VIRTUAL APPLIANCE

Virtual Appliance

Active Directory OpenLDAP

RCDevs Virtual Appliance Startup Guide

The RCDevs VMware Appliance is a standard and minimal CentOS 7 (64Bit) Linux installation with the RCDevs software packages already installed with yum. The Appliance contains the following (already configured) components:

- WebADM Server (installed in /opt/webadm/).
- WebADM Web Services: OpenOTP, SMSHub, OpenSSO, SpanKey, TiQR (installed in /opt/webadm/websrvs/).
- WebADM WebApps: SelfDesk, SelfReg, PwReset, OpenID (installed in /opt/webadm/webapps/).
- OpenOTP Radius Bridge (installed in /opt/radiusd/).
- RCDevs Directory Server (OpenLDAP in /opt/slapd/).
- MySQL Database Server (MariaDB).
- Postfix local Mail Transfer Agent.

To use the RCDevs VMware appliance, proceed as follows:

1. Download and Start the Appliance

Go to RCDevs Website to download the Appliance ZIP archive. The Appliance is provided in both VMX and OVF formats. The appliance is compatible with VMware ESX, ESXi, Workstation and Oracle VirtualBox. Unzip the archive and in VMware and choose *Import Appliance*. Select the VMX or OVF file.

Important

Do not copy and run the appliance directly without importing because the Appliance will fail during the boot process with a read-only filesystem error.

If required, you can adjust the CPU and memory settings of your Appliance. By default, it is configured with virtual 2 CPUs and 1GB memory.

In case you choose to use the VMX import format (and not the preferred OVF format), you will need to set up the VM system by yourself and use the VMX as SCSI storage file. The following configuration information may be useful:

- System type: Linux 64Bit (2 CPUs and 1Go RAM)
- Disk controller: SCSI LsiLogic
- Drive: the VMX file is a dynamically allocated 20 Go drive
- Network: PCnet-FAST III (Am79C973) card

Keep the boot console opened during the boot process to track any startup error. The Appliance is configured to get its IP address via DHCP.

2. VirtualBox Import

In the VirtualBox Menu click on **File** then **Import Appliance**. Now select the RCDevs Virtual Appliance File **RCDevs-VM.ovf** to import and click on **Continue**.

Now click on **Import**.

⚠ The guest operating system 'rhel7_64Guest' is not supported

If you encountered this kind of message during the RCDevs VM import, then you have to adjust the compatibility mode according to your ESXi, Workstation, Fusion or Player version. Have a look at the VMWare website to have more information about virtual hardware versions supported according to your VMWare version. To change the hardware version on the VM, have a look at the VM settings > Compatibility mode and change the hardware version with one supported by your VMWare software.

Finally, click on **Start** to boot the RCDevs Virtual Appliance.

3. Start the Setup Script

This script occurs only once (at first boot) and does not require a login password. You can open the console or access with ssh to do the setup at first boot. You can restart it with `vm_init` command.

The WebADM setup script asks for:

- Your time zone.
- Optionally to set the network interface.
- Choose and configure an LDAP server (the default LDAP server is already configured).

After this short setup is completed, the script will start all the services:

- WebADM HTTP, SOAP, PKI and Session Manager Services.
- Radius Bridge Service
- LDAP Server
- SQL server

3.1 Setup with the Local LDAP Database

```
------------------------------------------------------------------------
Welcome to RCDevs VMWare Appliance 1.7.0!
------------------------------------------------------------------------

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? 8
```

We choose the time zone, for example, Luxembourg in Europe.

```
Please select a country.
 1) Albania    18) Guernsey      35) Poland
 2) Andorra    19) Hungary      36) Portugal
 3) Austria    20) Ireland      37) Romania
 4) Belarus    21) Isle of Man     38) Russia
 5) Belgium    22) Italy      39) San Marino
 6) Bosnia & Herzegovina  23) Jersey      40) Serbia
 7) Britain (UK)   24) Latvia      41) Slovakia
 8) Bulgaria    25) Liechtenstein     42) Slovenia
 9) Croatia    26) Lithuania      43) Spain
10) Czech Republic   27) Luxembourg     44) Sweden
11) Denmark    28) Macedonia      45) Switzerland
12) Estonia    29) Malta      46) Turkey
13) Finland    30) Moldova      47) Ukraine
14) France    31) Monaco      48) Vatican City
15) Germany    32) Montenegro     49) Åland Islands
16) Gibraltar    33) Netherlands
17) Greece    34) Norway
#? 27

The following information has been given:

 Luxembourg

Therefore TZ='Europe/Luxembourg' will be used.
Local time is now: Thu Jul 13 13:36:07 CEST 2017.
Universal Time is now: Thu Jul 13 11:36:07 UTC 2017.


This VM is running with dynamic IP assignment (DHCP)
The current IP address is 192.168.3.160
```

All following options are set with the default value in square brackets. You can keep it by pressing enter.

```
Do you want to configure a static IP ([y]/n)?
y
Please type the fixed IP address [192.168.3.160]:
192.168.3.160
Please type the network mask [255.255.255.0]:
255.255.255.0
Please type the gateway address [192.168.3.254]:
192.168.3.254
Please type your primary DNS server IP [8.8.8.8]:
8.8.8.8
Please type your secondary DNS server IP []:

Fixed IP address: 192.168.3.160
Network address: 192.168.3.0
```

```
Network mask: 255.255.255.0
Gateway IP address: 192.168.3.254
Primary DNS server: 8.8.8.8
Do you confirm ([y]/n):
y
Writing /etc/sysconfig/network-scripts/ifcfg-ens33
Restarting network...

SSetup WebADM as master server or slave (secondary server in a cluster) ([m]/s)? m
WebADM proposes 4 default configuration templates:
  1) Default configuration (RCDevs Directory)
  2) Other generic LDAP server (Novell eDirectory, Oracle, OpenLDAP)
  3) Active Directory with schema extention (preferred with AD)
  4) Active Directory without schema extention
Choose a template number [1]:  1

Starting WebADM setup script /opt/webadm/bin/setup
Checking system architecture...Ok
Generating CA private key... Ok
Creating CA certificate... Ok
Generating SSL private key... Ok
Creating SSL certificate request... Ok
Signing SSL certificate with CA... Ok
Adding CA certificate to the local trust list... Ok
Setting file permissions... Ok
Adding systemd service... Ok
Adding logrotate scripts... Ok
Generating secret key string... Ok
WebADM has successfully been setup.

Starting services...
Created symlink from /etc/systemd/system/multi-user.target.wants/slapd.service to
/usr/lib/systemd/system/slapd.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/radiusd.service to
/usr/lib/systemd/system/radiusd.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/ldproxy.service to
/usr/lib/systemd/system/ldproxy.service.
Ok

You can connect your server via SSH with 'ssh root@192.168.3.160'.
SSH root password is 'password'.

You can login RCDevs WebADM Admin Portal at 'https://192.168.3.160'.
WebADM login username is 'admin'.
WebADM login password is 'password'.

WARNING: This appliance is configured with permissive firewall,
dummy certificates, default passwords for services and root access.
You MUST re-configure your appliance before any production use!

Press any key to finish!
```

We are now ready to use WebADM.

Have a look at the following documentation to register a token and perform an authentication.

3.2 Setup with an Active Directory Server

```
------------------------------------------------------------------------
Welcome to RCDevs VMWare Appliance 1.6.8!
------------------------------------------------------------------------

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? 8
```

We choose the time zone, for example, *Luxembourg* in *Europe*.

```
Please select a country.
 1) Albania    18) Guernsey      35) Poland
 2) Andorra    19) Hungary      36) Portugal
 3) Austria    20) Ireland      37) Romania
 4) Belarus    21) Isle of Man     38) Russia
 5) Belgium    22) Italy      39) San Marino
 6) Bosnia & Herzegovina  23) Jersey      40) Serbia
 7) Britain (UK)   24) Latvia      41) Slovakia
 8) Bulgaria    25) Liechtenstein     42) Slovenia
 9) Croatia    26) Lithuania      43) Spain
10) Czech Republic   27) Luxembourg     44) Sweden
11) Denmark    28) Macedonia      45) Switzerland
12) Estonia    29) Malta      46) Turkey
13) Finland    30) Moldova      47) Ukraine
14) France    31) Monaco      48) Vatican City
15) Germany    32) Montenegro     49) Åland Islands
16) Gibraltar    33) Netherlands
17) Greece    34) Norway
#? 27

The following information has been given:

 Luxembourg

Therefore TZ='Europe/Luxembourg' will be used.
Local time is now: Thu Jul 13 14:04:58 CEST 2017.
Universal Time is now: Thu Jul 13 12:04:58 UTC 2017.


This VM is running with dynamic IP assignment (DHCP)
The current IP address is 192.168.3.160
```

All following options are set with the default value in square brackets. We can keep it by pressing enter.

```
Do you want to configure a static IP ([y]/n)?
y
Please type the fixed IP address [192.168.3.160]:
192.168.3.160
Please type the network mask [255.255.255.0]:
255.255.255.0
Please type the gateway address [192.168.3.254]:
192.168.3.254
Please type your primary DNS server IP [8.8.8.8]:
8.8.8.8
Please type your secondary DNS server IP []:

Fixed IP address: 192.168.3.160
Network address: 192.168.3.0
Network mask: 255.255.255.0
Gateway IP address: 192.168.3.254
Primary DNS server: 8.8.8.8
Do you confirm ([y]/n):
y
Writing /etc/sysconfig/network-scripts/ifcfg-ens33
Restarting network...

Setup WebADM as master server or slave (secondary server in a cluster) ([m]/s)? m
WebADM proposes 4 default configuration templates:
  1) Default configuration (RCDevs Directory)
  2) Other generic LDAP server (Novell eDirectory, Oracle, OpenLDAP)
  3) Active Directory with schema extention (preferred with AD)
  4) Active Directory without schema extention
Choose a template number [1]:  4
```

We need to choose `3` or `4` instead of `1` for `Active Directory` and configure it. Option 3 will require an Active Directory schema extension.

```
Please type the name/ip of the LDAP server [localhost]:192.168.3.139
Please type the port fort LDAP [389]:
389
Checking port...Ok
Please choose the encryption ([TLS]/SSL/NONE)?
TLS
Please type domain FQDN (i.e. dc=lab,dc=local) []:dc=lab,dc=local
```

We enter an administrator user for this short configuration. We can change it later in `/opt/webadm/conf/webadm.conf` if we need. More information for fine-grained permissions are available in chapter 22 *LDAP Permissions* of Administrator Guide.

```
Please type a user with read/write acces to LDAP
[cn=Administrator,cn=Users,dc=lab,dc=local]:
cn=Administrator,cn=Users,dc=lab,dc=local
Please type the user password:
Testing user access...Ok
Please type the WebADM container [cn=WebADM,dc=lab,dc=local]:
cn=WebADM,dc=lab,dc=local
Starting WebADM setup script /opt/webadm/bin/setup
Backuping previous configuration to /opt/webadm/conf/backup/
Checking system architecture...Ok
Generating CA private key... Ok
Creating CA certificate... Ok
Generating SSL private key... Ok
Creating SSL certificate request... Ok
Signing SSL certificate with CA... Ok
Adding CA certificate to the local trust list... Ok
Setting file permissions... Ok
Adding systemd service... Ok
Adding logrotate scripts... Ok
Generating secret key string... Ok
WebADM has successfully been setup.

Starting services...
Ok

You can connect your server via SSH with 'ssh root@192.168.3.160'.
SSH root password is 'password'.

You can login RCDevs WebADM Admin Portal at 'https://192.168.3.160'.
WebADM login user DN is 'cn=Administrator,cn=Users,dc=lab,dc=local'.

WARNING: This appliance is configured with permissive firewall,
dummy certificates, default passwords for services and root access.
You MUST re-configure your appliance before any production use!

Press any key to finish!
```

Now we connect to the web interface on `https://192.168.3.160` and `cn=Administrator,cn=Users,dc=lab,dc=local` user as indicated above. We will be able to use `administrator` after the first configuration.

We need to click on `Create default containers and objects` for creating ldap configurations under `cn=webadm,dc=lab,dc=local`.

Please, log out and login with the `Administrator` user as indicated above.

We need to create the configuration for `MFA Authentication Server`. For that, we click on `Not Registered`.

We click on `REGISTER`.

`MFA Authentication Server` is now enabled. We are ready to use WebADM.

3.2.1 Test User Authentication

Now, it's time to test your OpenOTP installation by enrolling a Sofware Token and test a user authentication. Please, follow this documentation OpenOTP Quick Start. If you don't have a Hardware Token to register then you need to install the OpenOTP Token Mobile Application (Software Token) for the smartphone. Please, read this documentation OpenOTP Token Mobile Application.

4. Resetting the Appliance

At any moment, you can reset the VMware appliance to its original state by running the `vm_reset` command from the shell (for example if we want to restart the initial setup). You can also re-run the initial setup script by using the `vm_init` command. Be aware that re-running the `vm_reset` or `vm_init` script will remove any work data in the VM.

You can find the WebADM setup script in `/opt/webadm/bin/` and the Radius Bridge setup script in `/opt/radiusd/bin/`. With the RCDevs Directory Server version, you can find the OpenLDAP setup script in `/opt/slapd/bin/`.

Please look at the INSTALL and README files in `/opt/webadm/`, `/opt/radiusd/` and `/opt/slapd/`.

Thanks for trying RCDevs Security solutions.

5. Upgrade the Appliance

To upgrade the RCDevs appliance, you just need to perform the following command:

```
yum update
```

Every RCDevs packages and others installed on the RCDevs appliance will be updated. A restart may be required.

6. Testing your OpenOTP Installation

6.1 Enroll a Software Token

Your OpenOTP Server is now working and you can start enrolling a test user. We will enroll a Software Token for a new user with Google Authenticator.

1. On your iPhone or Android phone, go to the AppStore and search for Google Authenticator. Download and install the application on your mobile.
2. Create a WebADM Account test user in your LDAP tree. Go to the top menu in WebADM, and click the `Create` button. Choose the `WebADM Account` object and create a user with login name 'testing' and password 'test'. Alternatively, you can use an existing WebADM user for your tests. Set the Container (LDAP folder) to a location below you Domain User Search Base.

3. Once the user is created, edit it and click the `MFA Authentication Server` button in the Application Actions box.

4. Click the `Register / Unregister Token` button.

5. Check the Google Authenticator Time-based or Event-based checkbox. Immediately, a QRCode is displayed on the page.

6. Start the OpenOTP Token or Google Authenticator application on your mobile phone and click the `Camera` button. Scan the QRCode to register a new Software Token on your mobile phone. When done, click the `Register` button on the screen. The Software Token is now registered in OpenOTP.

6.2 Configure the User Authentication Method

You have registered an OpenOTP Token or a Google Authenticator Software Token for your test user. We will now configure the user to work with 'TOKEN' authentication mode.

1. Edit the user and click the `CONFIGURE` button in the Object Details box.

2. Select `MFA Authentication Server` in the Application list box.

3. Check the 'OTP Type' checkbox and select `TOKEN`. If `TOKEN` is already the default OTP Type, then you do not need to configure this setting.

4. Save the user settings by clicking the `Apply` button at the bottom of the page.

6.3 Test User Authentication

1. Return to the `MFA Authentication Server` in the Application Actions box for the user and click the `Test User Authentication` action.

A login form is displayed. Enter 'test' in the LDAP Password field and let the rest empty. Click the `Start` button.

2. You didn't enter the OTP in the login and OpenOTP also activates the Challenged-OTP mode. A new window is displayed with a message asking for your Token password. Enter the password displayed on your Google Authenticator mobile application.

3. WebADM displays the authentication result and server message.

You can have a look at the 'WebADM Server Log Files' in the 'Database' menu to see what happened.

7. Testing a Web Server Integration

You can download and use the RCDevs sample PHP Login Form for OpenOTP to experiment a very simple Web integration with OpenOTP:

loginform.zip

Copy the ZIP archive to your public Web server's document root (for example */var/www/html*), and unzip it. It will create a loginform directory. The testing URL on your Web server will be *http://yourwebsite.com/loginform/*

Be sure to have PHP and the PHP-SOAP extension installed on your public Web server. On a RedHat server, You can install it with:

```
yum install php php-soap
```

Enter the loginform directory and edit the index.php file. You need to adjust the OpenOTP SOAP web service URL (server_url) at the beginning of the file. Remember that the web service URLs are displayed in the Applications menu in WebADM.

```
$server_url = "http://mywebadmserver:8080/openotp/";
```

You can now go to the login form URL at http://mywebsite.com/loginform/ with a Web browser to test the sample OpenOTP login integration.

Enter the username and LDAP password. You can enter the OTP password in this screen or in the challenge screen (after pressing the 'Login' button) as we did in our authentication test previously.

8. Configure your VPN Server with OpenOTP

The configuration of your VPN server depends on your VPN software. Get your vendor documentation and look for a section explaining how to use a RADIUS server for remote authentication. As a general rule, you will need to set up a RADIUS server connection by specifying the IP address of the Radius Bridge and the RADIUS shared secret. On your Radius Bridge server, you will need to edit the /opt/radiusd/conf/clients.conf and add a RADIUS client block (with the IP address of the VPN server and the shared RADIUS secret). Please look at RCDevs' Radius Bridge Manual for details about the RADIUS server configuration and integration.

Appendix A - OpenOTP Server SOAP API & WSDL

Please, refer to the following documentation.