# The process for Windows differs a bit from Linux, see below:

Please first check if we can use the AD created accounts on VF-ROOT or VODACOM.CORP to be able to login to these machines.

These accounts can be added to the Local Admin groups on each server from one of the domains itself.

1. Create the following user on the server and ensure that it is added to the local server admin group: zsvc\_pamrecon
2. You can either rename the administrator account on the server to winadm or leave it named as administrator. Please let me know what you decide.
3. Zsvc\_pamrecon should have rights to reset credentials for the winadm/administrator account
4. Provide a valid server name (FQDN) that I can ping/connect to
5. Let me know which domain the server resides on i.e. Vodacom, vf-root, vodadealers, etc.
6. Lastly, provide the credentials for winadm/administrator

# Unix/linux

1. Create the following users on the server: pamlogon, pamrecon
2. pamrecon needs rights to reset credentials to all managed accounts
3. pamlogon needs the ability to "sudo" to other users (especially root)
4. Permanently remove the password min age requirement
5. Provide a valid server name (FQDN) that I can ping/connect to

        6.  Lastly, provide the credentials for pamrecon

## CyberARK – Adding Systems

CyberArk URL is: <https://cyberark.vodacom.corp/PaaaswordVault/>

(CyberArk authenticates against the eDir auth Storre or EAS.vodacom.corp.)

### Server setup of ***pamlogon*** and ***pamrecon:***

Prior to creating the CyberArk entries ensure that the accounts are correctly setup o the server itself.

Here the command to use in a “copy-paste” format (instead of a picture):

groupadd -g 9000 pamrecon

groupadd -g 9001 pamlogon

groupadd -g 9002 dna

useradd -u 9000 -g 9000 -c "CyberArk pamrecon, SYSADM" pamrecon

useradd -u 9001 -g 9001 -c "CyberArk pamlogon, SYSADM" pamlogon

useradd -u 9002 -g 9002 -c "CyberArk dna, SYSADM" dna

echo 'pamrecon:Vodacom99'|chpasswd

echo 'pamlogon:Vodacom99'|chpasswd

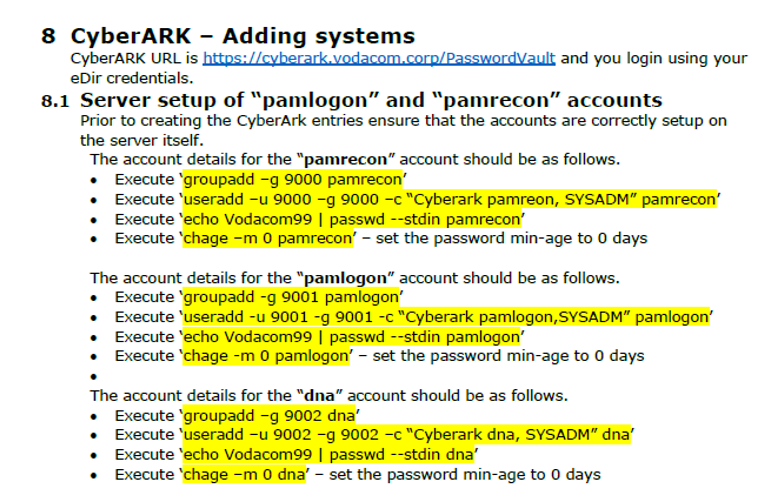
echo 'dna:Vodacom99'|chpasswd

chage -m 0 parecon

chage -m 0 pamlogon

chage -m 0 dna

The “chpasswd” command is also better to use as not all systems support “passwd –stdin”.



## The sudo config for CyberArk accounts example: (/etc/sudoers)

## Sudoers allows particular users to run various commands as

## the root user, without needing the root password.

##

## Examples are provided at the bottom of the file for collections

## of related commands, which can then be delegated out to particular

## users or groups.

##

## This file must be edited with the 'visudo' command.

##

## Host Aliases

## Groups of machines. You may prefer to use hostnames (perhaps using

## wildcards for entire domains) or IP addresses instead.

# Host\_Alias FILESERVERS = fs1, fs2

# Host\_Alias MAILSERVERS = smtp, smtp2

#

## User Aliases

## These aren't often necessary, as you can use regular groups

## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname

## rather than USERALIAS

# User\_Alias ADMINS = jsmith, mikem

#

# Defaults specification

#

# Refuse to run if unable to disable echo on the tty.

#

Defaults !visiblepw

#

#

# Preserving HOME has security implications since many programs

# use it when searching for configuration files. Note that HOME

# is already set when the the env\_reset option is enabled, so

# this option is only effective for configurations where either

# env\_reset is disabled or HOME is present in the env\_keep list.

#

Defaults always\_set\_home

Defaults match\_group\_by\_gid

#

Defaults env\_reset

Defaults env\_keep = "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS\_COLORS"

Defaults env\_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC\_ADDRESS LC\_CTYPE"

Defaults env\_keep += "LC\_COLLATE LC\_IDENTIFICATION LC\_MEASUREMENT LC\_MESSAGES"

Defaults env\_keep += "LC\_MONETARY LC\_NAME LC\_NUMERIC LC\_PAPER LC\_TELEPHONE"

Defaults env\_keep += "LC\_TIME LC\_ALL LANGUAGE LINGUAS \_XKB\_CHARSET XAUTHORITY"

#

#

# Adding HOME to env\_keep may enable a user to run unrestricted

# commands via sudo.

#

# Defaults env\_keep += "HOME"

#

Defaults secure\_path = /sbin:/bin:/usr/sbin:/usr/bin

#

## Next comes the main part: which users can run what software on

## which machines (the sudoers file can be shared between multiple

## systems).

## Syntax:

##

## user MACHINE=COMMANDS

##

## The COMMANDS section may have other options added to it.

##

## Allow root to run any commands anywhere

##

root ALL=(ALL) ALL

#

## Allows people in group wheel to run all commands

%wheel ALL=(ALL) ALL

#

#-----------------------------------------------------------

################### CyberArk ############################

#

Cmnd\_Alias CYBER\_ARK\_PASS = /usr/bin/passwd, /usr/bin/su

Cmnd\_Alias CYBER\_ARK\_SU = /usr/bin/su

#

pamlogon ALL=(ALL) NOPASSWD: CYBER\_ARK\_SU

pamrecon ALL=(ALL) NOPASSWD: CYBER\_ARK\_PASS

##

#-----------------------------------------------------------