Installing and configuring Active Directory on Rocky (RADS)

V1.0

Contents

[Introduction: 2](#_Toc157175343)

[Installing Rocky Linux: 4](#_Toc157175344)

[Creating the VM: 4](#_Toc157175345)

[Retrieve the Installer from GitHub 12](#_Toc157175346)

[Configure chronyd 16](#_Toc157175347)

[Configure Samba for AD 17](#_Toc157175348)

[Validating the Install 21](#_Toc157175349)

[Checking Kerberos 21](#_Toc157175350)

[Checking DNS Records 22](#_Toc157175351)

[Adding Reverse DNS zone for AD 24](#_Toc157175352)

[Managing the AD server 25](#_Toc157175353)

[Resources 30](#_Toc157175354)

[Modifying chronyd to serve clients NTP 31](#_Toc157175355)

[Additions and Addendums 32](#_Toc157175356)

# Introduction:

This guide is designed to assist in setting up an Active Directory server on Rocky Linux for lab testing. It is assumed that you have some experience with

* ESXI
* RHEL (RedHat Enterprise Linux), or RHEL variants
* An understanding of Networking and Virtualization
* An understanding of Active Directory concepts

In this document we will be implementing the following:

* Install Rocky Linux
  + Configure the Base OS
  + Configure the Server for AD Domain Requirements
* Download the RADS Script from Github
  + Letting RADS configure the Server.
* Testing Samba Connectivity
  + Samba Processes
  + Kerberos
  + Host query for SRV (ldap\_tcp and UDP Kerberos) and A records

# Installing Rocky Linux:

Rocky Linux is installed in a virtual environment, in this example. Of course, you can install it on dedicated hardware, but that is outside of the scope of this document. At the time of this writing, the latest version of Rocky Linux is 9.3 and can be downloaded at:

<https://rockylinux.org/download/>

We will be installing on X64 bit architecture, using the minimal Install ISO.

The minimal ISO can be downloaded here:

<https://download.rockylinux.org/pub/rocky/9/isos/x86_64/Rocky-9.3-x86_64-minimal.iso>

This ISO will be uploaded to the ESXI platform and used for installation.

## Creating the VM:

In this example, the Rocky Linux VM is installed on an ESXI 7x platform. To deploy the VM successfully, on the select Name and Guest OS page of ESXI Select these options:

* Guest OS Family: Linux
* Guest OS Version CentOS9 (64-bit)

You can select the defaults for the VM, although the suggested configuration is:

* 2 vCPU
* 2048 GB RAM (Minimum)

Once we have set our configuration, we will power on the VM, where we will be greeted with the installer. A screenshot of a computer

Description automatically generated

Select Install Rocky Linux (Press Enter)

You will be presented with a graphical installer.

1. Select English and click continue.

A screenshot of a computer

Description automatically generated

You will be presented with an overview for the installer. We will modify the following settings:

Disk:

1. Click on Installation destination
2. When presented with the Disk layout, just click Done

Hostname:

1. In the hostname field, provide the FQDN of the server. This field will map as the AD server, so it should follow the same requirements as an AD DC (FQDN).
2. Click the Apply button next to the hostname field once you have entered it.

Network:

1. Click the configure button on the right-hand side of the screen
2. Select the IPV4 Settings Tab
3. Click the Method pull down menu and change to manual
4. Click the add button
5. Type the IP address/netmask and gateway for this device
6. Specify an External DNS Server (i.e 208.67.222.222)
7. Specify your AD DNS search domain that you will be using
8. Click Save

A screenshot of a computer

Description automatically generated

You will be returned to the previous screen.

A screenshot of a computer

Description automatically generated

There should be:

* Configured FQDN (bottom right of the screen)
* Configured Network Settings

This completes the Network configuration:

1. Click Done at the top left of the screen.

Note\* Make sure that the domain you created for the FQDN of this host is the NAME of the Domain you want to advertise via the Samba AD/DC. Changing this later can break Kerberos, etc.. so make sure you have a dedicated static IP and domain name you want to use.

Root Password Settings:

*\*Note: In this configuration, we will be allowing root access and we will be logging in as root. In a real world environment, we would be using sudo, however, for sake of simplicity and a functioning install, we will leverage the root account. You can harden the server after installation of all the services upon successful (radiusd) connectivity.*

1. Click Root Password under the User settings
2. Uncheck “Lock root account”
3. Check “Allow Root SSH login with password”
4. Specify the password for the root account
5. Click Done

After you have completed these steps, you should be back at the original install screen.

A screenshot of a computer

Description automatically generated

To start the actual installation of the configuration

1. Click “Begin Installation”

The installer will now deploy a minimal installation of Rocky.

Installation of the OS is complete!

A screen shot of a computer

Description automatically generated

After your successful installation:

1. Click “Reboot System”

## Retrieve the Installer from GitHub

Once the system reboots, we are presented with a login that should look similar, on the ESXI console.

A black screen with white text

Description automatically generated

We will now use our terminal of choice to login to the VM from our personal workstation.

On your terminal type:

ssh root@FQDN (or IP address) of your host

In this lab, the server was configured with an IP address of 192.168.240.9 (dc.test.int)

Once you are logged in via terminal, we will install wget and then start the retrieval of the RADS Installer

In this step, we will:

* Install wget
* Retrieve the RADS Installer

1. Copy and paste the following snippets of code into your terminal (you can copy all at once):

cd /root/

dnf -y install wget

wget https://raw.githubusercontent.com/fumatchu/RADS/main/DC-Installer.sh

chmod 700 ./DC-Installer.sh

/root/DC-Installer.sh

The system will start a basic install of wget with Perl dependencies.

You will be presented with the actual installer:

A screenshot of a computer program

Description automatically generated

The system will start to install all the dependencies for the samba AD installation. This script will also do the following:

1. Disable SELinux (you may set it back to permissive mode, but YMMV)
2. Disable the Firewall
3. Install the REPOS and update them:
   1. EPEL-Release
   2. CRB
   3. (dnf-plugins-core)
4. Install Cockpit (GUI management on port 9090)
5. Export paths needed for samba
6. Disable unwanted services
7. Create a Folder in /root/(called ADDCInstaller)

After this is completed, you will be presented with the following screen:

A screenshot of a computer

Description automatically generated

Pressing “Any Key” will disconnect your session. You can immediately log back into the server (as root) via terminal and continue the installation process (Phase 2)

When logging back in, you will be presented with the second phase of the installer.

A screenshot of a computer

Description automatically generated

In this portion of the install, the script will setup the following:

* Configure chronyd (but it will not service clients)
* Download the latest version of samba from samba.org
* Create a temp file structure in /root for compiling the code
* Prompt you to manually adjust the DNS entry of the system via nmtui
  + Since this is an AD server, it must point to itself first.
  + The earlier DNS entry will be complied into smb.conf for forwarding
* Setup Kerberos and krb5
* Create the samba-ad-dc service for service management
* Validate that the server is configured correctly

# Configure chronyd

chronyd is the daemon that will service time keeping requests.

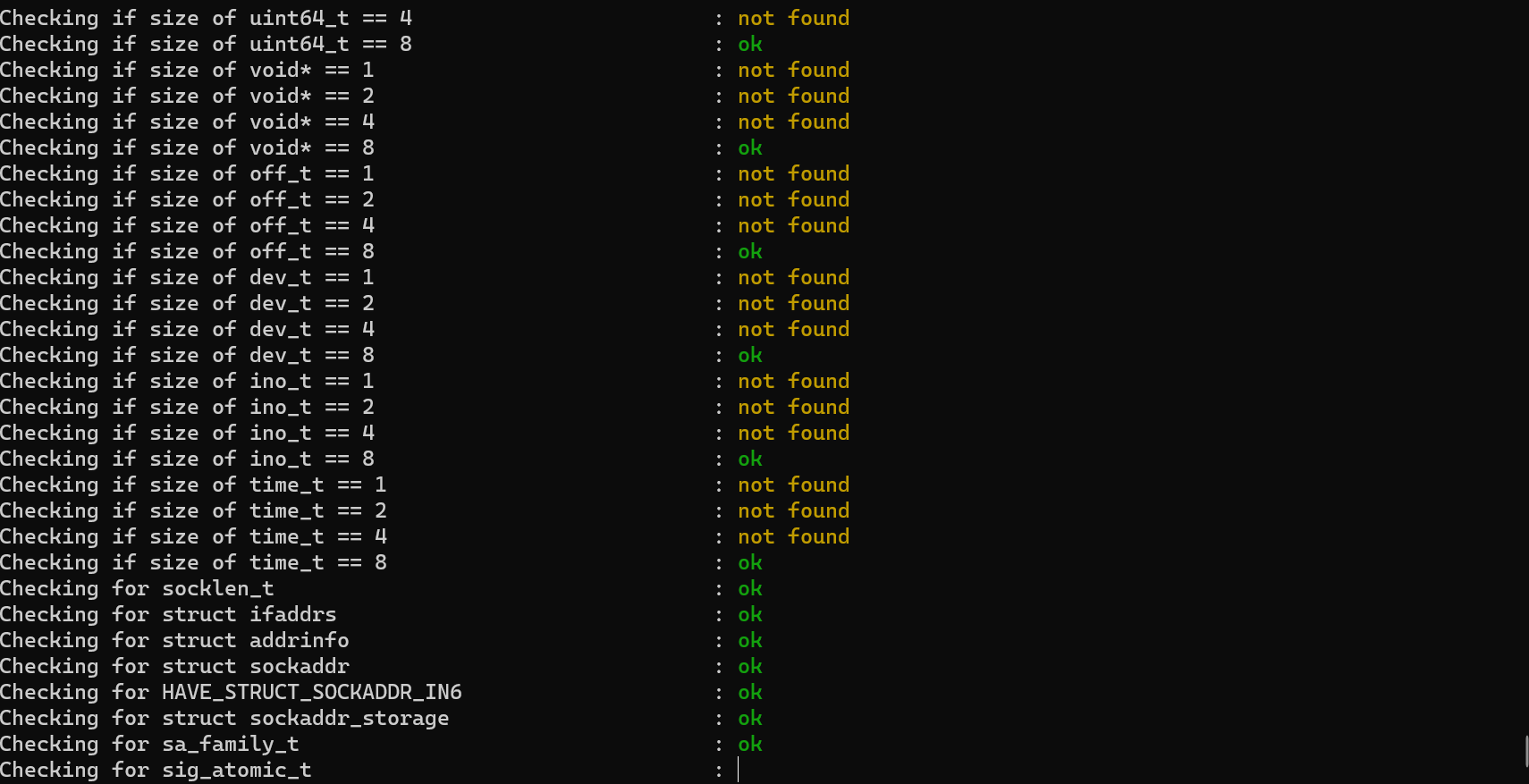
The script will modify chronyd to point to the pool: pool.ntp.org

It will also validate that it is getting proper time

\*NOTE: By default we will not service clients for ntp. You will have to manually allow the subnets you deem appropriate if you want this to be an NTP server for clients

# Configure Samba for AD

The server will download the Samba code and start compiling



The next steps will configure the server for AD

You will be presented with the following screen:

A black screen with white text

Description automatically generated

Notice how the installer took all previous knowledge of the Server and “created” the domain settings for you?

Just accept all the defaults

* Realm (derived from FQDN of the machine)
* Doamin(Derived from the Realm)
* Server Role, by default is dc. This is what we want
* DNS Backend should be left as SAMBA\_INTERNAL
* DNS forwarder: If you want to use the prexisting DNS entry you used earlier, you can, otherwise select a different forwarding server for unknown Resolver requests

When asking for the password prompt, this is the password you are creating for the Windows Administrator account (when you type, characters will not appear on the screen)

The server will then create the schema and DB for AD

A screenshot of a computer screen

Description automatically generated

Press Any Key

The script will now detect your primary IP and interface. We should remove all DNS entries from resolv.conf via nmtui and use only the “Main” IP address of this server, bound to it’s primary interface.

You will be presented with nmtui to modify the DNS entry.

1. Edit a Connection
2. Select your primary Interface (i.e ens192)
3. Use the arrow keys to edit and press enter
4. Use the Arrow Keys to navigate to DNS Servers and edit the current IP to the Servers IP

Like So:

A computer screen shot of a computer

Description automatically generated

1. Use the arrows to navigate ALL THE WAY DOWN to OK
2. Then use the arrow keys to navigate to back
3. Then select quit

# Validating the Install

The Next screen will show the service process of samba (for validation samba -D)

A computer screen with white text

Description automatically generated

The following test came from the samba.org website:

<https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller#Troubleshooting>

We will validate samba as a service is operational via systemctl

A screenshot of a computer

Description automatically generated

You can scroll through the Process with the up and down arrow keys. When you are satisfied press the “q” key.

## Checking Kerberos

The script will now produce a ticket for the system to validate Kerberos

You will be prompted for a password. This is the password you created in the domain provisioning

A computer screen with green text

Description automatically generated

Note\* you can see that the password will expire in 41 days. In the resources section, command will be provided to change that

## Checking DNS Records

The script will validate \_ldap.\_tcp

It will provide an example format and the real result

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A computer screen shot of a black screen

Description automatically generated

Upon validation, the script will complete.

## Adding Reverse DNS zone for AD

The script will see what subnet you are in and declare an appropriate reverse zone for you, for just the local subnet. It will provide the output you can just copy and paste, however, if you need to adjust, please do so.

samba-tool dns zonecreate dc.test.int 240.168.192.in-addr.arpa -U Administrator

A screenshot of a computer program

Description automatically generated

Type reboot on your terminal

# Managing the AD server

You may either manage the AD service via SSH with samba-tool command line (which will include some examples in the resources section), or you may use windows RSAT tools. The Samba AD supports the following RSAT tools:

* DNS
* Active Directory Users and Computers
* (Some) Group Policy

If you have a windows 11 Client, you do not have to have it joined to the domain to manage the AD server via RSAT. However, you do need to install the RSAT modules above to interact with it. In order to do this you need to:

1. Right click on the start menu
2. Select Settings

A screenshot of a computer

Description automatically generated

1. On the left had side, click system
2. Then, on the right pane, scroll down and click optional features
3. Click the button to “view features from the “Add an Optional Feature” Selection

A screenshot of a computer

Description automatically generated

There you will have the optional features to install

A screenshot of a computer

Description automatically generated

1. Select the Modules:
   1. RSAT: DNS Server Tools
   2. RSAT: Active Directory Domain Services and Lightweight Directory Services Tools
   3. RSAT: Group Policy Management Tools

This may take a while to install. Once they are installed, they will be in the Windows tools group

A screenshot of a computer

Description automatically generated

If the computer you are going to manage it on is NOT in the domain, you can:

1. Adjust your DNS on your laptop to point to the AD server for DNS resolution

Copy this script as a bat file or use the command line (THIS MUST BE AN ELEVATED COMMAND PROMPT-RunAsAdministrator):

runas /netonly /noprofile /u:DOMAIN\Administrator mmc.exe

This will allow you to load the snap-ins via MMC and manage the environment

After you add the snap-ins, you may get an error about PDC validation or one not being found. This is OK.

Once the Snap-ins are installed:

1. For DNS Snap-in, Select another computer, and put the FQDN in the field (not the IP Address)
2. For Active Directory Users and Computers
   1. Right click on the snap-in and select Change domain controller
   2. Put the FQDN of the domain controller and click off the field, it should pend status to OK
   3. Then select the entry and click OK

This is just an expanded view of the snap-ins where, if you are comfortable modifying here, you can

A screenshot of a computer

Description automatically generated

# Resources

## Modifying chronyd to serve clients NTP

The chrony.conf file is located in the /etc directory

vi /etc/chrony.conf

Change

#allow 192.168.0.0/16

To an appropriate network segment and restart the chrony service

service chronyd restart

If using Free RADIUS integration, we must add the following to smb.conf

/usr/local/samba/etc/smb.conf

ntlm auth = mschapv2-and-ntlmv2-only

(In the GLOBAL Section)

NEED to ADD CLI Commands Will Update

# Additions and Addendums

If you find any errors in this document, or have suggestions please contact me via Github (fumatchu)