



Федеральное государственное автономное образовательное учреждение высшего образования «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина»

Факультет комплексной безопасности ТЭК



Ролевой доступ в решении РЕД Виртуализация. Интеграция с внешними каталогами.

Выполнил: Лазорин Д.С., группа КС-21-04.



Цель курсовой работы

Исследование модели ролевого доступа, интегрированной с внешним каталогом FreeIPA, для платформы виртуализации РЕД Виртуализация с целью повышения уровня безопасности и управления правами пользователей.



Задачи курсовой работы

1. Провести анализ предметной области.
2. Изучить модели ролевого доступа в РЕД Виртуализация.
3. Провести настройку стенда для проведения эксперимента.
4. Провести интеграцию внешнего каталога с системой РЕД Виртуализация.



Анализ предметной области

Научные исследования доказывают эффективность интеграций систем управления доступом с внешними каталогами на основе LDAP.

Позволяет осуществлять централизованное управление уз ПП, упрощать администрирование и масштабируемых инфраструктурах.



Обзор программного решения

РЕД Виртуализация – это система управления виртуальными машинами, которая работает через удобный веб-интерфейс и использует библиотеку libvirt в качестве основного инструмента администрирования.

Обзор программного решения

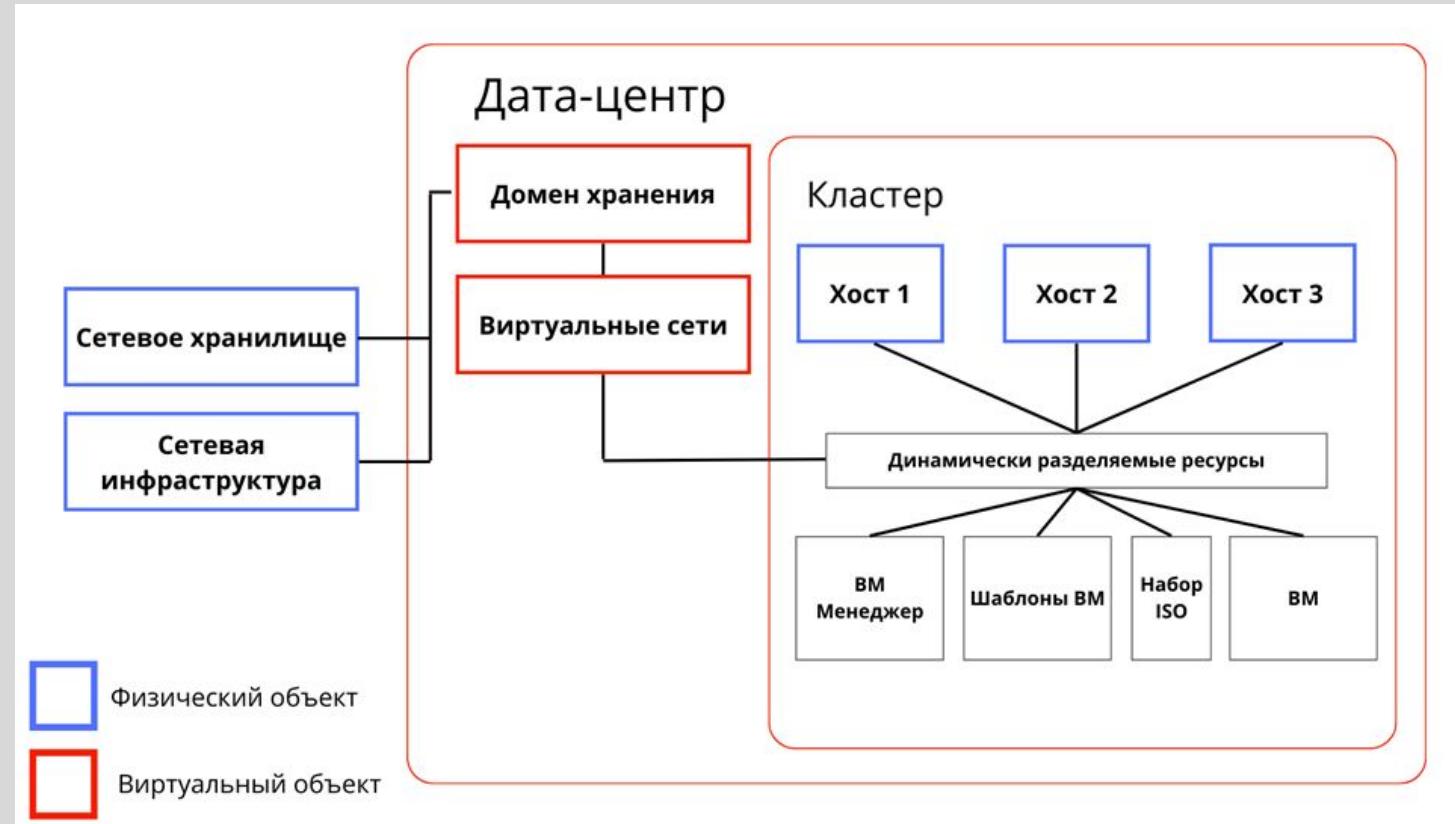


Рисунок 1 – Архитектура системы РЕД Виртуализация



Обзор программного решения

Роли и разрешения определяют возможности пользователя в системе. Многоуровневое администрирование позволяет выстроить подробную иерархию прав доступа.



Обзор программного решения

В этом случае один пользователь может иметь доступ к работе с конкретной виртуальной машиной без права изменять ее настройки, в то время как другому могут быть назначены системные права для внесения изменений в конфигурацию этой виртуальной машины.



Обзор программного решения

В таблицу 1 вынесены основные роли администратора.

Роль	Привилегии	Описание
SuperUser	Системный администратор среды РЕД Виртуализация	Имеет полные разрешения на все объекты и уровни, может управлять всеми объектами во всех центрах обработки данных



Обзор программного решения

Роль	Привилегии	Описание
ClusterAdmin	Администратор кластера	Обладает правами администратора для всех объектов в определённом кластере
DataCenter Admin	Администратор дата-центра	Обладает правами администратора для всех объектов в определённом центре обработки данных, за исключением хранилища



Обзор программного решения

Управление учётными записями во внутреннем домене РЕД Виртуализация необходимо использовать инструмент командной строки **ovirt-aaa-jdbc-tool**.



Практическая часть

В рамках подготовки к проведению эксперимента в качестве внешнего сервера каталогов было решено использовать FreeIPA.

Данное решение представляет собой комплексную систему управления идентификацией в инфраструктурах Linux, включающую в себя LDAP-каталог, Kerberos, DNS и центр сертификации. FreeIPA будет установлен на ALT Linux.



Практическая часть

На рисунке 6 представлена схема стенда, которая использовалась в курсовой работе.

Практическая часть

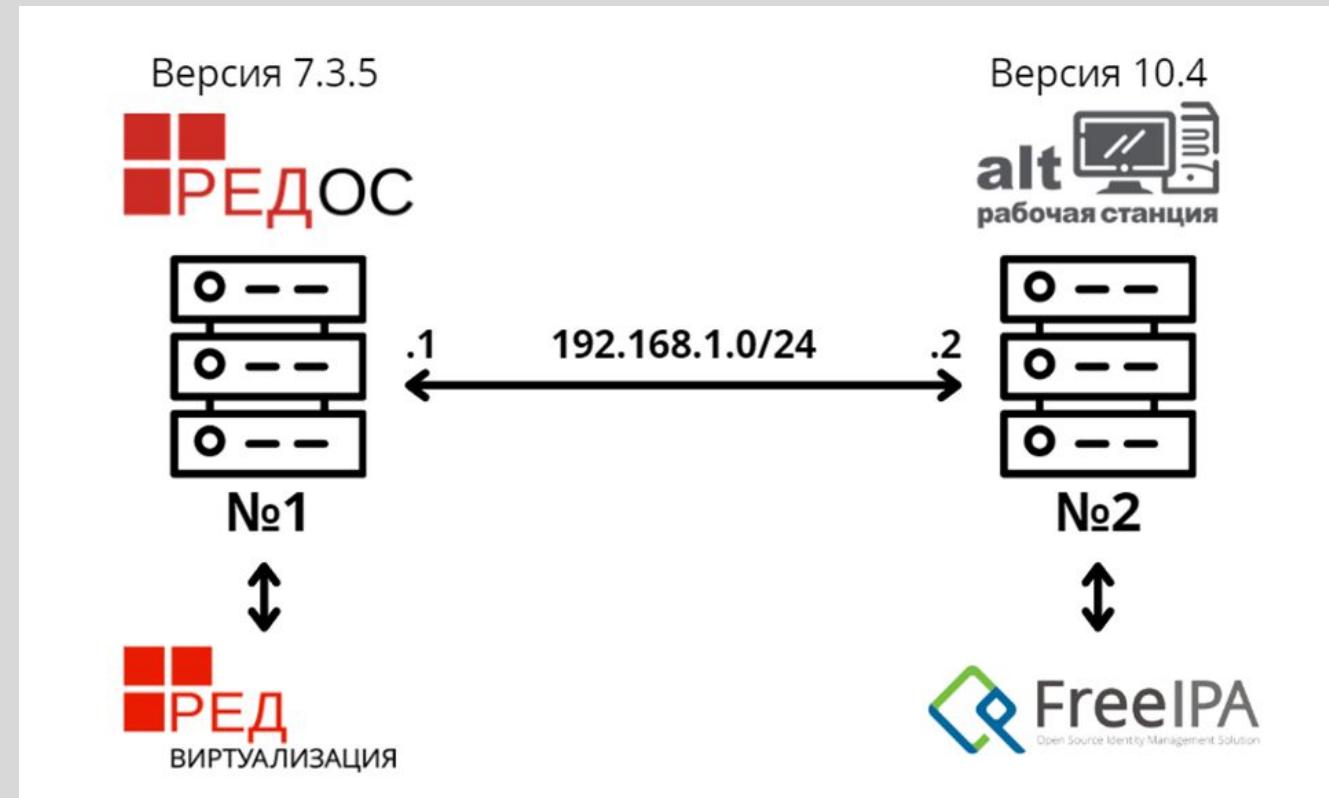


Рисунок 2 – Схема стенда в курсовой работе



Практическая часть

```
[root@vm1 ~]# ipa-server-install --setup-dns --no-dnssec-validation --allow-zone-overlap --reverse-zone=192.168.1.in-addr.arpa --skip-mem-check
```

Рисунок 3 – Результат начала установки FreeIPA

```
NetBIOS domain name [RED]:  
  
Do you want to configure CHRONY with NTP server or pool address? [no]: no  
  
The IPA Master Server will be configured with:  
Hostname: vm1.red.test  
IP address(es): 192.168.1.2  
Domain name: red.test  
Realm name: RED.TEST  
  
The CA will be configured with:  
Subject DN: CN=Certificate Authority,O=RED.TEST  
Subject base: O=RED.TEST  
Chaining: self-signed  
  
BIND DNS server will be configured to serve IPA domain with:  
Forwarders: 10.0.2.3, 8.8.8.8  
Forward policy: only  
Reverse zone(s): 192.168.1.in-addr.arpa., 1.168.192.in-addr.arpa.  
  
Continue to configure the system with these values? [no]: yes
```

Рисунок 4 – Результат установки FreeIPA

Практическая часть

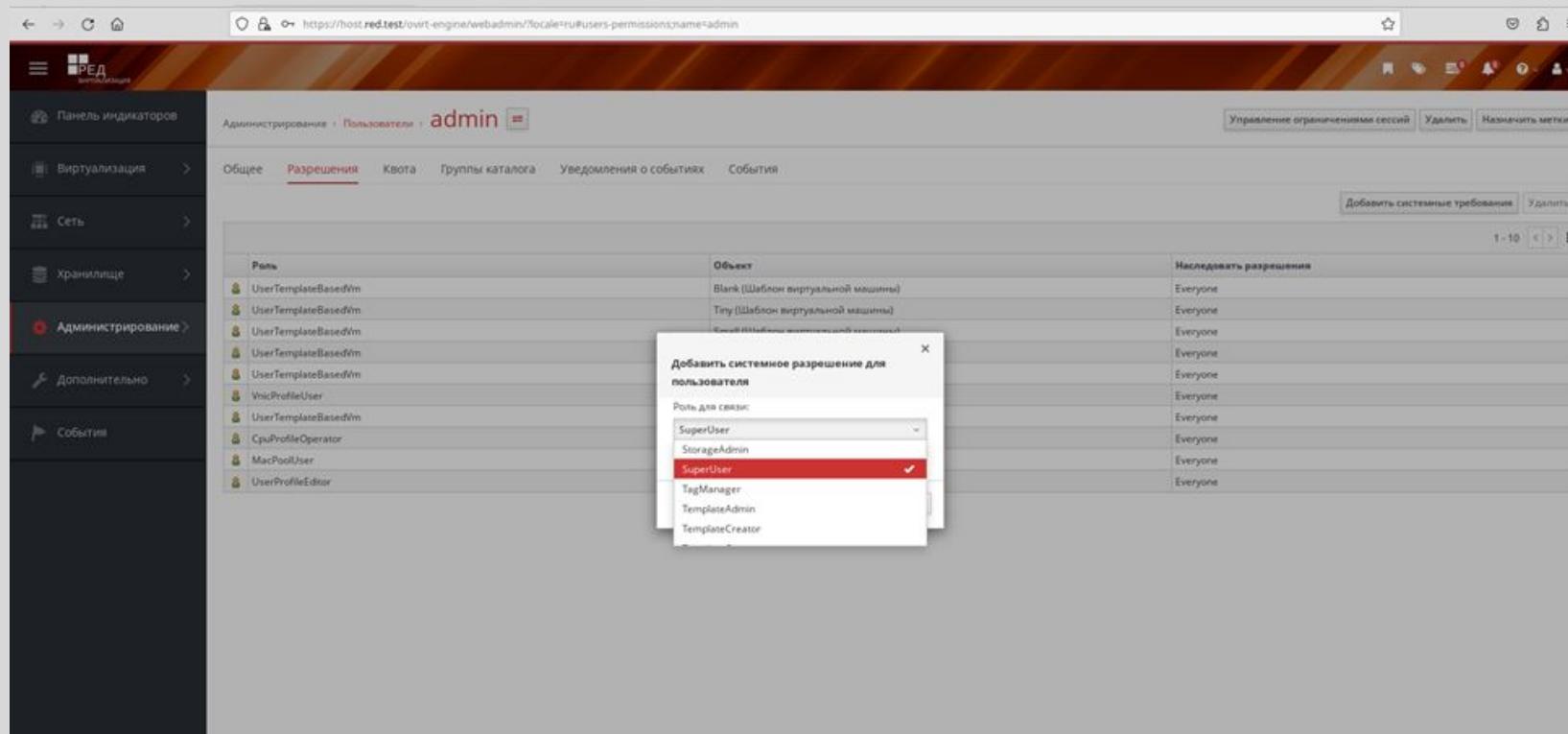


Рисунок 5 – Результат назначения системного разрешения

Практическая часть

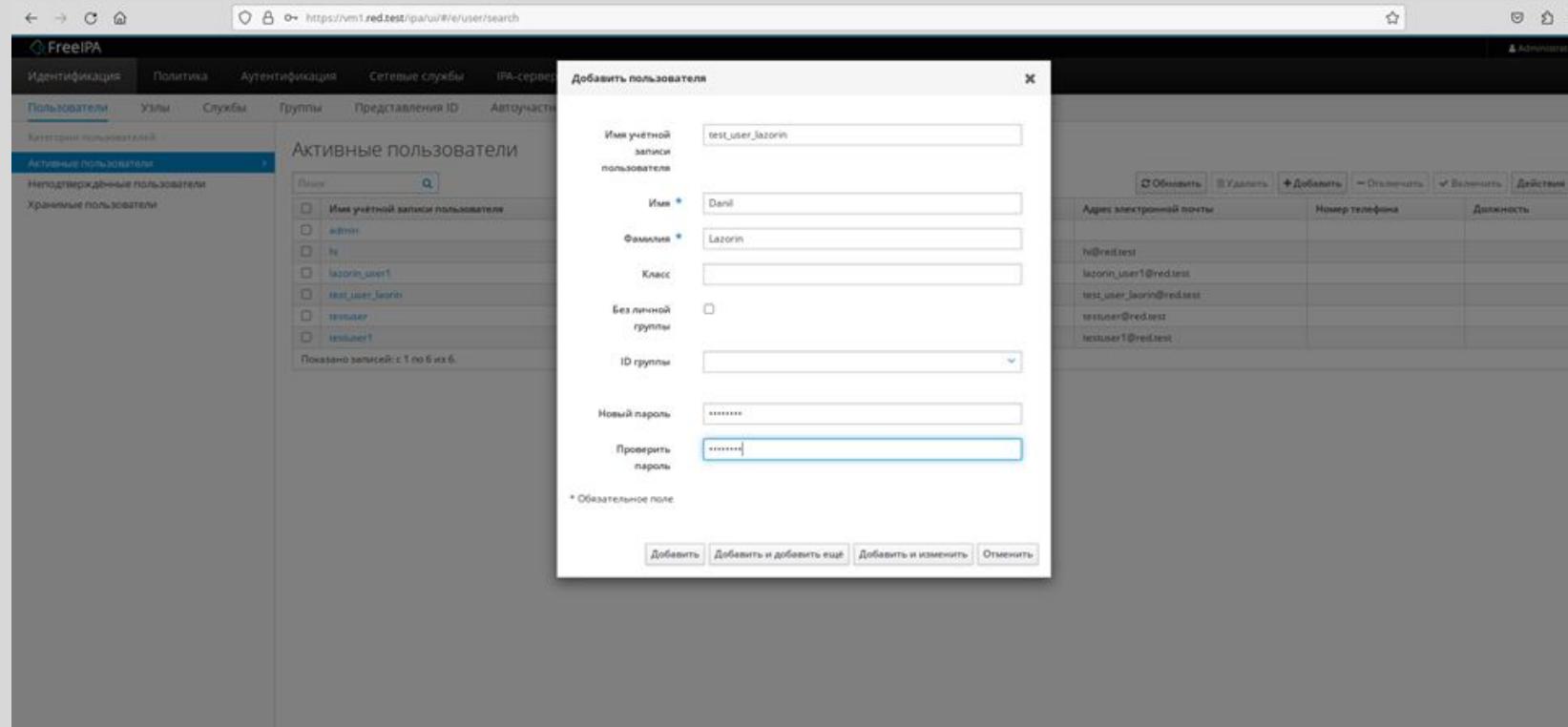


Рисунок 6 – Результат создания пользователя через FreeIPA

Практическая часть

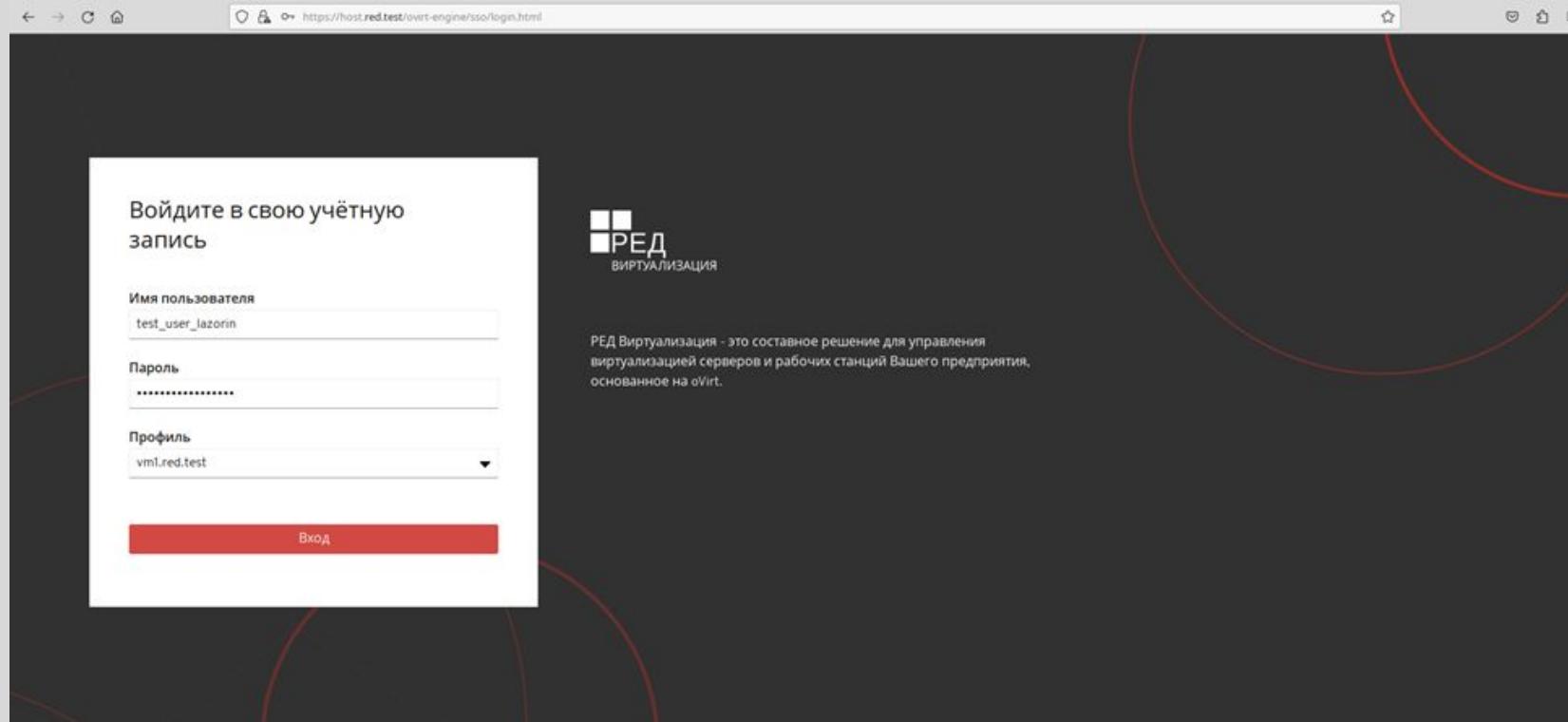


Рисунок 7 – Результат авторизации в системе РЕД Виртуализация



Практическая часть

44	5.841292986	192.168.1.1	192.168.1.2	LDAP	346 searchRequest(3) "dc=red,dc=test" wholeSubtree
46	5.857997037	192.168.1.2	192.168.1.1	LDAP	344 searchResEntry(3) "uid=admin,cn=users,cn=accounts,dc=red,dc=test"
47	5.858599196	192.168.1.2	192.168.1.1	LDAP	105 searchResDone(3) success [1 result]
50	5.875972570	192.168.1.1	192.168.1.2	LDAP	121 bindRequest(3) "uid=admin,cn=users,cn=accounts,dc=red,dc=test" simple
52	5.944343813	192.168.1.2	192.168.1.1	LDAP	68 bindResponse(3) success
54	5.950350425	192.168.1.1	192.168.1.2	LDAP	86 extendedReq(4) LDAP_SERVER_WHO_AM_I_OID

Рисунок 8 – Результат захваченных пакетов с помощью Wireshark

Практическая часть

```
▶ Transmission Control Protocol, Src Port: 39310, Dst Port: 389, Seq: 1, Ack: 1, Len: 306
- Lightweight Directory Access Protocol
  ▶ LDAPMessage searchRequest(3) "dc=red,dc=test" wholeSubtree
    messageID: 3
  ▶ protocolOp: searchRequest (3)
    ▶ searchRequest
      baseObject: dc=red,dc=test
      scope: wholeSubtree (2)
      derefAliases: neverDerefAliases (0)
      sizeLimit: 0
      timeLimit: 0
      typesOnly: False
    ▶ Filter: (&(&(objectClass=person)(ipaUniqueID=*)))(uid=admin@vm1.red.test))
    ▶ attributes: 13 items
  [Response In: 42]
- controls: 1 item
  ▶ Control
    controlType: 1.2.840.113556.1.4.319 (LDAP_PAGED_RESULT_OID_STRING)
  ▶ SearchControlValue
    size: 100
    cookie: <MISSING>
```

Рисунок 9 – Результат анализа пакета протокола LDAP

Практическая часть

```
▶ Filter: (&(&(objectClass=person)(ipaUniqueID=*)))(uid=admin@vm1.red.test))
- attributes: 13 items
    AttributeDescription: ipaUniqueID
    AttributeDescription: uid
    AttributeDescription: cn
    AttributeDescription: displayName
    AttributeDescription: department
    AttributeDescription: givenName
    AttributeDescription: sn
    AttributeDescription: title
    AttributeDescription: mail
    AttributeDescription: krbpasswordexpiration
    AttributeDescription: krbLastFailedAuth
    AttributeDescription: krbLoginFailedCount
    AttributeDescription: krbLoginFailedCount
```

Рисунок 10 – Результат анализа пакета протокола LDAP

Практическая часть

```
> Transmission Control Protocol, Src Port: 389, Dst Port: 39360, Seq: 1, Ack: 293, Len: 290
-> Lightweight Directory Access Protocol
  -> LDAPMessage searchResEntry(3) "uid=admin,cn=users,cn=accounts,dc=red,dc=test" [1 result]
    messageID: 3
    -> protocolOp: searchResEntry (4)
      -> searchResEntry
        objectName: uid=admin,cn=users,cn=accounts,dc=red,dc=test
        -> attributes: 7 items
          -> PartialAttributeList item ipaUniqueID
            type: ipaUniqueID
            -> vals: 1 item
              > vals: 1 item
          -> PartialAttributeList item uid
            type: uid
            -> vals: 1 item
              AttributeValue: admin
          -> PartialAttributeList item cn
            type: cn
            -> vals: 1 item
              AttributeValue: Administrator
          -> PartialAttributeList item sn
            type: sn
            -> vals: 1 item
              AttributeValue: Administrator
          -> PartialAttributeList item krbpasswordexpiration
            type: krbpasswordexpiration
            -> vals: 1 item
              AttributeValue: 20260127203028Z
          -> PartialAttributeList item krbLastFailedAuth
            type: krbLastFailedAuth
            -> vals: 1 item
              AttributeValue: 20251030005915Z
          -> PartialAttributeList item krbLoginFailedCount
            type: krbLoginFailedCount
            -> vals: 1 item
              AttributeValue: 0
[Response to: 44]
[Time: 0.016704051 seconds]
```

Рисунок 11 – Результат анализа пакета протокола LDAP

Практическая часть

```
▶ Transmission Control Protocol, Src Port: 389, Dst Port: 39360, Seq: 291, Ack: 293, Len: 51
└ Lightweight Directory Access Protocol
    └ LDAPMessage searchResDone(3) success [1 result]
        messageID: 3
        protocolOp: searchResDone (5)
            searchResDone
                resultCode: success (0)
                matchedDN: <MISSING>
                errorMessage: <MISSING>
                [Response To: 44]
                [Time: 0.017306210 seconds]
            controls: 1 item
                Control
                    controlType: 1.2.840.113556.1.4.319 (LDAP_PAGED_RESULT_OID_STRING)
                    SearchControlValue
                        size: 0
                        cookie: <MISSING>
```

Рисунок 12 – Результат анализа пакета протокола LDAP



Заключение.

1. Успешно реализованы этапы интеграции РЕД Виртуализация с внешним каталогом FreeIPA.
2. Обеспечена корректная авторизация пользователей и распределение прав доступа к вычислительным ресурсам виртуальной среды.
3. Проведена проверка пакетов протокола LDAP с помощью утилиты Wireshark.