929f21cb01000000691a10d10dd7d3aa93f3c8ba (good)
;; QUESTION SECTION:
;_kerberos._tcp.example.local. IN SRV

;; ANSWER SECTION:
_kerberos._tcp.example.local. 86400 IN SRV 0 100 88 ipa2.example.local.
_kerberos._tcp.example.local. 86400 IN SRV 0 100 88 ipa1.example.local.

;; ADDITIONAL SECTION:
ipa1.example.local. 1200 IN A 192.168.10.10
ipa2.example.local. 1200 IN A 192.168.10.11

;; Query time: 2 msec
;; SERVER: 192.168.10.10#53(ipa1.example.local) (UDP)
;; WHEN: Sun Nov 16 20:58:41 MSK 2025
;; MSG SIZE rcvd: 193
```

Рисунок 4 — SRV-записи Kerberos, используемые клиентами для автоматического выбора доступного KDC.

Тестирование отказоустойчивого DNS также подтвердило корректность работы. При недоступности основного DNS-сервера клиенты успешно переключались на вторую зону, что обеспечило непрерывное разрешение имён для Kerberos, LDAP и внутренних сервисов FreeIPA. Работа SSSD-кэша позволила сохранить работоспособность механизма входа в систему даже при кратковременных потерях связи.

```
nameserver 192.168.10.10
nameserver 192.168.10.11
search example.local
```

Рисунок 5 — Конфигурация клиента с двумя DNS-серверами для обеспечения отказоустойчивости.

Анализ журналов подтвердил отсутствие конфликтов и целостность данных после восстановления мастер-сервера.

```
[root@ipa1 ~]# ipa topologysegment-find ca
-----
установлено соответствие 1 сегмента
-----
Имя сегмента: ipa1.example.local-to-ipa2.example.local
Левый узел: ipa1.example.local
Правый узел: ipa2.example.local
Возможность подключения: both
-----
Количество возвращённых записей 1
-----
```

Рисунок 6 — Состояние репликационных сегментов между серверами FreeIPA.

Анализ конфигурации FreeIPA показал, что служба LDAP доступна по защищённому порту 636.

```
[root@ipa1 ~]# ss -tlnp | grep 636
tcp LISTEN 0 128 *:636 *: users:(("ns-slapd",pid=1235,fd=9))
```

Рисунок 7 – Подтверждение слушания порта 636

Трафик-анализ подтвердил использование LDAPS: TLS-шифрование исключает перехват учетных данных в открытом виде.

No.	Time	Source	Destination	Protocol	Length	Info
56	25.313800846	192.168.10.20	192.168.10.10	ILSv1.3	571	Client Hello (SNI=ipa1.example.local)
58	25.367389020	192.168.10.10	192.168.10.20	ILSv1.3	3086	Server Hello, Change Cipher Spec, Application Data, App
60	25.368887311	192.168.10.20	192.168.10.10	ILSv1.3	134	Change Cipher Spec, Application Data
64	25.370164727	192.168.10.10	192.168.10.20	ILSv1.3	357	Application Data
68	25.370470977	192.168.10.10	192.168.10.20	ILSv1.3	357	Application Data
76	25.383337927	192.168.10.20	192.168.10.10	ILSv1.3	2536	Application Data
78	25.383459052	192.168.10.20	192.168.10.10	ILSv1.3	179	Application Data
82	26.808757612	192.168.10.10	192.168.10.20	ILSv1.3	1271	Application Data
83	26.808858529	192.168.10.10	192.168.10.20	ILSv1.3	96	Application Data
86	26.840794967	192.168.10.10	192.168.10.20	ILSv1.3	78	Application Data
91	27.075785902	192.168.10.20	192.168.10.10	ILSv1.3	571	Client Hello (SNI=ipa1.example.local)
93	27.081927107	192.168.10.10	192.168.10.20	ILSv1.3	3086	Server Hello, Change Cipher Spec, Application Data, App
95	27.082618523	192.168.10.20	192.168.10.10	ILSv1.3	134	Change Cipher Spec, Application Data
96	27.082708273	192.168.10.10	192.168.10.20	ILSv1.3	357	Application Data
97	27.082760815	192.168.10.20	192.168.10.10	ILSv1.3	612	Application Data
98	27.082812940	192.168.10.20	192.168.10.10	ILSv1.3	148	Application Data
101	27.091467726	192.168.10.10	192.168.10.20	ILSv1.3	357	Application Data
103	27.865302822	192.168.10.10	192.168.10.20	ILSv1.3	932	Application Data
105	27.866277988	192.168.10.10	192.168.10.20	ILSv1.3	96	Application Data
108	27.868330570	192.168.10.10	192.168.10.20	ILSv1.3	78	Application Data

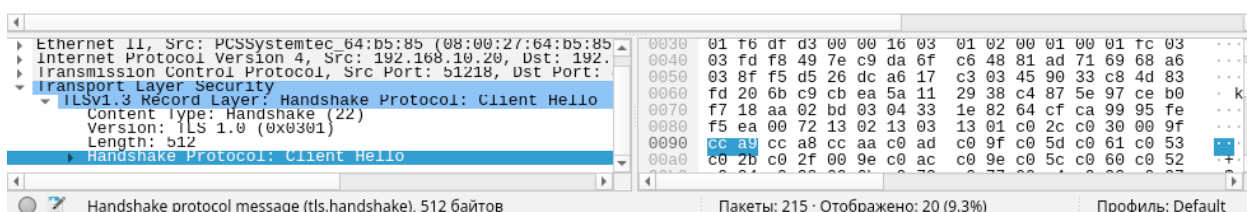


Рисунок 8 — Анализ трафика при нормальной работе клиента

Для подтверждения корректности настроек безопасности доменной инфраструктуры были проанализированы параметры Kerberos и LDAPS. Проверка показала, что KDC использует современные алгоритмы шифрования AES, для пользователей корректно применяется ролевая модель RBAC, максимальный срок жизни билета составляет один день, что соответствует рекомендациям по обеспечению безопасности, а LDAPS-сертификат

находится в состоянии MONITORING, что означает его автоматическое отслеживание и продление службой certmonger.

```
[root@ipal ~]# getcert list -d /etc/dirsrv/slapd-EXAMPLE-LOCAL/ -n Server-Cert
Number of certificates and requests being tracked: 9.
Request ID '20251116164602':
-----
status: MONITORING
stuck: no
key pair storage: type=NSSDB,location='/etc/dirsrv/slapd-EXAMPLE-LOCAL',nickname='Server-Cert',token='NSS Certificate DB',pinfile='/etc/dirsrv/slapd-EXAMPLE-LOCAL/pwdfile.txt'
certificate: type=NSSDB,location='/etc/dirsrv/slapd-EXAMPLE-LOCAL',nickname='Server-Cert',token='NSS Certificate DB'
CA: IPA
issuer: CN=Certificate Authority,0=EXAMPLE.LOCAL
subject: CN=ipal.example.local,0=EXAMPLE.LOCAL
issued: 2025-11-16 19:46:02 MSK
expires: 2027-11-17 19:46:02 MSK
dns: ipal.example.local
principal name: ldap/ipal.example.local@EXAMPLE.LOCAL
key usage: digitalSignature,nonRepudiation,keyEncipherment,dataEncipherment
eku: id-kp-serverAuth,id-kp-clientAuth
profile: caIPAServiceCert
pre-save command:
post-save command: /usr/libexec/ipa/certmonger/restart_dirsrv EXAMPLE-LOCAL
track: yes
auto-renew: yes
[root@ipal ~]#
```

Рисунок 9 — Подтверждение работы LDAPS и корректного TLS-сертификата FreeIPA

```
[root@ipal ~]# ipa krbtpolicy-show
Максимальный срок жизни: 86400
Максимальный срок для обновления: 604800
```

Рисунок 10 – Проверка сроков жизни билетов

```
[root@ipal ~]# ipa role-show "User Administrator"
Имя роли: User Administrator
Описание: Responsible for creating Users and Groups
Privileges: User Administrators, Group Administrators, Stage User Administrators, Subordinate ID Administrators
```

Рисунок 11 – Проверка роли User Administrator

```
[root@ipal ~]# cat /var/lib/kerberos/krb5kdc/kdc.conf | grep supported_encetypes
supported_encetypes = aes256-sha2:normal aes128-sha2:normal aes256-cts:normal aes128-cts:normal
```

Рисунок 12 — Разрешённые криптографические алгоритмы Kerberos

Проверка протокола Kerberos подтвердила корректный обмен сообщениями AS-REQ и AS-REP между клиентом и контроллером домена. Передача ключевого материала и служебных данных осуществляется в зашифрованном виде, что соответствует требованиям безопасной аутентификации.

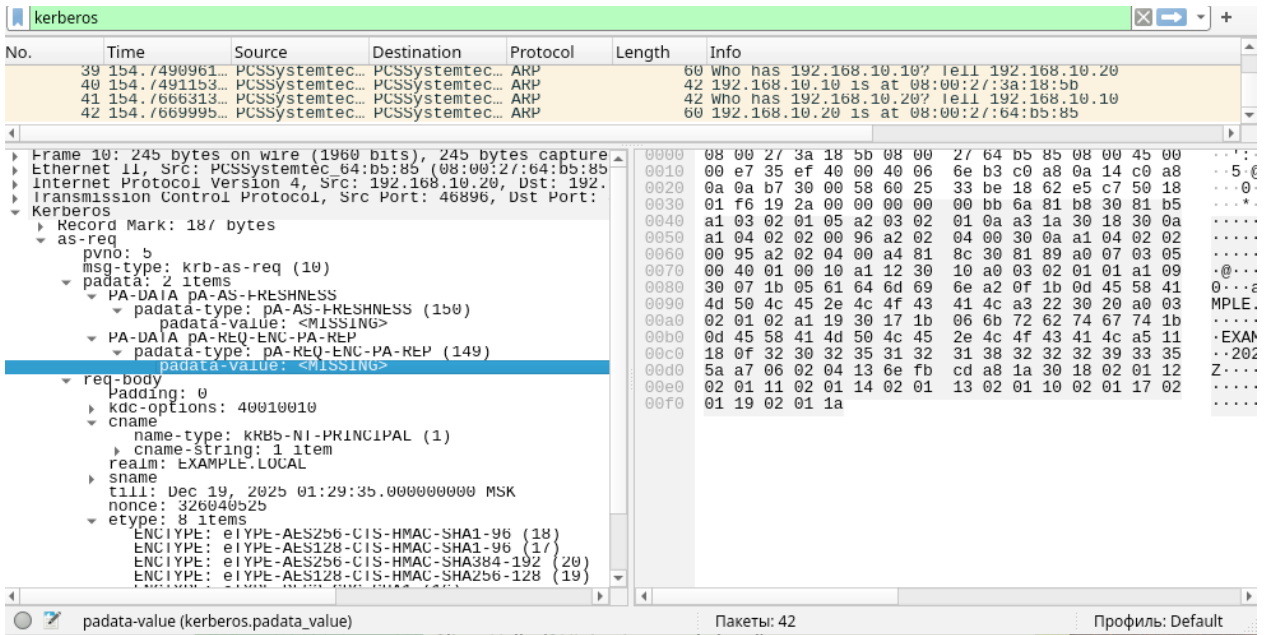


Рисунок 13 — Трафик Kerberos при kinit admin

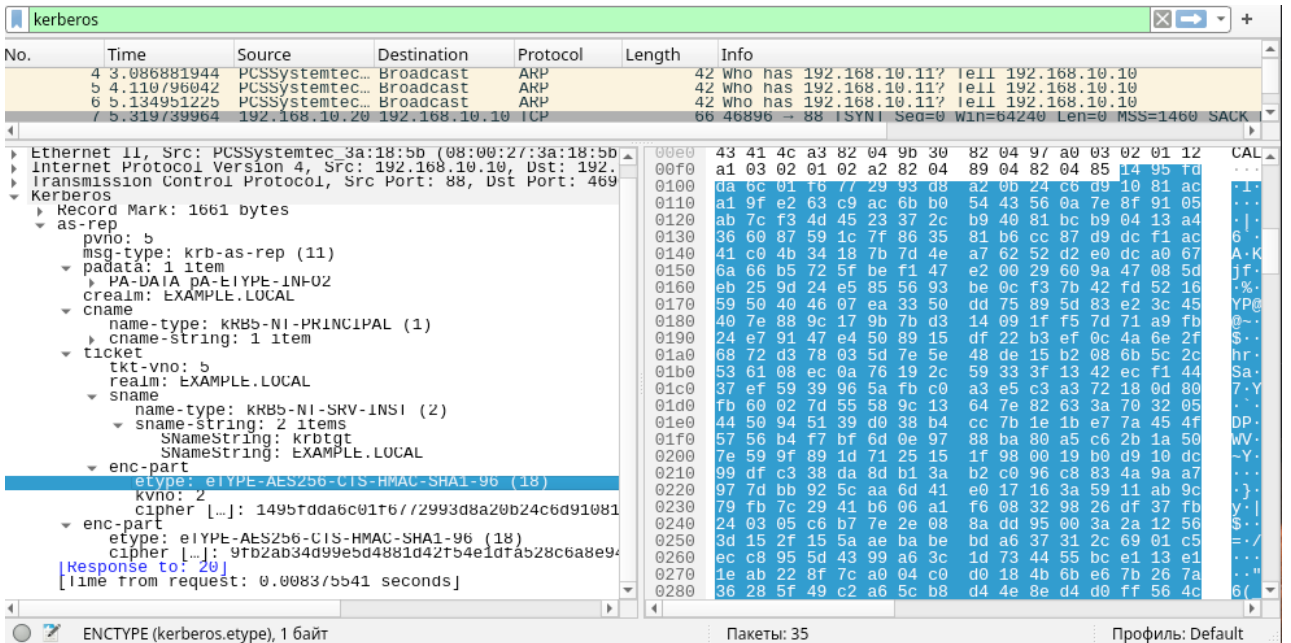


Рисунок 14 — Трафик Kerberos при kinit admin

Примененная политика паролей (длина, сложность, блокировка) минимизирует риски подбора и соответствует стандартам безопасности.

```
[root@ipa1 ~]# ipa pwpolicy-mod global_policy \
--maxlife=60 \
--minlife=24 --history=24 \
--minclasses=3 \
--minlength=12 \
--maxfail=3 \
--failinterval=60 \
--lockouttime=900 \
--grace=5
Группа: global_policy
Максимальный срок действия (в днях): 60
Минимальный срок действия (в часах): 24
Размер журнала : 24
Классы символов: 3
Минимальная длина: 12
Максимальное количество ошибок: 3
Интервал сброса ошибок: 60
Длительность блокировки: 900
Grace login limit: 5
```

Рисунок 15 — Настройки политики паролей FreeIPA

При попытках перебора паролей механизм аутентификации корректно реагирует на подозрительную активность. После превышения допустимого числа неудачных попыток входа учётная запись переводится в заблокированное состояние, а дальнейшие запросы аутентификации отклоняются сервером, что подтверждает эффективность защиты от атак типа brute force.

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of packets, with packet 83 highlighted in blue. The middle pane shows the details of this packet, which is a Kerberos error message (KRB5KDC_ERR_CLIENT_REVOKED) from the server to the client. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
73	5.813636030	192.168.10.10	192.168.10.20	TCP	54	88 → 36422 [ACK] Seq=157 Ack=193 Win=64128 Len=0
74	5.912741590	PCSSystemtec...	Broadcast	ARP	42	Who has 192.168.10.11? [ethII] 192.168.10.10
75	6.936915030	PCSSystemtec...	Broadcast	ARP	42	Who has 192.168.10.11? [ethII] 192.168.10.10
76	7.959539294	PCSSystemtec...	Broadcast	ARP	42	Who has 192.168.10.11? [ethII] 192.168.10.10
77	8.983882652	PCSSystemtec...	Broadcast	ARP	42	Who has 192.168.10.11? [ethII] 192.168.10.10
78	16.280588018	192.168.10.20	192.168.10.10	TCP	60	46904 → 88 [SYN] Seq=0 Win=0 MSS=1460
79	16.280616726	192.168.10.10	192.168.10.20	TCP	60	88 → 46904 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
80	16.280825019	192.168.10.20	192.168.10.10	TCP	60	46904 → 88 [ACK] Seq=1 Ack=1 Win=64256 Len=0
81	16.280825061	192.168.10.20	192.168.10.10	KRBS	245	AS-REQ
82	16.280846728	192.168.10.10	192.168.10.20	TCP	54	88 → 46904 [ACK] Seq=1 Ack=192 Win=64128 Len=0
83	16.282479488	192.168.10.10	192.168.10.20	KRBS	209	KRB Error: KRB5KDC_ERR_CLIENT_REVOKED
84	16.282603156	192.168.10.10	192.168.10.20	TCP	54	88 → 46904 [FIN, ACK] Seq=156 Ack=192 Win=64128 Len=0
85	16.282997325	192.168.10.20	192.168.10.10	TCP	60	46904 → 88 [ACK] Seq=192 Ack=156 Win=64128 Len=0
86	16.283032867	192.168.10.20	192.168.10.10	TCP	60	46904 → 88 [FIN, ACK] Seq=192 Ack=157 Win=64128 Len=0
87	16.283038034	192.168.10.10	192.168.10.20	TCP	54	88 → 46904 [ACK] Seq=157 Ack=193 Win=64128 Len=0
88	29.00717175	192.168.10.20	192.168.10.10	NIP	90	NIP Version 4, client
89	29.007488134	192.168.10.10	192.168.10.20	NIP	90	NIP Version 4, server
90	60.901667221	fe80::68ca:c...::1	fc00::1	ICMPv6	118	Router Advertisement from 6a:ca:c4:1b:f2:64
91	94.043519438	192.168.10.20	192.168.10.10	NIP	90	NIP Version 4, client
92	94.043647856	192.168.10.10	192.168.10.20	NIP	90	NIP Version 4, server
93	99.334169240	PCSSystemtec...	PCSSystemtec...	ARP	60	Who has 192.168.10.10? [ethII] 192.168.10.20

Рисунок 16 — Анализ брутфорс атаки на Kerberos

Проверка механизма защиты DNS показала, что зона example.local защищена с помощью GSS-TSIG. Это исключает возможность внесения

изменений в DNS-записи неавторизованными клиентами и предотвращает атаки подмены записей.

```
[root@ipal ~]# ipa dnszone-show example.local
Имя зоны: example.local.
Активная зона: True
Полномочный сервер имён: ipal.example.local.
Адрес электронной почты администратора: hostmaster.example.local.
Номер SOA: 1764935309
Обновление SOA: 3600
Повторный запрос SOA: 900
Окончание действия SOA: 1209600
Минимальный срок жизни SOA: 3600
Политика обновления BIND: grant EXAMPLE.LOCAL krb5-self * A; grant EXAMPLE.LOCAL krb5-self * AAAA; grant EXAMPLE.LOCAL
krb5-self * SSHFP;
Динамическое обновление: True
Разрешить запрос: any;
Разрешить перенос: none;
```

Рисунок 17 — Состояние DNS-зоны example.local

No.	Time	Source	Destination	Protocol	Length	Info
4	5.302401421	PCSSystemtec...	PCSSystemtec...	ARP	42	192.168.10.10 is at 08:00:27:3a:18:5b
5	5.321135959	PCSSystemtec...	PCSSystemtec...	ARP	42	Who has 192.168.10.20? tell 192.168.10.10
6	5.321671004	PCSSystemtec...	PCSSystemtec...	ARP	60	192.168.10.20 is at 08:00:27:64:b5:85
7	9.090744179	192.168.10.20	192.168.10.20	NBNS	92	Name query NB SAMBA<id>
8	9.090941805	192.168.10.10	192.168.10.20	NBNS	104	Name query response NB 192.168.10.10
9	9.091035306	192.168.10.20	192.168.10.20	NBNS	104	Name query response NB 192.168.10.10
10	30.076237156	192.168.10.20	192.168.10.10	DNS	78	Standard query 0x3e55 SOA take.example.local
11	30.084603918	192.168.10.10	192.168.10.20	DNS	130	Standard query response 0x3e55 No such name SOA
12	30.085211214	192.168.10.20	192.168.10.10	DNS	94	Dynamic update 0x238b SOA example.local A 1.2.3
13	30.088238817	192.168.10.10	192.168.10.20	DNS	73	Dynamic update response 0x238b Refused SOA exam
14	34.612673979	fe80::68ca:c... ff02::1	ff02::1	ICMPv6	118	Router Advertisement from 6a:ca:c4:1b:f2:64
15	35.510449140	PCSSystemtec...	PCSSystemtec...	ARP	60	Who has 192.168.10.10? tell 192.168.10.20
16	35.510533891	PCSSystemtec...	PCSSystemtec...	ARP	42	192.168.10.10 is at 08:00:27:3a:18:5b
17	35.528532716	PCSSystemtec...	PCSSystemtec...	ARP	42	Who has 192.168.10.20? tell 192.168.10.10
18	35.528791259	PCSSystemtec...	PCSSystemtec...	ARP	60	192.168.10.20 is at 08:00:27:64:b5:85
19	55.024808525	PCSSystemtec...	broadcast	ARP	42	Who has 192.168.10.11? tell 192.168.10.10
20	56.073474707	PCSSystemtec...	broadcast	ARP	42	Who has 192.168.10.11? tell 192.168.10.10
21	57.096501432	PCSSystemtec...	broadcast	ARP	42	Who has 192.168.10.11? tell 192.168.10.10
22	58.121483044	PCSSystemtec...	broadcast	ARP	42	Who has 192.168.10.11? tell 192.168.10.10
23	59.145126314	PCSSystemtec...	broadcast	ARP	42	Who has 192.168.10.11? tell 192.168.10.10
24	60.168431373	PCSSystemtec...	broadcast	ARP	42	Who has 192.168.10.11? tell 192.168.10.10

Domain Name System (response)
Transaction ID: 0x238b
Flags: 0xa805 Dynamic update response, Refused
1... = Response: Message is a response
010 1... = Opcode: Dynamic update (5)
... 0... = Authoritative: Server is not authoritative
... 0... = Truncated: Message is not truncated
... 0... = Recursion desired: Don't do recursion
... 0... = Recursion available: Server does not support recursion
... 0... = Answer authenticated: Answer is authenticated
... 0... = Non-authenticated data: Unauthenticated data
... 0101 = Reply code: Refused (5)
Zones: 1
Prerequisites: 0
Updates: 0
Additional RRs: 0
Zone
example.local: type SOA, class IN
Name: example.local
[Name Length: 13]
[Label Count: 2]
type: SOA (6) (Start of a zone or Authority)

Рисунок 18 — Анализ трафика при попытке DNS-spoofing

Результаты тестирования, включая анализ сетевого трафика, подтвердили корректную работу механизмов защиты — TLS/LDAPS, криптографических алгоритмов Kerberos, ролевого разграничения прав, политик паролей и защиты DNS-зоны, что свидетельствует о соответствии предложенной конфигурации современным требованиям информационной безопасности.

Заключение

Экспериментальные результаты показали, что двухузловая конфигурация с многомастерной репликацией обеспечивает непрерывность процессов аутентификации при недоступности одного из узлов, переключение клиентов происходит автоматически, а потеря данных отсутствует.

Дополнительно проведённая проверка мер безопасности, в том числе с использованием анализа сетевого трафика, продемонстрировала корректность применения защищённого канала LDAPS, использование современных криптографических алгоритмов Kerberos, работу усиленных политик паролей и защиту DNS-зоны с использованием GSS-TSIG. Это подтверждает, что предложенная архитектура обеспечивает не только отказоустойчивость, но и соответствие актуальным требованиям информационной безопасности и промышленной эксплуатации.

Таким образом, полученные данные могут быть использованы при разработке и внедрении доменных решений на базе открытого программного обеспечения, а также служить основой для дальнейших исследований масштабируемости, распределённых топологий и интеграции с внешними системами федерации идентичности.

Список использованных источников

1. FreeIPA в ОС ALT Linux: установка сервера, настройка репликации и клиентской части [Электронный ресурс] // ALT Linux Wiki. – URL: <https://www.altlinux.org/FreeIPA> (дата обращения: 17.11.2025).
2. FreeIPA Project Documentation: Multi-Master Replication, Backup and Restore [Electronic resource] // FreeIPA Project Official Website. – URL: <https://www.freeipa.org/page/Documentation> (дата обращения: 17.11.2025).
3. Man-страницы ipa-server-install, ipa-replica-install, ipa-backup [Электронный ресурс] // Linux man pages online. — Режим доступа: <https://man7.org/linux/man-pages/>. — Дата обращения: 17.11.2025.
4. SSSD Configuration — ipa_server parameter [Электронный ресурс] // SSSD Documentation. — Режим доступа:

https://sssd.io/docs/design_pages/ipa_failover.html. — Дата обращения:
17.11.2025.

5. RFC 4120: Kerberos V5 / RFC 4510: LDAP Technical Specification [Electronic resource] // IETF Datatracker. – URL: <https://datatracker.ietf.org/> (дата обращения: 17.11.2025).

6. ЦИФРОВЫЕ ДВОЙНИКИ СЕТЕВЫХ ИНФРАСТРУКТУР: ТОЧНОСТЬ, МЕТОДЫ И ПРАКТИЧЕСКИЕ РЕШЕНИЯ Уймин А.Г. Радиотехнические и телекоммуникационные системы. 2023. № 3 (51). С. 44-52.