Autoprovision через ActiveDirectory

Обо мне:

- Образование - высшее, техническое
- Информационных систем и технологий

План доклада

- Цель
- Необходимые сервисы и оборудование
- Детальная настройка
- Логика работы
- Подводные камни

Цель доклада

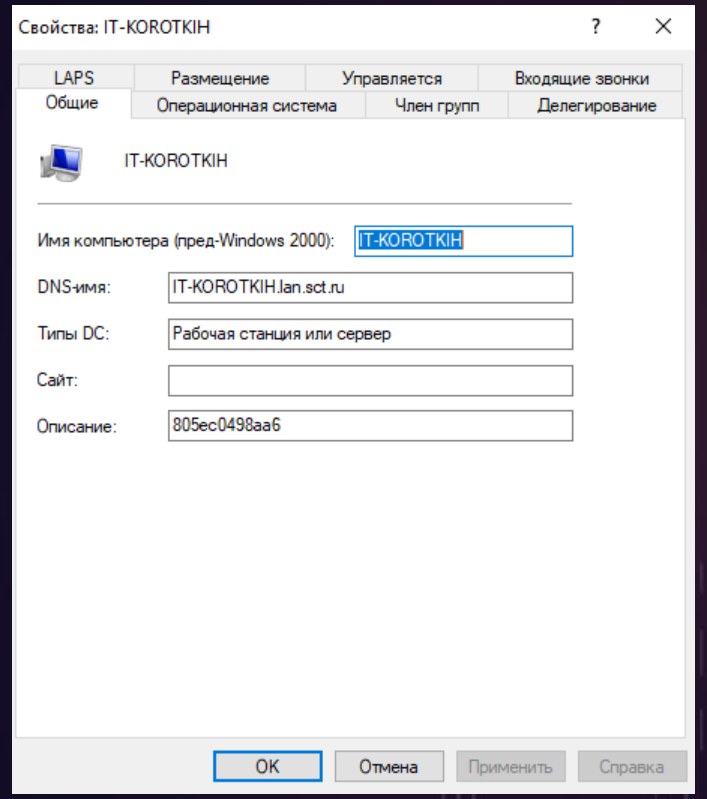
- Показать вариант интеграции Asterisk и AD
- Облегчить жизнь сотрудникам
- Облегчить жизнь админам

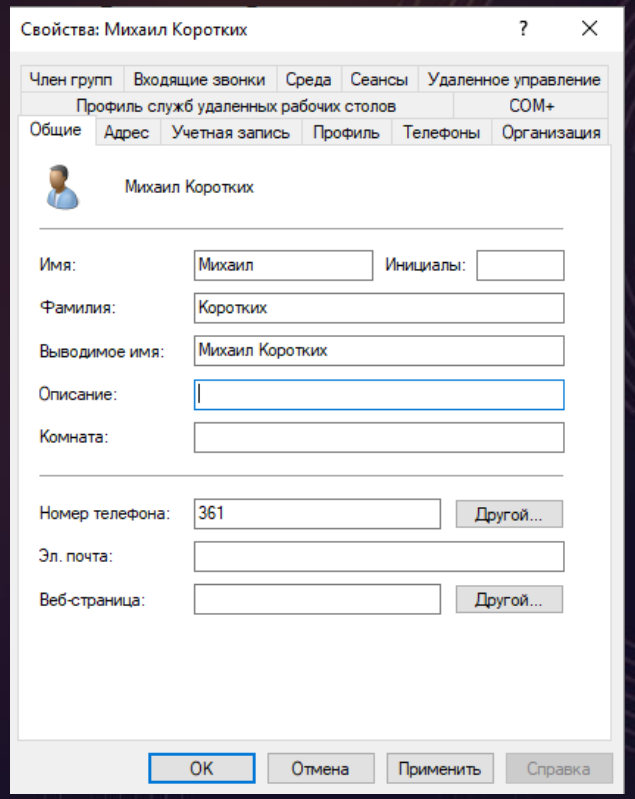
Необходимые сервисы и оборудование

- DHCP сервер
- Active Directory
- ПК в домене
- Телефонный аппарат
- Сервер с Asterisk, samba, openldap и tftp
- Скрипты для интеграции сервера Asterisk с Active Directory

Настройки Active Directory

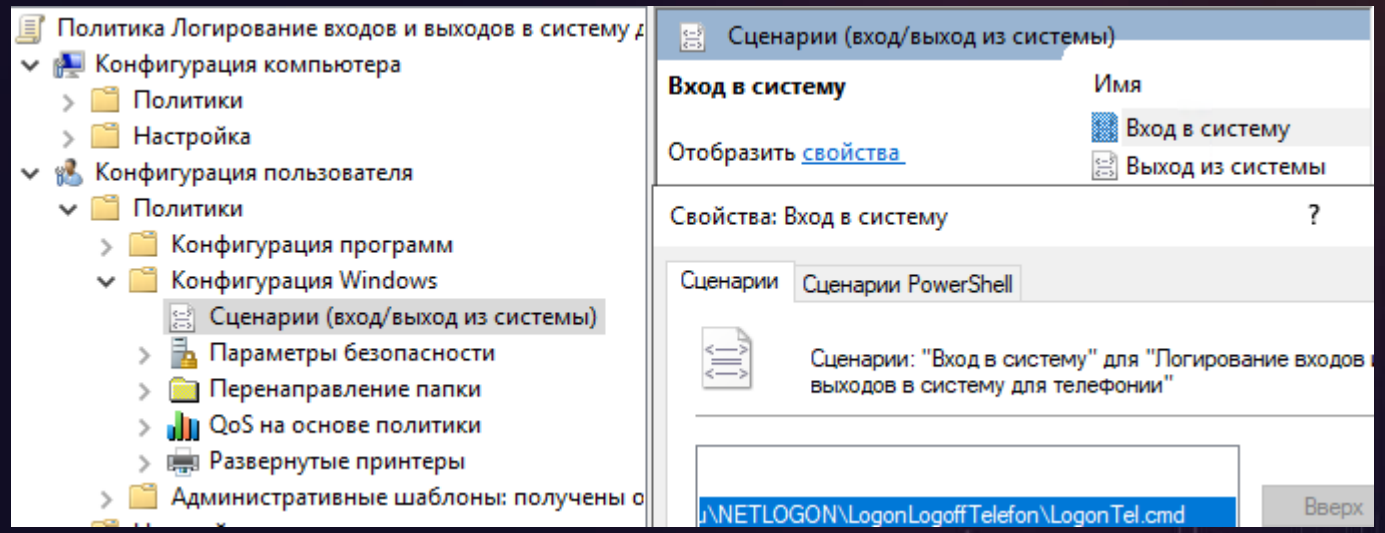
- MAC-адрес телефона указать в свойства ПК
- Номер телефона пользователя указать в сущности пользователя

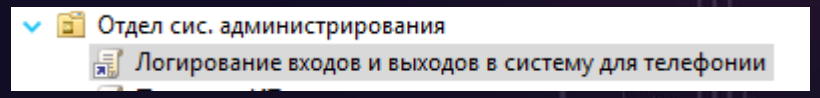




Групповая политика Active Directory

- Создать политику для регистрации входов/выходов из системы
- Связать политику с подразделениями пользователей





Сценарии (вход/выход из системы)

- **Создать и разместить в папке NETLOGON скрипты регистрации входа/выхода из системы: \\ваш_домен\NETLOGON**
- `echo logon %username% %computername% %time% %date% > \\IP_Astersik\asterisk_share\%computername%.txt`
- `echo logoff %username% %computername% %time% %date% > \\IP_Astersik\asterisk_share\%computername%.txt`

Настройки сервера с Asterisk

- Установить tftp сервер: dnf install tftp tftp-server
- Установить openldap: dnf install openldap-clients
- Установить samba, сделать сетевую шару, доступную для записи для всех пользователей
- Создать и добавить в cron скрипт для генерации conf файлов телефонов:
  */1 * * * * /var/lib/asterisk/agi-bin/ldap-search/ldap-search.sh

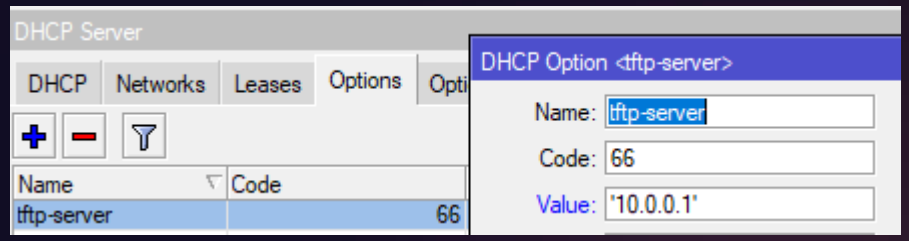
Настройки samba

- dnf install samba samba-client
- /etc/samba/smb.conf
- map to guest = Bad Password
- [asterisk_share]
  comment = aster
  path = /mnt/shared_for_asterisk
  public = yes
  guest ok = yes
  read only = no
  create mask = 0666
  directory mask = 0666

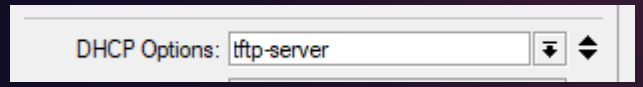
Листинг скрипта

```
SHAREDFOLDER=/Ваша_шара_на_asterisk
TFTPFOLDER=/var/lib/tftpboot
# SIPCONF=/etc/asterisk/sip.conf
if [ -n "$(ls -A $SHAREDFOLDER)" ]; then
 for file in $SHAREDFOLDER/*; do
  if [ -n "$(cat "$file")" ]; then
   ACTION=`cat "$file" | cut -f 1 -d' '`
   USERNAME=`cat "$file" | cut -f 2 -d' '`
   COMPUTERNAME=`cat "$file" | cut -f 3 -d' '`
   COMPUTERMAC=`ldapsearch -LLL -x -H ldap://Имя_вашего_DC -D "Имя_Учётки@Ваш_домен" -w «Пароль_от_учётки" -b
"OU=Ваш_OU,DC=Ваш_DC3,DC=Ваш_DC2,DC=Ваш_DC1" sAMAccountName=$COMPUTERNAME$ description | grep '^description:' | cut -f 2 -d' '`
   USERTELNUMBER=`ldapsearch -LLL -x -H ldap://Имя_вашего_DC -D "Имя_Учётки@Ваш_домен" -w «Пароль_от_учётки" -b
"OU=Ваш_OU,DC=Ваш_DC3,DC=Ваш_DC2,DC=Ваш_DC1" sAMAccountName=$USERNAME telephoneNumber postalCode | grep '^telephoneNumber:' | cut -f 2 -d' '`
   if [[ -n $USERTELNUMBER ]]; then
    # USERPASSWORD=`grep -A 1 "<$USERTELNUMBER>" $SIPCONF | grep '^secret=' | cut -f 2 -d'='`
    USERPASSWORD=$(mysql asterisk -s -uUser -pPass<<<"SELECT password FROM asterisk.ps_auths where id=$USERTELNUMBER")
   fi
   if [[ -n $COMPUTERMAC ]] && [[ -n $USERPASSWORD ]]; then
    if [ "$ACTION" == "logon" ]; then
     ACCAUNTENABLE=1
    else
     ACCAUNTENABLE=0
    fi
    echo "#!version:1.0.0.1" > $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "local_time.ntp_server1 = IP_вашего_NTP" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "account.1.enable = $ACCAUNTENABLE" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "account.1.label = $USERTELNUMBER" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "account.1.display_name = $USERTELNUMBER" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "account.1.auth_name = $USERTELNUMBER" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "account.1.password = $USERPASSWORD" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "account.1.user_name = $USERTELNUMBER" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "account.1.sip_server_host = IP_вашего_Asterisk" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "account.1.sip_server_port = 5060" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "security.user_name.admin = admin" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "security.user_password = admin:Ваш_пароль" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "auto_provision.repeat.enable = 1" >> $TFTPFOLDER/$COMPUTERMAC.cfg
    echo "auto_provision.repeat.minutes = 1" >> $TFTPFOLDER/$COMPUTERMAC.cfg
   fi
  fi
 rm "$file"
 done
fi
```

Настройки DHCP сервера



- Создать DHCP Option код 66 с адресом tftp сервера
- Указываем данную опцию в свойствах DHCP Lease наших телефонов



Настройки телефона

- При условии корректного выполнения предыдущих слайдов настройка телефона не требуется.

Логика работы

- При входе/выходе из системы запускается скрипт групповой политики, формирующий на сетевой шаре Asterisk файл с описание действия пользователя на компьютере.
- На Asterisk по CRON выполняется скрипт, проверяющий сетевую шару из п 1 и парсящий файлы, находящиеся в ней, при их наличии. На основе информации из этих файлов формируются конфигурационный файлы для телефонных аппаратов.

Логика работы

- Включаем телефон из коробки с заводскими настройками, предварительно подключив его к локальной сети.
- Телефон получает сетевые настройки с DHCP сервера, включая адрес TFTP сервера.
- Через технологию AutoProvision телефон получает свой конфигурационный файл с сервера Asterisk.

Подводные камни

- Одновременный логон одного сотрудника на нескольких ПК
- Отключение SIP учётки при перезагрузке ПК
- Некорректные данные в AD

Спасибо за внимание!

Буду рад ответить на все ваши вопросы сейчас или свяжитесь со мной в будущем:

Михаил Коротких

mkorotkih@gmail.com

t.me/mikhail_korotkikh