Переход с Microsoft Active Directory на РЕД АДМ. Два подхода к миграции ИТ-инфраструктуры

Окружение

- **Версия ОС:** 7.3
- **Конфигурация ОС:** 7.3
- **Версия ПО:** redadm-1.1.0

В рамках текущей статьи будет рассмотрено *два подхода* к переносу ИТ-инфраструктуры на отечественную систему централизованного управления, а именно – обзор возможностей и пошаговая инструкция, подготовка домена к миграции, установка доверительных отношений или создание параллельной инфраструткуры.

В РЕД АДМ используется подход «*в центре всего есть контроллер*». Далее будет подробнее рассмотрен процесс перехода от инфраструктуры на базе продуктов Microsoft Windows на решения РЕД СОФТ.

Существует несколько сценариев миграции. Следует понимать, что все эти сценарии «сферические в вакууме», их нужно **адаптировать** для каждого конкретного случая, однако, общие подходы необходимо рассмотреть. Часть из этих сценариев рассмотрены в нашем обучающем курсе, другие будут добавлены в курс в будущем.

Примечание.

Обратите внимание, что изменения в инфраструктуре необходимо **сначала** проверять **в тестовой среде** и только потом реализовывать изменения в продуктовой среде!

Репликация

Рассмотрим ситуацию, когда в организации существует контроллер на базе MS AD. К контроллеру подключены клиентские машины на базе ОС Windows, предоставлены различные сервисы – файловое хранилище, возможность централизованной установки ОС на новые машины, получение клиентскими машинами настроек с помощью GPO.

Репликация — один из самых удобных способов выполнения миграции с MS AD. При этом, в отличие от описанных далее способов, при репликации нет необходимости настраивать параллельный доступ к используемым сервисам из двух доменов. Необходимо просто добавить новый контроллер домена РЕД АДМ в домен, проверить работоспособность инфраструктуры и сервисов, и, по готовности, вывести контроллер домена Windows из эксплуатации.

Перед вводом новых контроллеров в домен следует убедиться, что в нем отсутствуют ошибки репликации, а также пройден чек-лист «здоровье домена». Каждый системный администратор должен иметь такой чек-лист и периодически проверять «здоровье» вверенного ему домена.

Чек-лист проверки «здоровья домена»

Для проверки «здоровья» домена необходимо выполнить следующий алгоритм действий:

1. Проверить состояние репликации, выполнив:

```
repadmin /replsum
repadmin /showrepl
```

2. Проверить состояние служб домена, выполнив:

```
dcdiag /q
```

Проверить, что все контроллеры домена (если их несколько) используют **DFS-R** для репликации **SYSVOL**:

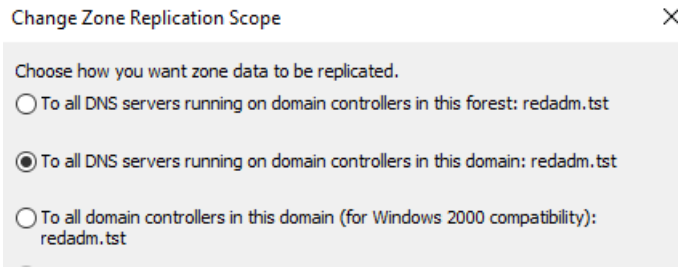
```
dfsrmig /getmigrationstate
```

Провести миграцию репликации **SYSVOL** на **DFS-R**, если она не была проведена ранее. Миграция необходима, если изначально домен был развернут с уровнем

домена леса **2008 или ниже**, т.к. до уровня 2008 для репликации каталога **SYSVOL** использовался механизм **FRS**.

Провести диагностический отчет по репликации **DFS-R** («Оснастка DFS management» — «Replication» — «Create Diagnostic Report»). При наличии ошибок необходимо их устранить.

3. В оснастке DNS проверить свойства прямых и обратных зон («Свойства зоны» — вкладка «General» — «Replication»).



Должен быть установлен один из первых двух вариантов.

Проверьте зону `_msdcs` на присутствие записей старых контроллеров, в случае необходимости — удалите старые записи от несуществующих контроллеров.

4. Проверьте, что все **FSMO** роли находятся на действующих контроллерах домена:

```
netdom query fsmo
```

5. Проведите анализ логов контроллера MS AD и убедитесь в отсутствии ошибок («Application and Services Logs» — «Directory Service»).

6. Проведите анализ логов DNS и убедитесь в отсутствии ошибок («Application and Services Logs» — «DNS Server»).

Настройка управления групповыми политиками

Вы можете подключить к контроллеру домена MS AD клиентские машины на базе РЕД ОС. Но может возникнуть вопрос — как ими управлять, ведь групповые политики MS AD могут управлять только рабочими станциями на базе ОС Windows. Для управления рабочими станциями на базе РЕД ОС можно использовать такой инструмент, как *Ansible*. При использовании инструмента *Ansible* может потребоваться подготавливать плейбуки вручную, не говоря уже о том, что этот инструмент работает только в режиме **push**.

Благодаря клиентскому приложению в РЕД АДМ, можно легко управлять групповыми политиками и использовать конфигурации как в формате **push**, так и в формате **pull**:

- *push-режим* позволяет отправить конфигурации непосредственно с РЕД АДМ — данный способ не всегда удобен, т.к. часть машин может быть выключена, или настройки должны быть доставлены в момент входа пользователя в систему;
- с помощью *pull-режима* конфигурация будет применена по запросу клиентской машины, а чтобы клиентская машина вовремя запросила нужные данные с сервера, доступен клиентский агент РЕД АДМ.

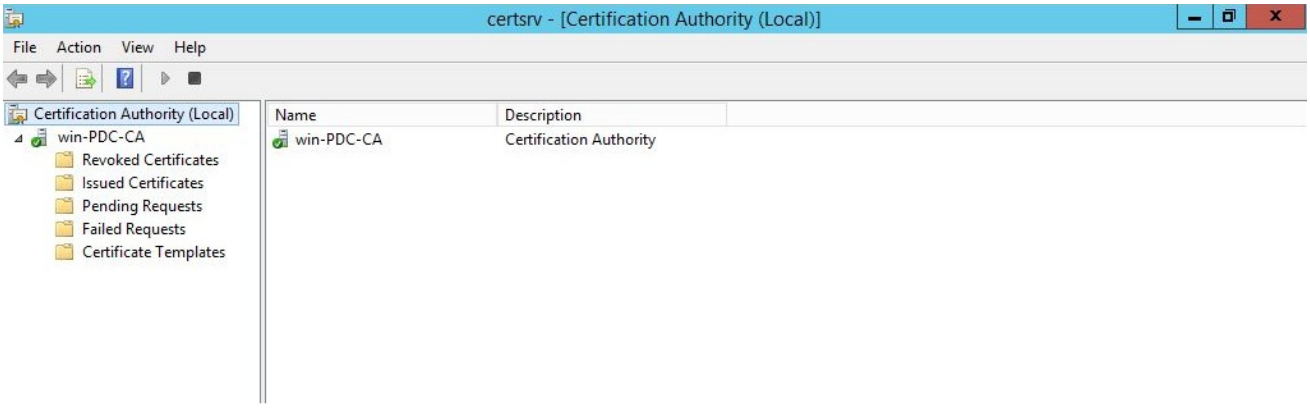
Ввод контроллера домена РЕД АДМ

Следующим действием станет ввод контроллера домена РЕД АДМ в существующий домен на базе MS AD. Данную процедуру можно выполнить из графического интерфейса РЕД АДМ.

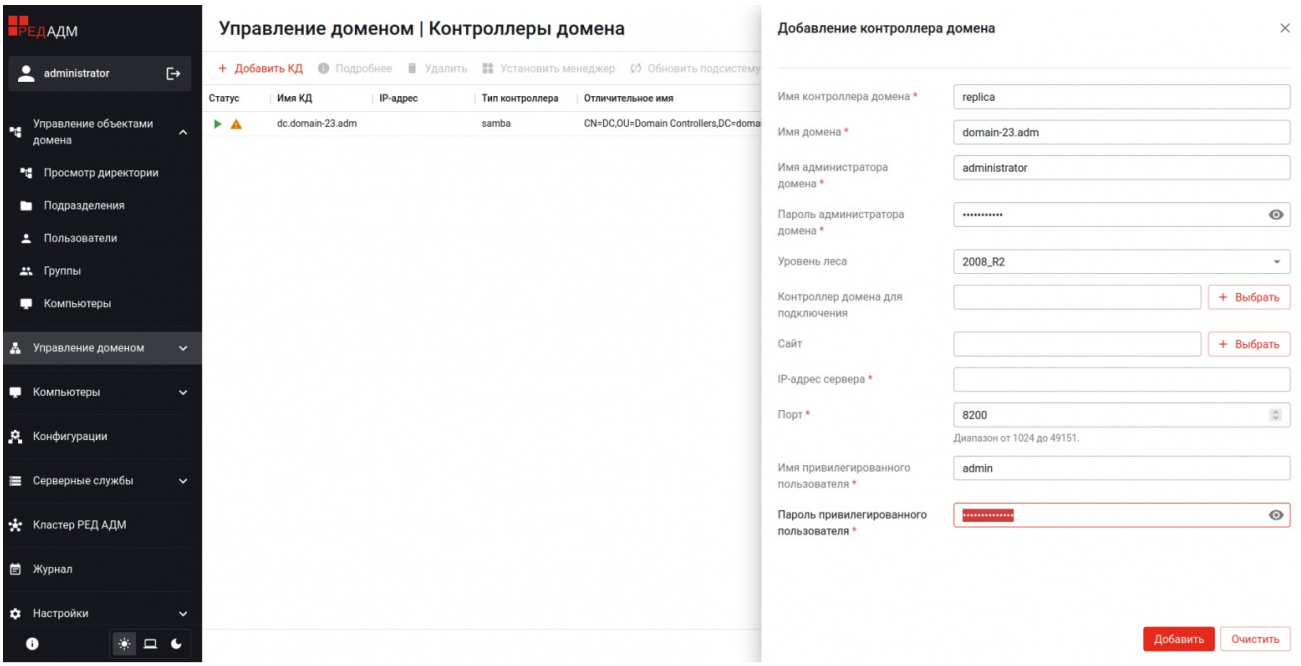
1. Сначала необходимо установить РЕД АДМ и создать локальную базу данных.

2. На этапе подключения или создания нового контроллера домена необходимо выбрать «Подключиться к существующему». При подключении по доменному имени нужно проверить, что контроллер доступен по доменному имени с хоста, где установлен РЕД АДМ (проверить настройки DNS).

3. Для подключения РЕД АДМ к контроллеру домена на базе MS AD необходимо разрешить возможность подключения по **ldaps**. Для этого создайте на MS AD роль центра сертификации (если по каким-либо причинам данный вариант не подходит, рекомендуется воспользоваться документацией — в ней описано, как подключиться к MS AD без роли центра сертификации).



4. Затем необходимо создать новый контроллер и присоединить его к существующему. Сделать это можно через «Управление доменом в РЕД АДМ». Нажмите на кнопку «Добавить КД» и укажите — на каком хосте этот контроллер будет развернут и к какому контроллеру его нужно присоединить — все остальные настройки будут подобраны автоматически.



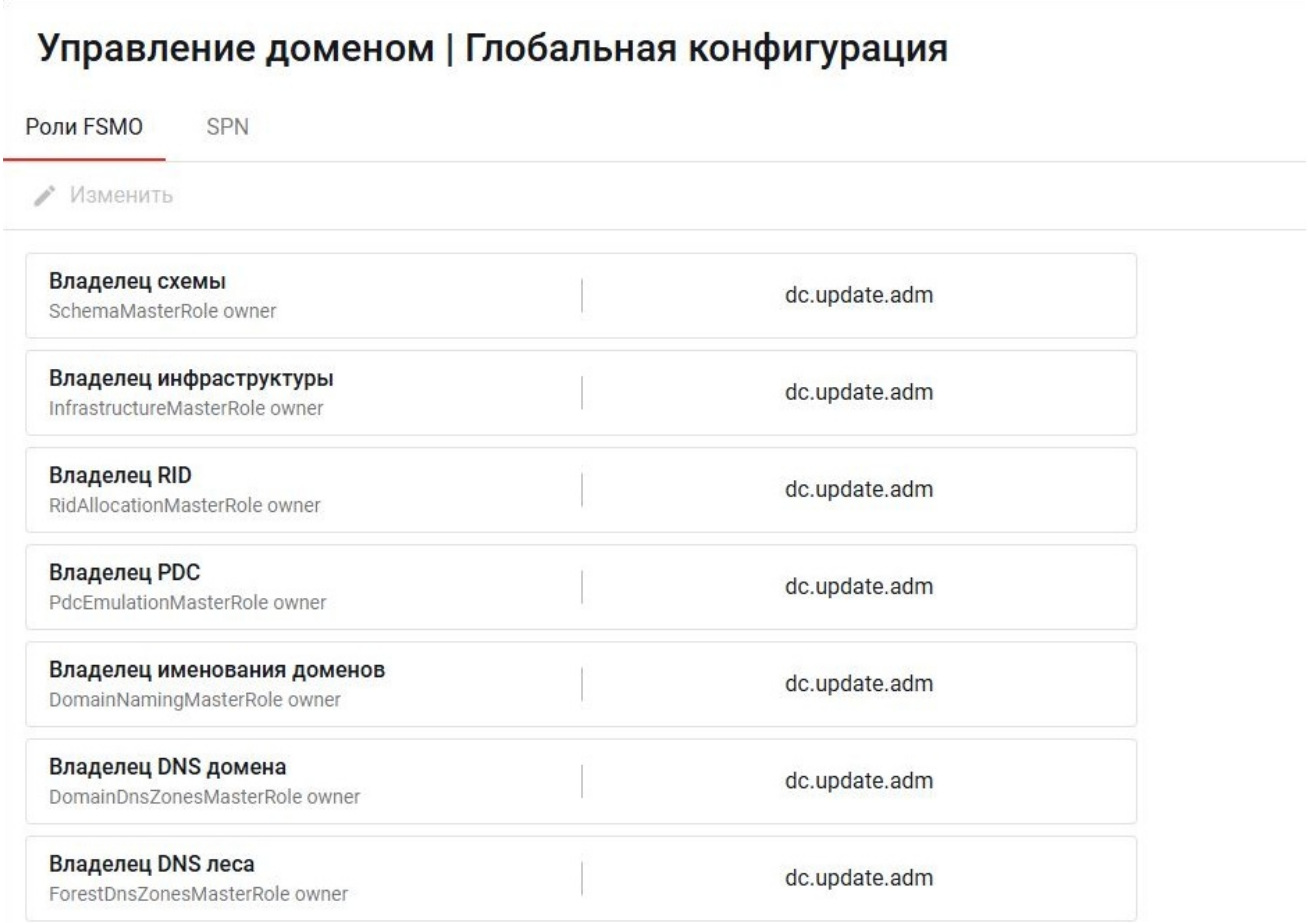
Миграция клиентских машин

Теперь в инфраструктуре работают два контроллера домена, причем один из них может управлять машинами на базе РЕД ОС. Далее необходимо начать процесс перевода парка клиентских машин на РЕД ОС. Управление РЕД ОС будет производиться с помощью конфигураций из РЕД АДМ.

Если в домене будет организована *гетерогенная среда* (будут использоваться как машины на базе ОС Windows, так и машины на базе РЕД ОС) необходимо выполнить некоторые подготовительные действия:

1. Выполнить репликацию каталога **SYSVOL**. Данное действие необходимо для того, чтобы все групповые политики, которые были созданы для хостов на базе ОС Windows, продолжили работать. Подробную информацию о данном этапе можно просмотреть в документации.

2. После репликации каталога **SYSVOL** следует передать роли **FSMO** с контроллера MS AD на контроллер РЕД АДМ. Для этого нужно перейти в «Управление доменом» — «Глобальная конфигурация».



3. Для управления реплицированными политиками потребуется машина с Windows, на которую необходимо установить **RSAT**.

4. Далее необходимо выключить контроллер на базе Windows, проверить работоспособность групповых политик, понизить роль первого контроллера и вывести его из эксплуатации.

Примечание.

Обратите внимание, что РЕД АДМ пока **не работает** с почтовым сервером **MS Exchange**. Поэтому, если такое решение еще используется в вашей инфраструктуре, полностью отказываться от контроллеров на базе MS Windows не рекомендуется. Однако можно рассмотреть варианты аналогичных сервисов от российских вендоров.

После выполненных действий в инфраструктуре нет контроллеров на базе MS AD. Клиентские машины постепенно мигрируют с Windows на РЕД ОС.

Построение параллельной инфраструктуры

Бывают ситуации, когда невозможно произвести никаких действий с существующим доменом. В этом случае можно построить параллельную инфраструктуру на базе РЕД АДМ и выстроить между доменами доверительные отношения.

Плюсы такого решения — проводить миграцию можно длительное время, постепенно перемещая сопутствующие сервисы на новые решения. При этом не так важно, насколько корректно работает ваш исходный домен — например, в нем могут возникать какие-либо ошибки, которые нельзя оперативно решить. Также в этом случае можно полностью избавится от унаследованных проблем в доменной инфраструктуре, создав всё заново.

Развертывание нового домена

Далее будет кратко рассмотрен процесс настройки доверительных отношений. для получения подробной информации см. документацию. В примерах будет использоваться исходных домен на MS AD — **windows.red** и новый домен на РЕД АДМ **example.tst**.

1. Настройка доверительных отношений происходит после установки контроллера РЕД АДМ, поэтому сначала необходимо установить РЕД АДМ и развернуть новый домен.

2. На контроллере РЕД АДМ необходимо отредактировать файл **/etc/named.conf** и после корневой зоны «**.**» добавить зону пересылки запросов в доверенный домен:

```
zone "windows.red" IN {

 type forward;

 forwarders { 192.168.100.5; };

 };
```

где в параметре `forwarders` необходимо указать адрес контроллера домена MS AD, с которым необходимо установить доверительные отношения.

3. На контроллере домена РЕД АДМ также необходимо отредактировать файл **/etc/krb5.conf** и в секции `[realms]` и `[domain_realm]`.

```
[realms]
```

```
EXAMPLE.TST = {

kdc = dc1.example.tst

admin_server = dc1.example.tst

}

WINDOWS.RED = {

kdc = windc.windows.red

admin_server = windc.windows.red

}

[domain_realm]

.example.tst = EXAMPLE.TST

example.tst = EXAMPLE.TST

.windows.red = WINDOWS.RED

windows.red = WINDOWS.RED
```

4. Далее на РЕД АДМ необходимо перезапустить службы:

```
systemctl restart reddc named
```

5. На контроллере домена MS AD необходимо настроить сервер условной пересылки.

Установка доверительных отношений

Теперь можно приступить к настройке доверительных отношений, предварительно проверив доступность контроллеров друг с другом, командой:

```
nslookup <имя_КД>
```

Если сервера доступны, создайте доверительные отношения командой:

```
samba-tool domain trust create windows.red --type=external --direction=both --create-location=both -U Administrator@WINDOWS
```

где:

- type — тип доверительных отношений - external (внешнее) — РЕД АДМ поддерживает тип отношений external;
- direction — направление доверительных отношений, со следующими возможными значениями:
  - both — двухсторонние доверительные отношения. Контроллер домена РЕД АДМ будет доверять контроллеру домена Active Directory и наоборот — обе стороны смогут обмениваться аутентификационной информацией и ресурсами;
  - outgoing — односторонние доверительные отношения только для исходящих запросов: например, контроллер домена Active Directory будет доверять контроллеру домена РЕД АДМ, например, при получении запросов на аутентификацию от пользователей из СК РЕД АДМ, но не наоборот;
  - incoming — односторонние доверительные отношения только для входящих запросов: например, контроллер домена РЕД АДМ будет доверять контроллеру домена Active Directory, например, при получении запросов на аутентификацию от пользователей из домена Active Directory, но не наоборот.

В случае успешного создания доверительных отношений, в конце вывода результатов работы команды в терминале должно быть выведено сообщение success.

После построения доверительных отношений необходимо еще раз перезапустить службы **reddc** и **named** и проверить установленные доверительные отношения при помощи команды:

```
samba-tool domain trust list
```

Для того чтобы убедиться в корректности выполненных выше команд, рекомендуется проверить целостность получения файла **PAC dump** при помощи следующей команды (запуск следует выполнять с правами суперпользователя **root**):

```
net ads kerberos pac dump -U Administrator@WINDOWS.RED
```

Источник: https://redadm.red-soft.ru/base/red-adm/ra-useful-articles/migration-on-red-adm/