BASIS

Программное обеспечение «Виртуальные рабочие столы «Тионикс». Руководство по эксплуатации

RU.НРФЛ.00001-01.97.01

Москва

01/18/2023

Содержание

1 Аннотация

Настоящий документ предназначен для технического администратора ПО и содержит инструкции по выполнению работ, необходимых для эксплуатации ПО.

2 Назначение руководства

Настоящее руководство по техническому обслуживанию содержит инструкции по выполнению следующих работ:

- сопровождение и обслуживание ПО;
- диагностику, локализацию и устранение проблем.

3 Перечень эксплуатационных документов

Дополнительно к настоящему документу технические администраторы должны использовать следующие документы:

- «ПО «Виртуальные рабочие столы «Тионикс». Руководство по установке. RU.НРФЛ.00001-01.96.01;
- «ПО «Виртуальные рабочие столы «Тионикс». Руководство администратора RU.НРФЛ.00001-01.95.01.

4 Идентификационные данные документа

Идентификационные данные ПО	**Программа для ЭВМ «Виртуальные рабочие столы «Тионикс»**
Название документа	«ПО «Виртуальные рабочие столы «Тионикс». Руководство по эксплуатации»
Обозначение документа	RU.НРФЛ.00001-01.97.01
Автор документа	ООО «БАЗИС»

5 Требования к составу и квалификации обслуживающего персонала

Системный инженер – должностное лицо, служебная деятельность которого обеспечивает качественную и безопасную эксплуатацию оборудования ЦОД или виртуального ЦОД – облачной платформы после внедрения (ввода в эксплуатацию).

Администратор ОП – должностное лицо, служебная деятельность которого связана с эксплуатацией программных продуктов и стороннего ПО, используемого при создании среды функционирования: ОС Linux, Python3, OpenStack и др.

Системный инженер должен иметь навыки проектирования или настройки аппаратных и программных конфигураций компьютерных сетей, обслуживания локальных вычислительных сетей. Кроме того, он может быть ответственен за организацию защиты информации и производить установку антивирусов и другого программного обеспечения, обновление ПО. Полезным будет также навык анализа затрат на системное обслуживание, составление отчетов и поиск способов оптимизации расходов.

Оперативный персонал (системный инженер), осуществляющий манипуляции с оборудованием на площадке, должен иметь допуск к эксплуатации электроустановок до 1000В. Категория допуска должна быть согласована со службами эксплуатации ЦОД.

Обычными задачами системного администратора, в зависимости от инфраструктуры, являются контроль работы компьютерных программ и устранение ошибок в их работе, разовая диагностика/ремонт ПК и другой офисной техники.

Системный (облачный) администратор должен уметь использовать множество утилит и инструментов администрирования облачной платформы с целью:

- контроля работоспособности облачной платформы (проверки основного функционала);
- проверки работоспособности отдельных системных служб (ОС Linux);
- конфигурирования виртуальных сервисов облачной платформы;
- резервного копирования и восстановления виртуальных машин.

Для выполнения задач по сопровождению настоящего ПО необходимо иметь опыт работы, связанный с системным администрированием серверного оборудования, а также понимать основные принципы резервного копирования и восстановления данных.

Деятельность системного инженера регулируется и контролируется отделом информационной безопасности, а также внутренними регламентами предприятия, нацеленными на обеспечение безопасности данных и соблюдение конфиденциальности.

6 Назначение

ПО «Виртуальные рабочие столы «Тионикс» позволяет организовать инфраструктуру виртуальных рабочих столов (VDI), которая обеспечивает предоставление виртуальных и удаленных компьютеров на базе единой платформы, а также доступ конечных пользователей к любым Windows/Linux и веб-ресурсам в рамках унифицированной рабочей области. Сценарии использования:

1. Предоставление персонального виртуального рабочего стола, который закрепляется за конкретным пользователем.
2. Предоставление пользователю типового виртуального рабочего стола, развернутого на базе «золотого образа».
3. Предоставление одного виртуального рабочего места нескольким пользователям поочередно.

7 Функциональность

1. Предоставление пользователям виртуальных рабочих столов, развернутых на базе поддерживаемых операционных систем;
2. Возможность формирования горячего резерва виртуальных рабочих столов для новых пользователей;
3. Возможность определения квот на выделение вычислительных ресурсов для определенного пула виртуальных рабочих столов;
4. Возможность автоматического именования рабочих столов по определенной маске;
5. Поддержка различных протоколов удаленного доступа (RDP, VNC, RX);
6. Автоматический ввод рабочих столов в домен Active Directory и другие службы каталогов;
7. Поддержка перемещаемых профилей пользователей для персонализации виртуального рабочего стола;
8. Разграничение прав доступа в виртуальных рабочих столах на базе групповых политик;
9. Регистрация пользовательских и системных событий;
10. Возможность перевода инфраструктуры виртуальных рабочих столов в режим обслуживания;
11. Высокая доступность и автоматическая балансировка нагрузки;
12. Поддержка проброса видеокарт и других PCI-устройств в виртуальный рабочий стол;
13. Доступ пользователя к виртуальному рабочему столу через веб-портал;
14. Привязка выделенного IP-адреса к пользователю виртуального рабочего стола.

8 Обеспечение работоспособности терминальных протоколов

Если в системе не установлено должным образом ПО, реализующее указанный в конфигурации протокол удаленного доступа (по умолчанию – RDP), то может возникнуть *ошибка подключения*.

Обратитесь к администратору проекта, ответственного за эксплуатацию инфраструктуры TIONIX VDI или документу Руководство администратора настоящего комплекта.

8.1 Выбор терминального протокола

Внимание

тут необходимо провести ревизию (смена функционала)

8.1.1 HTTPS

Потребуется скопировать корневой сертификат (testCA.crt) на СВТ с установленным ПО клиента TIONIX VDI (Linux). В окружение (env) потребуется добавить переменную с корневым сертификатом:

> *export REQUESTS_CA_BUNDLE=/path/to/your/testCA.crt*

Запустите TIONIX.VDIclient и произведите пробное подключение к точке входа с указанием протокола HTTPS.

8.1.2 SPICE

Пользователь не может самостоятельно изменить параметры сессии, созданной функционирующим на стороне бэкэнда (в облаке) ПО сервера VDI.

9 Обновление «золотого» образа

Ниже описан способ получения образа виртуальной машины, предназначенной для помещения в облачную среду виртуализации, построенную на основе СПО OpenStack и ПО «Базис.Cloud».

На этапе развертывания инфраструктуры виртуальных рабочих столов (VDI) подготавливается шаблон виртуальной машины «Золотой образ» – эталонный образ, который содержит состояние гостевой ОС с заранее внесёнными настройками и установленным ПО. Такой образ пригоден к дальнейшему развёртыванию на множестве однотипных компьютерных устройств (виртуальных машин).

«Золотой образ» зависит от потребностей заказчика и не имеет строгого стандарта по наполнению. Создается корпоративный шаблон (VDI-машины), отвечающий требованиям типового пользователя облачной платформы.

Загрузка «золотого образа» может быть выполнена из заранее созданного репозитория. Из готового шаблона администратор может оперативно создать в инфраструктуре виртуального ЦОД типовые виртуализованные Рабочие столы, интерфейсы и окружение которых совместимы с используемыми в организации бизнес-приложениями.

Ниже подробно описаны этапы, из которых состоит процедура подготовки и обновления «Золотого образа»:

- создание ВМ из «Золотого образа»;
- оптимизация образа (опционально);
- выполнение Sysprep (см. пример ниже);
- создание и запуск ВМ (VDI-машины).

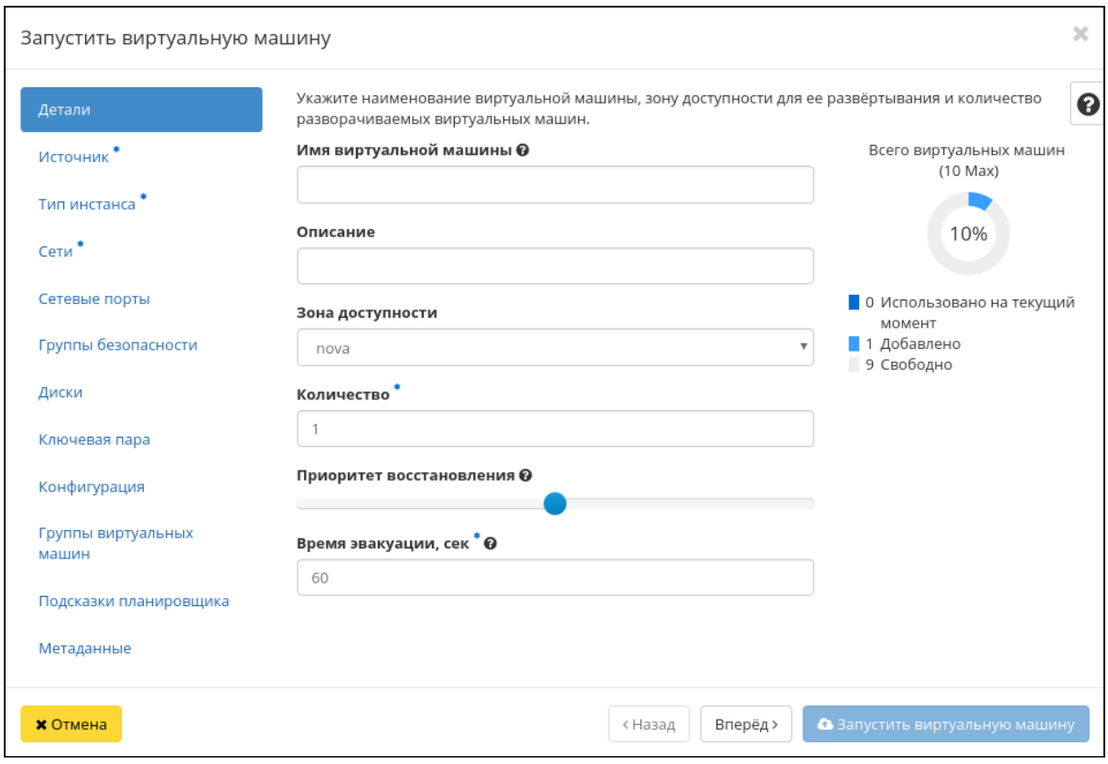
> *Примечание.*
> *Sysprep – средство отвязки операционной системы от драйверов комплектующих конкретного компьютера и отдельных профильных данных. Такая отвязка предусматривается преимущественно для подготовки эталонного (Золотого) образа Windows.*

9.1 Создание ВМ из «Золотого образа»

Все действия по созданию ВМ производятся из АРМ администратора, при помощи панели управления (веб-) интерфейса управления.

1. Авторизоваться в интерфейсе управления (TIONIX.Dashboard).
2. Перейти: Проект >> Вычисления >> Виртуальные машины.
3. Нажать на кнопку [Создать машину].

В открывшемся окне мастера создания и запуска виртуальной машины следуйте указаниям мастера, выбирая параметры текущего золотого образа.



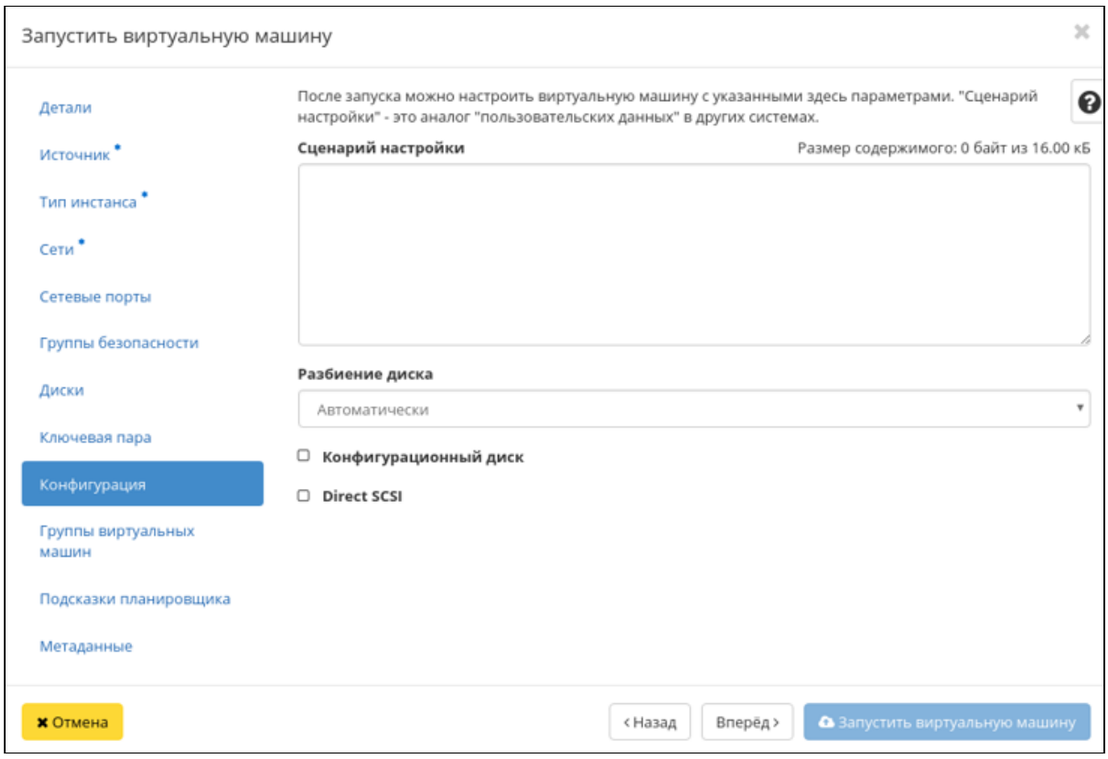
Запуск ВМ. Детали

Во внутренней вкладке «Источник» выбрать образ VDI-машины.

Перейти на страницу вкладки «Конфигурация».

Ввести в поле «Сценарий настройки» текст скрипта:

```
#ps1_sysnative
$password=convertto-securestring "45697845" -asplaintext -force
New-LocalUser "vdi-user1" -Password $password
Add-LocalGroupMember -SID "S-1-5-32-544" -Member "vdi-user1"
Restart-Computer
```



Запуск ВМ. Окно «Конфигурация» (Сценарий настройки)

Сценарий настройки (скрипт) выполняется для обеспечения доступности локальной учетной записи администратора.

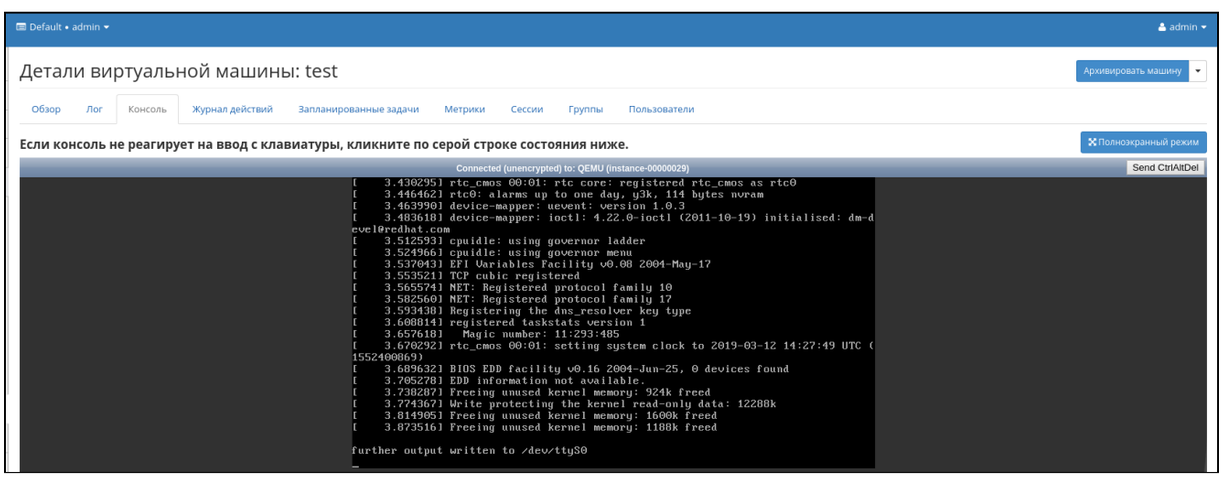
После заполнения параметров ВМ нажать на кнопку [Запустить виртуальную машину].

Дождаться окончания создания виртуальной машины.

> *Примечание.*
> *Текущий образ должен содержать пакет ПО `cloud-init`, для поддержки пары ключей SSH и ввода пользовательских данных. При использовании SSH будет обеспечен доступ в виртуальную машину (ВМ) с приватным ключом и учетной записью по умолчанию. Если пакет cloud-init отсутствует, то его необходимо установить.*

Перейти на страницу ВМ «Детали ВМ».

Открыть вкладку «Консоль», предоставляющую доступ к консольному управлению (выбранной) VDI-машиной и внести изменения обновлений.



9.2 Пример выполнения Sysprep для Windows 10

1. Перейти по ссылке:.
2. Выбрать опции команды запуска на странице сайта, также внести файл ответов.
3. Открыть консоль и из командной строки запустить Sysprep.

ВАЖНО.

Запуск **sysprep** следует выполнить с правами администратора.

После окончания выполнения Sysprep завершите работу виртуальной машины (выберите действие – Выключить ВМ).

9.3 Создание ВМ с обновленным «Золотым образом»

В панели управления (веб-интерфейсе Dashboard, выберите пункт меню:

> *Администратор » Вычисления » Виртуальные машины*

Выберите строку с текущей ВМ, нажать на знак раскрывающегося списка кнопки в конце строки, выбрать в меню опцию «Создать образ».

В общем списке и во вкладках с детальной информацией выберите опцию и нажмите на кнопку [Создать].

Подтвердите создание снимка, после чего снимок отобразится во вкладке «Образы» – со статусом «Активный».

Примечания.

Образу автоматически присваивается имя. Формат имени:

> *<имя машины>_ГГ-ММ-ДД_ЧЧ-ММ-СС*

Созданный образ отображается во вкладке «Образы» со статусом «Активный».

9.4 Запуск VDI-машины с обновленным «Золотым образом»

Перейдите:

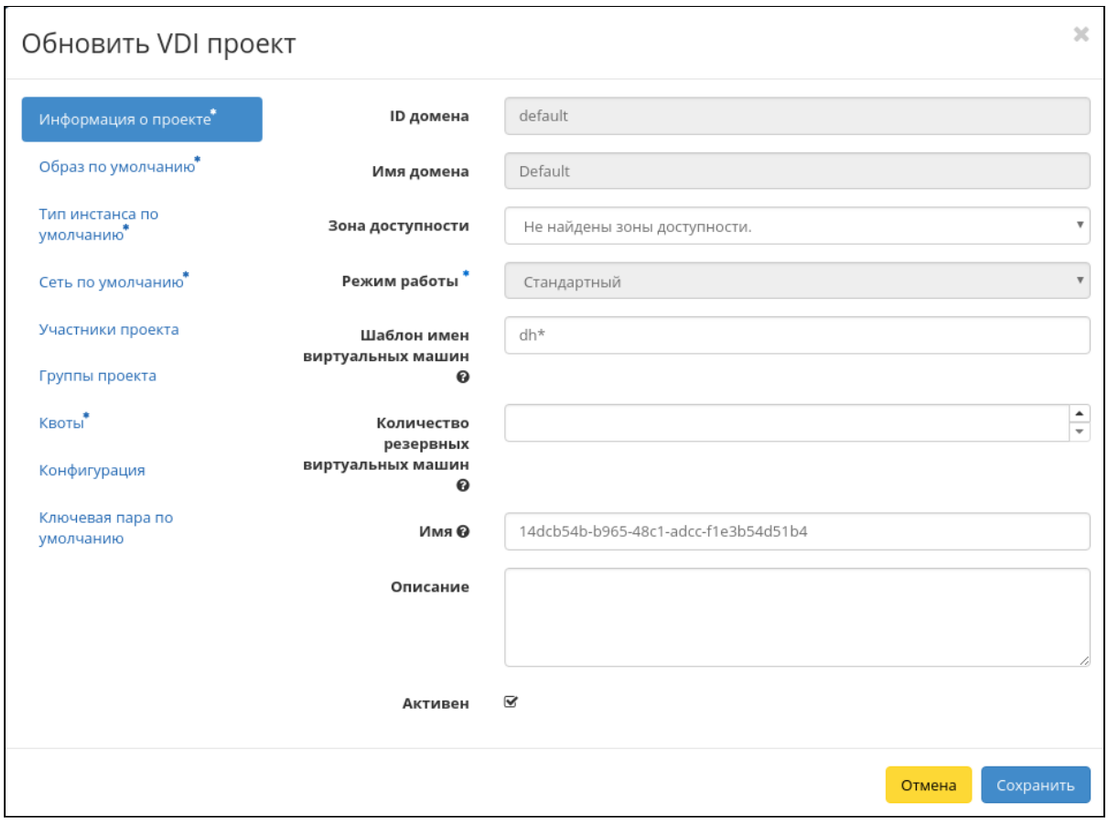
> *Тионикс >> VDI >> Проекты.*

Вкладка «Проекты» отображает перечень VDI проектов.

Выберите строку с текущим проектом, нажатием на значке раскрывающегося списка (кнопки в конце строки).

Из меню выберите опцию «Редактировать проект».

После вызова действия откроется окно «Обновить VDI проект» на внутренней вкладке «Информация о проекте».



Далее, следует перейти во внутреннюю вкладку «Образ по умолчанию».

При указании образа по умолчанию:

- Выделенные – отображается перечень выделенных образов;
- Доступные – отображается перечень всех доступных образов.

Нажмите на кнопку [Сохранить].

Теперь все вновь запускаемые VDI-машины будут использовать новый образ. Для вступления изменений в силу перезагрузите те VDI-машины, которые используют (сохраненный) образ.

9.5 Пример файла ответов (AutoUnattend.xml)

Файл ответов (`AutoUnattend.xml`) предназначен для 64-разрядной Windows 10 и должен располагаться в корне носителя, используемого для хранения программы установки (Windows setup).

Ниже приведено содержимое файла ответов для Windows 10:

```
<?xml version="1.0" encoding="utf-8"?>
<!-- http://www.outsidethebox.ms/19924/ -->
<unattend xmlns="urn:schemas-microsoft-com:unattend">
<settings pass="windowsPE">
<component name="Microsoft-Windows-International-Core-WinPE"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral"
versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<InputLocale>en-US; ru-RU</InputLocale>
<SystemLocale>ru-RU</SystemLocale>
<UILanguage>en-US</UILanguage>
<UserLocale>en-US</UserLocale>
</component>
<component name="Microsoft-Windows-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
<UserData>
<!-- KMS keys https://docs.microsoft.com/windows-server/get-started/kmsclientkeys -->
<ProductKey>
<Key></Key>
</ProductKey>
<AcceptEula>true</AcceptEula>
</UserData>
```

```
</component>
</settings>
<settings pass="oobeSystem">
<component name="Microsoft-Windows-International-Core" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
<InputLocale>en-US; ru-RU</InputLocale>
<SystemLocale>ru-RU</SystemLocale>
<UILanguage>en-US</UILanguage>
<UserLocale>en-US</UserLocale>
</component>
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
<OOBE>
<HideOnlineAccountScreens>true</HideOnlineAccountScreens>
<ProtectYourPC>3</ProtectYourPC>
</OOBE>
<UserAccounts>
<LocalAccounts>
<LocalAccount wcm:action="add">
<Group>Administrators</Group>
<Name>Admin</Name>
<!--<Password>
<Value>goofy reward replica danger</Value>
<PlainText>true</PlainText>
</Password> -->
</LocalAccount>
</LocalAccounts>
</UserAccounts>
<!-- <AutoLogon>
<Password>
<Value>goofy reward replica danger</Value>
<PlainText>true</PlainText>
</Password>
<Username>Admin</Username>
<LogonCount>1</LogonCount>
<Enabled>true</Enabled>
</AutoLogon> -->
</component>
</settings>
</unattend>
```

10 Аутентификация

10.1 Интеграция с Active Directory

Служба идентификации OpenStack – Keystone – проверяет подлинность определенных пользователей доменных служб Active Directory (AD DS), сохраняя при этом параметры авторизации и критически важные учетные записи служб в БД службы идентификации.

Служба Keystone имеет доступ к AD DS с правами «только для чтения» – это необходимо для проверки подлинности учетных записей пользователей. При этом управление привилегиями, назначенными проверенным учетным записям, сохраняется.

10.1.1 Интеграция службы идентификации с доменными службами

Начальные условия:

– доменные службы Active Directory настроены и работают;

– платформа виртуализации настроена и работает;

– разрешение DNS-имен полностью функционально, все хосты зарегистрированы соответствующим образом;

– трафик аутентификации AD DS шифруется с помощью LDAP.

Настройка доменных служб Active Directory

Для взаимодействия служб Keystone и Active Directory требуется следующая информация:

- путь к серверу AD (в т.ч и через широковещательный порт);
- путь к пользователям «OU» (Organizational Unit).

OU представляет собой контейнер в домене Active Directory 1, который может содержать различные объекты из того же самого домена: другие контейнеры, группы, аккаунты пользователей и компьютеров.

Примечание.

OU представляет собой единицу административного управления внутри домена, на который администратор может назначить объекты групповых политик и назначить разрешения другим пользователем.

Две основные задачи использования OU, кроме хранения объектов Active Directory:

1. Делегирование управления и административных задач внутри домена другим администраторам и обычным пользователям без предоставления им прав администратора домена.
2. Назначение групповых политик на все объекты (пользователей и компьютеры), которые находятся в данном подразделении (OU).

Обычно учетные записи пользователей не размещаются в одной OU, а создаётся несколько OU.

Должна быть создана OU - группа безопасности и указан путь к созданному OU.

Должна быть организована фильтрация по группам. Процесс структурирования выглядит следующим образом:

– OU + фильтрация:

> *списки групп → Проекты → Сети/Образы;*

– три группы:

> - 1 группа - базовый доступ к платформе;
> - 2 и 3 группы - разделение внутри платформы по проектам.

Такая организационная структура позволяет администратору AD не углубляться в платформу виртуализации, а управлять процессами непосредственно из AD.

Настройка взаимодействия

В облачной платформе настраивается внутренняя сеть с использованием доменной адресации – DNS. В данном случае ресурсы DNS являются адресами самой службы AD.

Взаимодействие платформы виртуализации (контроллера) и AD происходит двумя способами:

Через инфраструктурную сеть (может использоваться любая другая сеть).

После создания доступа контроллер/УУ производит считывание списка пользователей, групп, запрашивает учетные данные, необходимые для авторизации (credential). Также поступают запросы от VDI-брокера к Keystone; далее запрос идет на AD.

Через внутреннюю сеть ВМ (VLAN).

Доступ к AD осуществляется через Сетевой шлюз (Gateway). В качестве DNS прописываются адреса AD, которые используются при создании ВМ (на старте) – это позволяет ВМ получать доступ в домен.

10.1.2 Планирование развертывания AD

Перед тем как приступать к развертыванию ПО, администратору AD рекомендуется составить **план действий**.

Параметры, необходимые для развертывания инфраструктуры VDI поверх ОП и интеграции с AD, перечислены в таблице 1.

Таблица 1 - План действий администратора AD

№	Содержание действия	Подробное описание
1	Создать сервисные учетные записи системы VDI, предоставить необходимые параметры для интеграции	Учетная запись администратора платформы виртуализации с учетными данными (credential):
		Чтобы администрировать проекты VDI(tenant), относящиеся к домену пользователя, нужно авторизоваться на платформе (через домен).
		Для этого создается учетная запись с паролем для авторизации через домен в платформе Tionix с ролью – Администратор платформы.
		Учетная запись для пользователя из OU для ВМ имеет права ввода в домен ВМ (при создании VDI машины с помощью автоматизации происходит вход в домен).
		Данная учетная запись (user =), например vdi_srv, имеет право считывать список пользователей из OU (user_tree_dn =), которые платформа увидит (при необходимости фильтровать по атрибутам).
		Система не будет видеть данную учетную запись в списке пользователей.
		Одним из исключений является следующий пример: не вносить ее в
		• тот же список пользователей user_tree_dn = ;
		• группу безопасности user_filter = .
		(memberOf=cn=USERS,cn=PC_USERS,cn=AB,dc=cd,dc=ru) , при осуществлении фильтрации.
		Best-practice. Создаются следующие учетные записи:

№	Содержание действия	Подробное описание
		vdi_srv - считывает список пользователей и доступные группы;
		tnx_user - в списке, который считывает vdi_srv и является администратором в платформе.
		Также пользователь с одной из этих учетных записей имеет право на ввод в домен (для ВМ).
2	Создать сетевую папку для перенаправляемых профилей	Создание сетевой папки для перенаправляемых профилей пользователей системы VDI, если данные пользователей сохраняются в перенаправляемых папках профилей пользователей на выделенном сетевом ресурсе.
3	В AD создать отдельный контейнер (OU)	В созданном контейнере будут размещены все пользователи системы VDI и компьютеры (удаленные рабочие столы), произведена настройка групповых политик данного контейнера (VDI).

Таблица 2 - План развертывания VDI и интеграции с AD

№	Название	Дополнительная информация (пример, формат,доп.действие)
1	Полное название домена	Domain.local
2	Суффикс UPN(при наличии)	suffix = dc=ab,dc=cd,dc=ru
3	Наименование и размещение контейнера (OU), в котором будут размещены пользователи VDI	user_tree_dn = ou=PC_USERS,ou=USERS,ou=AB,dc=AB,dc=CD,dc=RU
4	Наименование и размещение контейнера (OU), в котором будут размещены виртуальные машины VDI	ou=COMPUTERS,ou=MACHINES,ou=AB,dc=AB,dc=CD,dc=RU
5	Наименование и размещение Групп безопасности данного AD	group_tree_dn = cn=Group,dc=genp,dc=loc
6	Фильтр пользователей группы AD (при наличии)	user_filter = (memberOf=cn=USERS,cn=PC_USERS,cn=AB,dc=cd,dc=ru)
		Примечание. Параметр необязателен.

№	Название	Дополнительная информация (пример, формат,доп.действие)
7	Данные о сервисных учетных записях системы VDI, в т.ч. правах, присвоенных сервисным учетным записям	user = cn=vdi_srv, ou=SERVICE_ACCOUNTS, ou=AB, dc=AB, dc=CD, dc=RU
		Пользователь должен обладать следующими правами:
		• право входа в домен и получения списка пользователей и групп;
		• право ввода виртуальных машин в соответствующую группу.
		Примечание. Пароль, вводимый пользователем, передается по безопасному каналу (соблюдение конфиденциальности).

10.1.3 Дополнительные вопросы, возникающие при планировании интеграции

Q: На каких хостах/серверах будет выполнена настройка интеграции с AD? A: - На управляющих узлах (контроллере(ах).

Q: Сколько учетных записей требуется создать в каждом из контуров – ОК и КК ?(при условии, что архитектура содержит контуры)

A: - В зависимости от архитектуры и доступов.

> *Если AD доступна в обоих контурах, можно использовать одну учетную запись AD, разделение по контурам будет за счет разных адресов брокеров VDI. Однако, более разумным будет разделение контуров в AD с разными группами безопасности. Также, любая учетная запись должна иметь права на ввод в домен в определенную OU.*

Q: Для чего требуется указать размещение групп безопасности? A: - Можно не указывать.

> *Но на практике гораздо удобнее предоставлять пользователям доступ к брокеру, добавлением его учетной записи в соответствующую группу безопасности.*

Примеры листингов, иллюстрирующие пояснения:

```
[identity]

driver = keystone.identity.backends.ldap.Identity

[ldap]

url = ldap:\/\/xxx.xxx. x . x

адрес ldap сервера

#url = ldap:\/\/ xxxxxxx .ru:389

#пользователь ldap сервера

user = CN=svc9500vdikeystone,OU=VDI_Service Accounts,OU=9500,OU=VDI_
XXX ,OU=Projects,OU=9500,OU=FT,DC= xxxxxx ,DC=ru
password = xxxxx
suffix = OU=FT,DC=xxxxx,DC=ru
use_dumb_member = False
allow_subtree_delete = False

#путь к ou с пользователям
user _ tree _ dn = OU = FT , DC =xxxxxx, DC = ru
user_objectclass = person
```

```
#путь к ou с группами
group_tree_dn = OU=FT,DC=xxxxxxx,DC=ru
group_objectclass = group

user_allow_create = False
user_allow_update = False
user_allow_delete = False
group_allow_create = False
group_allow_update = False
group _ allow _ delete = False

#фильтр пользователей по группам
user _ filter = (&( objectClass = person )(!( objectClass = computer ))(|( memberOf = CN
=9500- vdi - users , OU = VDI _ Groups , OU =9500, OU = VDI _ RTK ,
OU = Projects , OU =9500, OU = FT , DC =xxxxxx, DC = ru )( memberOf = CN =9900- vdi -
users , OU = VDI _ Groups , OU =9900, OU = VDI _XXX, OU = Projects ,
OU =9500, OU = FT , DC =xxxxxxx, DC = ru )( memberOf = CN =9600- vdi - users , OU = VDI _
Groups , OU =9600, OU = VDI _XXX, OU = Projects , OU =9500, OU = FT ,
DC =xxxxxxx, DC = ru )))

#фильтр групп по маскам имен

group _ filter = (&( objectClass = group )(|( cn =*- vdi - users )( cn =*- vdi -
admins )))

#атрибуты тонкой настройки
query _ scope = sub
user_id_attribute = sAMAccountName
user_name_attribute = sAMAccountName
user_mail_attribute = mail
user_pass_attribute = userPassword
user_default_project_id_attribute = None
group_id_attribute = sAMAccountName
group_name_attribute = sAMAccountName
group_member_attribute =
group_desc_attribute = description
tls_req_cert = never
```

10.1.4 Настройка множественных доменов

Приведенные ниже операции по настройке выполняются после успешного подключения к УУ (контроллеру) с использованием протокола SSH.

Конфигурация Keystone

1) Отредактируйте конфигурационный файл службы Keystone – `/etc/keystone/keystone.conf`. Добавьте указанные ниже параметры в секцию [identity]:

```
[identity]

driver = keystone.identity.backends.sql.Identity

domain_specific_drivers_enabled = True
domain_config_dir = /etc/keystone/domains
```

2) Создайте каталог `/etc/keystone/domains`:

```
mkdir /etc/keystone/domains
```

3) Создайте конфигурационный файл с именем `DOMAIN_NAME.conf`, где DOMAIN_NAME – имя домена (в OpenStack).

4) Пропишите владельца директории и файла:

```
chown -R keystone:keystone /etc/keystone/domains
```

Пример конфигурации домена

Если домен планируется назвать как «CHD», то директория будет выглядеть так:

> */etc/keystone/domains/keystone.CHD.conf*

Отредактировать конфигурационный файл и указать следующие параметры:

```
[identity]

driver = keystone.identity.backends.ldap.Identity

[ldap]

url = ldap://LDAP_IP
user = cn=admin,cn=Users,dc=example,dc=com
password = openstack
suffix = dc=example,dc=com
use_dumb_member = False
allow_subtree_delete = False

user_tree_dn = cn=Users,dc=example,dc=com
user_objectclass = InetOrgPerson

group_tree_dn = cn=Groups,dc=example,dc=com
group_objectclass = groupOfNames

user_allow_create = False
user_allow_update = False
user_allow_delete = False

group_allow_create = False
group_allow_update = False
group_allow_delete = False
```

В `Active Directory` и `Samba 4` используются другие объектные классы для пользователя и группы:

```
[ldap]
...
user_objectclass = person
group_objectclass = group
```

Потребуется указать маппинг атрибутов LDAP и видов данных Keystone:

```
user_id_attribute = sAMAccountName
user_name_attribute = sAMAccountName
user_mail_attribute = mail
user_pass_attribute = userPassword

group_id_attribute = sAMAccountName
group_name_attribute = sAMAccountName
group_member_attribute =

group_desc_attribute = description
group_filter =
```

Перезапуск службы веб-сервера

После внесения изменений в конфигурацию домена, для вступления изменений в силу, перезапустите службу веб-сервера. На контроллере (УУ) выполните команду:

```
systemctl restart httpd
```

Настройка данных Keystone

Перед выполнением команд с помощью утилиты клиента **openstack:**

1) Настройте окружение OpenStack:

```
source /root/admin-openrc.sh
```

2) Создайте домен `CHD`:

```
openstack domain create CHD
```

3) Получите список пользователей домена `CHD`:

openstack user list --domain CHD

| ID.....| Name |+-------------------------+----------------+
| ae7a1e0c02...18cb8d | admin |+-------------------------+----------------+
| 2b19a35430...7ba6a1 | Guest |+-------------------------+----------------+

4) Создайте проект admin в домене CHD:

openstack project create --domain CHD admin

5) Добавьте пользователя admin с правами администратора на проект admin в домене CHD:

openstack role add --user-domain CHD --project-domain CHD --project admin --user admin admin

6) Присвойте права администратора пользователю admin на домен CHD:

openstack role add --user-domain CHD --user admin --domain CHD admin

Используя эти учетные данные, авторизуйтесь в интерфейсе управления (см. Руководство администратора настоящего комплекта ЭД).

10.1.5 Настройка политик Active Directory

Для того, чтобы начать пользоваться виртуальным рабочим столом, потребуется настроить разрешение подключение по протоколу RDP.

Когда в инфраструктуре эксплуатируется множество ВМ, обслуживающих рабочие столы пользователей, необходимо сначала произвести настройку политик доступа.

Авторизуйтесь в графическом интерфейсе управления с правами администратора и перейдите:

> *Проект >> Вычисления >> Виртуальные машины*

Выберите виртуальную машину, несущую функцию контроллера AD, в обзоре деталей ВМ откройте «Консоль» (горизонтальную вкладку).

> *Примечание.*
> *См. документ Руководство администратора ОП (Управление виртуальными машинами).*

Разрешение подключений RDP

Из виртуальной машины Active Directory (Windows Server) запустите редактор политик безопасности (Group Policy Management Editor) – оснастку Group Policy Management (GPolicy_Management).

> *Примечание.*
>
> *За запуск оснастки отвечает файл gpmc.msc – расширение консоли управления Microsoft.*

В оснастке необходимо из леса доменов (Forest:) определить тот домен, в котором требуется произвести изменения, раскрыв **Domains**.

Домен имеет (групповую) политику по умолчанию, однако, рекомендуется создать отдельную политику (для RDP), например – rdp. Для этого кликом правой кнопки мыши на имени домена откройте контекстное меню и из него выберите:

> *Create GPO in this domain, and Link it here*

После привязки OU необходимо добавить Users, в неё добавить политику и выставить для неё (из контекстного меню) флаг Link enabled. Таким образом, политика будет активирована с помощью созданной привязки.

Группу безопасности, в которой состоят пользователи VDI, необходимо добавить в группу «Пользователи удаленного рабочего стола».

Параметры политик настраиваются из Панели управления (MS Windows):

> *Конфигурация компьютера -> Административные шаблоны -> Компоненты Windows -> Службы удаленного рабочего стола -> Узел сеансов удаленных рабочего стола -> Подключения*

> *Примечание.*
>
> *Настройки политик производятся в соответствии с потребностями конкретных пользователей.*

Настройка функций в GPO

Для корректной работы VDI необходимо произвести настройку групповых политик данного контейнера.

1) Произведите настройку функций GPO, открыв окно редактора локальной групповой политики.

2) Для корректной работы VDI необходимо создать контейнер (OU), в котором будут размещены пользователи системы. Выберите VDI и компьютеры (удаленные рабочие столы) и произведите настройку групповых политик данного контейнера.

3) Далее потребуется выставить значения параметров для политик, приведенные в таблице "Значения параметров групповых политик (GPO)".

Таблица 3 – Значения параметров групповых политик (GPO)

Путь	**Политика**	**Значение**
Конфигурация компьютера/ Административные шаблоны/Система	Выводить очень подробные сообщения о состоянии системы	Включено
Конфигурация компьютера/ Административные шаблоны/Система/ Вход в систему	Всегда ждать сеть при запуске и входе в систему	Включено
Конфигурация компьютера/ Административные шаблоны/Система/ Перенаправление устройств/ Ограничения перенаправления устройств	Запретить перенаправление устройств с каким либо из этих кодов	Отключено
Примечание. При наличии пункта Перенаправление устройств во вкладке Система	Предотвращение перенаправления USB-устройств	Отключено
Конфигурация компьютера/ Административные шаблоны/ Компоненты Windows/Службы удаленных рабочих столов/Клиент подключения к удаленному рабочему столу/Перенаправление USB устройств RemoteFX	Разрешать RDP-файлы от допустимых издателей и пользовательские параметры RDP, заданные по умолчанию	Включено
	Разрешать RDP-файлы от неизвестных издателей	Включено
	Отключение UDP на клиенте	Отключено
Конфигурация компьютера/ Административные шаблоны/ Компоненты Windows/Службы удаленных рабочих столов/Узел сеансов удаленных рабочих столов/ Перенаправление устройств и ресурсов	Запретить перенаправление видеозахвата	Отключено
Примечание. В случае необходимости проброса дисков, смарт-карт и прочих устройств, подключить опции раздела и установить значения соответственно	Разрешить перенаправление воспроизведения звука и видео	Включено

Путь	Политика	Значение
	Разрешить перенаправление записи звука	Включено
	Разрешить перенаправление часового пояса	Включено
Конфигурация компьютера/ Административные шаблоны/ Компоненты Windows/Службы удаленных рабочих столов/Узел сеансов удаленных рабочих столов/ Подключения	Выбор транспортных протоколов RDP: использовать UDP и TCP	Включено
Конфигурация компьютера/ Конфигурация Windows/ Параметры безопасности/Локальные политики/ Параметры безопасности/	Контроль учетных записей: все администраторы работают в режиме одобрения администратором	Отключено
	Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав	Отключено
	Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором	Повышение прав без запроса
	Контроль учетных записей: повышение прав для UIAccess-приложений только при установке в безопасных местах	Отключено
	Контроль учетных записей: повышение прав только для подписанных и проверенных исполняемых файлов	Отключено
	Контроль учетных записей: разрешение UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол	Отключено
	Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора	Отключено
Конфигурация пользователя/ Административные шаблоны/ Компоненты Windows/Internet Explorer/ Панель управления браузером/ Вкладка «Безопасность»/ Список назначений зоны для веб-сайтов	Список назначений зоны для веб-сайтов	Включено

Путь	Политика	Значение

Настройки GPO для перемещаемых папок профилей пользователей

Для хранения перенаправляемых папок перемещаемых профилей пользователей создайте общую сетевую папку:

- создайте каталог redirection;
- назначьте каталог сетевым.

Основные настройки ACL:

- каждый пользователь должен иметь доступ только к своему каталогу;
- группа администраторов должна иметь доступ ко всем каталогам.

Дополнительные настройки ACL произвести следующим образом:

1. Перейти: Свойства каталога >> Безопасность >> Дополнительно.
2. Отключить опцию «Наследование» в дополнительных параметрах безопасности каталога.
3. Выбрать группу пользователей и предоставить пользователям этой группы особые права доступа.
4. Потребуется добавить нужную группу и нажать кнопку [Изменить].
5. Включить опцию «Отображение дополнительных разрешений».
6. Включить флаг, разрешающий «Создание папок / дозапись данных».
7. Для предоставления пользователю полного доступа к своему каталогу:

> - добавить субъект «создатель-владелец»;
> - предоставить субъекту полный доступ – «только для подпапок и файлов»;
> - добавить субъект «система», группу системных администраторов и предоставить им полный доступ, выбрав – «для этой папки и её подпапок».

Дополнительные групповые политики при использовании перемещаемых профилей

Значения дополнительных групповых политик, настраиваемые при использовании перемещаемых профилей – папок, содержащих настройки пользовательских профилей – представлены в остальных таблицах (см. ниже):

Таблица 4 - Дополнительные групповые политики при использовании перенаправляемых папок

Путь	Политика	Значение
Конфигурация пользователя/ Конфигурация Windows/ Перенаправление папки	*BAppData(перемещаемая) Путь:\\%dc1%\%share%\%USERNAME%\AppData\Roaming*	*Перенаправление папок всех пользователей в одно расположение*
	Параметры	
	Предоставить права монопольного доступа пользователю к папке AppData(перемещаемая)	Отключено
	Переместить содержимое папки AppData(перемещаемая) в новое место расположения	Отключено
	Также применить политику перенаправления для операционных систем Windows 2000, Windows 2000 Server, Windows XP и Windows Server 2003	Отключено
	Процедура удаления политики:а) после удаления политики оставить папку в новом расположении;б) после удаления политики перенаправить папку обратно в локальный профиль пользователя.	Оставить содержимое: а) Включено; б) Выключено

Путь	Политика	Значение
	Управление конфигурацией	Групповая политика
	Оценка основного компьютера	Оценка не выполнена, так как политика основного компьютера не включена

Папка «Видео»

Путь	Политика	Значение
Конфигурация пользователя/ Конфигурация Windows/ Перенаправление папки/ Видео	*Поле «Политика»: Следовать за папкой «Документы»*	*Расположить внутри папки «Документы»*

Папка «Главное меню»

Путь	Политика	Значение
Конфигурация пользователя/ Конфигурация Windows/ Перенаправление папки/ Главное меню	*Путь: \\%dc1\share%\%USERNAME%\Start MenuПоле «Политика»: Перенаправлять папки всех пользователей в одно расположение;Поле «Расположение целевой папки»: Создать папку для каждого пользователя на корневом пути;Поле «Корневой путь»: Прописать корневой путь*	Перенаправление папок всех пользователей в одно место
	Параметры	
	Предоставить права монопольного доступа пользователю к папке Главное меню	Отключено
	Переместить содержимое папки Главное меню в новое место расположения	Отключено
	Также применить политику перенаправления для операционных систем Windows 2000, Windows 2000 Server, Windows XP и Windows Server 2003	Отключено
	Процедура удаления политики	Оставить содержимое
	Управление конфигурацией	Групповая политика
	Оценка основного компьютера	Оценка не выполнена, так как политика основного компьютера не включена

Папка «Документы»

Путь	Политика	Значение
Конфигурация пользователя/ Конфигурация Windows/ Перенаправление папки/ Документы	Путь: \\%dc1\share%\%USERNAME%\DocumentsПоле «Политика»: Перенаправлять папки всех пользователей в одно расположение;Поле «Расположение целевой папки»: Создать папку для каждого пользователя на корневом пути;Поле «Корневой путь»: Прописать корневой путь	Перенаправление папок всех пользователей в одно место
	Параметры	
	Предоставить права монопольного доступа пользователю к папке Документы	Отключено
	Переместить содержимое папки Документы в новое место расположения	Отключено
	Также применить политику перенаправления для операционных систем Windows 2000, Windows 2000 Server, Windows XP и Windows Server 2003	Отключено
	Процедура удаления политики	Оставить содержимое
	Управление конфигурацией	Групповая политика
	Оценка основного компьютера	Оценка не выполнена, так как политика основного компьютера не включена

Папка «Загрузка»

Путь	Политика	Значение
Конфигурация пользователя/Конфигурация Windows/Перенаправление папки/Загрузка	Путь: \\%dc1\share%\%USERNAME% \Downloads.Поле «Политика»: Перенаправлять папки всех пользователей в одно расположение;Поле «Расположение целевой папки»: Создать папку для каждого пользователя на корневом пути;Поле «Корневой путь»: Прописать корневой путь	Перенаправление папок всех пользователей в одно место
	Параметры	
	Предоставить права монопольного доступа пользователю к папке Загрузка	Отключено
	Переместить содержимое папки Загрузка в новое место расположения	Отключено
	Также применить политику перенаправления для операционных систем Windows 2000, Windows 2000 Server, Windows XP и Windows Server 2003	Отключено

Путь	Политика	Значение
	Процедура удаления политики:После удаления политики оставить папку в новом расположении.После удаления политики перенаправить папку обратно в локальный профиль пользователя	1. Включено; 2. Выключено (неактивна)
	Управление конфигурацией	Групповая политика
	Оценка основного компьютера	Оценка не выполнена, так как политика основного компьютера не включена

Папка «Избранное»

Путь	Политика	Значение
Конфигурация пользователя/Конфигурация Windows/Перенаправление папки/Избранное	Путь: \\%dc1\share%\%USERNAME%\FavoritesПоле «Политика»: Перенаправлять папки всех пользователей в одно расположение;Поле «Расположение целевой папки»: Создать папку для каждого пользователя на корневом пути;Поле «Корневой путь»: Прописать корневой путь	Перенаправление папок всех пользователей в одно место
	Параметры	
	Предоставить права монопольного доступа пользователю к папке Избранное	Отключено
	Переместить содержимое папки Избранное в новое место расположения	Отключено
	Также применить политику перенаправления для операционных систем Windows 2000, Windows 2000 Server, Windows XP и Windows Server 2003	Отключено
	Процедура удаления политики:После удаления политики оставить папку в новом расположении.После удаления политики перенаправить папку обратно в локальный профиль пользователя	1. Включено; 2. Выключено (неактивна)
	Управление конфигурацией	Групповая политика
	Оценка основного компьютера	Оценка не выполнена, так как политика основного компьютера не включена

Папка «Изображение»

Путь	Политика	Значение
Конфигурация пользователя/ Конфигурация Windows/ Перенаправление папки/ Изображение	Поле «Политика»: Следовать за папкой Документы	Расположить внутри папки Документы

Папка «Контакты»

Путь	Политика	Значение
Конфигурация пользователя/Конфигурация Windows/Перенаправление папки/Контакты	Путь: \\%dc1\share%\%USERNAME%\ContactsПоле «Политика»: Перенаправлять папки всех пользователей в одно расположение;Поле «Расположение целевой папки»: Создать папку для каждого пользователя на корневом пути;Поле «Корневой путь»: Прописать корневой путь	
Перенаправление папок всех пользователей в одно место		
	Параметры	
	Предоставить права монопольного доступа пользователю к папке Контакты	Отключено
	Переместить содержимое папки Контакты в новое место расположения	Отключено
	Также применить политику перенаправления для операционных систем Windows 2000, Windows 2000 Server, Windows XP и Windows Server 2003	Отключено
	Процедура удаления политики:После удаления политики оставить папку в новом расположении.После удаления политики перенаправить папку обратно в локальный профиль пользователя	1. Включено; 2. Выключено (неактивна)
	Управление конфигурацией	Групповая политика
	Оценка основного компьютера	Оценка не выполнена, так как политика основного компьютера не включена

Папка «Музыка»

Путь	Политика	Значение
Конфигурация пользователя/ Конфигурация Windows/ Перенаправление папки/ Музыка	Поле «Политика»: Следовать за папкой Документы	Расположить внутри папки Документы

Путь	Политика	Значение

Папка «Поиски»

Путь	Политика	Значение
Конфигурация пользователя/Конфигурация Windows/Перенаправление папки/Поиски	Путь: \\%dc1\share%\%USERNAME%\SearchesПоле «Политика»: Перенаправлять папки всех пользователей в одно расположение;Поле «Расположение целевой папки»: Создать папку для каждого пользователя на корневом пути;Поле «Корневой путь»: Прописать корневой путь	
Перенаправление папок всех пользователей в одно место		
	Параметры	
	Предоставить права монопольного доступа пользователю к папке Поиски	Отключено
	Переместить содержимое папки Поиски в новое место расположения	Отключено
	Также применить политику перенаправления для операционных систем Windows 2000, Windows 2000 Server, Windows XP и Windows Server 2003	Отключено
	Процедура удаления политики:После удаления политики оставить папку в новом расположении.После удаления политики перенаправить папку обратно в локальный профиль пользователя	1. Включено; 2. Выключено (неактивна)
	Управление конфигурацией	Групповая политика
	Оценка основного компьютера	Оценка не выполнена, так как политика основного компьютера не включена

Папка «Рабочий стол»

Путь	Политика	Значение
Конфигурация пользователя/Конфигурация Windows/Перенаправление папки/Рабочий стол	Путь: \\%dc1\share%\%USERNAME%\DesktopПоле «Политика»: Перенаправлять папки всех пользователей в одно расположение;Поле «Расположение целевой папки»: Создать папку для каждого пользователя на корневом пути;Поле «Корневой путь»: Прописать корневой путь	

Путь	Политика	Значение
Перенаправление папок всех пользователей в одно место		
	Параметры	
	Предоставить права монопольного доступа пользователю к папке Рабочий стол	Отключено
	Переместить содержимое папки Рабочий стол в новое место расположения	Отключено
	Также применить политику перенаправления для операционных систем Windows 2000, Windows 2000 Server, Windows XP и Windows Server 2003	Отключено
	Процедура удаления политики:После удаления политики оставить папку в новом расположении.После удаления политики перенаправить папку обратно в локальный профиль пользователя	1. Включено; 2. Выключено (неактивна)
	Управление конфигурацией	Групповая политика
	Оценка основного компьютера	Оценка не выполнена, так как политика основного компьютера не включена

Папка «Ссылки»

Путь	Политика	Значение
Конфигурация пользователя/Конфигурация Windows/Перенаправление папки/Ссылки	Путь: \\%dc1\share%\%USERNAME%\LinksПоле «Политика»: Перенаправлять папки всех пользователей в одно расположение;Поле «Расположение целевой папки»: Создать папку для каждого пользователя на корневом пути;Поле «Корневой путь»: Прописать корневой путь	
Перенаправление папок всех пользователей в одно место		
	Параметры	
	Предоставить права монопольного доступа пользователю к папке Ссылки	Отключено
	Переместить содержимое папки Ссылки в новое место расположения	Отключено

Путь	Политика	Значение
	Также применить политику перенаправления для операционных систем Windows 2000, Windows 2000 Server, Windows XP и Windows Server 2003	Отключено
	Процедура удаления политики:После удаления политики оставить папку в новом расположении.После удаления политики перенаправить папку обратно в локальный профиль пользователя	1. Включено; 2. Выключено (неактивна)
	Управление конфигурацией	Групповая политика
	Оценка основного компьютера	Оценка не выполнена, так как политика основного компьютера не включена

10.2 Интеграция с BVS (мультидоменный LDAP)

Излагаемый ниже материал опирается на инфраструктуру VDI, интегрированную с `Active Directory`.

Основной целью настоящего раздела является разъяснение способов настройки существующей инфраструктуры, интегрированной с облачной платформой таким образом, чтобы можно было использовать существующую инфраструктуру AD.

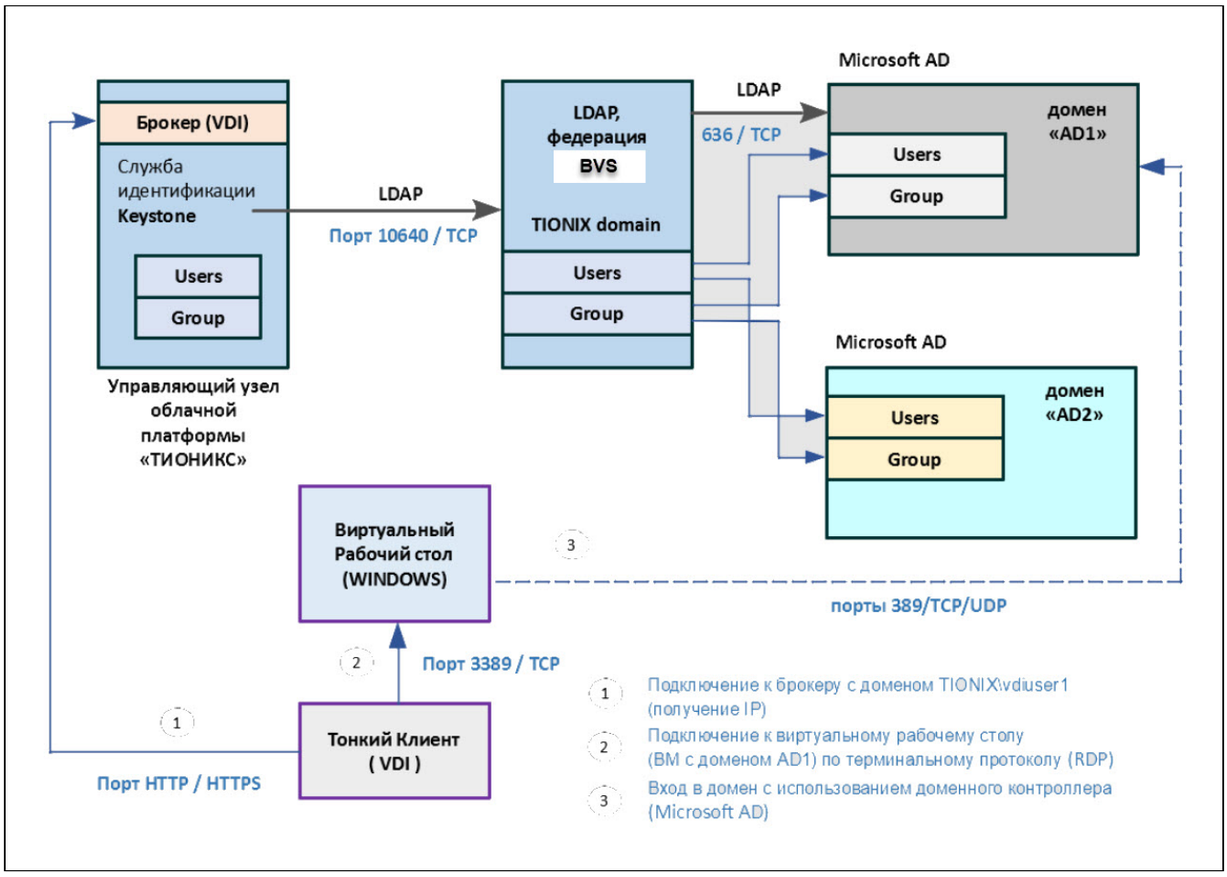


Схема взаимодействия цепочки «Клиентский AD – BVS – Keystone – VDI брокер»

10.2.1 Федерация LDAP

В Системе есть возможность подключать сторонние LDAP системы данных о пользователях. Для активации этой функциональности необходимо настроить федерацию LDAP (пункт меню Безопасность → Федерации).

Общая информация

В «Базис.Virtual Security» (далее BVS) имеется возможность подключения сторонних LDAP-систем, хранящих данные о пользователях. Для активации этой функциональности из панели управления BVS необходимо настроить федерацию LDAP (Безопасность >> Федерации).

BVS сначала выполняет поиск пользователя во внутреннем хранилище. Если он там не найден, то осуществляется поиск первого пользователя, соответствующего критериям, во внешних системах. Поиск выполняется с учетом приоритета, указанного для федерации. Есть возможность настроить импорт данных из внешнего LDAP и их дальнейшую синхронизацию, или убрать связь с внешним хранилищем, удалив импортированных пользователей.

Атрибуты пользователя (ФИО, e-mail и т.д.), группы, роли, хранимые во внешнем LDAP, могут быть перенесены с помощью настройки отображения.

По умолчанию, BVS импортирует пользователей из LDAP в локальную БД пользователей BVS. Копия пользователя синхронизируется либо по запросу (кнопка на форме «Синхронизация пользователей»), либо системой с периодичностью, указанной на вкладке «Настройки синхронизации».

Стоит отметить, что пароли - это единственное, что нельзя импортировать и их проверка всегда делегируется серверу LDAP.

Преимущества этого подхода в том, что все функции BVS будут работать, так как любые необходимые дополнительные данные для каждого пользователя хранятся локально. Обратной стороной этого подхода является то, что каждый раз, когда конкретный пользователь запрашивается впервые, выполняется сохранение данных в БД BVS.

Синхронизация импорта не требуется в том случае, если отображения LDAP настроены на чтение определенных атрибутов из LDAP, а не из БД. Кроме того, можно отказаться от импорта пользователей в БД пользователей BVS. В этом случае стандартная пользовательская модель, которую использует BVS, должна поддерживаться сервером LDAP. Это означает, что если LDAP не поддерживает часть данных, которая необходима функционалу BVS, то этот функционал не будет работать. Преимуществом этого подхода является отсутствие накладных расходов на импорт и синхронизацию копии пользователей. Этот режим хранения регулируется полем «Импортировать пользователей» в настройках федерации.

Если импорт пользователей отключен, то невозможно сохранять атрибуты профиля пользователя в БД BVS. Также невозможно сохранение метаданных, кроме метаданных профиля пользователя, которые имеют отображения LDAP (вкладка «Настройки отображения»).

Это может включать отображение ролей, отображение групп и другие метаданные на основе конфигурации отображений LDAP.

Обновление пользователя невозможно при попытке изменить некоторые данные пользователя, не имеющие отображение LDAP. Например, нельзя отключить пользователя LDAP, если флаг, характеризующий активность пользователя, не имеет отображения на соответствующий атрибут LDAP (что обычно не так).

Важные атрибуты и параметры настройки федераций

При настройке федерации потребуется заполнить поля атрибутов:

- атрибут Username в LDAP: атрибут LDAP, который отображается как имя пользователя;
  Для прочих серверов LDAP это может быть «uid». Для Active Directory это может быть «sAMAccountName» или «cn».
  Атрибут должен быть заполнен для всех LDAP записей пользователей, которые необходимо импортировать из LDAP;
- атрибут RDN LDAP: имя атрибута LDAP, который используется как RDN (верхний атрибут) типичного пользователя DN.
  Обычно это то же самое, что и атрибут Username LDAP, однако он не является обязательным.
  Например, для Active directory обычно используется «cn» в качестве атрибута RDN, когда атрибут «username» может иметь значение «sAMAccountName»; С обычным каталогом LDAP (не Active Directory), где пользователь DNs обычно uid=XXX,ou=people,dc=example,dc=com, следует использовать «uid».
  Атрибут RDN фактически используется при создании нового пользователя в BVS. Если в настройках федерации для параметра «Режим редактирования» установлено значение «С возможностью записи», то BVS синхронизирует его обратно в каталог LDAP, т. е. создает новую запись пользователя в LDAP.
  Для формирования полного DN нового пользователя необходим RDN и «Пользовательский DN».

- атрибут UUID LDAP: имя атрибута LDAP, который используется в качестве уникального идентификатора объекта (UUID) для объектов в LDAP.
  Для многих поставщиков серверов LDAP это «entryUUID», однако некоторые из них отличаются. Например, для Active Directory он должен иметь значение «objectGUID». Если сервер LDAP действительно не поддерживает понятие UUID, то можно использовать любой другой атрибут, который имеет уникальность для пользователей LDAP в дереве.
  Например, «uid» или «entryDN». Любой стандартный каталог LDAP v3 должен использовать entryUUID (OpenLDAP, OpenDJ и т.п.).
- опция «Синхронизировать регистрации»;
  Данная опция может быть включена, если необходимо, чтобы новые пользователи, созданные в BVS, добавлялись в LDAP, при условии поддержки LDAP-сервером функции добавления новых пользователей.
  Пользователи, через службу учетных записей пользователей, и администраторы, через консоль администратора, могут изменять метаданные пользователей.
  В зависимости от настроек можно обладать правами на обновление LDAP или нет. Параметр конфигурации «Режим редактирования» определяет политику редактирования в LDAP:

> *а) «Только для чтения»;*
> > *Имя пользователя, адрес электронной почты, имя, фамилия и другие сопоставленные атрибуты нельзя изменить. Система BVS будет показывать ошибку каждый раз, когда кто-нибудь пытается обновить эти поля. Также нет поддержки обновления паролей.*
> *б) «С возможностью записи».*
> > *Имя пользователя, адрес электронной почты, имя, фамилия и другие сопоставленные атрибуты и пароли могут быть обновлены и будут автоматически синхронизированы с LDAP.*

- опция «Несинхронизированный».
  Любые изменения имени пользователя, электронной почты, имени, фамилии и паролей будут храниться в локальном хранилище системы.
  Рекомендуется *не изменять* переключатель режима редактирования, сохраняя режим, заданный при создании федерации LDAP. При переключении режимов сложно будет понять какие данные внесены вручную, а какие были импортированы из LDAP.
  Это также относится к переключателю «Импорт пользователей».

Способы фильтрации пользователей

Существует несколько способов фильтрации пользователей. С помощью создания отображения типа:

- «Получение индивидуальной группы», т.е создание внутренних групп BVS;
- «Преобразование группы LDAP в отображение» и импортирование групп из AD в BVS.

Ещё один способ – с помощью фильтрации через «Дополнительный LDAP фильтр».

Создание и настройка федерации

В панели управления BVS для требуемого домена выбрать:

> *Безопасность >> Федерации*

Страница отображает список федераций в системе.

Из контекстного меню кнопки [Создать] выбрать – «LDAP». В открывшемся окне «Создание федерации LDAP» заполнить основную конфигурационную информацию о федерации.

> *Примечания.*
> *При нажатии на пиктограмму «i» рядом с наименованием поля параметра открывается push уведомление с подсказкой для заполнения.*
> *Обязательные для заполнения поля имеют красную подпись «Введите значение».*
> *После заполнения всех обязательных полей кнопка [Создать] становится доступной.*

Следует обратить внимание на важный атрибут «Классы ролевых объектов» – «groupOfNames,nestedgroup». Последний класс позволит отобразить роли в веб-интерфейсе.

Для успешной синхронизации ролей из BVS в LDAP необходимо указать наименование уникального атрибута у роли «Атрибут UUID в LDAP» - «cn»; если поле оставить не заполненным, то в качестве атрибута будет использован одноименный атрибут из федерации.

Например:

– для инсталляции `AD Windows` устанавливаются значения параметров:

> - «Атрибут Username в LDAP» - cn или sAMAccountName;
> - «Атрибут RDN в LDAP» - cn;
> - «Атрибут UUID в LDAP» - objectGUID.

– для инсталляции `LDAP Linux` устанавливаются значения параметров:

> - «Атрибут Username в LDAP» - uid;
> - «Атрибут RDN в LDAP» - uid;

- «Атрибут UUID в LDAP» – uuid.

Примечание.
Если изменить значение параметра «Атрибут Username в LDAP» на `UserPrincipalName`, то это значение параметра позволяет отображать имя пользователя с принадлежностью к домену и пользователи разделены по доменам.

После заполнения этих параметров кнопка [Создать] становится активной, создать федерацию нажатием на неё. Произойдет переход на страницу с детальной информацией о созданной федерации.

10.2.2 Настройка отображений

Отображения используются для интеграции системы с LDAP. Они запускаются, когда пользователь входит в систему через LDAP, или приходит запрос для пользователя из консоли администратора.

В состав федерации LDAP включается (автоматически) некоторый набор встроенных отображений. Пользователь может внести новые или вовсе удалить отображения. Ниже перечислен состав данного набора:

- преобразование атрибута LDAP в отображение;

Позволяет указать, какой атрибут LDAP сопоставлен с каким атрибутом пользователя BVS.
Например, можно настроить отображение почты LDAP в BVS. Для этой реализации отображения всегда существует взаимно-однозначное сопоставление (один атрибут LDAP сопоставляется с одним атрибутом BVS).

- преобразование полного имени LDAP в отображение;

Позволяет указать, что полное имя пользователя, хранимое в атрибуте LDAP (обычно cn), будет перенесено на атрибуты firstName и lastname пользователя BVS. Наличие в cn полного имени пользователя – частый случай.

- получение индивидуального атрибута;

Это преобразование поддерживается только в том случае, если включен параметр «Синхронизировать регистрации». При регистрации нового пользователя в системе будет создана запись о нем в LDAP с жестко заданным значением некоторого указанного атрибута.

- получение ролей из LDAP;

Позволяет настраивать отображение ролей из LDAP в BVS. Отображение ролей может использоваться для сопоставления ролей LDAP (обычно групп из определенной ветви дерева LDAP) в роли, соответствующие либо ролям области, либо ролям клиента указанного клиента.
Настроить несколько отображение ролей для одного и того же сервера LDAP довольно легко. Например, можно указать, что отображение ролей из групп в разделах ou=main,dc=example,dc=org будут ролями областей BVS, а отображение ролей из групп в разделах ou=finance,dc=example,dc=org будут ролями клиента BVS.

- получение индивидуальной группы;

Когда пользователь импортируется из LDAP, он автоматически добавляется в эту настроенную группу.

- получение индивидуальной роли;

Когда пользователь импортируется из LDAP, он автоматически добавляется в эту настроенную роль.

- преобразование MSAD LDS в отображение;

Отображение для настройки MSAD LDS. Он может интегрировать состояние учетной записи пользователя MSAD LDS в состояние учетной записи системы учетная запись включена, срок действия пароля истек и т.д.). Используются атрибуты msDS-UserAccountDisabled и pwdLastSet.
Например, если pwdLastSet равен 0, пользователю требуется обновить пароль, если `msDS-UserAccountDisabled` включено, пользователь также отключен и т.д. Отображение также может обрабатывать код исключения при аутентификации пользователя в LDAP.

- преобразование MSAD в отображение;

Отображение для настройки MSAD. Он может интегрировать состояние учетной записи пользователя MSAD в состояние учетной записи (учетная запись включена, срок действия пароля истек и т. Д.). Для этого используются атрибуты `userAccountControl` и `pwdLastSet` MSAD.
Например, если pwdLastSet равен 0, пользователю требуется обновить пароль, если `userAccountControl` равен 514 (отключенная учетная запись), пользователь также отключен и т.д. Отображение также может обрабатывать код исключения при аутентификации пользователя в LDAP.

- преобразование сертификата LDAP в отображение;

Используется для отображения единственного атрибута, который содержит сертификат пользователя LDAP, с атрибутом `UserModel` в базе данных системы;

- преобразование уникального атрибута LDAP в отображение;

Используется для сопоставления одиночного уникального атрибута пользователя LDAP с атрибутом `UserModel` в базе данных;

- получение ролей из LDAP;

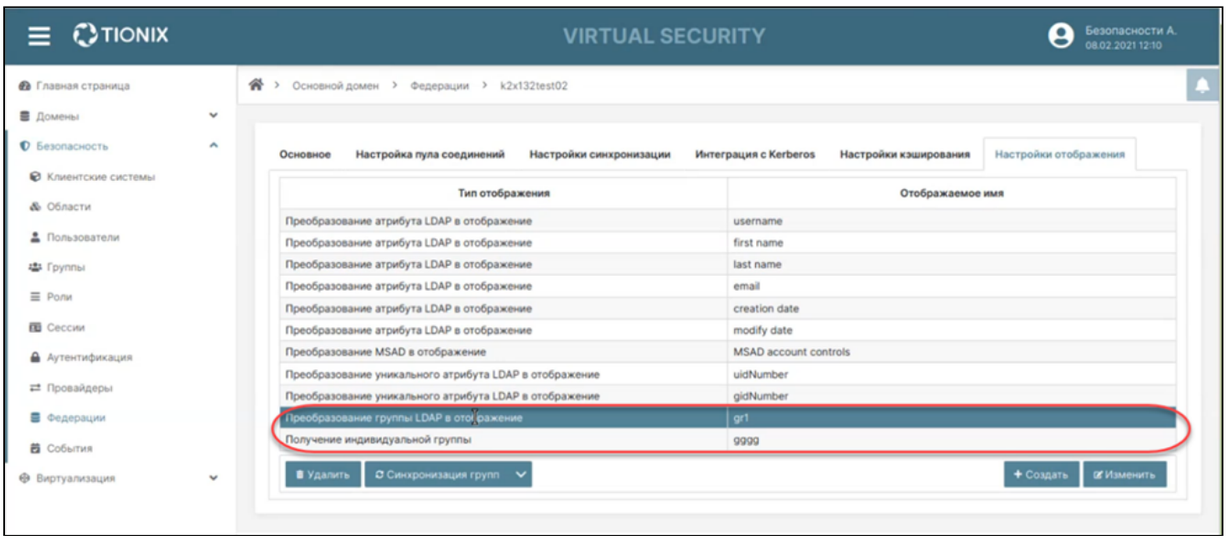
Используется для отображения ролей из LDAP DN;

- преобразование группы LDAP в отображение - отображение групп LDAP.

Создание отображений для импорта групп из AD

Во вкладке «Настройки отображения» по умолчанию отображается список из девяти отображений. Данные отображения отвечают за импорт пользователей, из AD в BVS.

Для импорта групп из удаленного AD в BVS необходимо создать два новых отображения. Например, с именами gr1 и gggg.



Создание отображения

Для создания отображений следует нажать на кнопку «Создать» в мастер-окне и заполнить поля:

- для отображения gr1 в поле «Тип отображения»:

> *выбрать опцию «Преобразование группы LDAP в отображение»;*

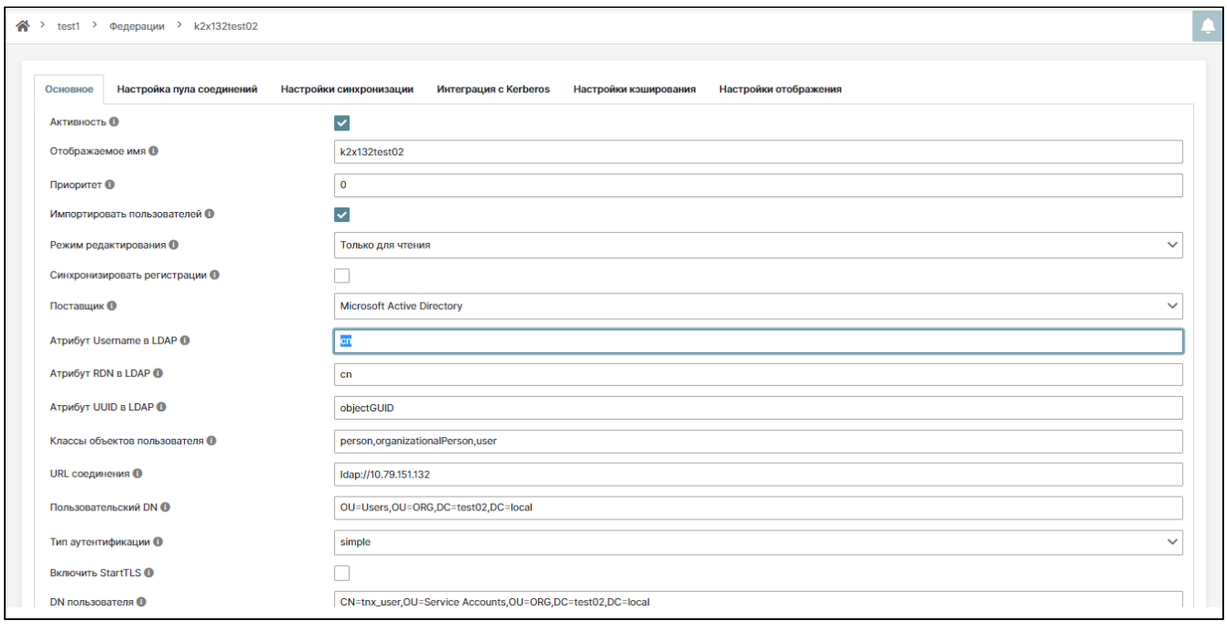
- в поле «LDAP группы DN:

> *внести наименование группы, где будет выполнено сохранение: `OU=Groups,OU=Org,DC=tst01,DC=local`.*

Настройка отображения

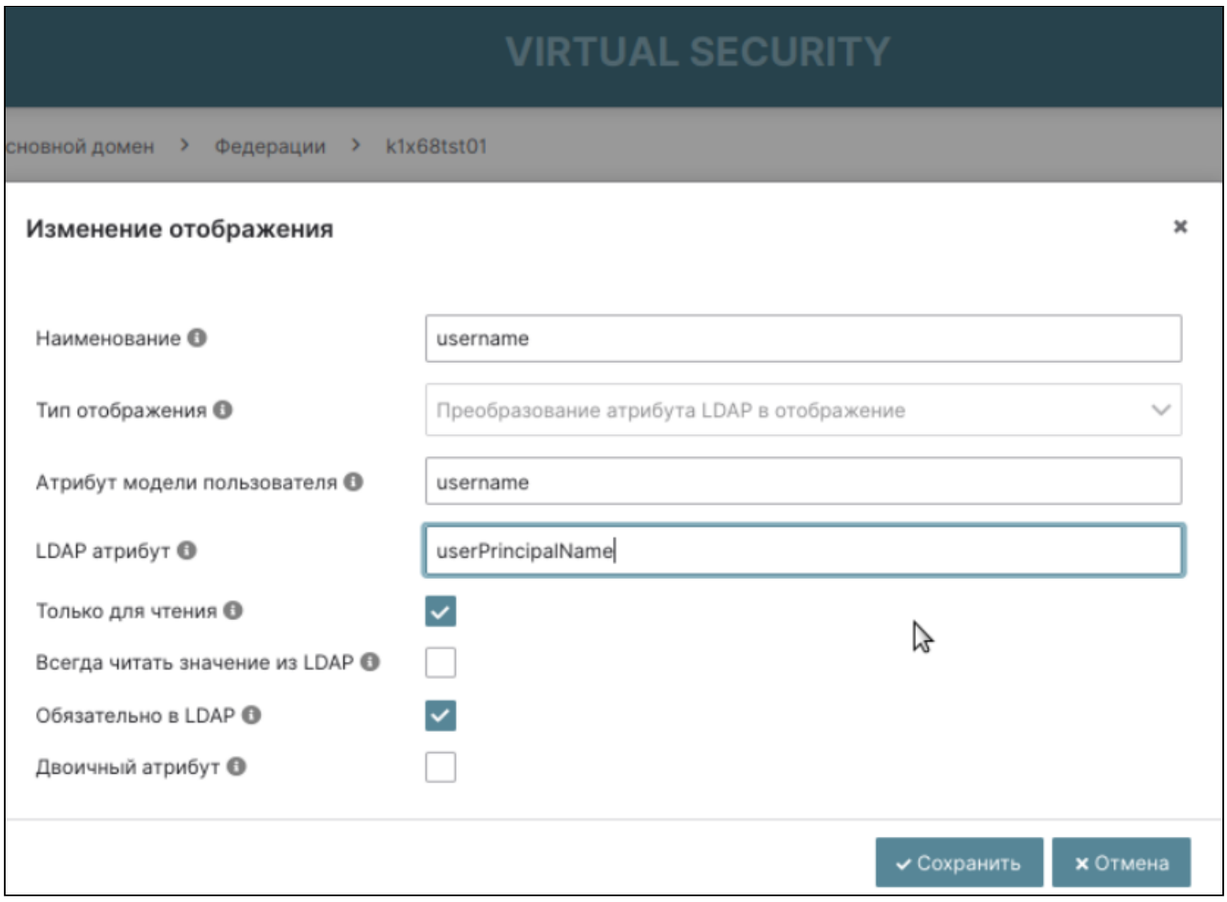
Для настройки отображения перейти в одноименную вкладку на странице детальной информации о федерации.

Выделить тип отображения «Преобразование атрибута LDAP в отображение» с отображаемым именем «username». Активизируется кнопка «Изменить». После нажатия кнопки отобразится окно «Изменение отображения».



Изменение отображения

В поле «LDAP атрибут» следует ввести значение: `userPrincipalName`.

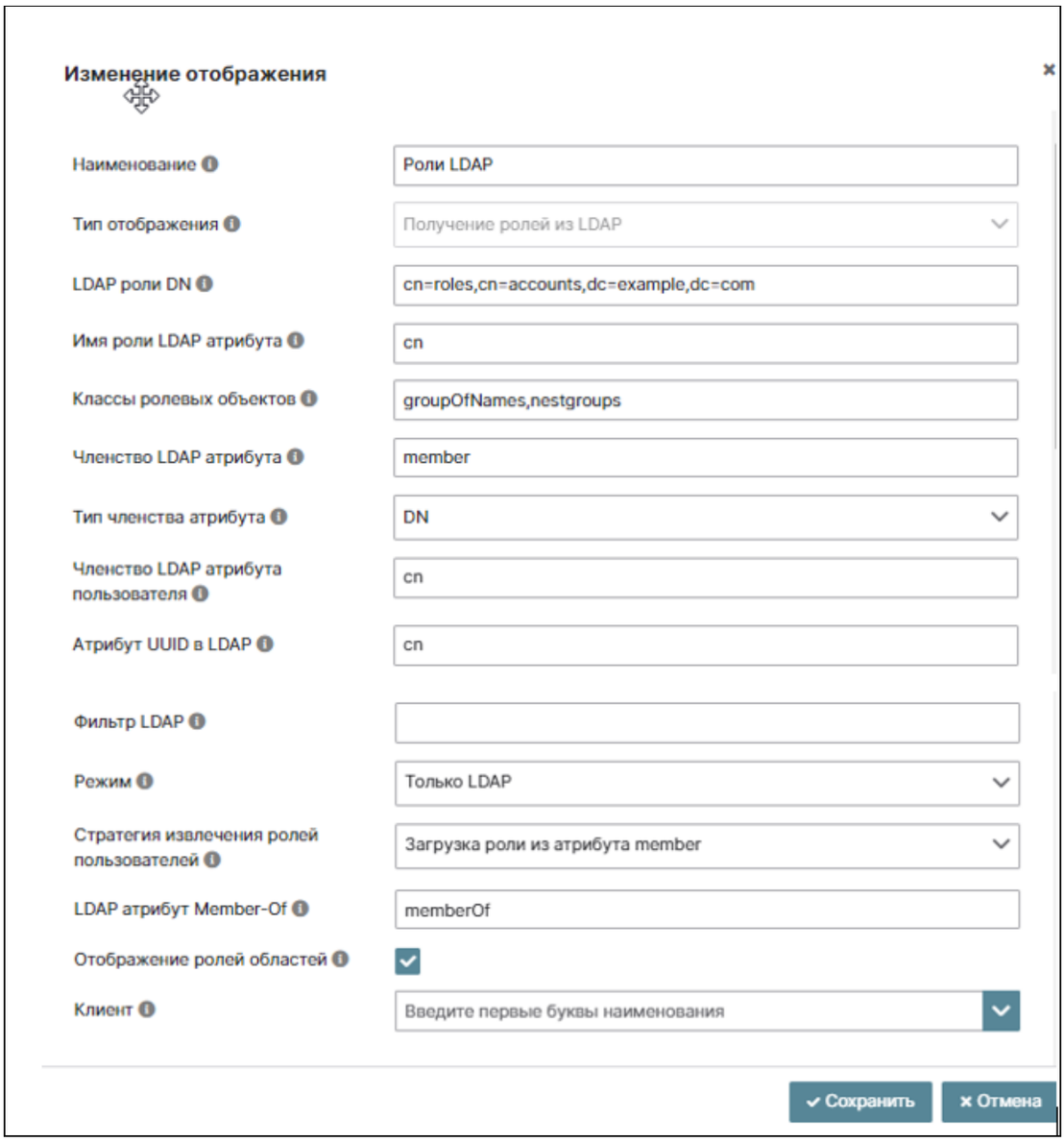


Значение атрибута LDAP - userPrincipalName

10.2.3 Роли LDAP

Настройка отображения ролей LDAP имеет параметры, указанные ниже:

- следует обратить внимание на важный атрибут «Классы ролевых объектов» - «groupOfNames,nestedgroup». Последний класс позволит отобразить роли в веб интерфейсе;
- для успешной синхронизации ролей из BVS в LDAP необходимо указать наименование уникального атрибута у роли «Атрибут UUID в LDAP» - «cn»;
- если поле оставить не заполненным, то в качестве атрибута будет использован одноименный атрибут из федерации.

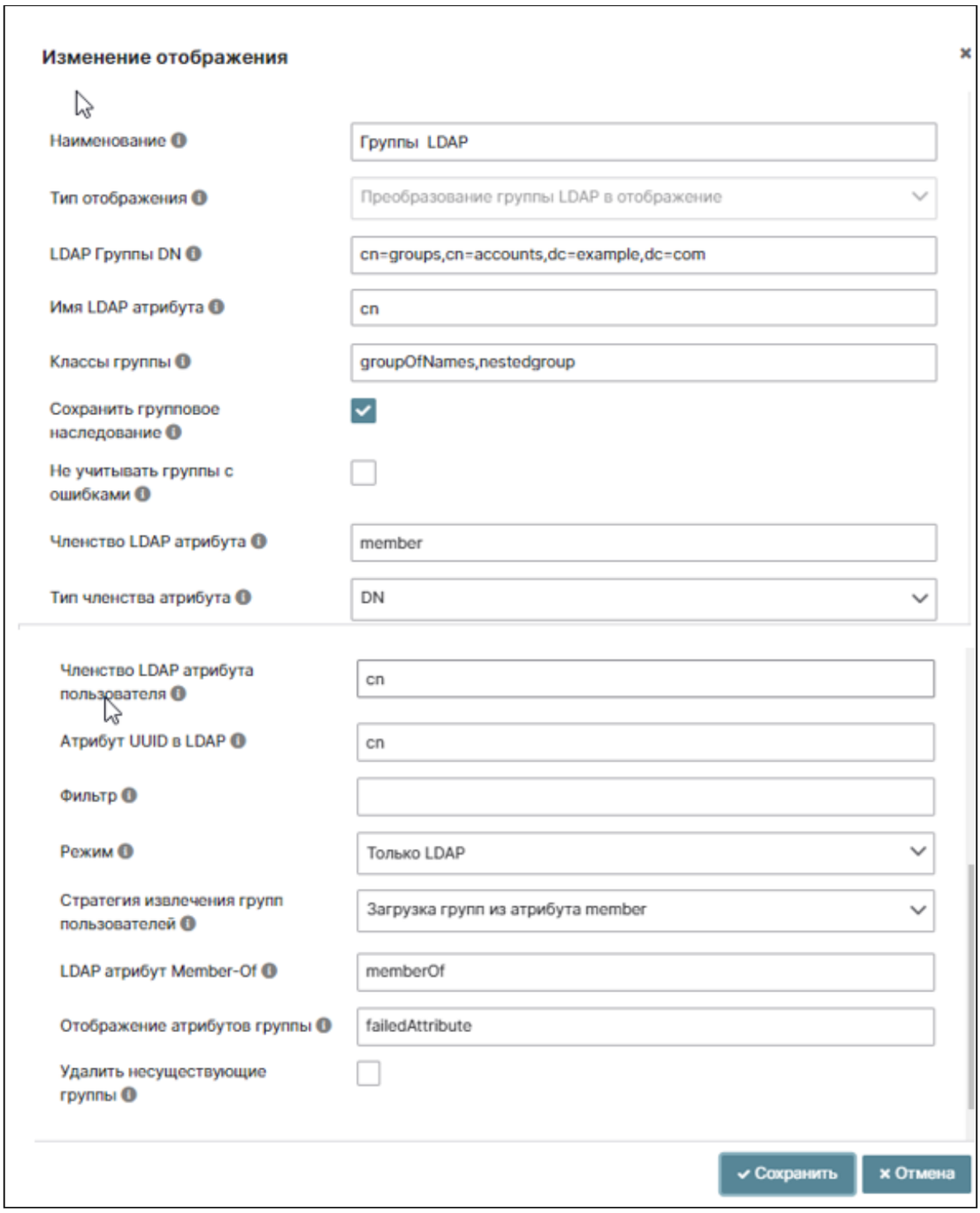


Настройка ролей LDAP

10.2.4 Группы LDAP

Настройка отображения групп LDAP имеет параметры, указанные ниже:

- важный атрибут «Классы группы» - «groupOfNames,nestedgroup,ipaUserGroup». Последние два класса позволят отобразить группы в веб интерфейсе.
- для успешной синхронизации групп из BVS в LDAP необходимо указать наименование уникального атрибута у группы «Атрибут UUID в LDAP» - «cn»;
- если поле оставить не заполненным, то в качестве атрибута будет использован одноименный атрибут из федерации.



Настройка групп LDAP

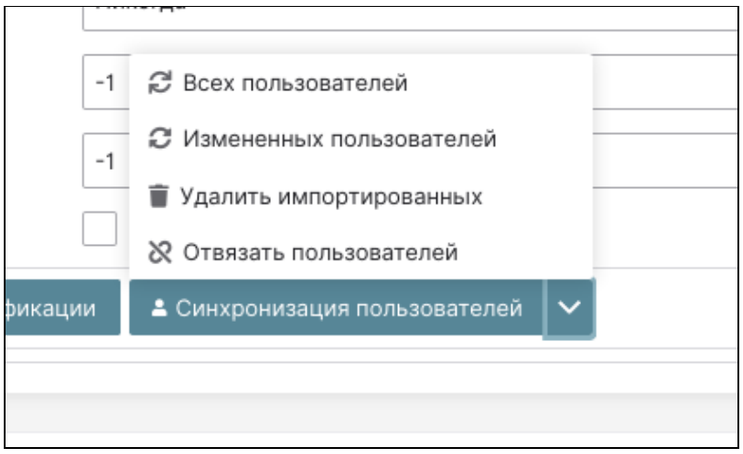
Для добавления группы следует выделить созданное отображение и нажать на кнопку «Изменить». Откроется окно «Изменение отображения».

Например, добавить группу для сохранения пользователей. В поле «Тип отображения» выбрать опцию «Получение индивидуальной группы» (indgroup). Завершить операцию создания (изменения) отображения нажатием кнопки «Создать» («Сохранить»). Создание отображения «Получение индивидуальной группы» позволяет помещать всех пользователей, приходящих из AD в BVS (в группу).

10.2.5 Синхронизация данных

В системе предусмотрена функция синхронизации данных (атрибуты пользователя, роли, группы). Синхронизация возможна по желанию пользователя.

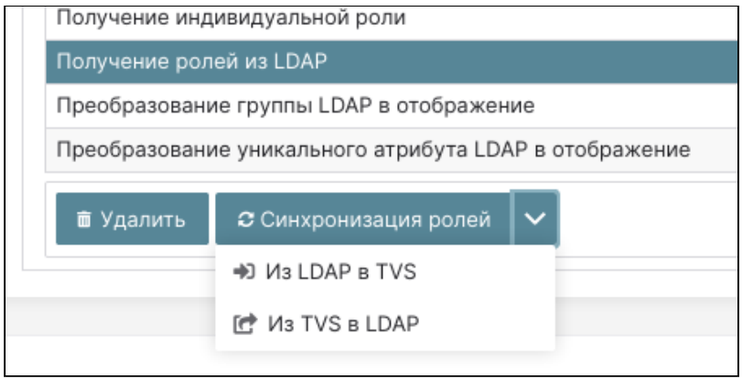
Кнопки, используемые для синхронизации, показаны ниже:



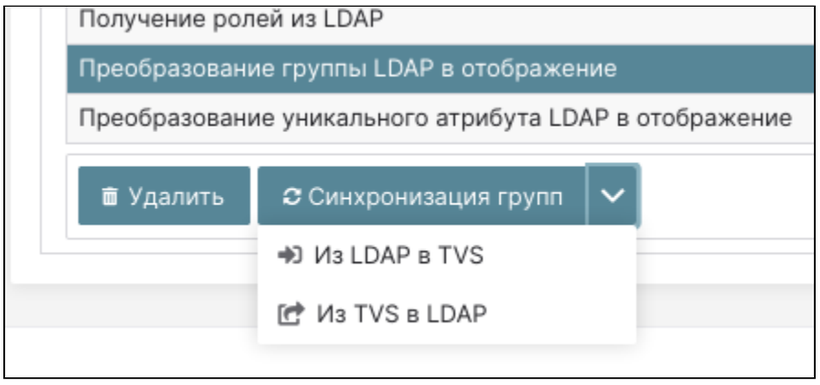
Опции синхронизации. Управление пользователями

Способы синхронизации:

- синхронизация ролей;
- синхронизация групп.



Опции синхронизации ролей



Опции синхронизации групп

При синхронизации пользователей одновременно выполняется синхронизация ролей и групп из LDAP в BVS, при наличии настроенного отображения. Если у группы в LDAP есть настроенные роли, то при синхронизации из LDAP связь не переносится.

На вкладке «Настройки синхронизации» можно настроить период обновления данных в автоматическом режиме.

Выполняется обновление пользователей, групп, ролей.

Для отображения групп, ролей можно использовать различные режимы синхронизации:

– «Только для чтения»:

> *импорт данных из LDAP возможен совместно с «Получение индивидуальной роли»/»Получение индивидуальной группы», но обратный импорт из BVS в LDAP запрещен. Синхронизируются данные при изменении в LDAP;*

– «Импорт»:

> *импорт данных из LDAP возможен совместно с «Получение индивидуальной роли»/»Получение индивидуальной группы», но дальнейшей синхронизации нет. Можно выполнить импорт изменений из BVS в LDAP;*

– «Только LDAP»:

> *выполняется импорт данных из LDAP без «Получение индивидуальной роли»/»Получение индивидуальной группы». Синхронизируются группы и роли пользователя, также можно выполнять импорт изменений из BVS в LDAP с добавлением новых данных.*

10.3 Интеграция службы идентификации Keystone с каталогом (AD, LDAP)

Каталог на основе `Active Directory` имеет структуру, построенную с помощью группировки объектов каталога. Для группировки объектов каталога используется объект типа «Организационные подразделения» – OU.

При построении структуры OU используется функционально-организационный принцип. При развертывании подсистемы каталога автоматически создаются встроенные OU и контейнеры. Такие организационные подразделения не могут быть переименованы.

На верхнем уровне домена создаются OU с префиксом, назначаемым на этапе проектирования. Внутри верхнего уровня OU создаются OU по организационному принципу, с указанием местного организационного кода для OU.

Далее, в соответствии с именованием корневых OU в созданных организационных подразделениях, располагаются учетные записи компьютеров и пользователей групп.

10.3.1 Модель групповых политик

Групповые политики используются для управления настройками свойств групп компьютеров и пользователей, в том числе: параметрами безопасности, развертыванием программного обеспечения, сценариями, перенаправлением папок и предпочтениями.

Предпочтения групповой политики (Preferences) – это более двадцати расширений групповой политики, увеличивающих количество настраиваемых параметров в объекте групповой политики.

По умолчанию, создаются следующие групповые политики для домена:

- политики паролей пользователей и политики блокировки учетных записей – Default Domain Policy;
- настройки для контроллеров домена, в том числе, настройки журналов событий, настройки репликации, фиксация сетевых портов и т. д. – Default Domain Controller Policy.

Для интеграции службы идентификации Keystone с BVS необходимы параметры конфигурации (OU и т.п.), приведенные в таблице реквизитов доступа.

10.3.2 Реквизиты доступа каталога

Для интеграции службы идентификации Keystone с каталогом Active Directory или LDAP требуются параметры каталога, которые послужат вводными данными для службы Keystone.

Перечень параметров (реквизитов доступа) приведен в таблице 5.

Таблица 5 - Реквизиты доступа по умолчанию

N	Название	Формат значения по умолчанию в BVS	Примечание
1	Домен	master.tionix.ru	Префикс по умолчанию «master», его добавляет сам BVS
2	Пользователь, который получает список ou	user = cn=osproxy,ou=system,dc=master,dc=tionix,dc=ru	Дефолтный пользователь osproxy в BVS
3	Суффикс	suffix = dc=tionix,dc=ru	Обратить внимание на то, что должен отсутствовать префикс «master»

N	Название	Формат значения по умолчанию в BVS	Примечание
4	Фильтр	#user_filter = (memberOf=cn=USERS,cn=PC_USERS,cn=AB,dc=cd,dc=ru)	Параметр необязателен
5	Список пользователей	user_tree_dn = ou=users,dc=master,dc=tionix,dc=ru	Значение параметра - путь к размещению пользователей
6	Группы	group_tree_dn = ou=groups,dc=master,dc=tionix,dc=ru	Значение параметра - путь к размещению группы
7	Область поиска	query_scope = one	Значения могут варьироваться. Для LDAP возможное значение = sub, а для BVS значение = one. Важен поиск на одном уровне

10.3.3 Подготовка конфигурационного файла службы Keystone

Добавить в конфигурационный файл `/etc/keystone/keystone.conf` секцию [identity]:

domain_specific_drivers_enabled = True
domain_config_dir = /etc/keystone/domains

Создание конфигурационного файла (для BVS):

/etc/keystone/domains/keystone.NAME_DOMAIN.conf

Рекурсивная смена права доступа на каталог

Выполнить команду:

sudo chown keystone:keystone -R /etc/keystone/domains

Привести конфигурационный файл `/etc/keystone/domains/keystone.NAME_DOMAIN.conf` к следующему виду:

```
[identity]

driver = ldap

[ldap]

#вместо ip адреса может быть dns имя
url = ldaps://10.7.11.22:10640

# ниже параметр отвечает за сертификат, доступный через
# `echo -n | openssl s_client -connect 10.7.11.22:10640`
tls_cacertfile = "/etc/openldap/certs/tvs.cert"

# ниже параметр имеет значение - “принимать все сертификаты, даже самоподписанные”.
# Используется при невозможности скачать сертификат и положить по указанному адресу (tls_cacertfile)
tls_req_cert = allow

user = cn=osproxy,ou=system,dc=master,dc=tionix,dc=ru
password = tvspass
suffix = dc=tionix,dc=ru
use_dumb_member = False
```

```
allow_subtree_delete = False

user_tree_dn = ou=users,dc=master,dc=tionix,dc=ru
user_objectclass = person

group_tree_dn = ou=groups,dc=master,dc=tionix,dc=ru
group_objectclass = group

user_allow_create = False
user_allow_update = False
user_allow_delete = False

group_allow_create = False
group_allow_update = False
group_allow_delete = False

# для TVS важно значение one
query_scope = one

user_id_attribute = uid
user_name_attribute = uid
user_mail_attribute = uid
user_pass_attribute = userPassword

group_id_attribute = uid
group_name_attribute = uid
group_member_attribute =
group_desc_attribute = description
```

10.3.4 Перезапуск службы httpd или nginx

Выполнить одну из команд:

sudo systemctl restart httpd.service
или
sudo systemctl restart nginx.service

10.3.5 Создание домена и проекта

Выполнить команды:

sudo openstack domain create NAME_DOMAIN
sudo openstack project create --domain NAME_DOMAIN NAME_PROJECT

10.3.6 Проверка успешности интеграции

Выполнить команду:

sudo openstack user list --domain NAME_DOMAIN

Вывод списка пользователей свидетельствует об успешной интеграции службы идентификации Keystone с BVS. Если на этом шаге вывод пуст или не содержит пользователей из BVS, то процесс интеграции не завершен и требуется искать причину.

Проверку доступности LDAP BVS можно произвести, выполнив команду:

ldapsearch -s one -w tvspass -x -D cn=osproxy,ou=system,dc=master,dc=tionix,dc=ru \
-H ldaps://10.7.11.22:10640 -x -b ou=users,dc=master,dc=tionix,dc=ru ""

В ОС CentOS может содержаться запрет на самоподписанные сертификаты, поэтому необходимо отредактировать конфигурационный файл (настройки ldapsearch):

nano /etc/openldap/ldap.conf

Доступ пользователя (с правами администратора домена)

Получить ID домена — *LAB*, выполнив команду:

sudo openstack domain show NAME_DOMAIN

```
# Пример вывода команды
+---------+-----------------------------------+
| Field   | Value                             |
+---------+-----------------------------------+
| включено | Истинный                         |
| id       | ID_NAME_DOMAIN                   |
| name     | LAB                              |
+---------+-----------------------------------+
```

Пример вывода команды получения ID домена

Получить ID пользователя-администратора, выполнив команду:

sudo openstack role list

```
# Пример вывода команды
+----------------------------------+---------------+
| ID                               | Name          |
+----------------------------------+---------------+
| ID_ADMIN_ROLE                    |user           |
| ID_USER_ROLE                     |admin
|
+----------------------------------+---------------+
```

Пример вывода команды получения ID пользователя

> *Примечания.*
> *Это не дает учетной записи администратора OpenStack никаких прав на фактический домен AD DS/ BVS/LDAP.*
> *Термин «домен» относится к использованию OpenStack в ключевом домене.*

Назначение пользователю домена роли администратора

Выполнить команду добавления роли с правами администратора пользователю домена, применив ранее полученные параметры (ID_NAME_DOMAIN, ID_USER):

sudo openstack role add --domain ID_NAME_DOMAIN --user ID_USER role_id

Предоставление доступа пользователю домена к выделенному проекту

Выполнить команду присвоения прав администратора в проекте (NAME_PROJECT) пользователю домена:

sudo openstack role add --project NAME_PROJECT --user ID_USER admin

Предоставление доступа к проекту группе AD (при наличии группы)

При условии создания группы в AD требуются дополнительные действия. Получить список групп AD, выполнив команду:

sudo openstack group list --domain LAB

Результат выполнения показан ниже:

```
# Пример вывода команды
+----------------------------------------+---------------------
+
| ID                                     |
Name                 |
+----------------------------------------+---------------------
+
|xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx        |grp-openstack
|xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx        |grp-openstack-admin
|xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx        |grp-openstack-demo
+----------------------------------------+---------------------
+
```

Пример вывода команды получения списка групп

Получить список ролей пользователей, выполнив команду:

sudo openstack group list --domain LAB

```
# Пример вывода команды
+----------------------------------------------------------++
| ID                                  |  Name                |
+----------------------------------------------------------++
|xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx | grp-openstack        |
|ID_ADMIN_____________________________ | grp-openstack-admin |
|ID_DEMO______________________________ | grp-openstack-demo  |
+----------------------------------------------------------++
```

Пример вывода команды получения списка ролей пользователей

Предоставить доступ к проекту группе AD, выполнив команду:

sudo openstack role add --project demo --group ID_DEMO _member_

10.3.7 Подключение к облачной платформе и создание ВМ

Авторизуйтесь в TIONIX.Dashboard от имени доменного пользователя и создайте виртуальные машины.

10.4 Веб-доступ к VDI-машине

Помимо использования клиента TIONIX VDI, доступ к виртуальному рабочему столу может быть осуществлен удаленно, через веб-интерфейс (HTTP/HTTPS).

Для перехода к консоли в веб-браузере укажите URL в формате:

> *<IP-адрес или имя хоста>:<номер порта (по умолчанию 8888)>/vdi/*

Авторизуйтесь с использованием реквизитов, выданных администратором проекта. В окне авторизации введите наименование домена и учетные данные пользователя. Нажмите кнопку «Войти» и ожидайте выполнения процесса авторизации.

> *Примечание.*
> *После успешной авторизации отобразится страница проекта и список доступных VDI машин. При отсутствии таковых в проекте для авторизованного пользователя будет создана новая машина.*
> *Для удаленного доступа к (веб-) консоли виртуальной машины используется сетевой порт 8888 .*
> *Функциональность обеспечивается модулем TIONIX.VDIserver.*

В общем списке ВМ выводятся VDI машины, найденные в проекте, доступном для авторизованного пользователя. Для каждого элемента списка отображаются параметры.

Таблица 6 - Параметры VDI машины

Наименование поля	**Описание**
Наименование	Имя VDI машины, присваивается пользователем при создании.
Проект	Проект, к которому относится VDI машина.
Имя образа	Имя образа VDI машины.
Размер	Мощности VDI машины, задаются при создании и могут быть изменены пользователем при помощи команды изменения размера машины.
Статус	Состояние машины, определяемое службами Openstack.
Питание	Состояние питания VDI машины.
Создан	Дата создания VDI машины.

По умолчанию, отображаются VDI машины со статусами: «Активна», «На паузе», «Отключена» и «В ошибке».

Для детального просмотра сессий перейдите во вкладку:

> *ТИОНИКС >> VDI >> Виртуальные машины >> Детали инстанса >> Сессия*

11 Обслуживание образов VDI машин

В данной главе рассмотрены два возможных сценария использования дисков, обслуживаемых службой Cinder:

1. Использование дисков Cinder в качестве корневых для машин VDI.
2. Использование дисков Cinder в качестве дополнительных для машин VDI.

> *Примечание.*
> *Оба варианта дисков могут как сохраняться после удаления ВМ, так и удаляться вместе с ней.*

Все операции с манипуляциями устройствами, обслуживаемыми Cinder, должны происходить исключительно силами `REST API`. Какие-либо альтернативные способы взаимодействия с Cinder не предусмотрены.

Также предполагается, что в рамках проекта VDI у пользователя может быть только одна ВМ с одним корневым и дата-дисками.

11.1 Параметры Cinder для проекта VDI

На вкладке `Project Volumes` содержатся начальные параметры, с которыми при создании VDI машин будут создаваться диски. Вкладка содержит два основных параметра:

- бинарный параметр `Create the root volume on block service` (yes/no). По умолчанию: no.
- бинарный параметр `Create the data volume on block service` (yes/no). По умолчанию: no.

При включении первого бинарного параметра (… root …) VDI-модуль перед фактическим запуском самой машины создаст корневой диск в Cinder, созданный из образа для проекта VDI.

При включении второго бинарного параметра (… data …) VDI-модуль перед фактическим запуском машины создаст диск в Cinder и примонтирует этот диск к ВМ, как второе блочное устройство.

При включении этих параметров должны появиться поля для настройки.

– для `Create the root volume on block service`:

- параметр `Default volume size` с числовым значением с размерностью «ГБ»;
- параметр `Default availability zone` для указания зоны доступности блочных устройств; По умолчанию: «nova».
- параметр `Default volume type` со списком доступных типов блочных устройств; По умолчанию: «default»; если его нет, то первый по алфавиту. Пустой список должен вызвать ошибку.
- бинарный параметр `Delete on terminate` (yes/no); По умолчанию: yes; если необходимо, оставлять/удалять диск после удаления машины VDI в проекте.
- параметр `Name template`, где можно указать шаблон для имен создаваемых дисков. Параметр опциональный. В случае отсутствия этого параметра диску выдается UUID; если имеется, то значение параметра используется как префикс к UUID, разделенный через дефис: coolproject-root-$UUID.
- бинарный параметр `Backup when delete` - во время удаления ВМ перед удалением диск сохраняется как образ в Glance. По умолчанию: no

– для `Create the data volume on block service`:

- параметр `Default volume size` с числовым значением с размерностью «ГБ».
- параметр `Default availability zone` для указания зоны доступности блочных устройств. По умолчанию: nova.
- параметр `Default volume type` со списком доступных типов блочных устройств. По умолчанию: «default», если его нет, то первый по алфавиту. Пустой список должен вызвать ошибку.
- бинарный параметр `Delete on terminate` (yes/no); По умолчанию: no; если необходимо, оставлять/удалять диск после удаления машины VDI в проекте.
- параметр `Name template`, где можно указать шаблон для имен создаваемых дисков. Параметр опциональный. В случае отсутствия этого параметра диску выдается UUID; если имеется, то значение параметра используется как префикс к UUID, разделенных через дефис: coolproject-data-$UUID.
- бинарный параметр `Backup when delete` - во время удаления ВМ перед удалением диск сохраняется как образ в Glance. По умолчанию: yes

11.2 Описание алгоритма создания дисков с помощью Cinder

При активации функции `Create the root volume on block` перед созданием VDI машины модуль должен:

1) Убедиться, что размер образа в `Default image` и параметр `Default volume size` совпадают или размер образа меньше, чем параметр Default volume size.

> *В противном случае должно отобразиться информационное сообщение о том, что размер корневого диска должен быть равен или больше размера образа. В качестве размера образа нужно брать виртуальный, а не фактический (актуально для qcow2-образов).*

2) Образ, указанный в Default image должен являться источником данных при создании диска.

3) При создании корневого диска нужно взять все параметры, которые были указаны в параметрах проекта.

4) Полученный образ нужно использовать как загрузочный для ВМ.

5) Если у пользователя сохранился корневой диск от прошлой ВМ, и если не указано иного, то нужно использовать уже имеющийся.

> *В противном случае необходимо вначале удалить старый корневой диск (опционально, предварительно сохранив старый корневой диск в образы Glance).*

При активации функции `Create the root volume on block` перед созданием VDI машины модуль должен:

- создать диск нужного размера;
- после запуска ВМ примонтировать дата-диск к ВМ;
- если у пользователя сохранился дата диск от прошлой ВМ, и если не указано иного, то нужно использовать уже имеющийся.

> *В противном случае необходимо вначале удалить старый дата диск (опционально предварительно сохранив его в образах Glance).*

11.3 Изменение параметров по умолчанию при создании ВМ VDI

По умолчанию предполагается, что диски для VDI машины будут создаваться параметрами, указанными в проекте VDI. Однако, может возникнуть ситуация, при котором конкретной ВМ нужно предоставить свои параметры дисков.

Поэтому предлагается добавить вкладку `Custom settings for volumes`. Она будет также разделена на два основных бинарных параметра:

– `Custom settings for root volume`.

– `Custom settings for data volume`.

Каждый параметр содержит в себе:

- `Volume size` с числовым значением с размерностью ГБ;
- `Delete on terminate` (бинарный параметр - yes/no);
- `Backup on delete` (бинарный параметр - yes/no).

Параметры, указанные во время создания ВМ, имеют приоритет над параметрами, указанными в проекте.

Замена зон доступности и типов дисков не предусмотрено, они всегда берутся из данных проекта.

11.4 Вариант резервного копирования дисков при их удалении

Удаление каких-либо данных - это всегда рискованная операция, поэтому для дата-дисков по умолчанию рекомендуется включить параметр `Backup on delete` – после создания образа диски удаляются. Данный параметр помогает (опосредованно) решить задачу запуска корневого или дата-диска в другом проекте.

Параметр можно включить и для корневых дисков, если требуется, например, сделать из него золотой образ.

Краткий алгоритм, при включении параметров `Backup on delete` и `Delete on terminate`: после запуска процесса удаления ВМ происходит удаление самой ВМ; в то же время, из диска (ов), которые были подключены к ВМ, создаются образы, которые сохраняются в Glance. Эту операцию можно производить в фоновом режиме.

11.5 Загрузка готовых образов

Готовые к загрузке/размещению в ОП образы, содержащие предустановленные гостевые ОС, могут быть скачаны по ссылке:

> *http://storage.tionix.ru/pub/cloud_images/windows/*

12 Обновление ПО

12.1 Обновление модуля TIONIX.VDIserver

Важно

Все команды выполняются только от суперпользователя.

Режим суперпользователя:

```
sudo -i
```

1. Обновление модуля из репозитория RPM-пакетов:
   ```
   yum clean all
   yum update --disablerepo=* --enablerepo=tionix-modules,tionix-extras python3-tionix_vdi_server
   ```
2. Выполнение настройки модуля:
   ```
   openstack tnx configure -n tnx_vdi_server tnx_client
   ```
   Важно
   При обновлении модуля на двух и более контроллерах необходимо синхронизировать содержание файла `/etc/tionix/.vdi_server_secret_key` на всех контроллерах.
3. Обновление базы данных:
   ```
   openstack tnx db migrate -n tnx_vdi_server
   ```
4. Перезапуск веб сервера:
   ```
   systemctl restart httpd
   ```

Завершение процедуры обновления, перезапуск служб модуля:

```
systemctl restart tionix-*
```

12.2 Обновление файла конфигурации модуля TIONIX.VDIserver

Важно

Все команды выполняются только от суперпользователя.

Режим суперпользователя:

```
sudo -i
```

Для того чтобы изменения в файле конфигурации вступили в силу, необходимо перезапустить веб-сервер, а также службы модуля:

```
systemctl restart httpd
systemctl restart tionix-vdi-*
```

12.3 Обновление модуля TIONIX.VDIclient

12.3.1 Для Linux

Важно

Все команды выполняются только от суперпользователя.

Режим суперпользователя:

```
sudo -i
```

Обновление модуля TIONIX.VDIclient:

RPM-пакет

Выполните:

```
yum clean all
yum update --disablerepo=* --enablerepo=tionix-modules,tionix-extras tionix-vdi-client
```

DEB-пакет

1. Подключите в системный каталог `/etc/apt/sources.list` репозиторий с DEB-пакетами:
   deb [trusted=yes] http://deb-repo.tionix.ru/stable tionix x.x

   Где: x.x - номер необходимой версии клиента.
   Подсказка
   Для установки последней разрабатываемой версии модуля укажите репозиторий:
   deb [trusted=yes] http://deb-repo.tionix.ru/release tionix-rc x.x

   Где: x.x - номер необходимой версии клиента.
2. Обновите список репозиториев:
   apt-get update
3. Обновите модуль TIONIX.VDIclient:
   apt-get upgrade tionix-vdi-client

12.3.2 Для Windows

Обновление клиента в Windows можно осуществить несколькими способами, поверх старой версии клиента или предварительно удалив старую версию клиента. Перед обновлением желательно удалить из домашней директории пользователя каталог `/user/.tionix-vdi-client`.

12.3.3 Для MacOS

1. Найдите приложение в «Launchpad» или в окне «Finder» в разделе «Applications».
2. Перетащите приложение в корзину либо выделите программу и выберите «Файл» - «Переместить в Корзину».
3. Скачайте новую версию приложения и произведите процедуру установки.

13 Удаление ПО

13.1 Полное удаление модуля TIONIX.VDIserver

Все команды выполняются только от суперпользователя.

Режим суперпользователя:

sudo -i

При возникновении необходимости удаления RPM-пакета модуля выполните команду:

yum remove python3-tionix_vdi_server

Примечание

Файлы настроек и лог файлы при этом не будут удалены так же, как и таблицы в базе данных.

13.2 Полное удаление модуля TIONIX.VDIserver

1. Удалите модуль TIONIX.VDIserver:
   yum remove python3-tionix_vdi_server
2. Удалите настройки модуля TIONIX.VDIserver:
   rm -rf /etc/tionix/vdi_server.yaml
3. Удалите базу данных MySQL модуля TIONIX.VDIserver:
   # Зайдите в базу данных, используя пароль пользователя root
   mysql -uroot -p
   # Удалите базу данных tionix_vdi_server
   DROP DATABASE tionix_vdi_server;
4. Удалите конфигурационные файлы Apache:
   rm -rf /etc/httpd/conf.d/tionix-vdi-web.conf
5. Удалите директорию с лог файлами модуля TIONIX.VDIserver:
   rm -rf /var/log/tionix/vdi-server
6. Удалите сервис VDIserver API:
   openstack service delete tnx-vdi
7. Удалите службы модуля в systemd:
   systemctl stop tionix-vdi-server-api.service
   systemctl disable tionix-vdi-server-api.service
   systemctl stop tionix-vdi-broker-api.service
   systemctl disable tionix-vdi-broker-api.service
   systemctl stop tionix-vdi-keystone-listener.service
   systemctl disable tionix-vdi-keystone-listener.service
   systemctl stop tionix-vdi-nova-listener.service
   systemctl disable tionix-vdi-nova-listener.service
   systemctl stop tionix-vdi-project-syncer.service
   systemctl disable tionix-vdi-project-syncer.service
   systemctl stop tionix-vdi-user-syncer.service
   systemctl disable tionix-vdi-user-syncer.service
   systemctl stop tionix-vdi-worker.service
   systemctl disable tionix-vdi-worker.service

   systemctl daemon-reload
   rm /usr/lib/systemd/system/tnx-vdi-*
   systemctl reset-failed
8. Выполните перезапуск веб-сервера:
   systemctl restart httpd
9. Перезапустите службу Nova:
   systemctl restart openstack-nova-api

13.3 Удаление модуля TIONIX.VDIclient

13.3.1 Для Linux

Важно

Все команды выполняются только от суперпользователя.

Режим суперпользователя:

```
sudo -i
```

При возникновении необходимости удаления RPM-пакета модуля выполните команду:

```
yum remove tionix-vdi-client
```

Для удаления DEB-пакета выполните команду:

```
apt-get remove tionix-vdi-client
```

13.3.2 Для Windows

Удаление осуществляется стандартными инструментами операционной системы. Для полного удаления клиента необходимо удалить из домашней директории пользователя каталог `/user/.tionix-vdi-client`.

13.3.3 Для MacOS

1. Найдите приложение в «Launchpad» или в окне «Finder» в разделе «Applications».
2. Перетащите приложение в корзину либо выделите программу и выберите «Файл» - «Переместить в Корзину».

14 Диагностика ПО

14.1 Диагностика модуля TIONIX.VDIclient

Важно

Все команды выполняются только от суперпользователя.

Режим суперпользователя:

sudo -i

14.1.1 Логирование служб, используемых модулем

Логирование осуществляется с помощью модуля `logging`.

Если в файле `client.conf` не указан параметр `log_file_location`, то логирование происходит в файл `tionix-vdi-client.log`, расположенный в домашней директории пользователя в каталоге `.tionix-vdi-client`. Если этот параметр указан, то в директории, путь до которой равен значению параметра, создается файл логов. В этом случае к наименованию файла добавляется имя пользователя, запустившего приложение, например, `tionix-vdi-client-admin.log`.

Подсказка

Для включения вывода трейсбека в файл с логами нужно задать в системе переменную окружения `TNX_DEBUG`.

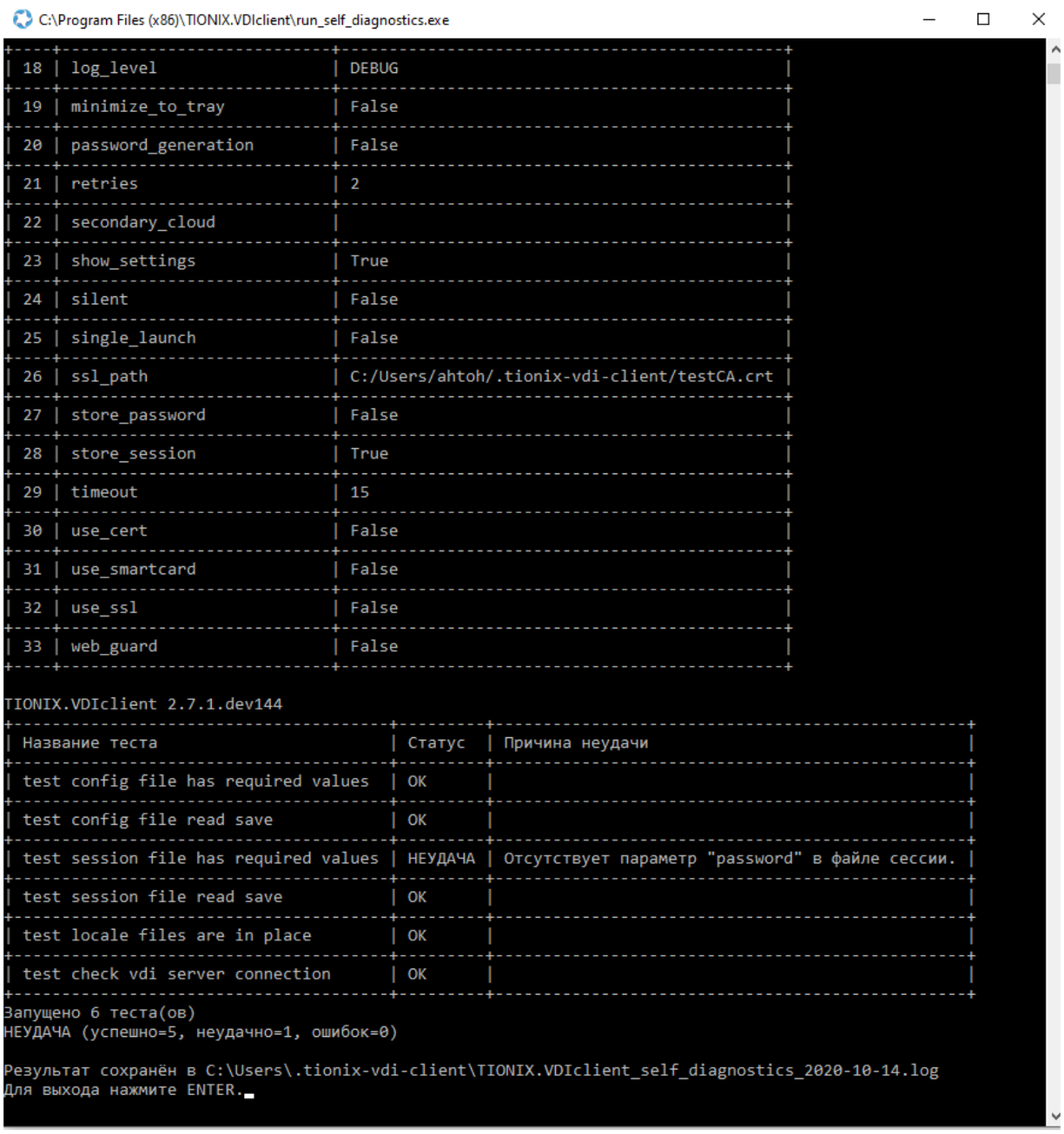
Примечание

С описанием процесса логирования, предоставляемого платформой OpenStack, можно ознакомиться в соответствующем разделе официальной документации.

14.1.2 Диагностика модуля в операционной системе Windows

Произвести самодиагностику модуля можно при помощи приложения `run_self_diagnostics.exe`, которое находится в корневом каталоге установленного модуля TIONIX.VDIclient.

Пример результата самодиагностики:



Диагностика модуля в Windows

Результат самодиагностики записывается в файл `TIONIX.VDIclient_self_diagnostics_YYYY-MM-DD.log` и сохраняется в каталоге, который задан для записи файлов логирования.

14.1.3 Диагностика модуля в операционной системе Linux

Произвести самодиагностику модуля в операционной системе Linux можно при помощи команды `tionix_vdi_client --diagnostic`.

Пример выполнения команды:

```
tionix_vdi_client --diagnostic
2019-05-15 12:26:44.333 17961 INFO tionix_vdi_client.settings [-] Log file path: /home/
user/.tionix-vdi-client/tionix-vdi-client.log

========================================
Извлеченные параметры: TIONIX.VDIclient
========================================
+----+---------------------------+-----------------------------------------+
| N | Variable name | Value |
+----+---------------------------+-----------------------------------------+
| 1 | PYKCS11LIB | |
+----+---------------------------+-----------------------------------------+
| 2 | SMARTCARD_OID | |
```

```
+----+---------------------------+-----------------------------------------+
| 3 | additional_clouds | |
+----+---------------------------+-----------------------------------------+
| 4 | cloud | test.stand.loc |
+----+---------------------------+-----------------------------------------+
| 5 | contact_support_message_en | Please contact system administrator. |
+----+---------------------------+-----------------------------------------+
| 6 | contact_support_message_ru | Обратитесь к системному администратору. |
+----+---------------------------+-----------------------------------------+
| 7 | domain_name | default |
+----+---------------------------+-----------------------------------------+
| 8 | get_vm_timeout | 5 |
+----+---------------------------+-----------------------------------------+
| 9 | ignore_domain | False |
+----+---------------------------+-----------------------------------------+
| 10 | ikecfg | |
+----+---------------------------+-----------------------------------------+
| 11 | language | ru |
+----+---------------------------+-----------------------------------------+
| 12 | log_file_location | |
+----+---------------------------+-----------------------------------------+
| 13 | log_level | INFO |
+----+---------------------------+-----------------------------------------+
| 14 | password_generation | True |
+----+---------------------------+-----------------------------------------+
| 15 | project | True |
+----+---------------------------+-----------------------------------------+
| 16 | retries | 2 |
+----+---------------------------+-----------------------------------------+
| 17 | secondary_cloud | |
+----+---------------------------+-----------------------------------------+
| 18 | show_settings | True |
+----+---------------------------+-----------------------------------------+
| 19 | store_session | True |
+----+---------------------------+-----------------------------------------+
| 20 | store_password | False |
+----+---------------------------+-----------------------------------------+
| 21 | timeout | 15 |
+----+---------------------------+-----------------------------------------+
| 22 | use_smartcard | True |
+----+---------------------------+-----------------------------------------+
| 23 | web_guard | False |
+----+---------------------------+-----------------------------------------+


TIONIX.VDIclient 2.1.0
+--------------------------------------+--------+-----------------+
| Название теста | Статус | Причина неудачи |
+--------------------------------------+--------+-----------------+
| test check vdi server connection | OK | |
+--------------------------------------+--------+-----------------+
| test config file has required values | OK | |
+--------------------------------------+--------+-----------------+
| test config file read save | OK | |
+--------------------------------------+--------+-----------------+
| test session file has required values | OK | |
+--------------------------------------+--------+-----------------+
| test session file read save | OK | |
+--------------------------------------+--------+-----------------+
| test locale files are in place | OK | |
+--------------------------------------+--------+-----------------+
Запущено 6 теста(ов)
OK (успешно=6, неудачно=0, ошибок=0)

Результат сохранён в /home/user/.tionix-vdi-client/
TIONIX.VDIclient_self_diagnostics_2019-05-15.log
```

15 Диагностика модуля TIONIX.VDIserver

Важно

Все команды выполняются только от суперпользователя.

Режим суперпользователя:

sudo -i

15.1 Логирование служб, используемых модулем TIONIX.VDIserver

Логирование происходит с помощью модуля `logging`.

По умолчанию, файл логов находится в директории `/var/log/tionix/vdi-server/`.

В каталоге находятся следующие файлы:

- `vdi-server-api.log` - файл сбора сообщений службы `tionix-vdi-server-api`;
- `vdi-broker-api.log` - файл сбора сообщений службы `tionix-vdi-broker-api`;
- `keystone-listener.log` - файл сбора сообщений службы `tionix-vdi-keystone-listener`;
- `project-syncer` - файл сбора сообщений службы `tionix-vdi-project-syncer`;
- `user-syncer` - файл сбора сообщений службы `tionix-vdi-user-syncer`;
- `nova-listener.log` - файл сбора сообщений синхронизации виртуальных машин между базой данных службы Nova и базой данных TIONIX.VDIserver;
- `worker.log` - файл сбора сообщений асинхронных задач модуля;
- `tionix_lntmov.log` - файл сбора сообщений о попытках пользователей авторизоваться и получить VDI машину через веб-интерфейс VDI или TIONIX.VDIclient. Логируются как успешные, так и неуспешные попытки. Включение или отключение процесса логирования определяется параметром `ALLOW_GETVM_LOG` в конфигурационном файле `vdi_server.yaml`. Подробное описание параметра `ALLOW_GETVM_LOG` доступно в разделе «Файл конфигурации». Записи в файле имеют следующий формат:
  [системное время VDI сервера] - идентификатор запроса - источник подключения (web/cli) - логин пользователя (который осуществляет попытку подключения) - статус получения IP-адреса VDI машины (OK/Error, а также детали ошибки) - ID групп, к которым принадлежит пользователь - проект подключения - IP-адрес пользователя
- `profiler.log` - файл сбора сообщений с идентификаторами запросов к API VDI и `tnx_vdi_worker` на каждом этапе:
  - получение запроса;
  - создание задачи;
  - запуск задачи;
  - ожидание мьютекса;
  - старт мьютекса;
  - отправка запроса в Nova на создание виртуальной машины;
  - получение ответа (профилирование процесса получения виртуальной машины).

  Также логируется общее время ожидания мьютекса для каждого запроса. Запись сообщений в данный файл осуществляется только в режиме `DEBUG`.

> *Примечание.*
> *С описанием процесса логирования, предоставляемого платформой OpenStack, можно ознакомиться в соответствующем разделе официальной документации.*

15.2 Отладка модуля TIONIX.VDIserver

В случае возникновения проблем в работе модуля существуют следующие пути решения:

1) Выставить уровень логирования в значение DEBUG, что позволит зафиксировать сообщения о событиях в лог-файлах с максимальной детализацией для диагностики и решения проблем.

2) Запустить утилиту самодиагностики модуля `openstack tnx tests`.

Пример использования:

```
openstack tnx tests --names tnx_vdi_server --modules
Диагностика модулей TIONIX началась.
Запускаем тесты для: tnx_vdi_server
```

```
+-------------------------
+-----------------------------------------------------------------------------------+
| Дата и время запуска | Пт 30 апр 2021 13:22:21 MSK |
+-------------------------
+-----------------------------------------------------------------------------------+
| Версия OpenStack | Victoria (22.2.0) |
+-------------------------
+-----------------------------------------------------------------------------------+
| Имя хоста | test.stand.loc |
+-------------------------
+-----------------------------------------------------------------------------------+
| Дистрибутив | CentOS Linux 8 |
+-------------------------
+-----------------------------------------------------------------------------------+
| Управляющие узлы | 1 |
+-------------------------
+-----------------------------------------------------------------------------------+
| Вычислительные узлы | 2 |
+-------------------------
+-----------------------------------------------------------------------------------+
| База данных | mysql Ver 15.1 Distrib 10.3.28-MariaDB, for Linux (x86_64) using readline
5.1 |
+-------------------------
+-----------------------------------------------------------------------------------+
| Источник пакетов | rpm-centos.tionix.ru |
+-------------------------
+-----------------------------------------------------------------------------------+
| Версия tionix-licensing | 3.0.0 |
+-------------------------
+-----------------------------------------------------------------------------------+

================
TIONIX.VDIserver
Версия: 3.0.0 (актуальная: текущая)
Лицензия: 07-002-972fb12437f60c4a5411 (действительна до 31.09.2021 03:00:00)
================
+--+--------------------------------------+--------
+-------------------------------------------------------------+
|N |Название теста |Статус |Причина неудачи |
+--+--------------------------------------+--------
+-------------------------------------------------------------+
|1 |test apache config enabled |УСПЕХ | |
+--+--------------------------------------+--------
+-------------------------------------------------------------+
|2 |test apache config existence |УСПЕХ | |
+--+--------------------------------------+--------
+-------------------------------------------------------------+
|3 |test config file existence |УСПЕХ | |
+--+--------------------------------------+--------
+-------------------------------------------------------------+
|4 |test connection to keystone |УСПЕХ | |
+--+--------------------------------------+--------
+-------------------------------------------------------------+
|5 |test connection to nova |УСПЕХ | |
+--+--------------------------------------+--------
+-------------------------------------------------------------+
|6 |test license validity |УСПЕХ | |
+--+--------------------------------------+--------
+-------------------------------------------------------------+
|7 |test migrations applied |УСПЕХ | |
+--+--------------------------------------+--------
+-------------------------------------------------------------+
|8 |test profiler log file accesses |ПРОПУЩЕН|Тест актуален только в случае, если в
LOG_LEVEL указан DEBUG. |
+--+--------------------------------------+--------
+-------------------------------------------------------------+
|9 |test registered celery tasks |УСПЕХ | |
+--+--------------------------------------+--------
+-------------------------------------------------------------+
```

```
|10|test registered tasks to schedule |УСПЕХ | |
+--+----------------------------------------+--------
+-------------------------------------------------------------+
|11|test request vm log file accesses |УСПЕХ | |
+--+----------------------------------------+--------
+-------------------------------------------------------------+
|12|test vdi api |УСПЕХ | |
+--+----------------------------------------+--------
+-------------------------------------------------------------+
|13|test vdi server api connection |УСПЕХ | |
+--+----------------------------------------+--------
+-------------------------------------------------------------+
|14|test vdi server api service registration|УСПЕХ | |
+--+----------------------------------------+--------
+-------------------------------------------------------------+
|15|test vdi server systemd services |УСПЕХ | |
+--+----------------------------------------+--------
+-------------------------------------------------------------+
|16|test vdi web |УСПЕХ | |
+--+----------------------------------------+--------
+-------------------------------------------------------------+
Запущено 16 за 47.537сек.
УСПЕХ (успешно=15, неудачно=0, ошибок=0)

====
ИТОГ
===
Запущено 16 за 47.537сек.
УСПЕХ (успешно=15, неудачно=0, ошибок=0)
```

16 Термины и определения

ACL – (англ. Access Control List) список контроля доступа, который определяет, кто или что может получать доступ к конкретному объекту, и какие именно операции разрешено или запрещено проводить над объектом (конкретному субъекту).
Active Directory – служба каталогов – программная система, которая хранит, организовывает и обеспечивает доступ к хранимой (каталожной) информации. С позиции программного инжиниринга, каталог – карта соответствий между именами и значениями. Служба каталогов позволяет выполнять поиск значений, заданных в виде имени, в полной аналогии со словарем.
AppImage – универсальный исполняемый формат (приложение в контейнере).
BIOS – (англ. Basic Input-Output System) базовая система ввода-вывода – программа, запускаемая в первую очередь, при включении персонального компьютера. Современные СВТ, не предназначенные для персонального использования (серверы или материнские платы архитектуры, отличной от Intel x86), зачастую не имеют прошивки BIOS, но при этом оснащаются специальной платой обслуживания (BMC).
BMC – (англ. Baseboard Management Controller) аппаратно-программное решение, известное также как IPMI. Возможности интеллектуального управления платформой – ключевой компонент обеспечения управления системами с высокой степенью готовности к эксплуатации на предприятии.
CLI – (англ. Command Line Interface) интерфейс командной строки – разновидность неграфического интерактивного интерфейса, при котором после ввода команд происходит выполнение некоторого процесса с последующим выводом полученного результата (сообщение, код ошибки, файл с данными).
DEB – формат программного пакета, предназначенного к установке в дистрибутивы Linux, совместимые с ОС Debian (www.debian.org).
Django – фреймворк, используемый веб-браузером при отображении элементов интерфейса управления инфраструктурой. Фактически – рабочая среда для создания каркасного графического интерфейса пользователя.
Glance – служба образов облачной платформы OpenStack.
GTK – фреймворк, содержащий набор виджетов – элементов графического интерфейса пользователя (формы, диалоги).
HTTPS – (англ. HyperText Transfer Protocol Secure) расширение протокола HTTP, поддерживающее шифрование. Передаваемые по протоколу HTTPS данные «упаковываются» посредством криптографических средств SSL или TLS, тем самым обеспечивая защиту данных. В отличие от HTTP, HTTPS использует для передачи TCP-порт 443 (по умолчанию).
IPMI – (от англ. Intelligent Platform Management Interface) интеллектуальный интерфейс управления платформой, предназначенный для автономного мониторинга и управления функциями, встроенными непосредственно в аппаратное и микропрограммное обеспечения серверных платформ.
LDAP – (Lightweight Directory Access Protocol) относительно простой протокол, использующий TCP/IP и позволяющий производить операции аутентификации (bind), поиска (search) и сравнения (compare), а также – операции добавления, изменения или удаления записей.
microSD – разновидность носителей на основе флеш-памяти, производимых в виде карт памяти.
Microsoft AD – синоним Active Directory.
NVMe – (англ. Non-Volatile Memory Host Controller Interface Specification) протокол доступа к твердотельным накопителям, подключённым по шине PCI Express. Также встречается в виде терминов NVM Express или NVMHCI. NVM обозначает энергонезависимую память, в качестве которой в SSD повсеместно используется флеш-память типа NAND.
OpenStack – группа проектов свободного ПО, составляющая основу открытой облачной платформы с поддержкой различных подсистем виртуализации.
OpenVPN – (англ. Open Virtual Private Network) открытая реализация логической сети, создаваемой поверх другой сети (например – Интернет). VPN позволяет объединить несколько офисов организации в единую сеть с использованием для связи между ними неподконтрольных каналов (сетей провайдера).
PCIe – (англ. Peripheral Component Interconnect Express) компьютерная шина, использующая программную модель шины PCI и высокопроизводительный физический протокол, основанный на последовательной передаче данных. На физическом уровне шиной не является, т.к. топологически представляет собой соединение типа «точка-точка».
RDP – (англ. Remote Desktop Protocol) проприетарный протокол прикладного уровня, который используется для обеспечения удаленной работы пользователя с сервером, на котором запущен сервис терминальных подключений.
REST API – интерфейс подготовки и отправки запросов, а также обработки ответов в микросервисной архитектуре, определяющей стиль взаимодействия компонентов распределённого приложения в сети.
RPM – формат программного пакета, предназначенного к установке в дистрибутивы Linux, совместимые с ОС RedHat (www.redhat.com).
SPICE – (англ. Simple Protocol for Independent Computing Environments) «простой протокол для независимой вычислительной среды» – протокол, используемый в рамках проекта системы отображения (рендеринга) удаленного дисплея, которая позволяет просматривать виртуальный рабочий стол, функционирующий в любой вычислительной среде. Открытое решение для удаленной работы с компьютером, обеспечивающее доступ клиента к дисплею и устройствам (клавиатура, мышь, звук) удаленной машины.
SSD – (англ. Solid State Drive) энергонезависимое, перезаписываемое компьютерное запоминающее устройство без движущихся механических частей. Твердотельный накопитель данных, реализованный для замены дискового накопителя (НЖМД); в таком накопителе для создания ячеек данных

долговременного хранения используется другой физический процесс, не опирающийся на магнитные свойства (доменных структур).
SSH - (англ.) протокол безопасного (удаленного) доступа к консоли.
SSL - (англ. Secure Socket Layer) протокол защищенной связи через Интернет в системе «клиент – сервер», использует обмен открытыми ключами для шифрования сообщений для идентификации участников платежей и защиты каналов связи. Клиенты и серверы могут аутентифицировать друг друга и обмениваться зашифрованными данными.
TCP - транспортный протокол Интернета. Сети и подсети, в которых совместно используются протоколы TCP и IP, называются сетями TCP/IP.
TCP/IP - «стек» протоколов передачи данных для всемирной глобальной сети Интернет, используемых управления передачей данных.
URL - (англ. Universal Resource Locator) универсальный локатор ресурсов; синоним – веб-ссылка.
UsbDk - (англ. USB Development Kit) библиотека, предназначенная для пользовательских приложений Windows, обеспечивающая прямой эксклюзивный доступ к USB-устройствам.
VDI - (англ. Virtual Desktop Infrastructure) технология, позволяющая создавать виртуальную IT-инфраструктуру и разворачивать полноценные рабочие места на базе физического сервера, обслуживающего множество виртуальных машин.
VLAN – (англ. Virtual Local Area Network) виртуальная локальная вычислительная сеть.
VNC - (англ. Virtual Network Computing) система удаленного доступа к рабочему столу компьютера, использующая протокол RFB (Remote FrameBuffer).
VNC - (англ. Virtual Networking Console) виртуальная сетевая консоль – сетевой протокол удаленного доступа к рабочему столу, функционирующему в настольной гостевой ОС виртуальной машины или на ПК.
VPN - (англ. Virtual Private Network) «виртуальная частная сеть» – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети (Интернет).
Авторизация - процедура проверки, в ходе которой выясняется, имеет ли пользователь, процесс или приложение право выполнить действие.
АРМ - автоматизированное рабочее место администратора инфраструктуры или пользователя виртуальной машины, подключение к которой осуществляется посредством VDI проекта.
ОС - операционная система – системное ПО, обеспечивающее для ПО (ОСПО) среду функционирования и доступ к ресурсам аппаратного или виртуального узла (оперативной памяти, файловым системам, сетевым интерфейсам, системным библиотекам и системам управления репозиториями).
ПК - (синоним - PC, от англ. personal computer) персональный компьютер.
ПО - программное обеспечение.
САВЗ - средство антивирусной защиты.
СВТ - средство вычислительной техники (персональный компьютер, тонкий клиент, ноутбук, нетбук, планшетный компьютер и т.п.).
СЗИ - средство защиты информации.
ТК - тонкий клиент (разновидность СВТ). Широко распространенный тип вычислительных устройств, подключаемых к информационной инфраструктуре предприятия по сети и предназначенных для выполнения операторских функций.