Шаг 1. Подготовка разделов каталога Active Directory®.

Создадим подразделения, необходимые для хранения объектов, содержащих конфигурацию шлюза и его подключений.

Шаг 2. Регистрация всех компьютеров, предоставляющих сервисы подключения и отсутствующих в каталоге.

Регистрационные записи компьютеров нужны для определения их FQDN, необходимого для создания подключения. Так же можно проверить правильность заполнения атрибута **dNSHostName** у компьютеров, зарегистрированных средствами Windows®-домена.

Шаг 3. Создание и экспорт шаблонов подключений на шлюзе.

Шаблоны подключений для внесения в каталог AD (текстовый список их параметров) можно получить с помощью утилиты GetConnection из подключений, существующих на шлюзе. На этом шаге создадим такие подключения и используем утилиту экспорта.

Шаг 4. Создание шаблонов подключений в каталоге.

Создадим группы-шаблоны подключений и импортируем в них параметры.

Шаг 5. Конфигурация пользовательских учётных записей.

Добавим пользователям разрешённые подключения.

Конфигурация шлюза. Создание объектов Active Directory®

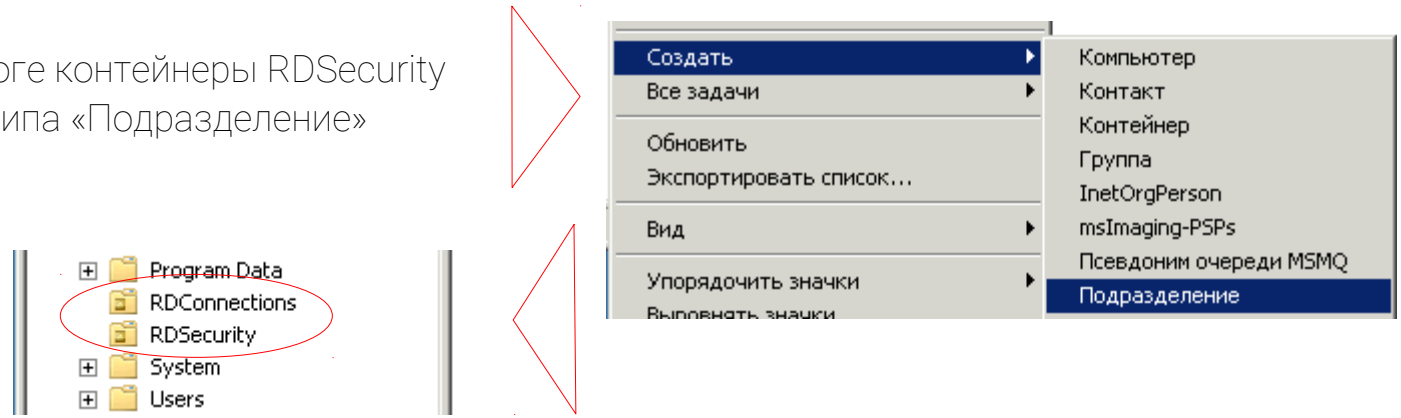
Подготовка разделов каталога Active Directory®

Для конфигурации подключения модуль шлюза auth-ad использует четыре объекта из каталога AD:

- в разделе групп доступа (в примере далее это «RDSecurity») ищется группа, членом которой является пользователь и её имя используется как имя группы пользователей на шлюзе, определяющей права доступа к объектам шлюза для пользователя;
- из учётной записи пользователя параметры «Личный виртуальный рабочий стол» и «Веб-страница»;
- из учётной записи компьютера параметр dNSHostName (FQDN компьютера);
- в разделе групп-шаблонов (в примере далее это «RDConnections»), для каждого компьютера разрешённого пользользователю и найденного на предыдуще шаге, ищется группа-шаблон, включающая этот компьютер.

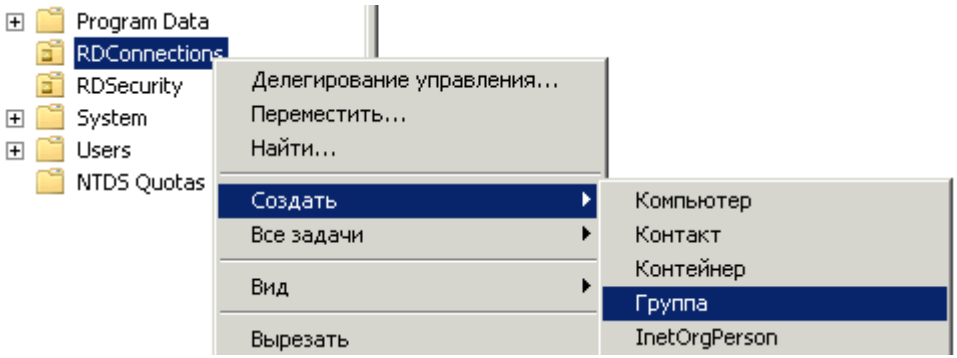
Для каждого найденного в группах-шаблонах компьютера формируется подключение из шаблона группы и имени компьтера. Полученный список подключений передаётся шлюзу. Если этот список содержит единственное подключение, то шлюз его инициирует немедленно, иначе же пользователю предлагается выбор.

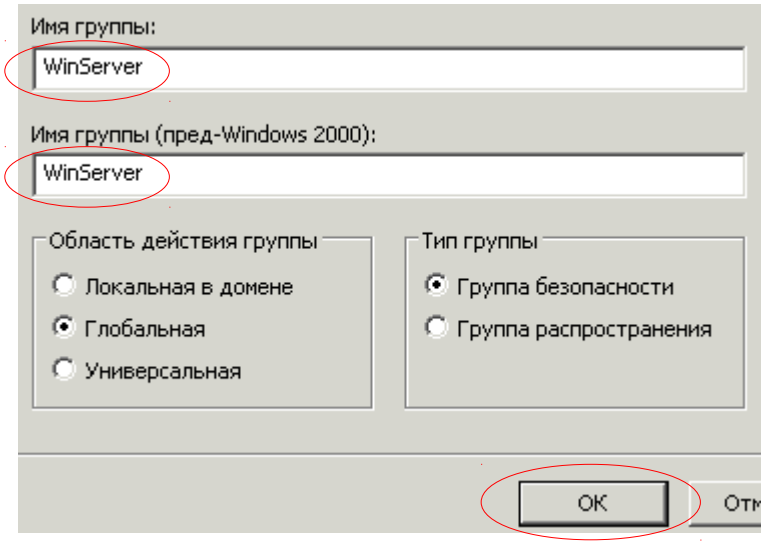
Создадим в каталоге контейнеры RDSecurity и RDConnections типа «Подразделение»



Конфигурация шлюза. Создание объектов Active Directory®

Создаём группы-шаблоны и группы контроля доступа





Аналогично создаём группу-шаблон

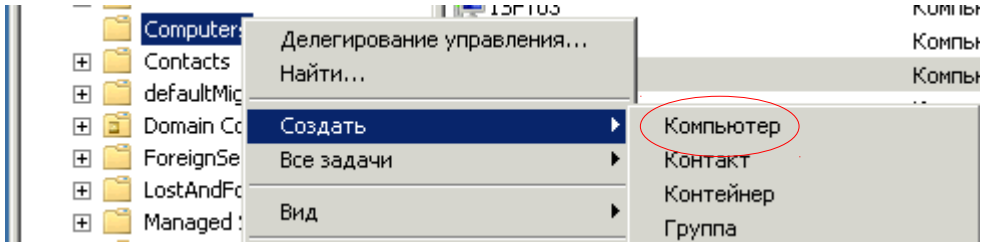
- «RDPServer» для соеднений к Linux xrdp
- «VNCServer» для соединения с VNC серверами

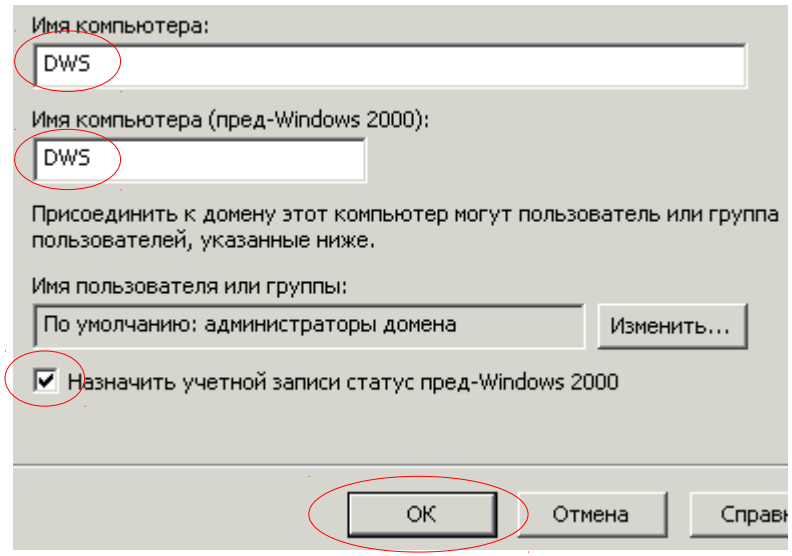
Далее, по аналогии с этой, создаём группы «RDUsers» и «RDAdmins» в контейнере RDSecurity каталога

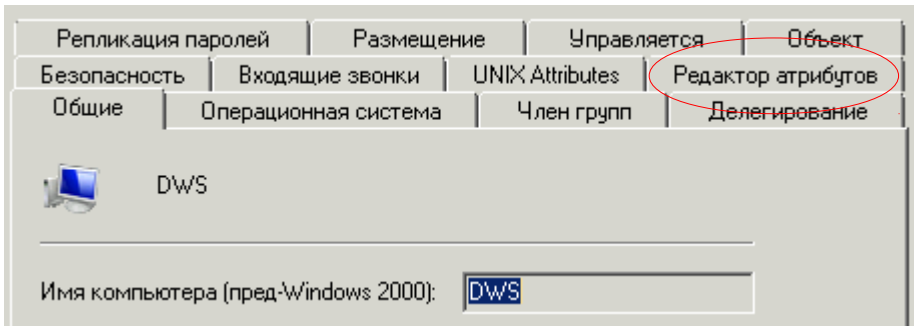
Конфигурация шлюза. Создание объектов Active Directory®

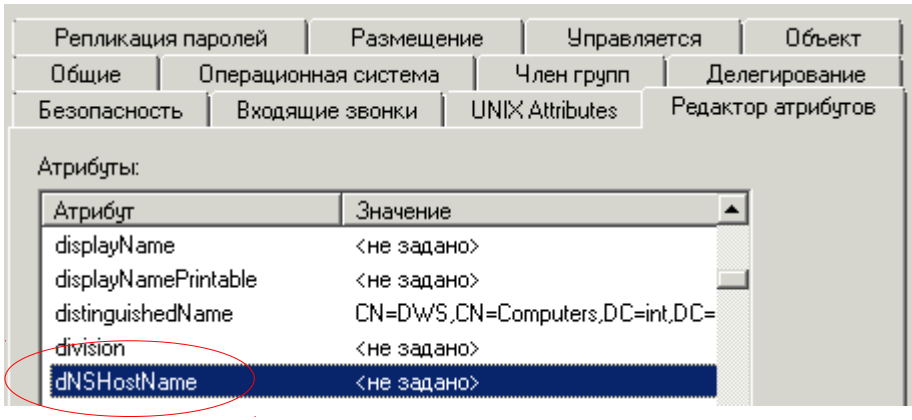
Регистрация компьютеров в каталоге

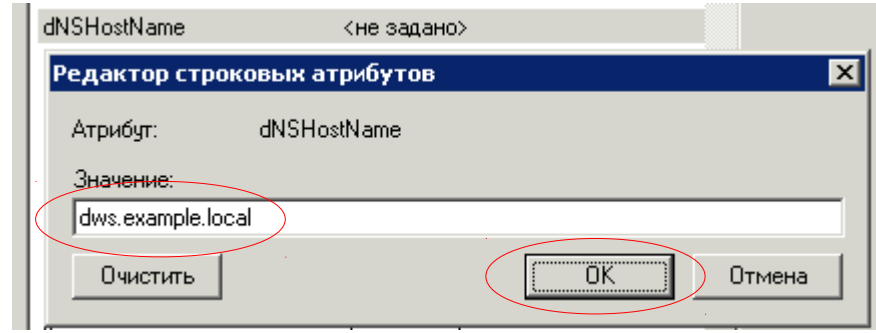
Все компьютеры, к которым шлюз будет делать подключения, должны иметь запись типа «Компьютер» в каталоге. Создаём записи для компьютеров без Windows-домена:









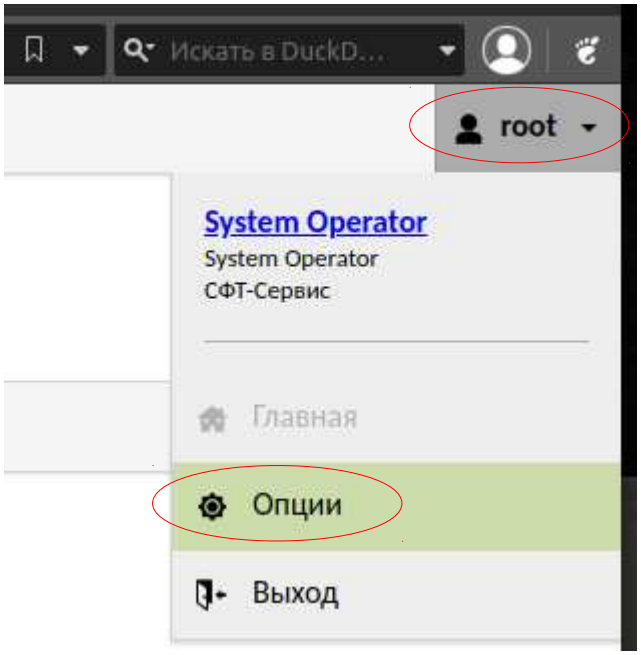


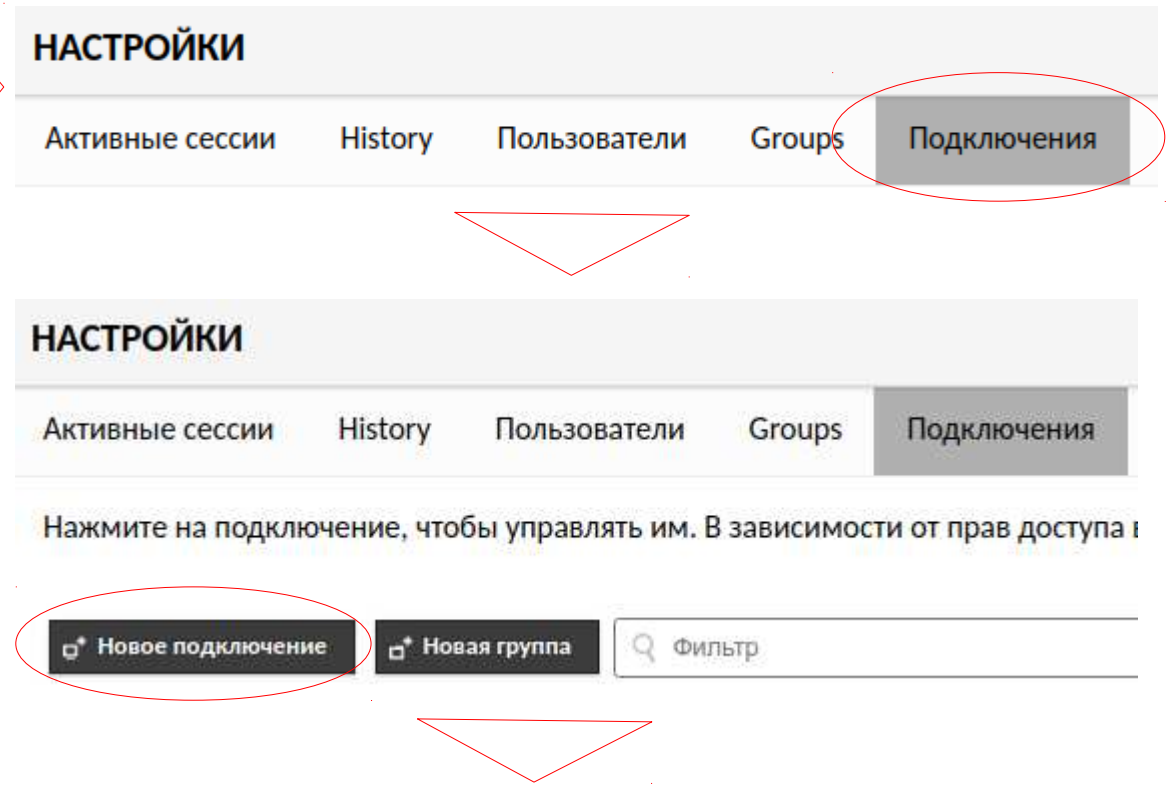
Повторим для всех компьютеров без Windows-домена.

Конфигурация шлюза. Создание объектов Active Directory®

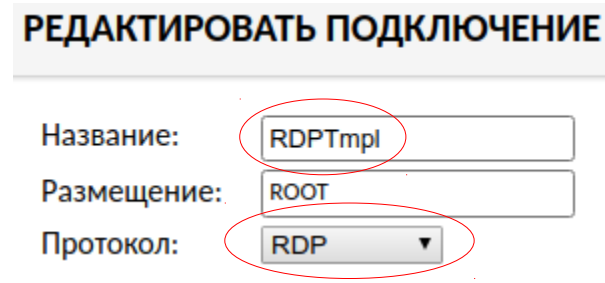
Создание шаблонов подключений на шлюзе.

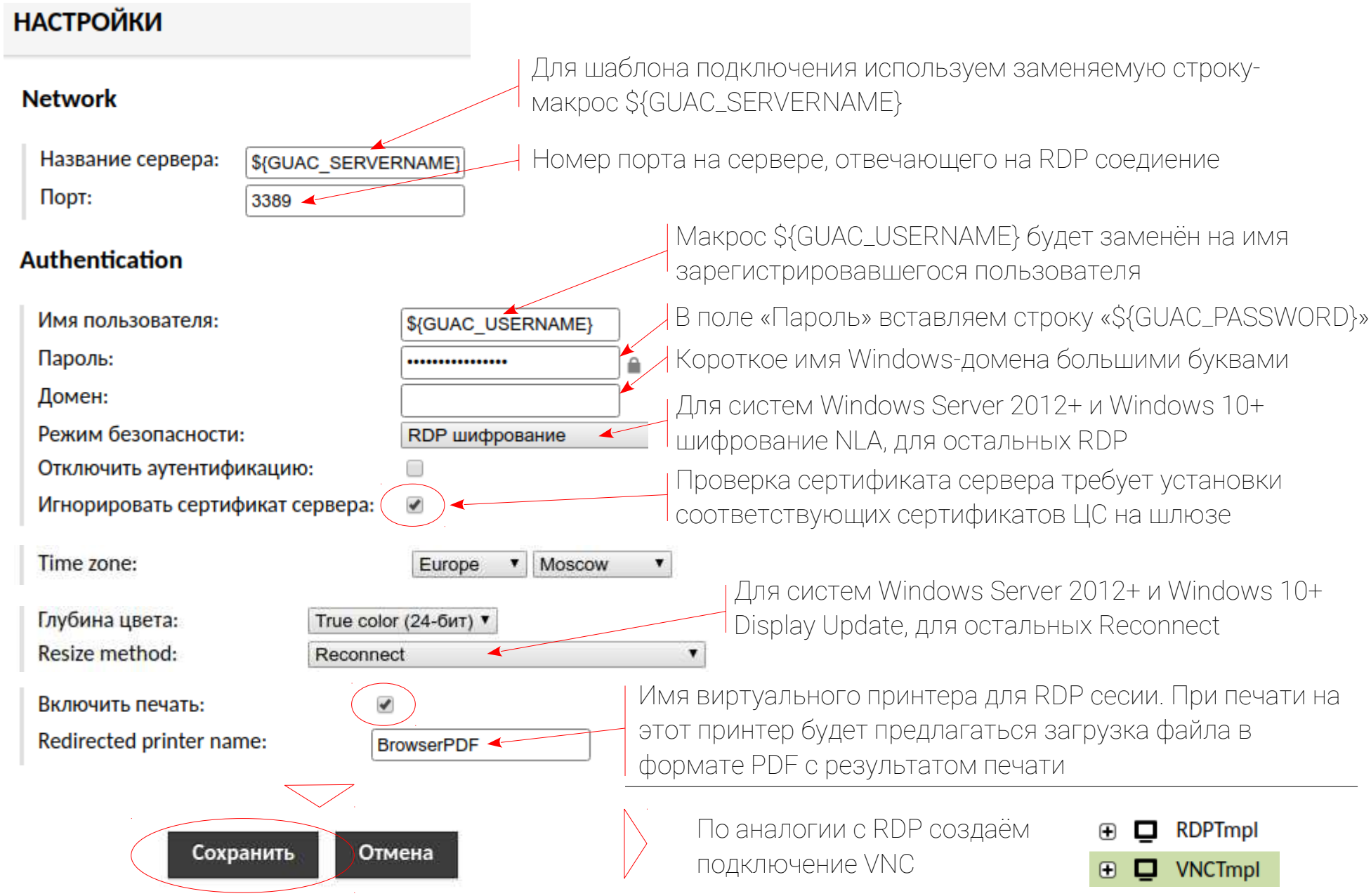
После регистрации на шлюзе адиминистративного пользователя, в правом верхнем углу страницы открываем меню и выбираем пункт «Опции»





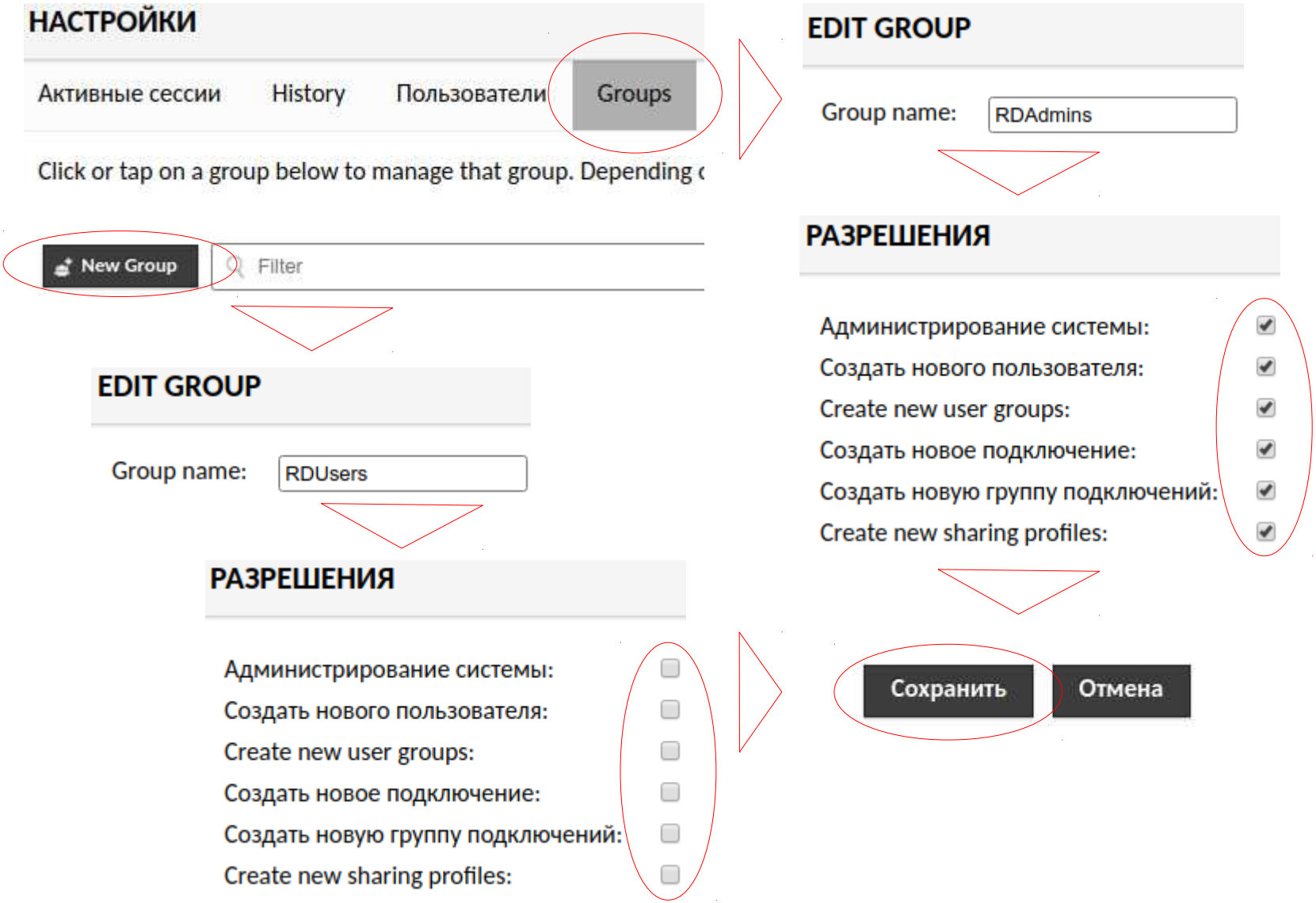
Называем новое (для нас шаблонное) соединение латинскими буквами и выбираем тип соединения RDP.




НАСТРОЙКИ
Network
Название сервера:
${GUAC_SERVERNAME}
Порт:
3389
Authentication
Имя пользователя:
${GUAC_USERNAME}
Пароль:
Домен:
Режим безопасности:
RDP шифрование
Отключить аутентификацию:
Игнорировать сертификат сервера:
Time zone:
Europe
Moscow
Глубина цвета:
True color (24-бит)
Resize method:
Reconnect
Включить печать:
Redirected printer name:
BrowserPDF
Сохранить
Отмена
Для шаблона подключения используем заменяемую строку-макрос ${GUAC_SERVERNAME}
Номер порта на сервере, отвечающего на RDP соединение
Макрос ${GUAC_USERNAME} будет заменён на имя зарегистрировавшегося пользователя
В поле «Пароль» вставляем строку «${GUAC_PASSWORD}»
Короткое имя Windows-домена большими буквами
Для систем Windows Server 2012+ и Windows 10+ шифрование NLA, для остальных RDP
Проверка сертификата сервера требует установки соответствующих сертификатов ЦС на шлюзе
Для систем Windows Server 2012+ и Windows 10+ Display Update, для остальных Reconnect
Имя виртуального принтера для RDP сесии. При печати на этот принтер будет предлагаться загрузка файла в формате PDF с результатом печати
По аналогии с RDP создаём подключение VNC
RDPTmpl
VNCTmpl

Конфигурация шлюза. Создание объектов Active Directory®

Создаём группы доступа на шлюзе



Конфигурация шлюза. Создание объектов Active Directory®

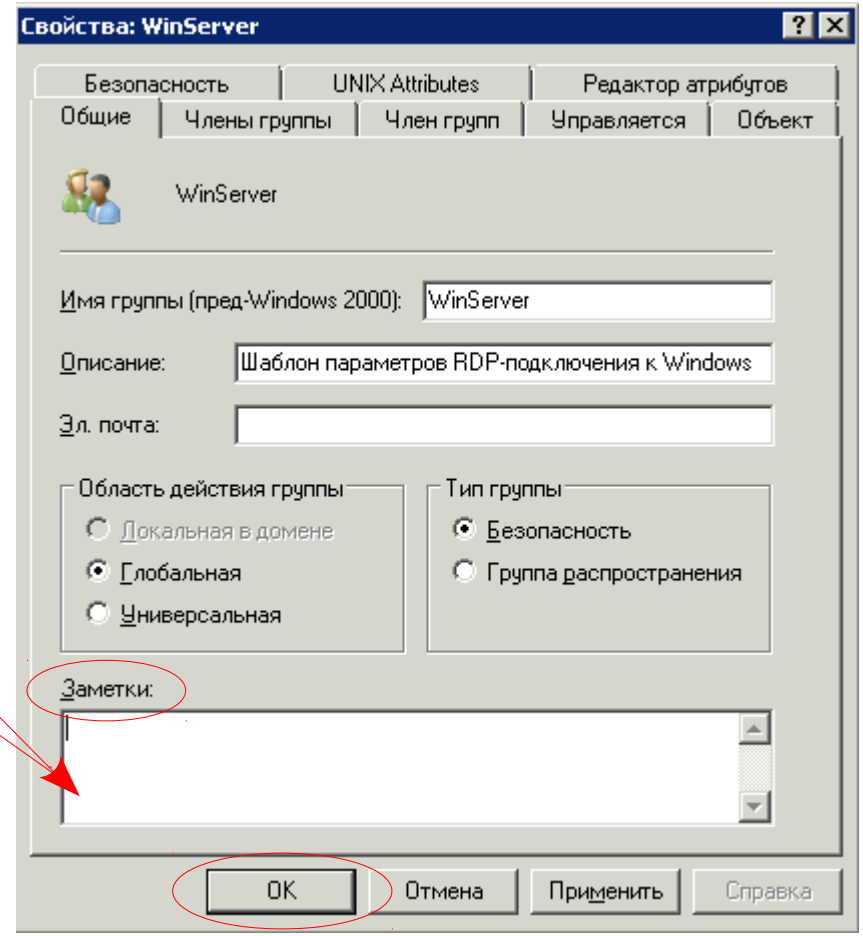
Экспорт конфигурации подключений

Загружаем программу экспорта параметров соединений с сайта производителя:


```
H:\> Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope LocalMachine

H:\> .\GetConnection.ps1 RDPTmpl -server rdgate -username gateadmin -password ???
```

```
protocol: rdp
enable-printing: true
resize-method: reconnect
timezone: Europe/Moscow
console-audio: true
enable-font-smoothing: true
color-depth: 24
security: rdp
hostname: ${GUAC_SERVERNAME}
password: ${GUAC_PASSWORD}
ignore-cert: true
printer-name: BrowserPDF
port: 3389
username: ${GUAC_USERNAME}
```

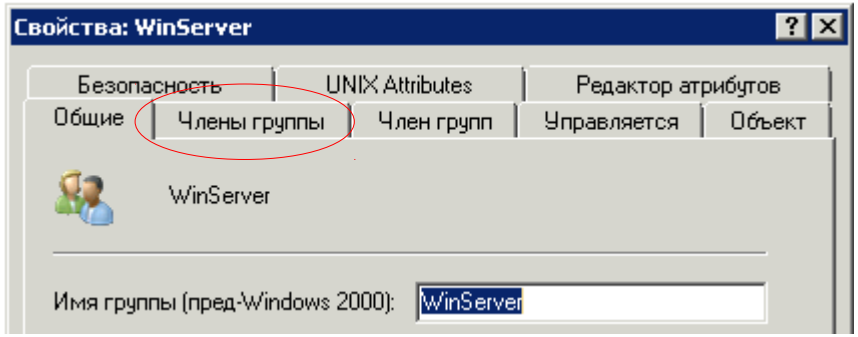


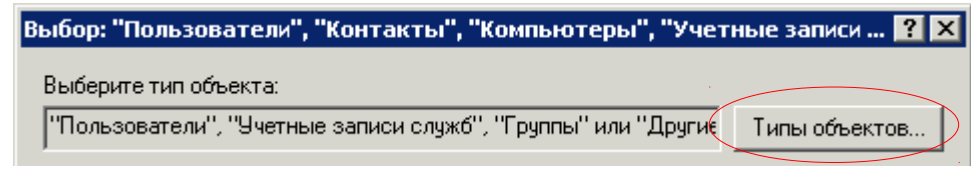
Переносим полученный текст в поле «Заметки» свойств ранее созданной в каталоге группы-шаблона «WinServer» и «RDPServer»

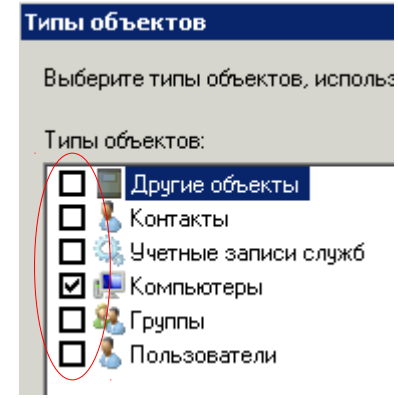
Аналогичные действия выполняем для шаблона «VNCTmpl» и группы «VNCServer»

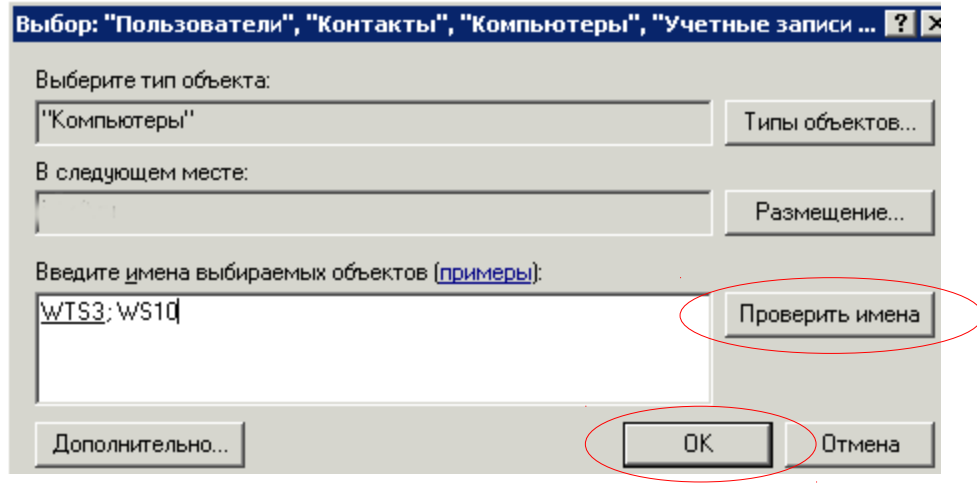
Конфигурация шлюза. Создание объектов Active Directory®

Добавляем компьютеры в группы - шаблоны







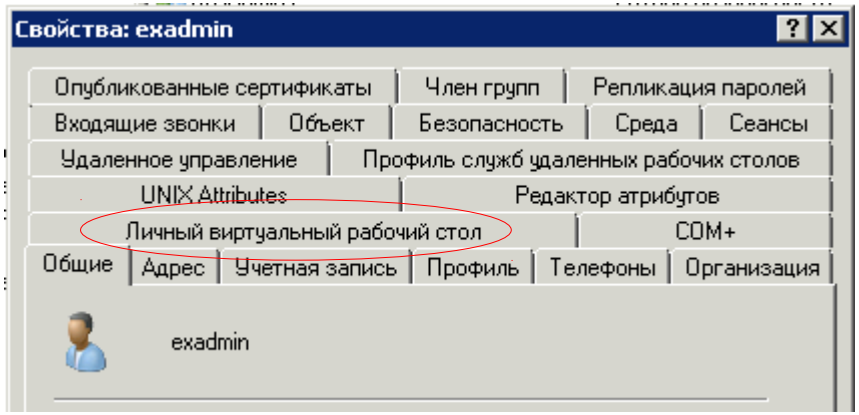


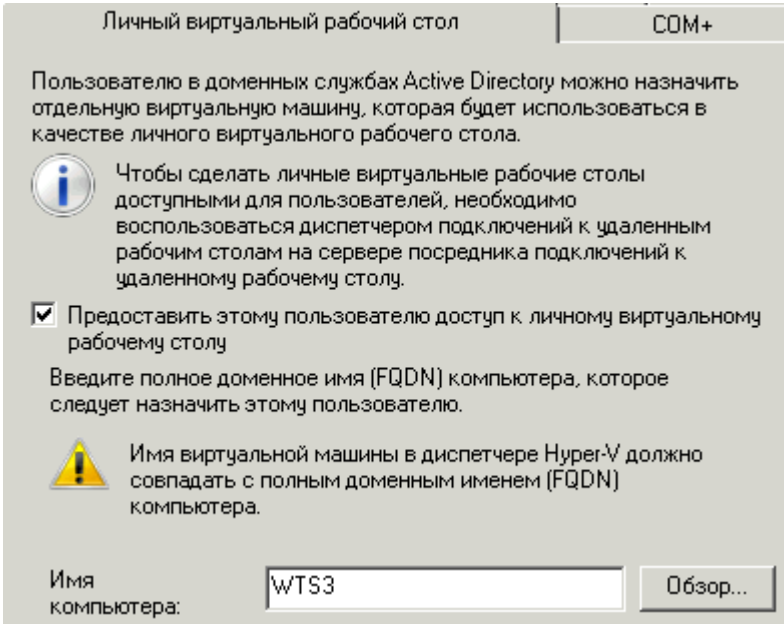
Далее, таким же способом, добавляем компьютеры «TS4» и «DWS» в группу «RDPServer»; компьютер «WTS3» в группу «VNCServer»

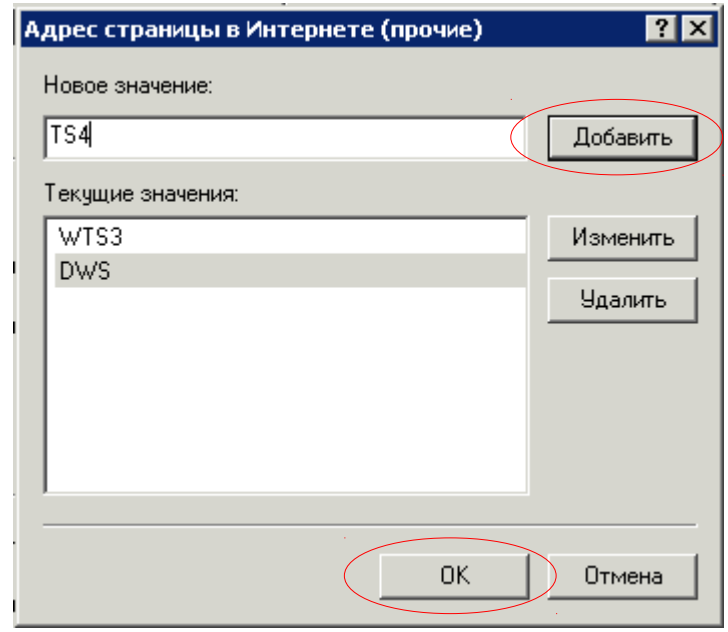
Пользователей, в соответствии с ролями, добавляем в группы подразделения «RDSecurity» «RDAdmins» и «RDUsers»

Конфигурация шлюза. Создание объектов Active Directory®

Конфигурация учётных записей пользователей







В малоиспользуемом атрибуте «Веб-страница» размещаем список имён доступных пользователю серверов.
Этот список **читается вне зависимости** от наличия Windows Terminal Services.

В случае, если в организации уже развёрнута инфраструктура Terminal Services и у пользователей имеются личные рабочие столы, то эти установки будут учтены модулем auth-ad

После регистрации пользователя на шлюзе появляется выбор из доступных подключений

exuser

- WS10 WinServer
- WTS3 WinServer

exadmin

- DWS RDPServer
- TS4 RDPServer
- WTS3 VNCServer
- WTS3 WinServer

СФТ СЕРВИС
Основан в 1992 г.

http://www.sft.ru/contacts

Консультации:

remote@sft.ru
+7 495 7883762(-63) доб. 112