USER MANUAL

RCCMD Client Software for vmMiniSlot Card

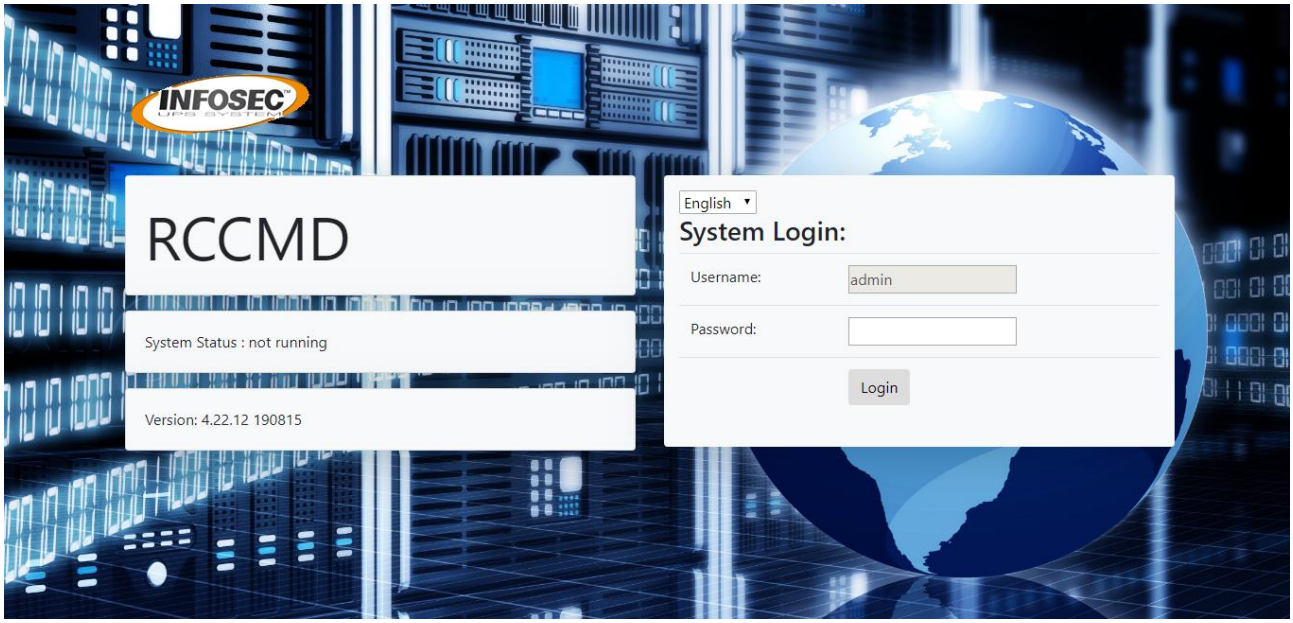
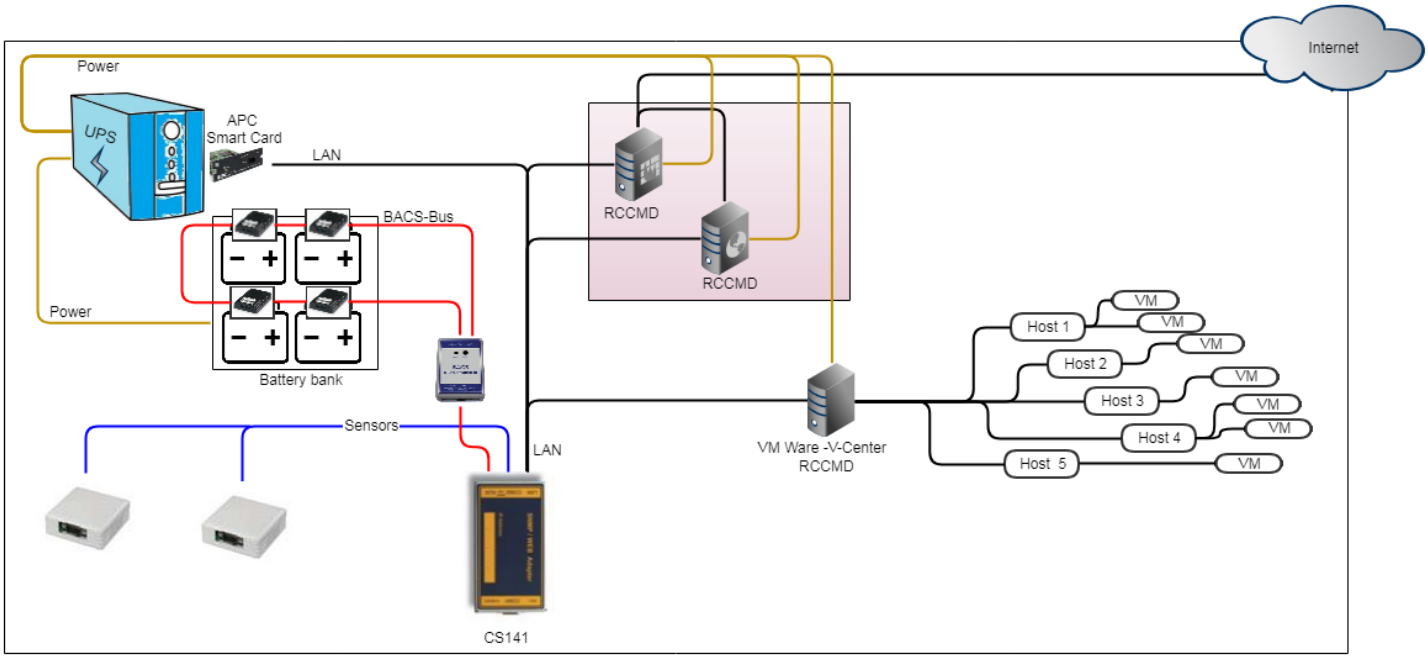


Table of contents

1. RCCMD technology



RCCMD is designed to shut down your systems in case emergency. In this case, an RCCMD server - usually a UPSMan or CS141 / CS121 - sends a shutdown command to the clients. The clients react to this signal accordingly.

Several basic conditions must be fulfilled for operation:

1. The RCCMD client needs a fixed IP address

The latter must be communicated to the RCCMD server to send them a unique shutdown command.

2. The corresponding RCCMD server must be authorized to send.

By default, RCCMD accepts any broadcast sent by a RCCMD server. If these receptions are not desired, an authorized transmitter can be defined. The customer will save all other orders but will no longer execute them

3. The following ports must be available on your network:

Port 8080 This port is used to call the local RCCMD web interface
Port 8443 This port is used to access the RCCMD web interface on another computer / server
Port 6003 The RCCMD client communicates via this port

2. Installing the RCCMD appliance with Windows

Note: The RCCMD installer uses the Java Runtime Environment version, which is used for installation and uninstallation. In addition, the RCCMD Web Configurator uses a Java Web server. You can disable the RCCMD service "RCCMDWebIf" in service administration and RCCMD will run without Java.

2.1. Installation and configuration

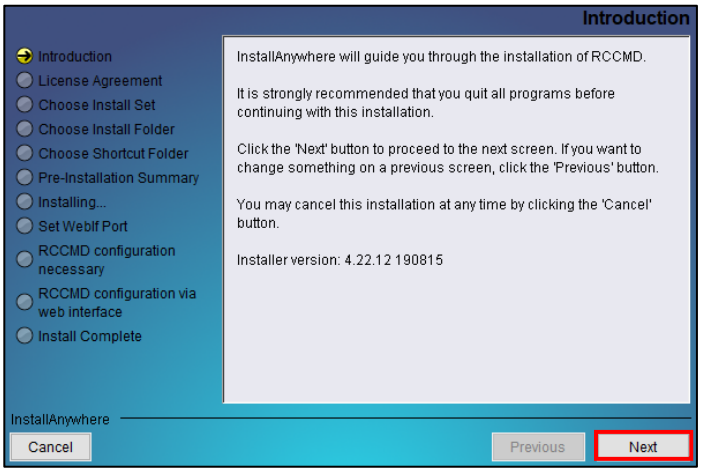
Before you begin the installation, make sure you have all administrator rights. Without having the rights, the installation will not succeed.

Insert the CD into the machine or download RCCMD from https://www.infosec-ups.com/fr/accessoires-et-logiciels/logiciel-client-rccmd.html.

« Introduction » menu

In the start menu you can see the different steps of the installation.

Click on "Next".



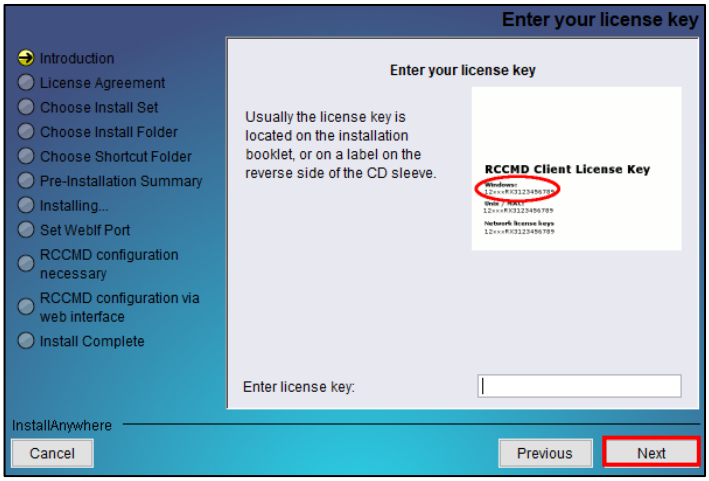
"License Agreement" Menu

Please enter your license key. The license used determines which module can be installed.

You need a special license key for your RCCMD software. You can identify the key with the "RX3" in the first part of the license key. Most of the time, you must order the key separately.

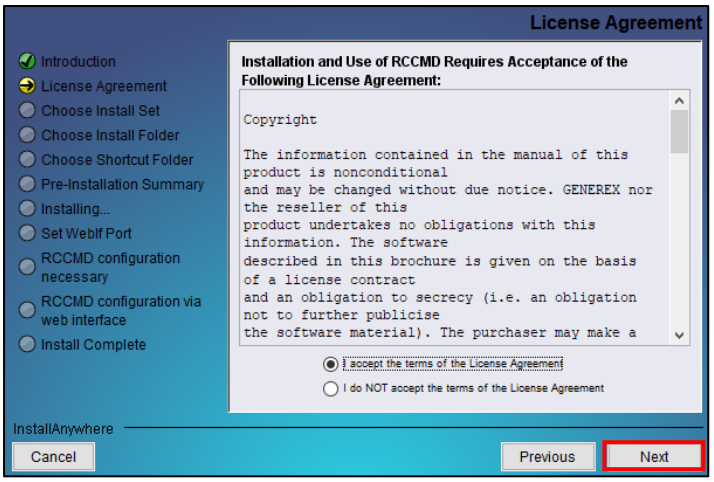
Click on "Next"

➔ If you do not enter a license key or enter it incorrectly, RCCMD will automatically assign a 30-day evaluation license



Check "I accept the terms of this license agreement".

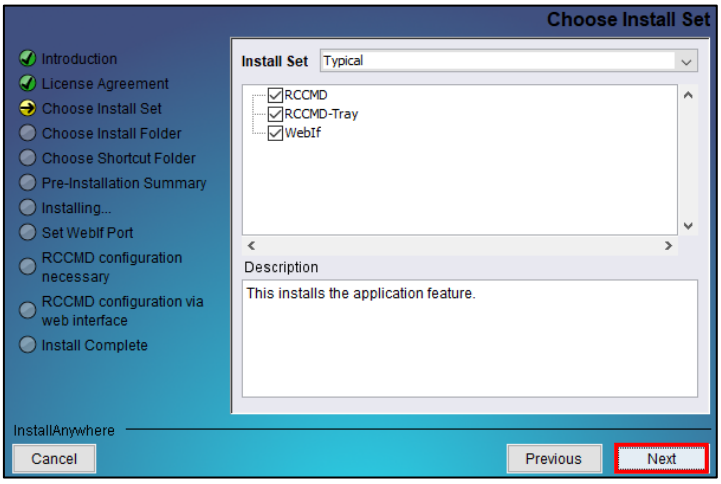
Click on "Next".



Selecting the type of installation

Select the items you wish to install.

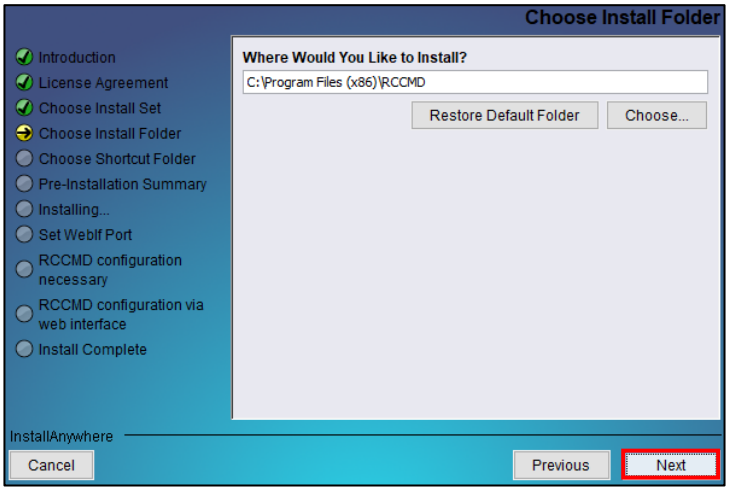
Click on "Next"



Selecting the installation folder

In this tab, it is necessary to fill in the installation path for RCCMD. By default, it is located in "C \ Program Files (x86) \ RCCMD"

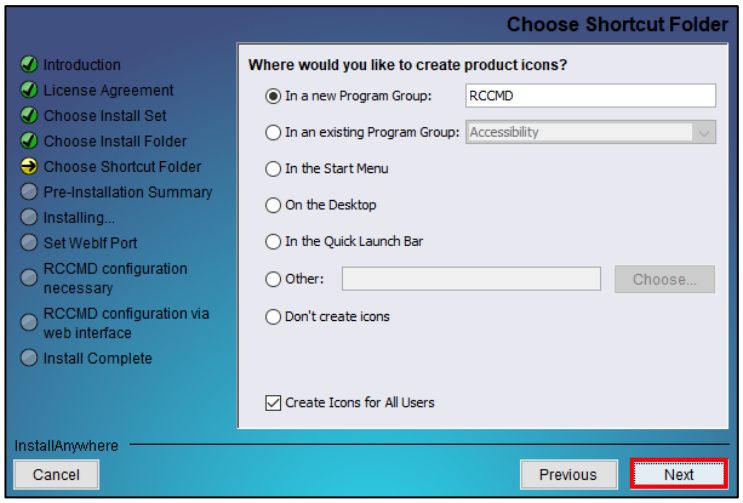
Click on "Next"



Selecting the shortcuts folder

Select the location where the shortcut will be stored to access RCCMD.

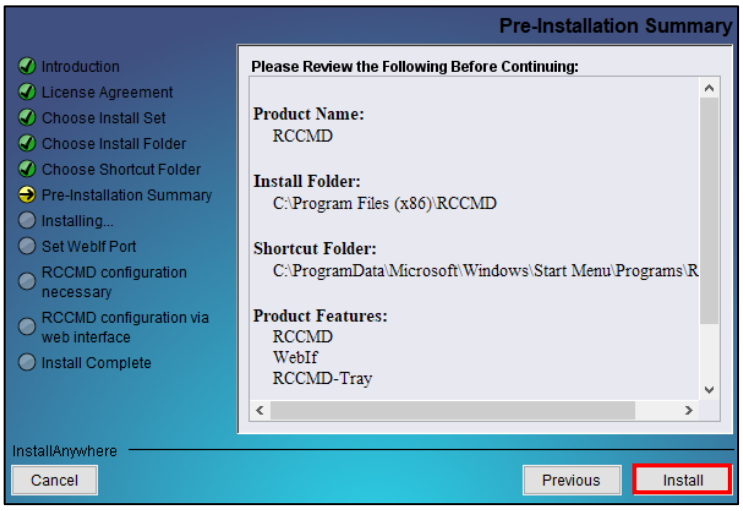
Click on "Next".



Pre-installation summary

Check the information you have entered.

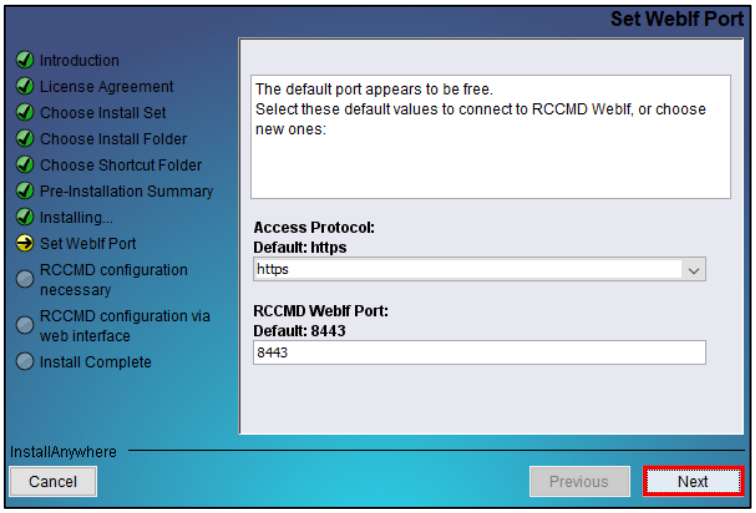
Once done, click on "Install".



"Set WebIf Port" menu

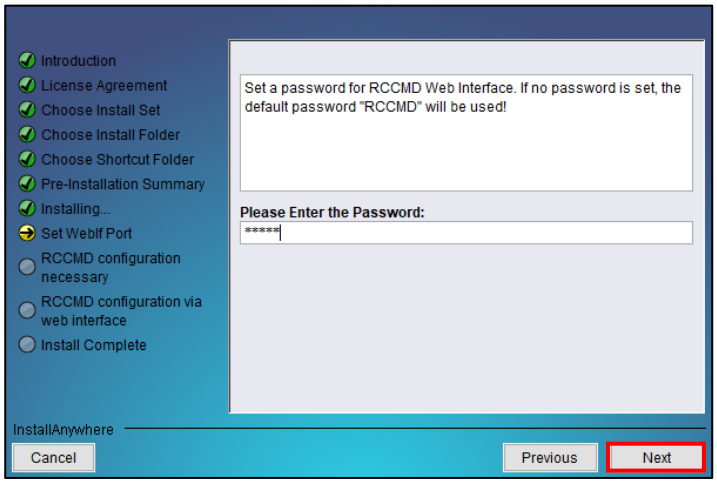
RCCMD uses the https protocol and the default port 8443. Please leave these defaults to avoid future malfunctions.

Click on "Next".



Enter the default password that is "RCCMD".

Click on "Next".

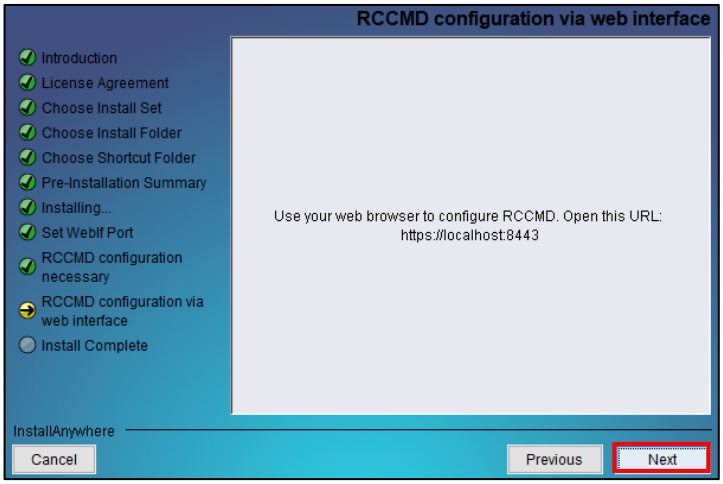


RCCMD configuration via web interface

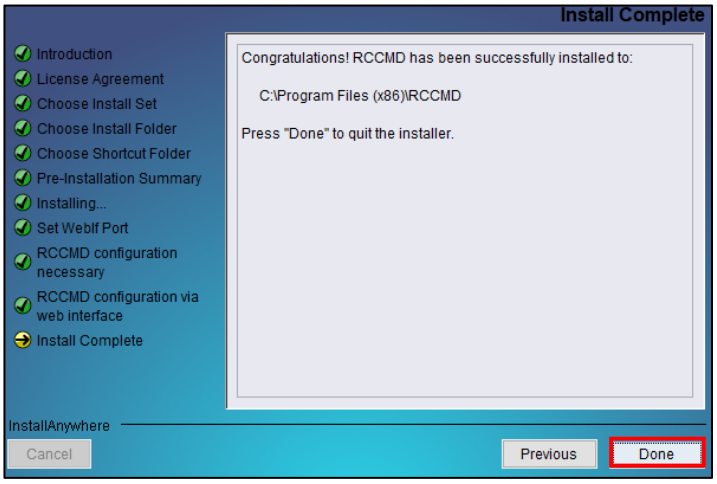
To configure RCCMD, use the following link:

https: // localhost: 8443.

Click on "Next"



Click on "Done" to finalize the installation and access RCCMD via the web interface.



3. Installing the RCCMD appliance with ESXi 6.0

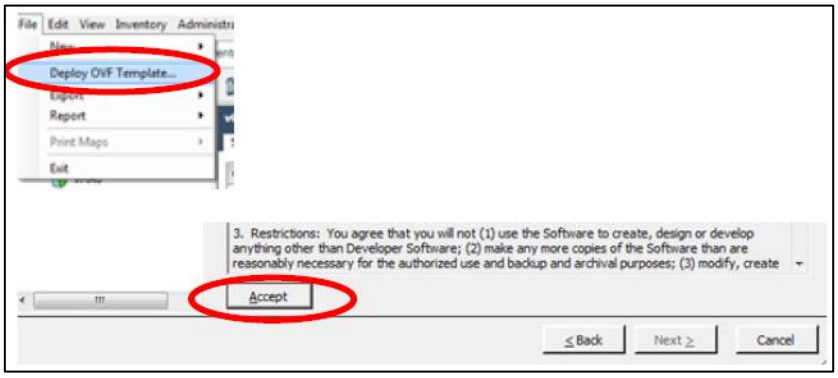
Prerequisites:

- VSphere Management Assistant (vMA): You can download version 6.0 from the VMware site. This appliance is required for the installation of RCCMD.
- FTP client (WinSCP): This will allow to transfer the RCCMD installation files to the vMA machine.
- Client terminal (PuttY): To control vMA for the installation of RCCMD in a simpler way.

3.1 Installation and configuration of vMA

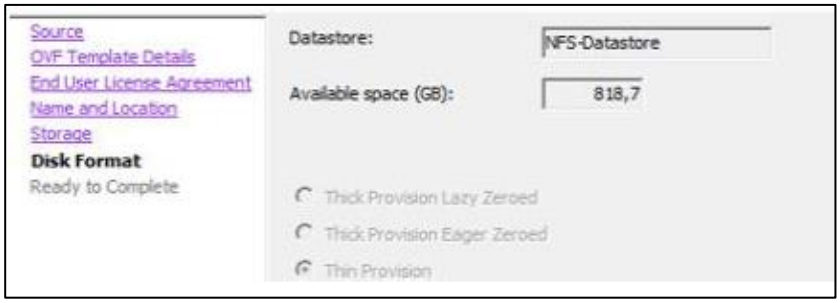
Click on "File", "Deploy OVF Template" and select the OVF file for vMA.

Accept the license and click on "Next"



Give the VM a name. The default name is "vMA". It is recommended to use a short but meaningful name. (For example: vMA_RCCMD)

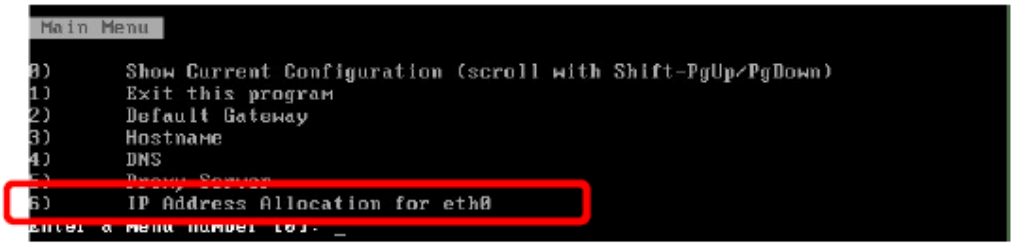
After choosing the storage location, the installation will start.



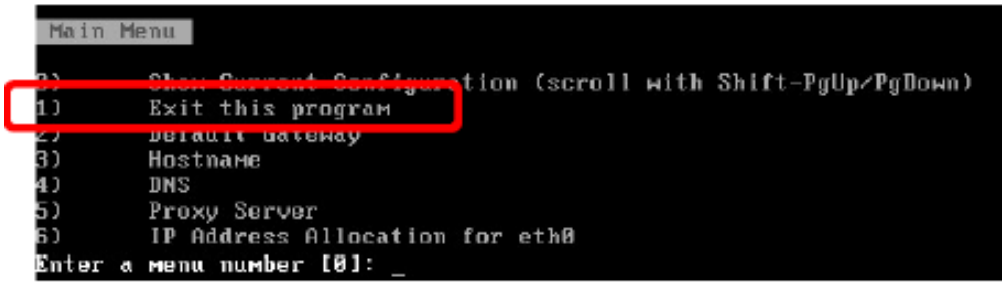
Start the VM and open a console.

Once the vm is started, you will come to the next menu.

Select menu 6 to configure the network.



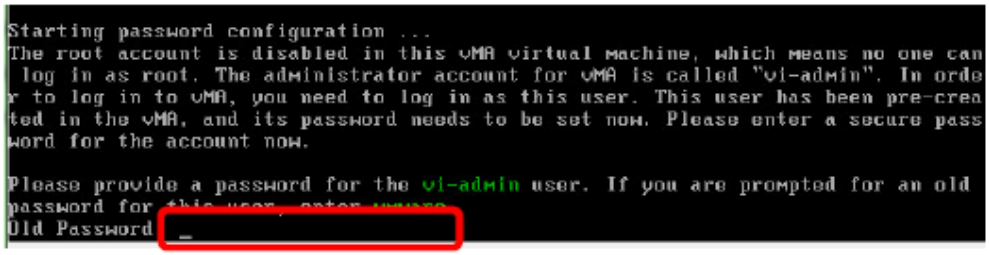
To exit this menu and enter shell mode, select menu 1.



Enter the default password ("vmware").

Then enter a new password that meets the following conditions:

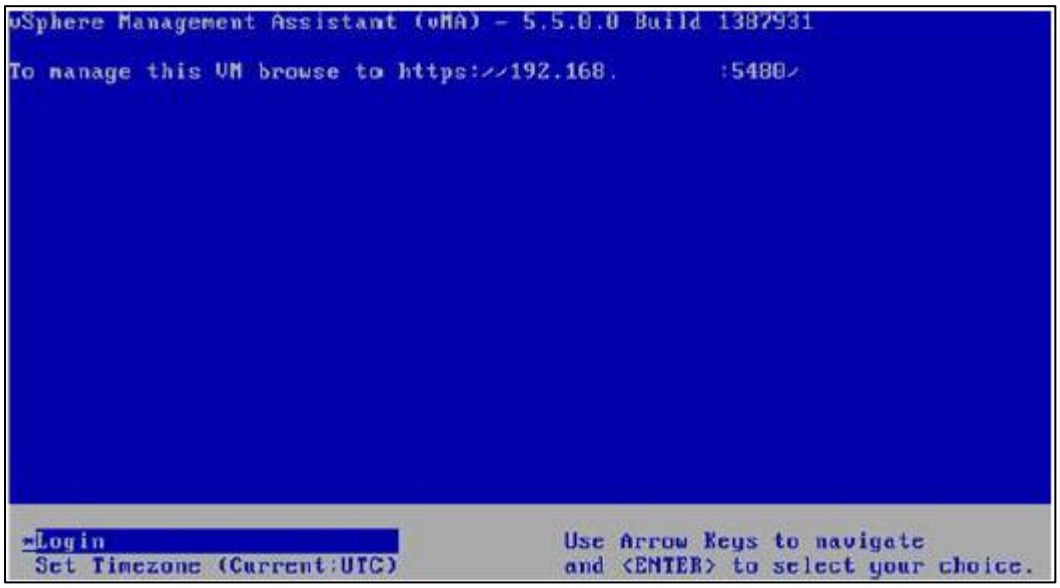
- Tiny letter
- Capital letter
- sales
- Special character



Once this is done, vMA is ready. You just have to press the Enter key and enter your login credentials.

User: vi-admin

Password: * password previously entered *



3.2. RCCMD installation

Now that the vMA appliance is ready, you need to import the archive containing the RCCMD installation. (Download link: https://www.infosec-ups.com/fr/accessoires-et-logiciels/logiciel-client-rccmd.html)

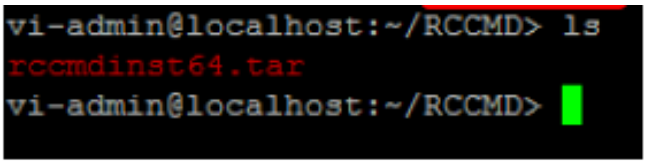
To import it into the VM, it is necessary to use an FTP client (WINscp for example.) Open it and connect you on the port 22 (FTP) with the vi-admin identifiers.

Then, drag a copy of your post to the VM in the folder of your choice (It is advisable to place it in / home / vi-admin /).

Connected to the terminal (PuttY for example). Enter the IP address and press "Open". Enter the vi-admin identifiers.

Go to the location where you placed the RCCMD archive using the command "cd / path_of_folder /". (Default: "cd / home / vi-admin")

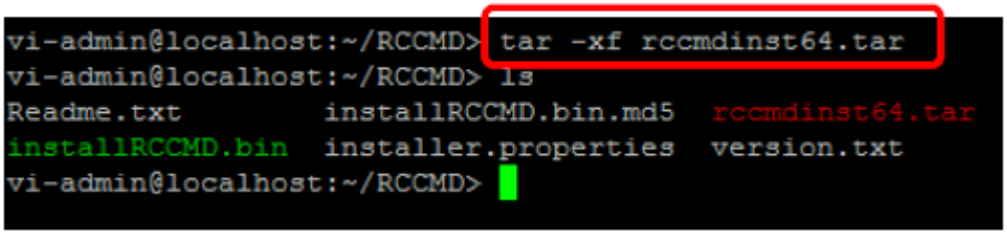
Type the command "ls" and check that the archive is present as here.



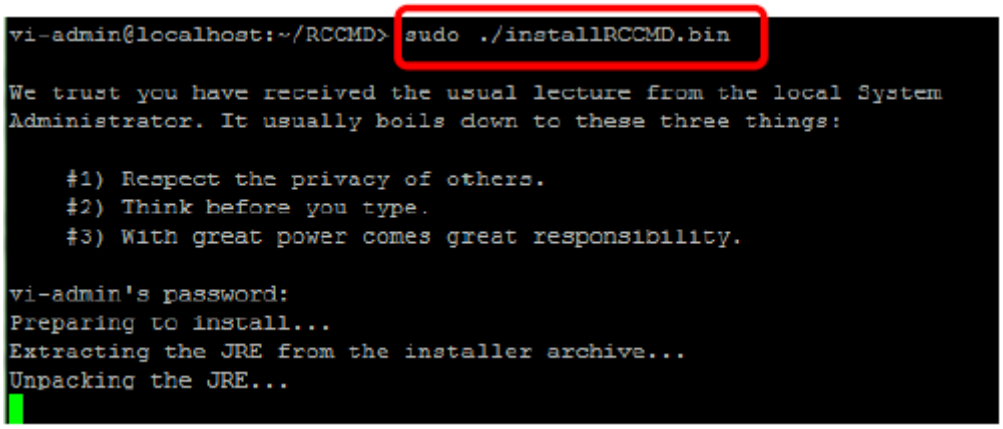
To decompress the archive, use the following command:

"Tar -xf archive_name"

You can check with the command "ls" that the archive has been uncompressed.



To start the installation of RCCMD, execute: "sudo ./installRCCMD.bin"



Choice of language. Select 2 for English.

```
Choose Locale...
----------------

    1- Deutsch
  ->2- English
    3- Espa?ol
    4- Fran?ais
    5- Italiano
    6- Portugu?s

CHOOSE LOCALE BY NUMBER:
```

Enter your license key provided.

```
Enter your license key
----------------------

Enter your license key
Usually the license key is located on the installation booklet, or on a label
on the reverse side of the CD sleeve.
Enter license key:
```

Accept the license agreement by writing "O" in the console.

```
the operating systems, loss of data or interruption of work processes, other
UPS problems or to other errors that may occur out of this combination.



DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): Y
```

Select the features you want to install. If you do not know, leave it as default and press Enter.

```
Choose Product Features
-----------------------

ENTER A COMMA_SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'.  PRESS <RETURN> WHEN YOU ARE DONE:

    1- [X] RCCMD
    2- [X] WebIf
    3- [X] XMessage

Please choose the Features to be installed by this installer.:
```

Now indicate the path in which RCCMD will be moving. It is advisable to leave it by default and press Enter.

```
Where would you like to install?

  Default Install Folder: /usr/rccmd

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
      :
```

If you have a vCenter and it is accessible, leave it as default and press Enter.

Otherwise, type 2 and then Enter.

```
If a vCenter is available, the credentials will be required. The vSpherePlugin
will be registered for use in the vSphere Client for Windows. RCCMD will then
be configured via that interface.

  ->1- Yes
    2- No

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT::
```

Then enter the information about an ESX that you want to manage. It is possible to add more then, using the WEB interface. If you do not want to fill in anything, type Enter.

```
What is your ESXi Host called?
------------------------------

Enter Name of one managed ESXi Host.
Additional Hosts may be configured in the Web interface after installation.

Name or IP-Address (Valeur par d?faut : ):
```

Select the options you want to have RCCMD messages. It is recommended to leave by default.

```
RCCMD Messages
--------------

By default rccmd will print the messages it receives from the network to
/dev/console.
Here you can choose additional output options.

  ->1- Display Messages on all terminals
  ->2- Log Messages
  ->3- Display Messages with Xmessage

ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED CHOICES, OR
   PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

Then, the terminal displays a summary of the installation. Remember to check all the information.

Press Enter to continue.

```
Please Review the Following Before Continuing:

Product Name:
    RCCMD

Install Folder:
    /usr/rccmd

Product Features:
    RCCMD,
    WebIf,
    XMessage

Messaging Options
    "Display Messages on all terminals","Log Messages","Display Messages with Xm
essage"

Disk Space Information (for Installation Target):
    Required:  229,867,211 Bytes
    Available: 93,032,448 Bytes

PRESS <ENTER> TO CONTINUE:
```

Select the WEB protocol of your choice. It is recommended to use HTTPS (default).

```
Set WebIf Protocol
------------------

This is the default protocol to access the RCCMD WebIf.
Select your preferred protocol here:

  ->1- https
    2- http

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT::
```

Enter a port for WEB access. The default is 8443. Leave as default.

```
Set WebIf Port
--------------

The default port appears to be free.
Select these default values to connect to RCCMD WebIf, or choose new ones:

Port: (Default: 8443):
```

The RCCMD installer informs us that he will create 2 exceptions on the firewall for port 8443 (WEB) and port 6003/5769 (RCCMD).

```
Firewall Exceptions
-------------------

Firewall Exceptions (Iptables only) will be added for:
Ports 8443 (WebIf Server)
Ports 6003 & 5769 (RCCMD)

PRESS <ENTER> TO CONTINUE:
```

Enter the default password and a password indication so you do not forget it.

```
Enter Password
--------------

Set a password for RCCMD Web Interface. If no password is set, the default
password "cs121-snmp" will be used!

Please Enter the Password::



================================================================================
Enter Password Hint
-------------------

Enter a hint for the Password.

Password Hint (Valeur par d?faut : ): name_card
```

Information about the RCCMD web connection.

```
RCCMD configuration necessary
-----------------------------

It is necessary to configure RCCMD. Please use the web interface at
"https://172.20.50.166:8443".

Should you decide to run RCCMD with this default configuration RCCMD will
accept messages from any ip-address!
Please set one or more valid ip-addresses that are allowed to send (shutdown-)
messages to this RCCMD.

PRESS <ENTER> TO CONTINUE:
```

RCCMD asks if you want to start it now or later.

```
Start RCCMD now?
----------------

It is recommended to start RCCMD from WebIf after all necessary configuration.
If you want to start it manually, use "/usr/rccmd/rccmdctl start"

Do you want to start RCCMD now?

  ->1- Yes
    2- No

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE
   DEFAULT:
```

The installation is finished; press Enter to exit the installation menu.

```
Installation Complete
---------------------

Congratulations. RCCMD has been successfully installed to:

   /usr/rccmd

PRESS <ENTER> TO EXIT THE INSTALLER:
```

4. Installing the RCCMD appliance with ESXi 6.5

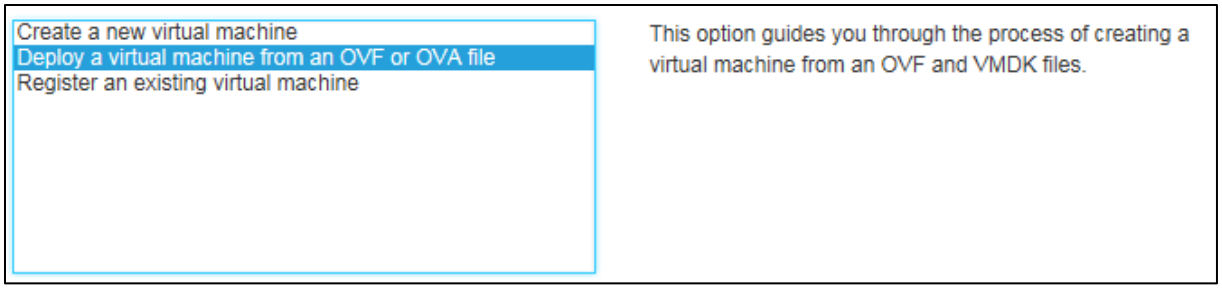
4.1. OVF/OVA deployment

Open your VMware ESXi – Host and login as root:

After successfully logging in create a new VM - For ESXi 6.5 you will find the corresponding tab in the upper bar:

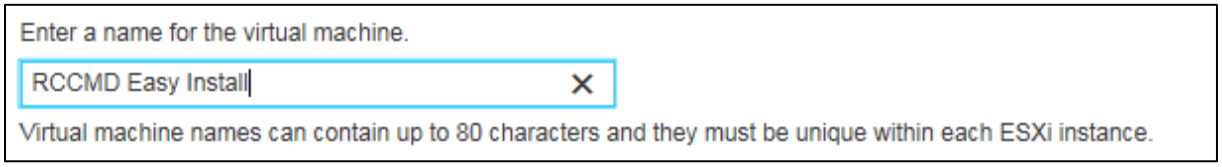
Then select the following option:

Deploy a virtual machine from an OVF or OVA file:

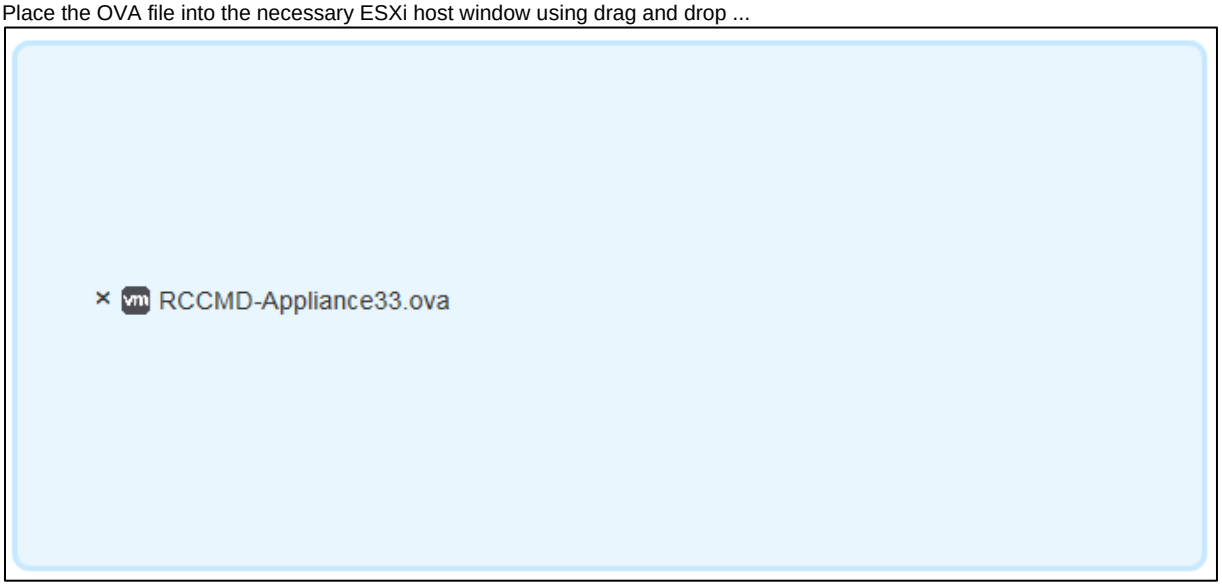


Click next to proceed to the next configuration dialogue:

Give your new RCCMD machine a unique name:

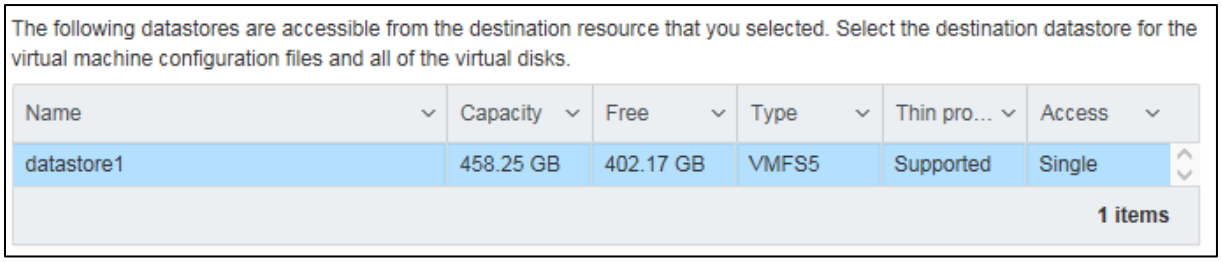


Place the OVA file into the necessary ESXi host window using drag and drop ...



… and click Next:

The OVA file is preconfigured, there is no need to do any additional settings:



Due to this fact, just click on next:

The RCCMD client will be managed by an according RCCMD server device. Therefore, this server device must be able to reach your RCCMD client over local network structures.
In general, you can accept the preconfigured settings.

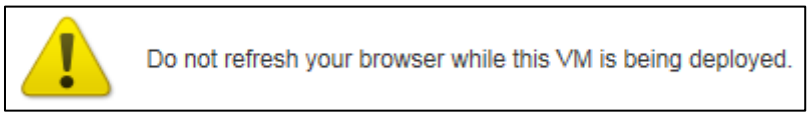
The same works for provisioning of the hard disk space. The RCCMD OVF file is preconfigured for best use unless your hardware platform differs from standard installation routines.

Once you have made the settings as you like, click *Next* to go to the next step:

This is the final step:
Please review all settings before clicking Finish:

Product	RCCMD-Appliance
VM Name	RCCMD Easy Install
Disks	RCCMD-Appliance33-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	bridged: VM Network
Guest OS Name	Unknown

Obey the special notification carefully to prevent damaging RCCMD during installation routine is running.

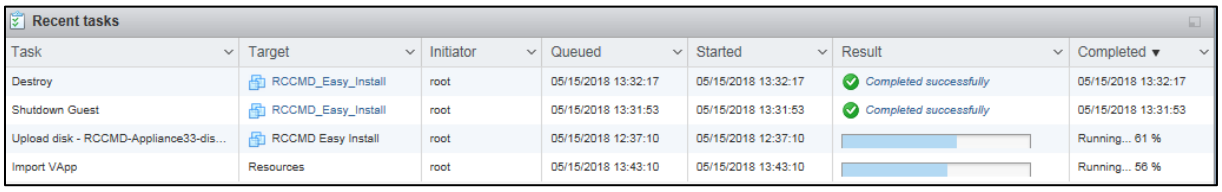


VMWare responds sensitive to browser updates during installation process. If the browser will be refreshed before installation is finished, the process will be aborted, rendering the virtual machine unusable.

Click finish to start the installation process:

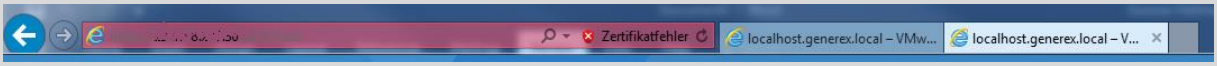
The automatic installation

Results and Completed shows the current installation state and proper success.



Obey the Daleks:
The administrator will wait for the installation to complete before updating this browser window.

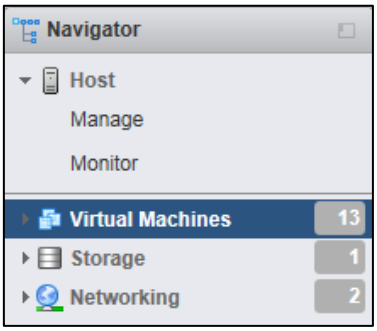
Note:



Use tabbed browsing to keep working. VMware will automatically detect the current session. By doing so, administrators will be allowed to continue working on the system while waiting for a finished RCCMD installation.

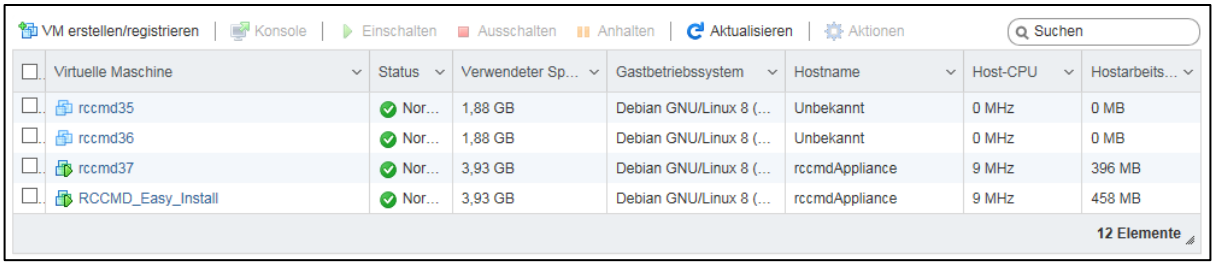
The Installation progress

On the left side you want to find a tool called navigator. The navigator displays an overview of all virtual machines installed on the system.
This installation example is called



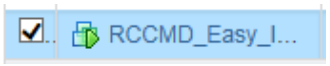
RCCMD_Easy_Install

Search for virtual machine including the RCCMD appliance.
Clicking on it will open advanced system information about the virtual machine.

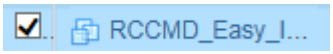


4.2. VM configuration (Network)

Ensure the virtual machine is running. Take a look at the list of all virtual machines and search for the RCCMD Appliance

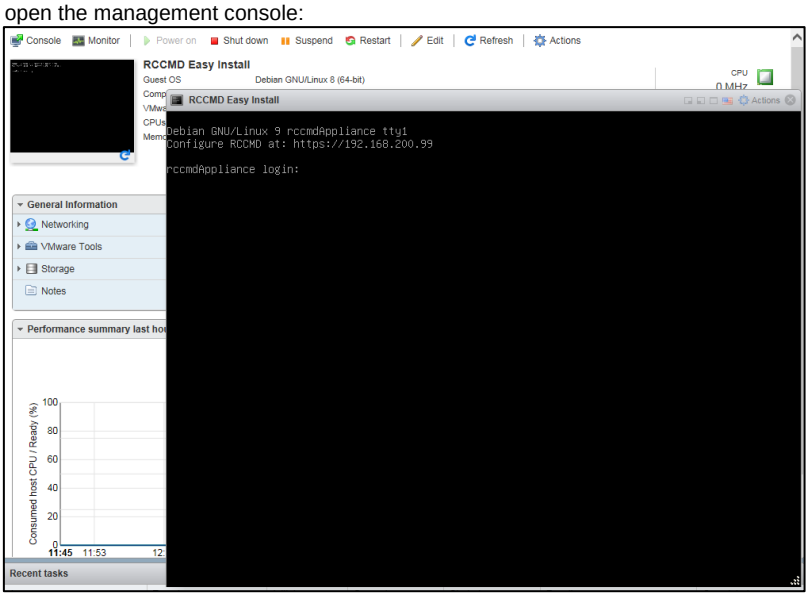


The virtual machine is running

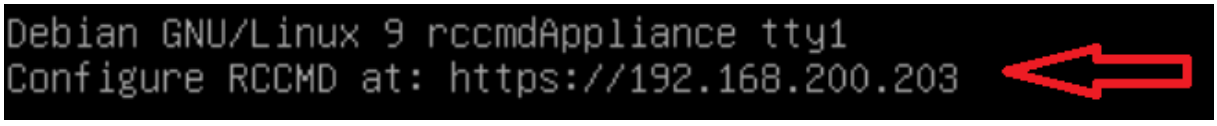


The virtual machine is off

Click on "Console" to open the management console:



If your network provides a DHCP server,
RCCMD will automatically display the current IP address.



If there is no valid IP address by DHCP, it is necessary to manually assign an IP address. In the appendix, you will find information about the procedure

Post installation console login

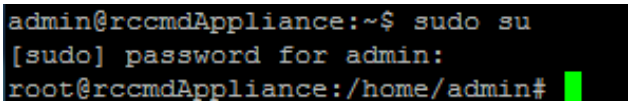
You can log on to the RCCMD appliance directly from the web console:

User: admin

Password: RCCMD

Gaining root privileges

The VMware Appliance is based on a Linux Debian 9 - The root privileges allow the manual re-installation of official packages as well as advanced configuration of the network interfaces.



command: sudo su

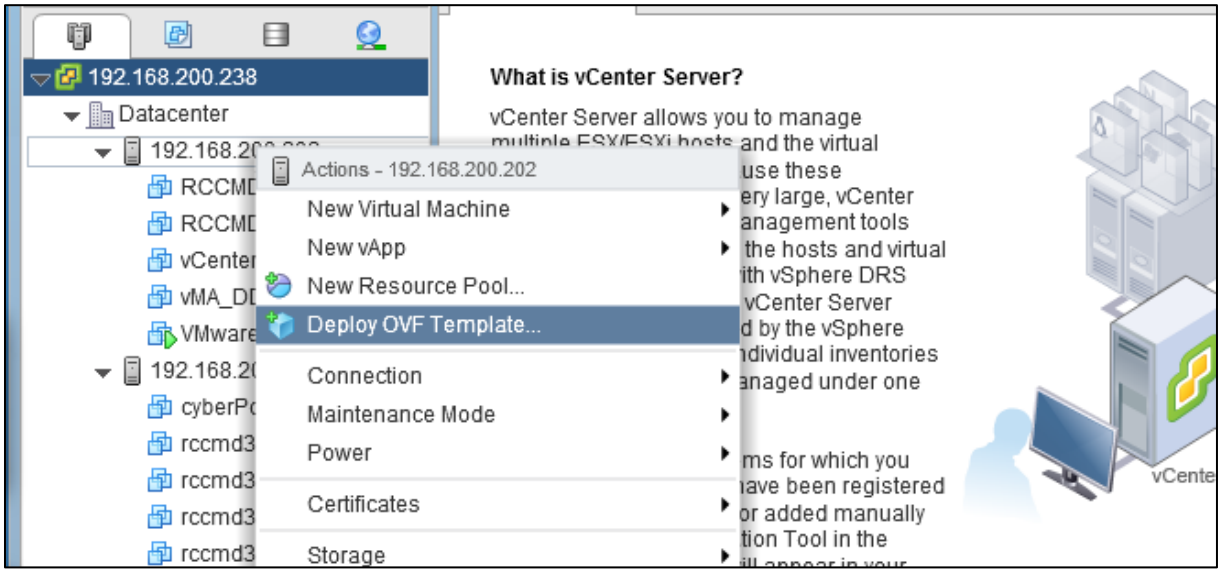
by default settings, admin has not been granted system privileges to make changes - you need to assign increased system privileges by using the Linux command sudo su.

The installation of the RCCMD appliance is now complete. For further configuration, refer the web interface. A configuration guide for assigning an IP address manually can be found in the appendix to this manual.

5. Installaling the RCCMD appliance with vCenter

5.1. OVF/OVA deployment

At VCenter context menu, start the RCCMD installation routine by choosing *Deploy OVF Template ...:*



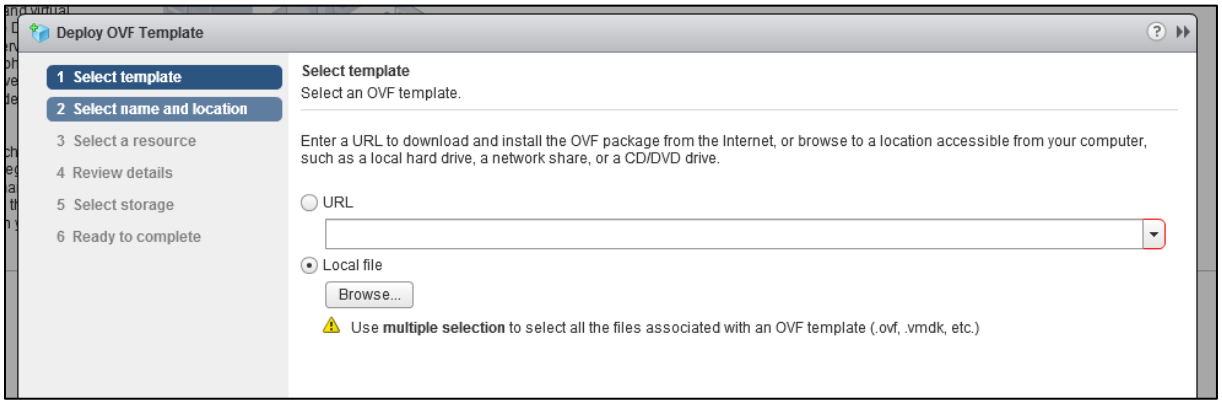
First, select the necessary file. vCenter provides two options:

URL:

If the OVF file is provided by web resources, specify the appropriate path.

Local File

If you have saved the OVF file as a local file, select the file directly.

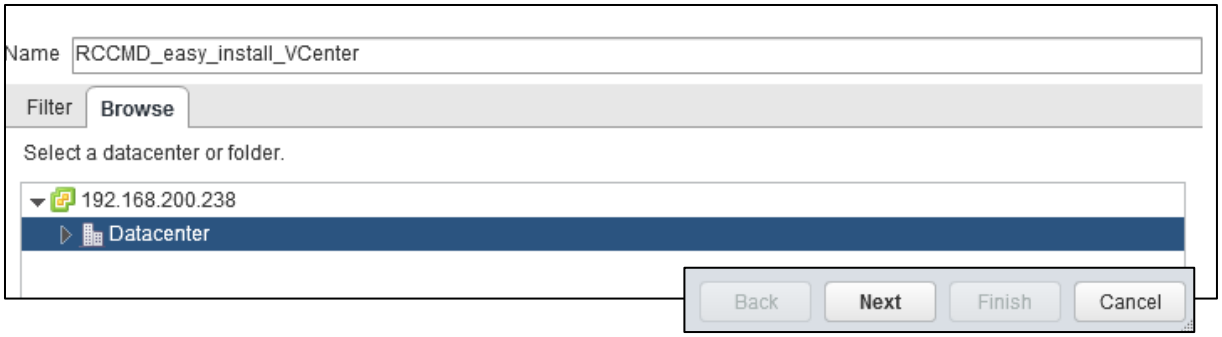


In this example installation, the local file will be used to install the RCCMD Appliance:

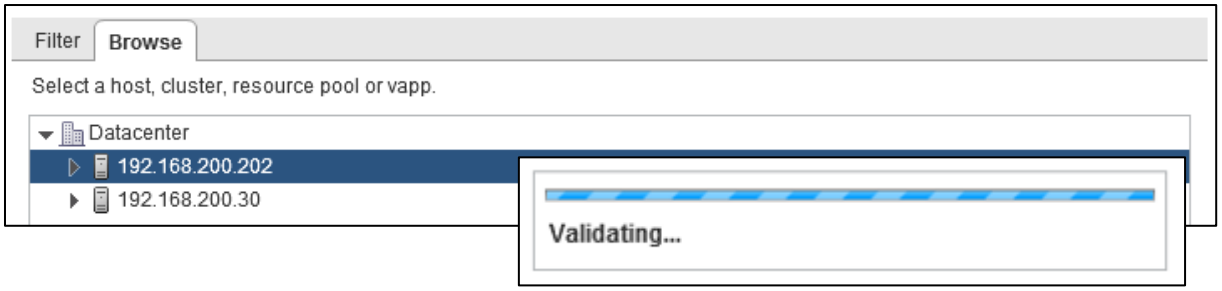
After selecting the local file, press Next to proceed to the next installation step:

The next step asks you to name the virtual machine VM a uniquely. This name is needed in the later configuration steps of RCCMD.

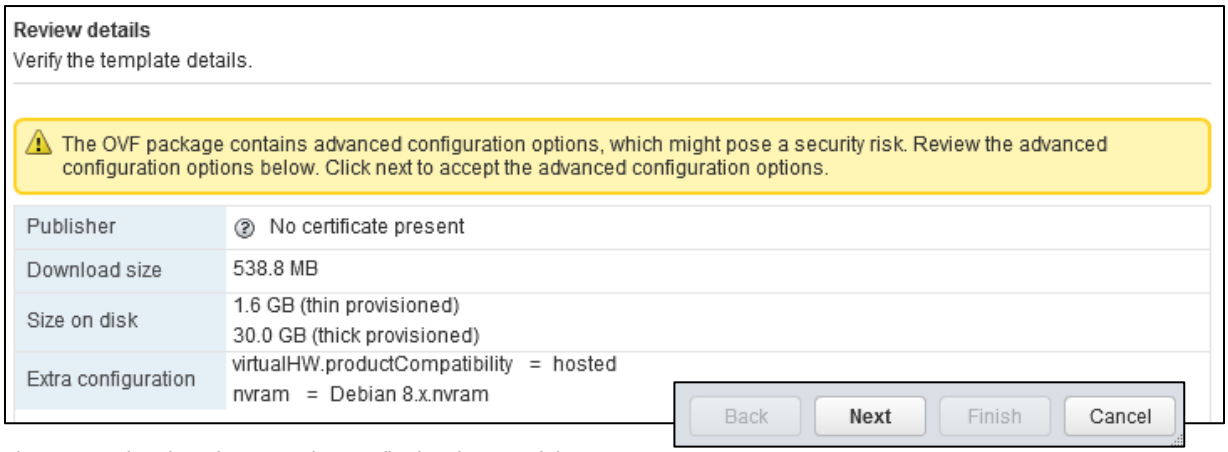
Click Next to proceed to next configuration step.



vCenter needs to know the destination host to set up and install the virtual machine

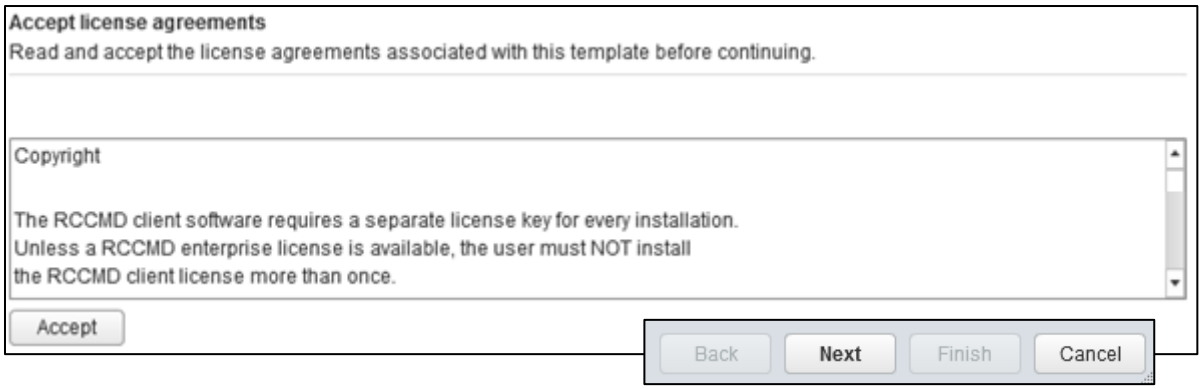


vCenter will provide a general overview of the settings according to the virtual machine. Press Next to continue.



Please note that there is no way but confirming the copyright terms...

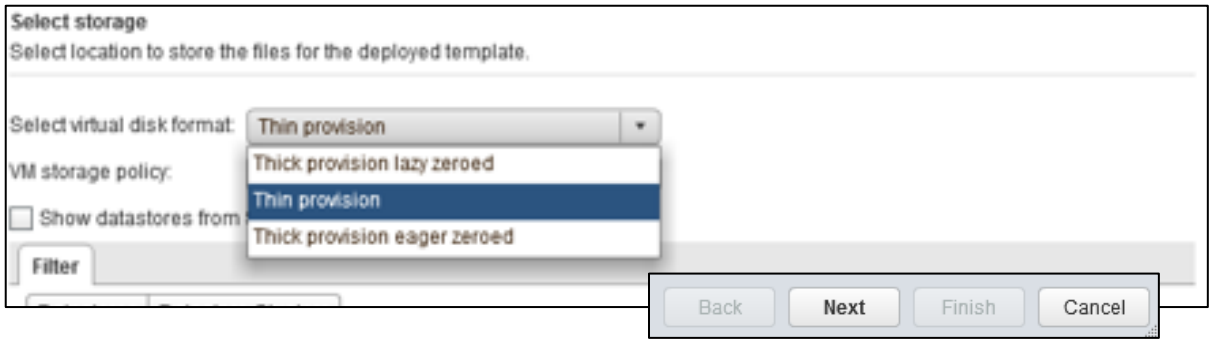
Please press Accept before proceeding the installation - the Next button will not work unless this has been happened.



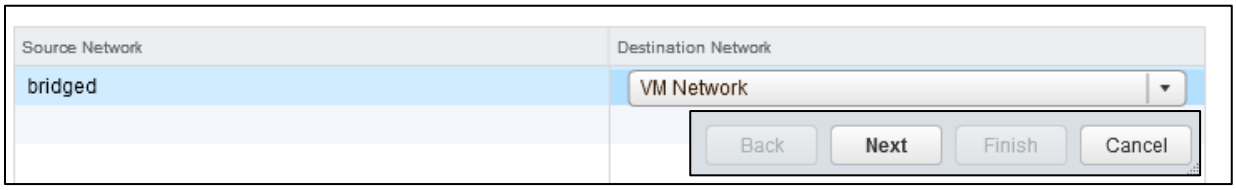
Disk usage may vary depending on the configuration of your system:

Please refer to local system administrators to get the correct setting.

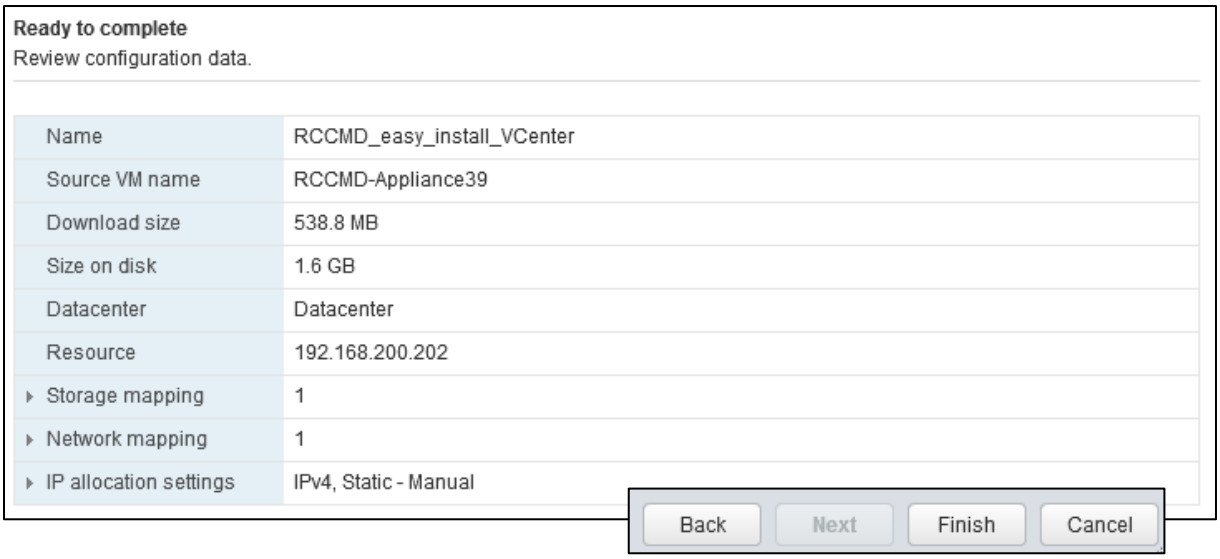
If you are unsure, select Thin provision and as VM storage policy none.



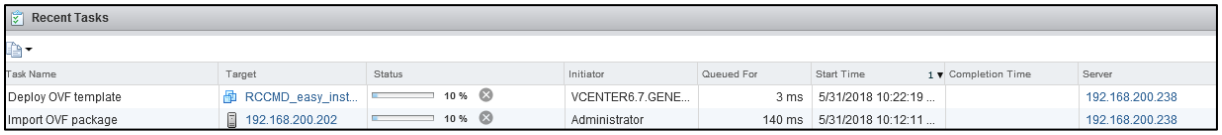
The appliance needs access to the network. Again, please refer your local system administrator...If you are unsure, first select VM Network in bridged mode. In this installation example, we use VM Network to correctly connect the VM to the network.



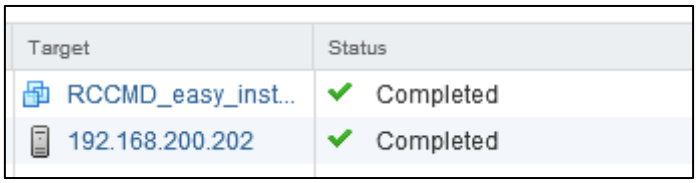
Take some time to review your settings: you will be shown an overview of your configuration. If the settings are to your liking, proceed by clicking *Finish*. This button will quit the configuration dialog and triggers the RCCMD appliance automatic installation routine.



Under Recent Tasks, you can track the current installation progress:

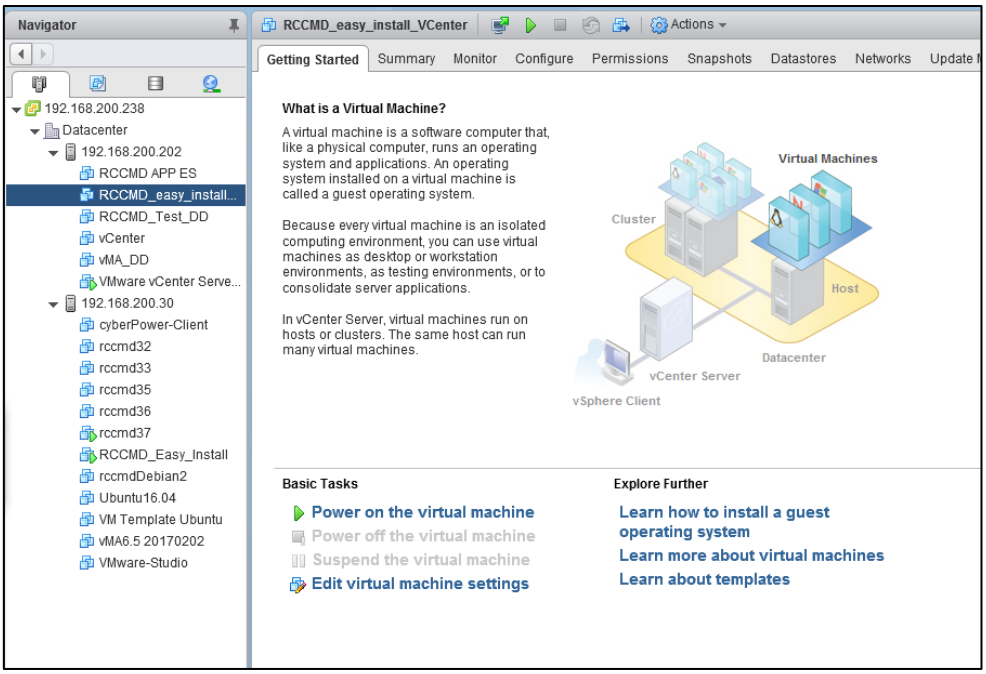


Please wait until the complete installation process is done and the status is set to *Completed*:

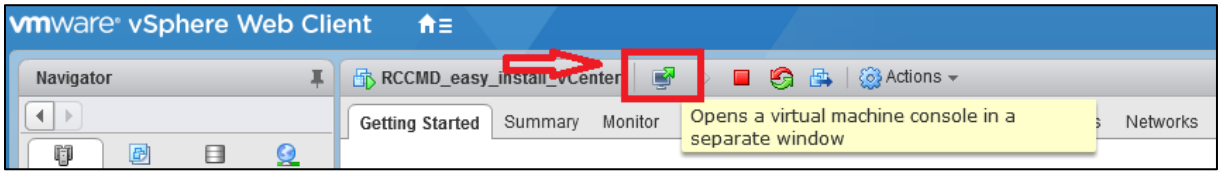


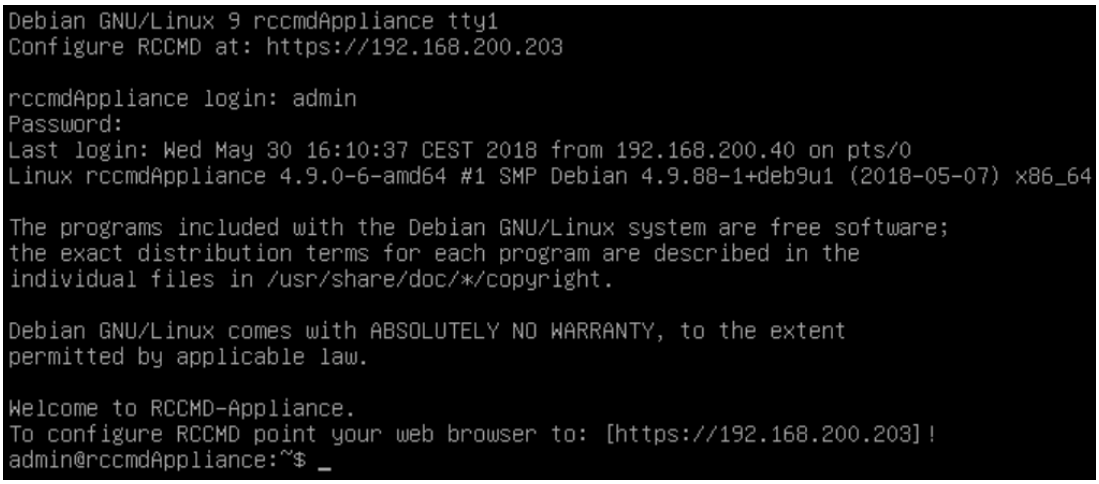
5.2. VM configuration (network)

At navigator, search for the corresponding virtual machine and power it up.

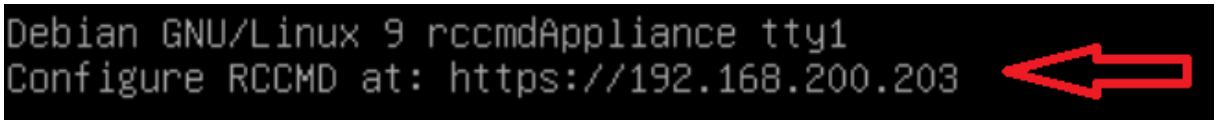


After the VM boots successfully, you can access the console directly from the vCenter console menu:





As a default, the appliance will ask for a valid IP address. If your network provides a DHCP server, RCCMD will automatically display the current IP address.



If there is no valid IP address by DHCP, it is necessary to manually assign an IP address. in the appendix, you will find information about the procedure

Post installation console login

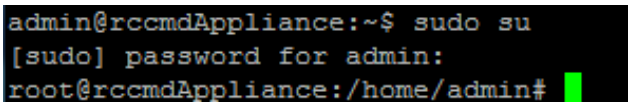
You can log on to the RCCMD appliance directly from the web console:

User: admin

Password: RCCMD

Gaining root privileges

The VMware Appliance is based on a Linux Debian 9 - The root privileges allow the manual re-installation of official packages as well as advanced configuration of the network interfaces.



command: sudo su

by default settings, admin has not been granted system privileges to make changes - you need to assign increased system privileges by using the Linux command sudo su.

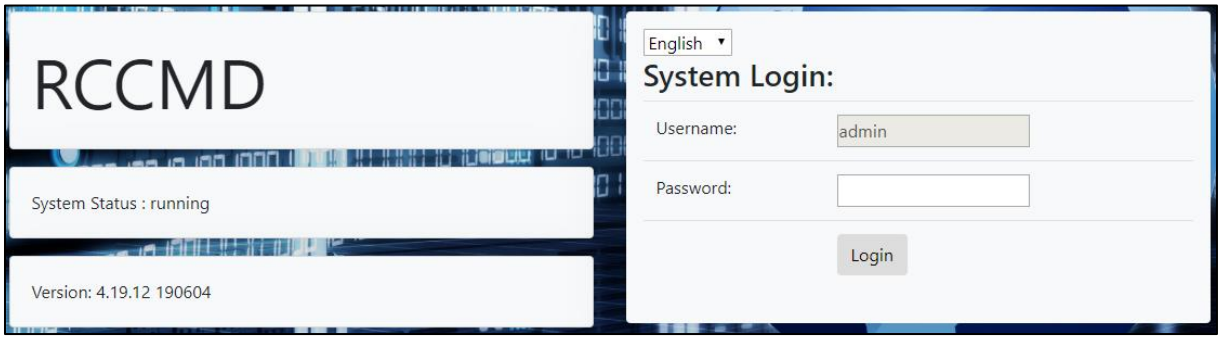
The installation of the RCCMD appliance is now complete. For further configuration, refer the web interface. A configuration guide for assigning an IP address manually can be found in the appendix to this manual.

6. RCCMD : interface web

6.1. Connection page

To access configuration screen of RCCMD, open a web browser and proceed to the IP address of you RCCMD installation:

https://<IP address of the RCCMD appliance >



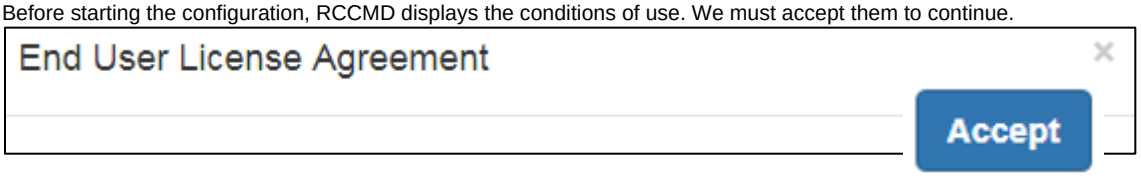
Use the default credentials to log in:

User: *admin*
Password: *RCCMD*

The home page shows the system status, the RCCMD version and the connection tab.

6.2. Licence key

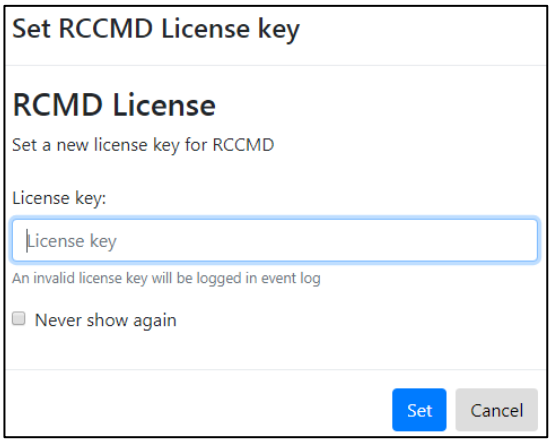
Before starting the configuration, RCCMD displays the conditions of use. We must accept them to continue.



You can read the terms of use and click on the Accept button.
Then RCCMD will ask you to enter a valid license key:

The key used by the RCCMD facility will work with the conditions:

1. One key = One RCCMD installation



In general, a key is used for a RCCMD client. If a key is accidentally assigned twice, the first RCCMD client will request a license. The following RCCMD clients that start will recognize a claimed license and display a corresponding log entry:

2018-05-30 09:17:51 rccmd[00490]: License fraud from IP address 192.168.200.144 detected. Functionality will deteriorate.

Please note that the demo key is a unique key that will be used for any installation:

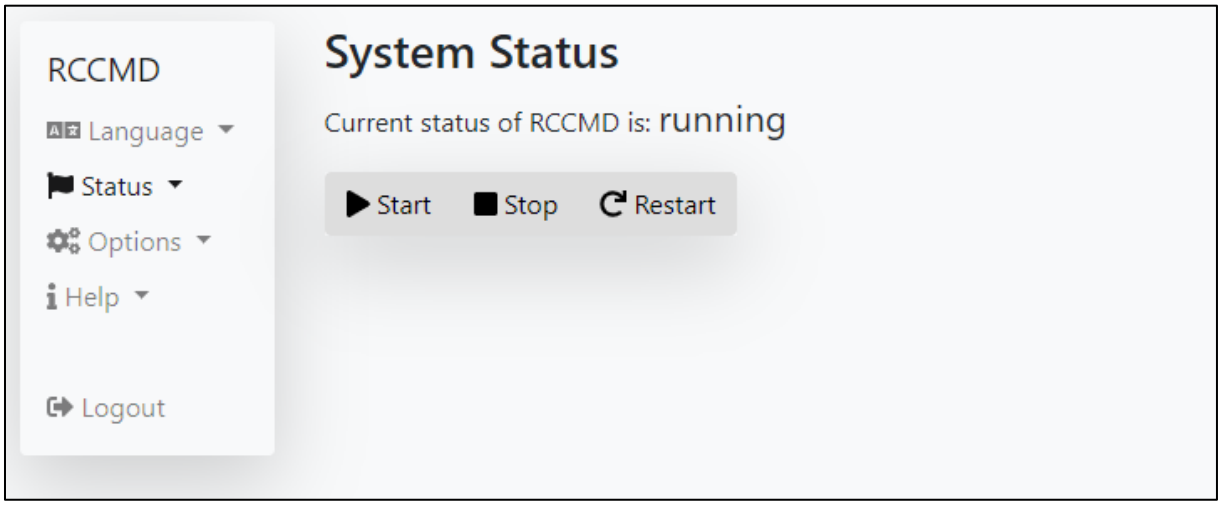
You may not use more than one trial version of the RCCMD in your network.

2. If there is no valid key present, RCCMD will be running in trial version

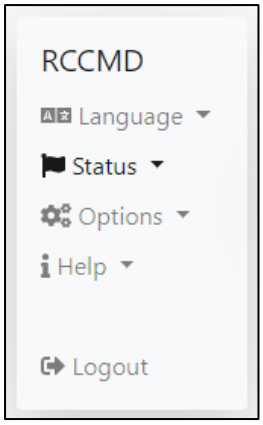
If you do not have the key or want to test the product, do not enter a key. As such, RCCMD will understand that this is a trial version and will use a built-in 30-day evaluation key. It is possible to change the key at any time (Options → Advanced Settings → RCCMD License).

6.3. Interface

After Login, RCCMD will show the configuration dialog:



On the left side, you will main categories. On click they will unfold and show sub menus:



➔ ***Language selection***

➔ ***Main system status and log files***

➔ ***RCCMD configuration dialog***

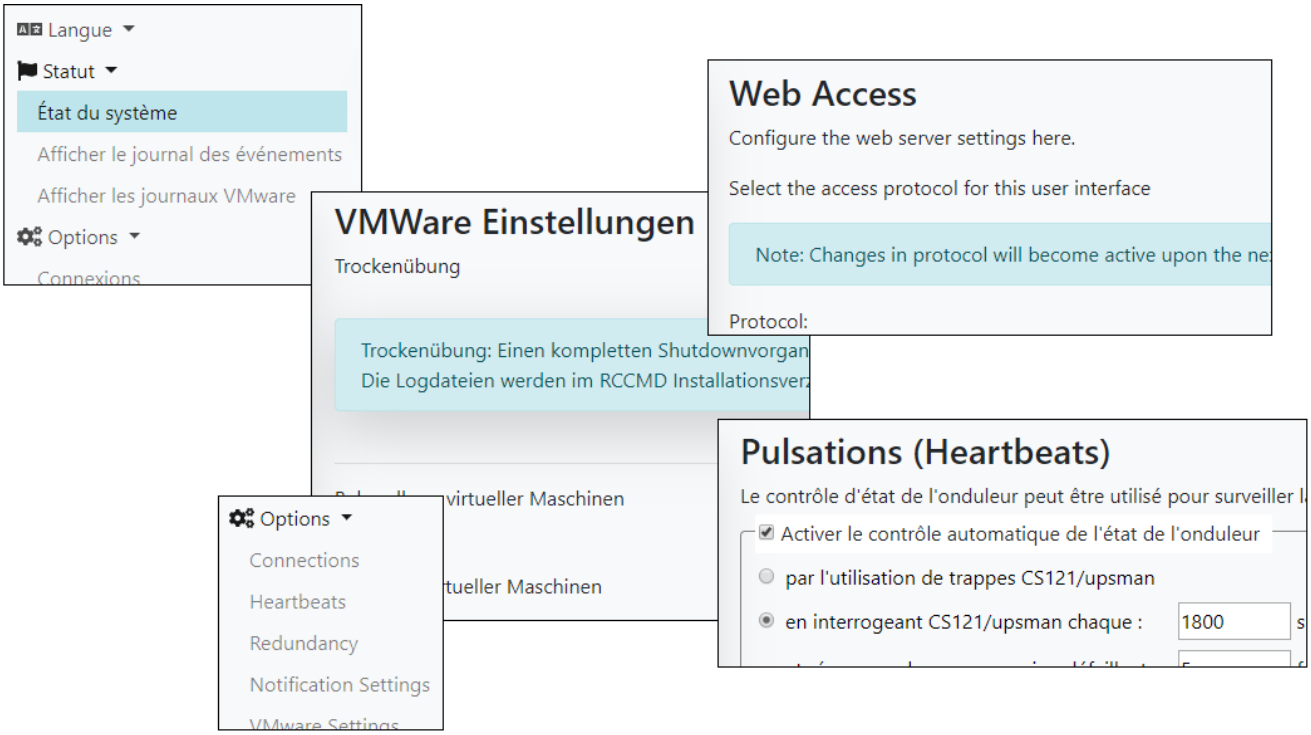
➔ ***Help topics, maunals and links***

➔ ***Logout and return to the login mask***

6.3.1. Languages

To select the desired language, go to the "Language" menu

RCCMD is available in German, English and French.



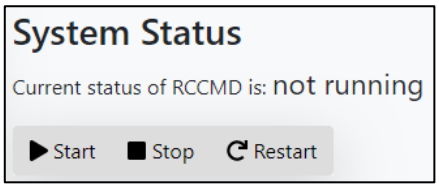
6.3.2. System status

Menu: Status → System Status

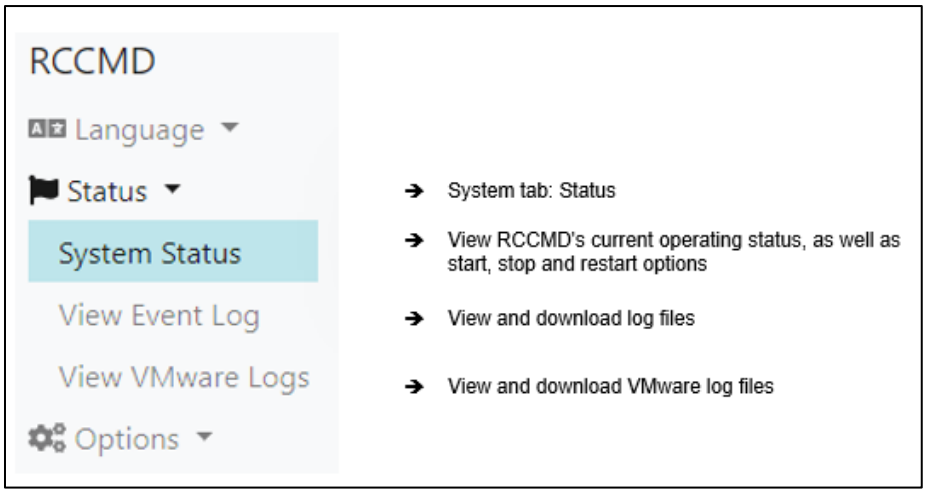
Click on system status and restart.

The following message informs us about the status and current configuration of RCCMD

not running	RCCMD is off
running	RCCMD is on



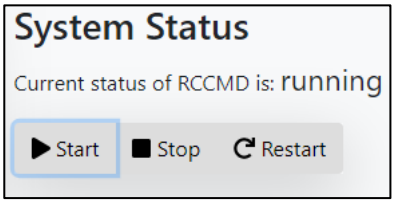
The following menu contains general information about RCCMD status as well as log files:



The system status page provides immediate information on the status and configuration of RCCMD.

The following buttons cause the following actions:

Start	On RCCMD When Off
Stop	Off RCCMD when turned on
Restart	Off RCCMD then turn it back on



6.3.3. Event logs

2019-06-13	13:41:12	rccmd[09099]: system: Operation now in progress
2019-06-13	14:10:42	rccmd[09099]: Trying to start program/job: /usr/rccmd/rccmd_notalive.sh 192.168.2.1 06/13/2019 14:10:42
2019-06-13	14:10:42	rccmd[09099]: error: check upsman failed, could not connect to 192.168.2.1
2019-06-13	14:10:42	rccmd[09099]: system: Operation now in progress
2019-06-13	14:10:57	rccmd[09099]: Trying to start program/job: /usr/rccmd/rccmd_notalive.sh 192.168.2.2 06/13/2019 14:10:57
2019-06-13	14:10:57	rccmd[09099]: error: check upsman failed, could not connect to 192.168.2.2
2019-06-13	14:10:57	rccmd[09099]: system: Operation now in progress
2019-06-13	14:11:12	rccmd[09099]: Trying to start program/job: /usr/rccmd/rccmd_notalive.sh 192.168.2.3 06/13/2019 14:11:12
2019-06-13	14:11:12	rccmd[09099]: error: check upsman failed, could not connect to 192.168.2.3

RCCMD event logs are for the RCCMD service:

- Notifications
- System event
- Actions
- Execution of scripts

The RCCMD logs have additional information:

- Event date
- Time the event occurred
- The IP address of the machine concerned
- Success / failure of the execution of an action

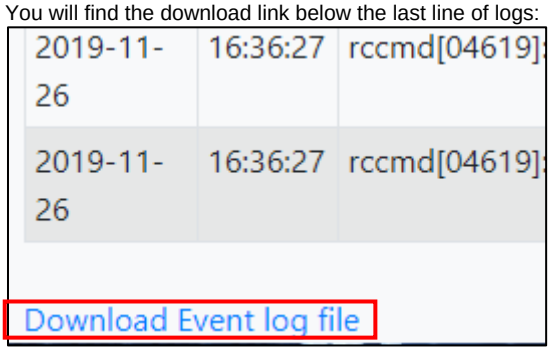
It is possible to know:

- When the server has been shut down
- Why he was
- That it was the speed of the system to react to the incident.

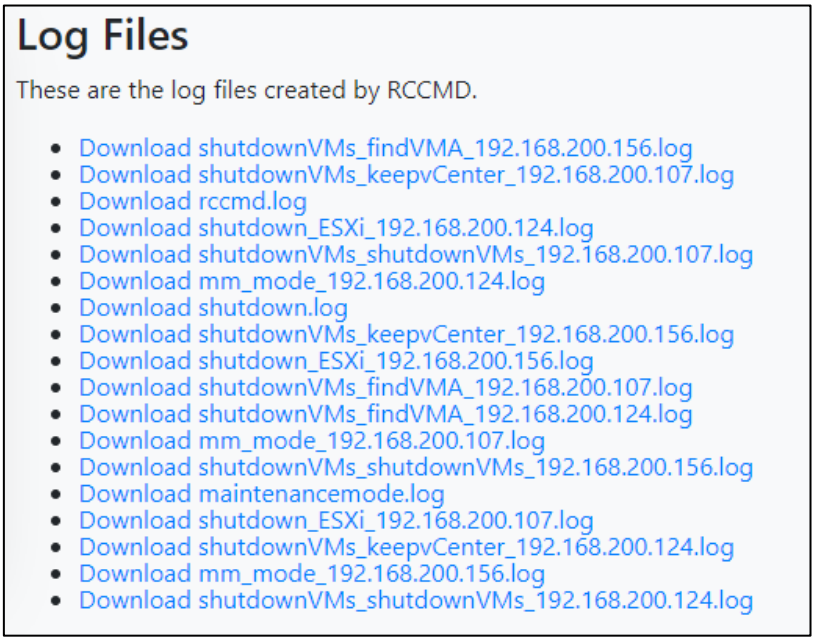
Event logs help to solve complex problems and predict future problems.

Download an event log

You will find the download link below the last line of logs:



6.3.4. VMware logs



The RCCMD appliance provides additional event logs for incident resolution.

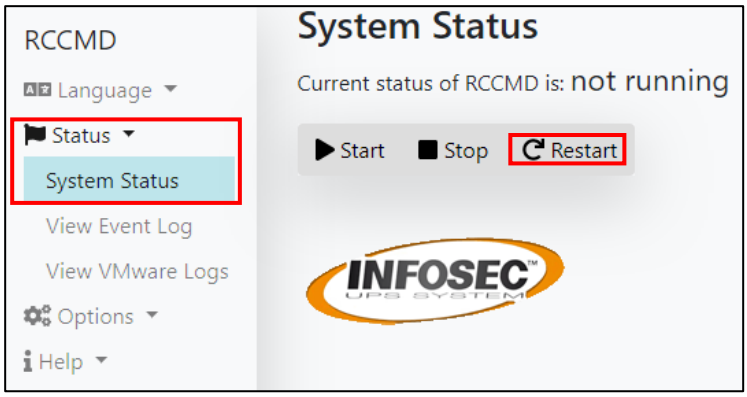
The RCCMD logs show the following information:

- ✓ Date
- ✓ Time
- ✓ Signals received
- ✓ Pending communication
- ✓ Running scripts
- ✓ Test results

7. RCCMD configuration

After a configuration change, it is necessary to restart the services:

If the services are not restarted, the data is saved but it is not transferred to the active configuration.



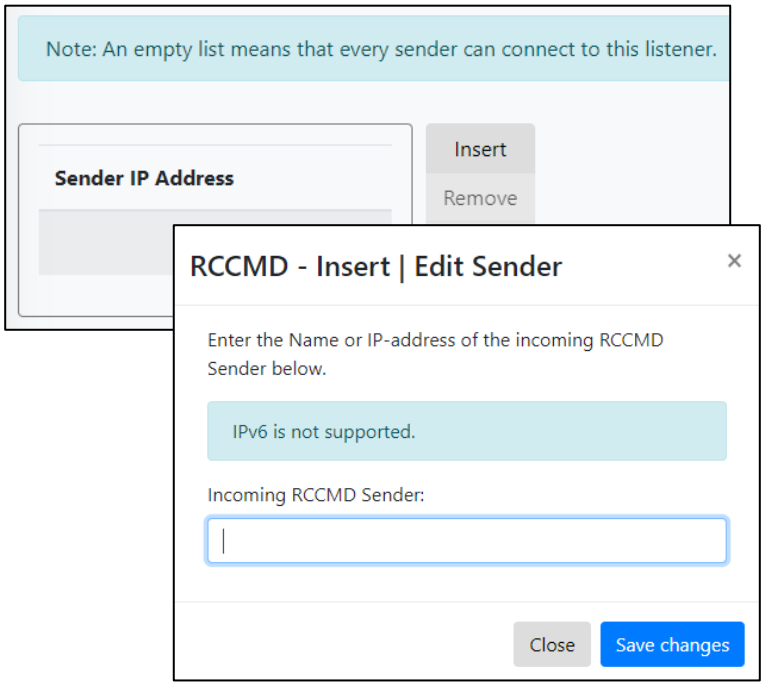
Menu: Open Options click on Connections

Protection against accidental server shutdown

Currently, each RCCMD transmitter can trigger a shutdown that cannot be taken back. The RCCMD client therefore offers you to limit these commands to specific stations.

Under Options, click on *Connections* to open the corresponding dialog. With *Insert* you can add a new IP address:

Enter the IP address expressly entitled to send an RCCMD shutdown command.



7.1. Connections

How long does a server stop take?

Basic stop

After entering all the data, it is possible to estimate the time required for a complete shutdown.

You can see this below the ESX host options (VMware Settings).

Total estimated Shutdown time for the System with current configuration: 00:01:30.

Note:

Each UPS can only provide backup power. When the batteries are discharged, the inverter stops itself to prevent damage to the batteries.

Moreover, these values are just a snapshot of your system based on the data you have entered! Check regularly whether the values entered correspond to the actual stopping state in case of emergency.

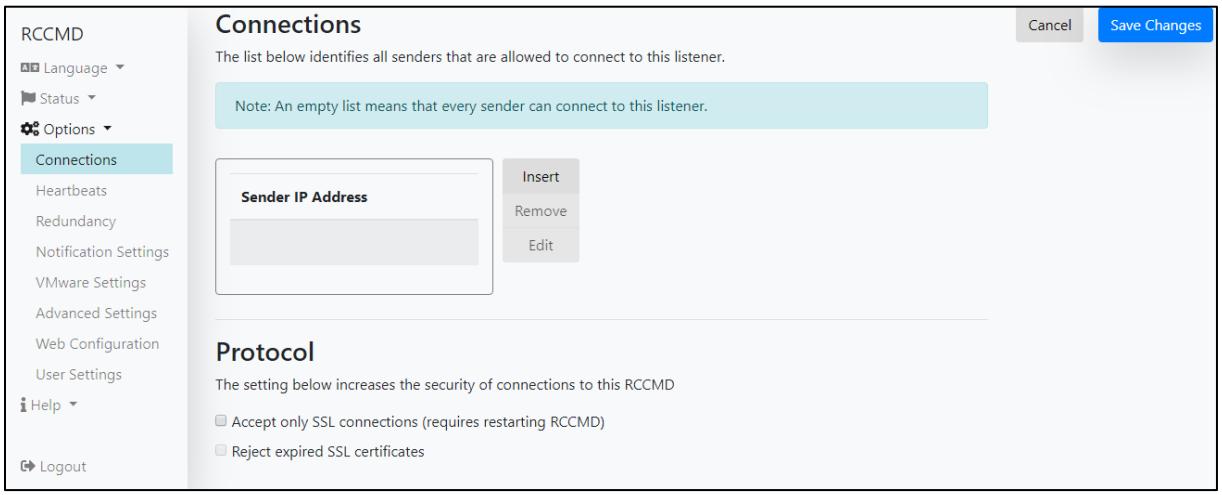
Remember that between two stop trials, conditions may change. When calculating and adjusting the average downtime, it is recommended to take a little longer than the minimum required time.

Define inbound connections allowed

If you leave this field blank, any incoming RCCMD stop signals can trigger a shutdown.

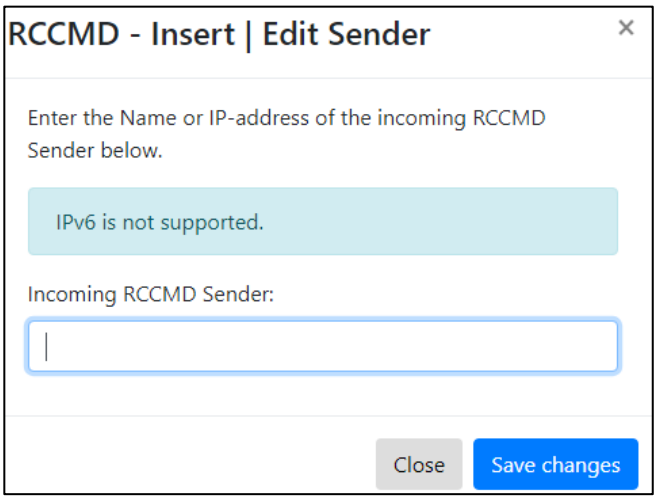
This is not recommended and should be changed. By entering an IP address from the sender, you limit the devices that are allowed to send a stop command to that RCCMD client.

RCCMD commands from unauthorized devices are seen by RCCMD, but their execution will be blocked.



Connection configuration
Insert and edit

Add: Add an IP address.



Save the changes when you add the IP address. Close the configuration page and repeat the operation for all authorized RCCMD stations.

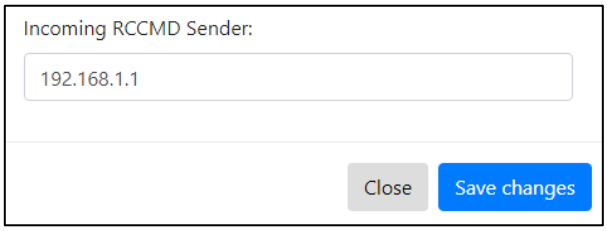
If there are changes to be made in the configuration, this can be changed:

Select an IP address and click on "Edit". A configuration page is displayed, so you can change the initial configuration. Save the changes to finish.

It is possible to set either the IP address of the sender or his host name.

This is more difficult with the host name:

You need a DNS server for the translation between the IP address and the name of the host. If the DNS server is no longer functional, or the communication with the server is faulty, RCCMD will not be able to contact the hosts and manage the shutdown commands.



RCCMD is functional with hostnames but in view of the problems that may occur it is strongly advised to use IP addresses.

RCCMD will still wait for an incoming signal! You must configure a RCCMD transmitter as the CS141 Web Manager:

When handling UPS events, select the "Shutdown" task, you can choose between the IP address or host name of the RCCMD client.

When managing critical resources, it is recommended to minimize interference as much as possible.

For example, if you need a server that can resolve hostnames to IP addresses, communication between the client and the sender will stop working as soon as the server becomes unavailable.

Therefore, it is recommended to use a manual IP address so that all devices in a network segment can communicate with each other without an additional server.

Note

If you configure the CS141 and want to see if the tasks you have configured are correctly received by RCCMD, you can use connections to create an incoming log. As long as the sender is not explicitly included in "Connections", RCCMD logs the execution but refuses to execute it.

However, at least one IP address must be entered to enable this filter function.

Preparing for UPS redundancy
Some settings depend on each other. If multiple UPSs are running simultaneously to secure the server infrastructure, it may be necessary to specify more than one UPS to trigger a shutdown command.

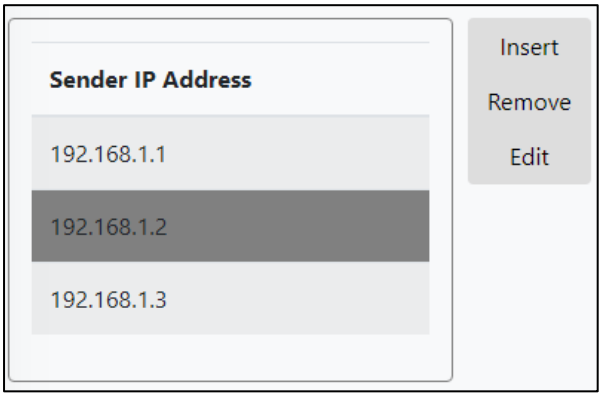
If you enter two or more valid IP addresses for a valid RCCMD signal, the "Redundancy" menu is automatically enabled and can be used.

RCCMD can be configured to handle valid RCCMD stop signals from different sources. For more details, see the "Redundancy" menu.

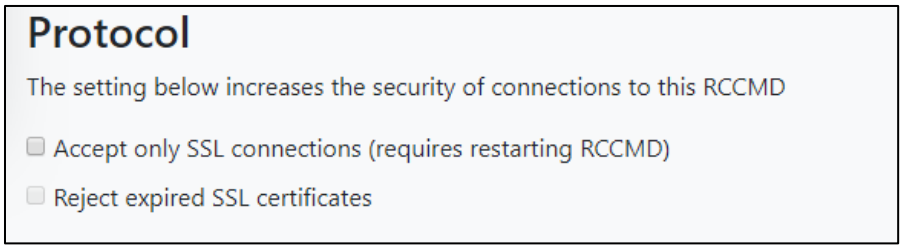
How to delete an IP address

Click on the desired IP address and click on "Remove".

Do not forget to click on "Save".



Increase the security of connections



This part adds security to your network, but it increases management and administration time.

You can ask RCCMD to accept encrypted communications (SSL) with a valid certificate.
If a sender does not have an SSL certificate to authenticate, the connection is broken.

In addition to this function, you can ask RCCMD to verify that SSL certificates are up to date. If the certificate is expired, it is considered invalid and the connection is terminated accordingly.

Note

If you enter or edit data, the data will be saved temporarily, but without any impact on the current configuration.
If your configuration is complete, you must write your local settings in the RCCMD configuration file.

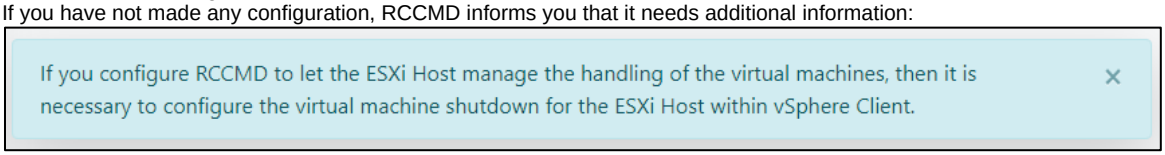
To activate the new configuration, RCCMD must be restarted. Just press the "Status" key followed by "Stop" and "Start" or "Restart". RCCMD will see the changes and will support the new configuration.

7.2. Shutdown control

7.2.1. ESXi

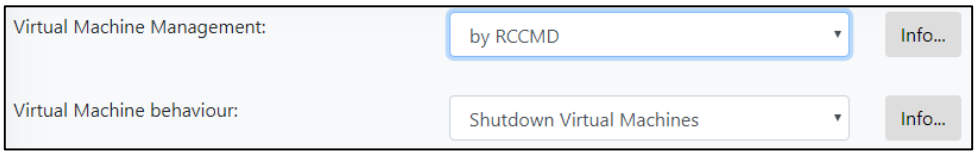
Menu: Options → Paramètres VMware

Go to "VMware Settings"
If you have not made any configuration, RCCMD informs you that it needs additional information:



Although RCCMD is installed as a virtual machine and is already ready for use, it can not yet perform its real function since the necessary access permissions have not yet been registered. Confirm this message with OK to open the VMware settings.

When using a single host, virtual machines can be powered down before the ESXi host itself shuts down.

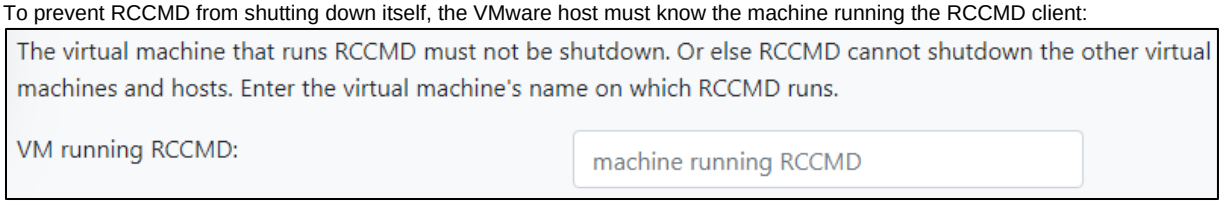


Note

The emergency stop causes the virtual machines to shut down and the host to shut down itself. The maintenance mode timeout defines how much time RCCMD gives vMotion before the host shutdown takes effect. The maintenance mode in the stopping behavior can therefore also be used to trigger a stop for different hosts, including a timer.

For "Virtual Machine Management" select "By RCCMD". And for the "Behavior of the virtual machine" select "Stop the machines".

To prevent RCCMD from shutting down itself, the VMware host must know the machine running the RCCMD client:

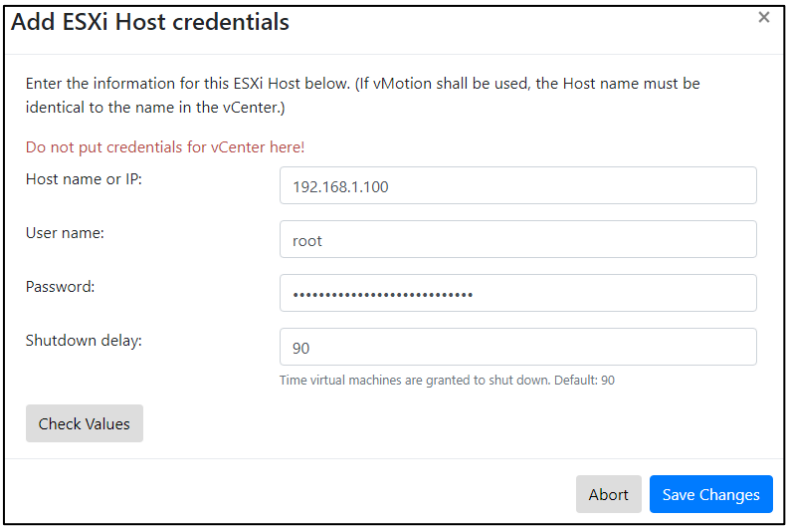


RCCMD requires the following information:

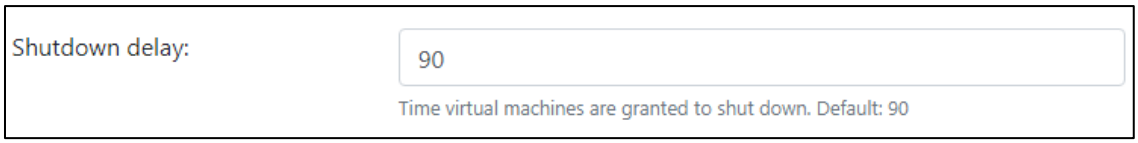
HOST / IP name
Normally, we recommend using the IP address of the RCCMD host here. You can, however, also enter the host name itself.

User
A user with the appropriate system privileges to shut down the VMware environment accordingly.

Password
The password assigned to the user that allows RCCMD to authenticate itself as authorized.



The next step will determine how much time RCCMD should allow the virtual machines to quit before the ESXi host powers down:



Virtual machines take different amounts of time to shut down and shut down properly.

The exact time, how long a machine needs, is very individual and depends strongly on the task and the promised hardware. To prevent data loss or damage to the virtual machine, the host can be instructed to give the machines a proper time window to shut themselves down before shutting down itself.

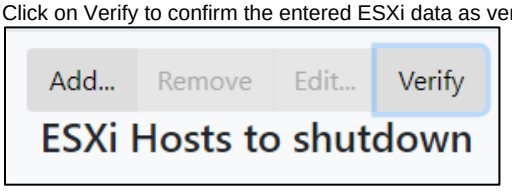
Shutdown delay indicates the time in seconds that the host waits before being turned off.

The Default setting is 90 seconds - virtual machines taking more will be turned off due to the fact the ESXi host powers down.

You can check the access data with Check Values:

If the test was successful, press Save Changes to exit the configuration dialog.

Click on Verify to confirm the entered ESXi data as verified server.



You will notice that at the bottom right the Save Changes has changed color:

You have made a change that requires RCCMD to be restarted to permanently save the inputs and apply them to the active configuration. This process is indicated by the green button.

7.2.2. vCenter

Menu: Options → Paramètres VMware

The vCenter differs with its operating modes from a standalone host. While the Standalone Host works on its own and shuts down virtual machines as needed, vCenter provides the so-called vMotion: The HA - High Availability - of vMotion allows virtual machines to be moved from one host to another before the host is intentionally powered down.

Please note:

Before you can use the RCCMD appliance with vMotion, the Distributed Resources Scheduler DRS must be configured to use the fully automatic mode.

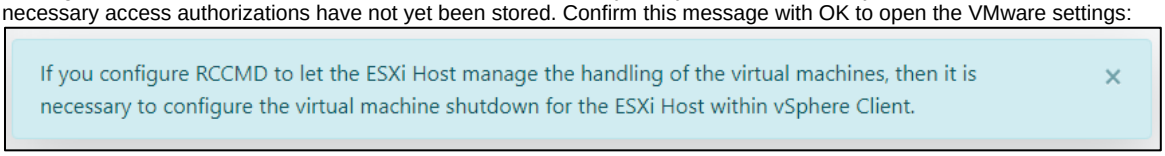
Note

Before using RCCMD in conjunction with vMotion, ensure to verify that each virtual machine running on the host has been tested working with the maintenance mode. If maintenance mode fails, non-migrated virtual machines will be switched off when the host is powering down.

Open VMware Settings:

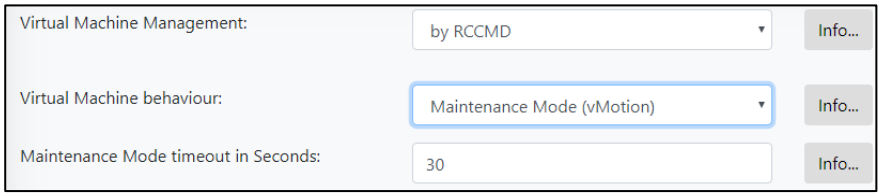
If you have not yet made any settings, RCCMD will inform you that RCCMD needs additional information:

Although RCCMD is installed as a virtual machine and is already ready for use, it cannot yet fulfill its actual function since the necessary access authorizations have not yet been stored. Confirm this message with OK to open the VMware settings:



When using a vCenter, virtual machines can from one host to another. Virtual machines will continue to work seamlessly. Please note the different data:

Under Virtual Machine Behavior, select Maintenance Mode (vMotion).

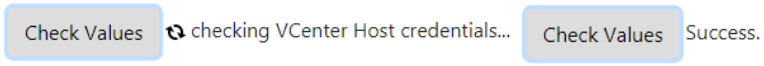


The Maintenance Mode time out in Seconds defines the time vCenter is given to move a virtual machine to another host. The behavior of vMotion is configured within the high availability (HA) within the vCenter. As soon as time is up, the standard shutdown procedure will be initiated:

remaining virtual machines will shut down due to the fact the host powers down.

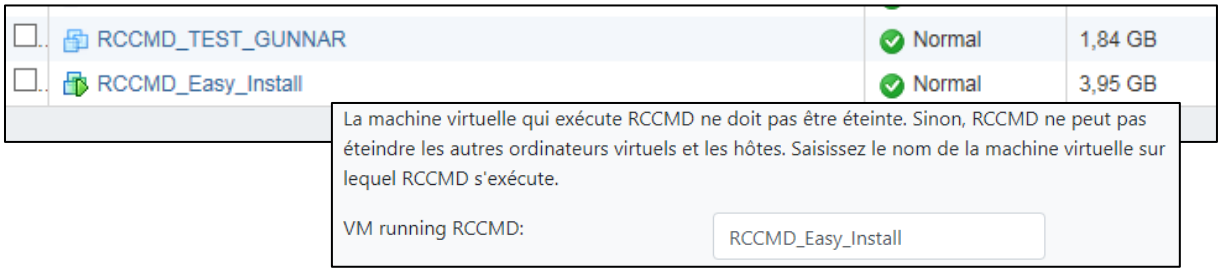
Unlike the standalone host, RCCMD requires user data with the corresponding authorizations of the vCenter:

Use Check Values validate the credentials of the vCenter - Check values will display whether the vCenter is reached and the access data has been entered correctly:



If RCCMD cannot reach the vCenter correctly, it will show a corresponding error message.

To prevent RCCMD from shutting itself down, the VMware host must know what the machine running the RCCMD Client itself is:

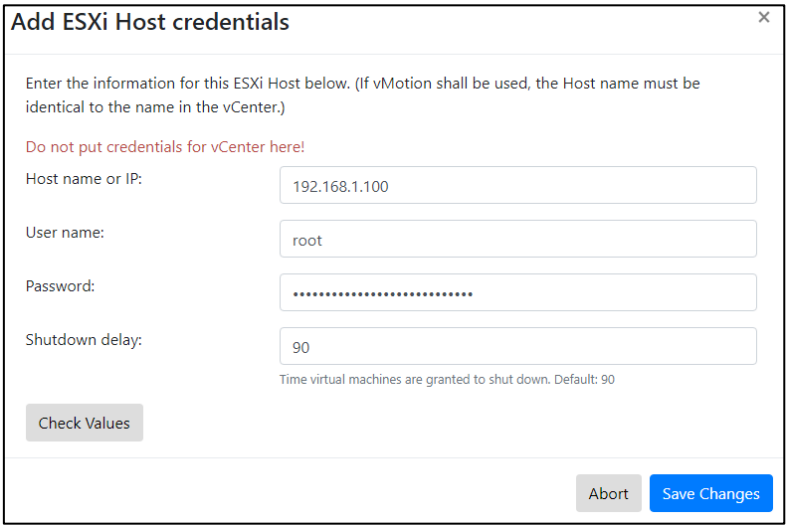


RCCMD requires the following information:

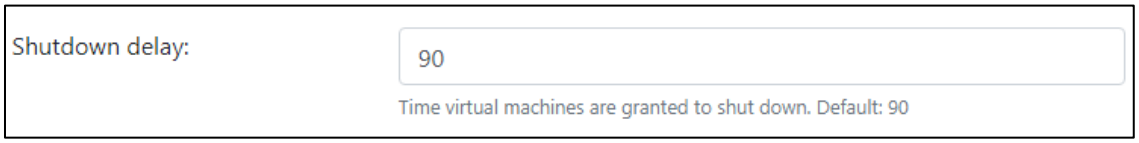
HOST / IP name
Normally, we recommend using the IP address of the RCCMD host here. You can, however, also enter the host name itself.

User
A user with the appropriate system privileges to shut down the VMware environment accordingly.

Password
The password assigned to the user that allows RCCMD to authenticate itself as authorized.



The next step will determine how much time RCCMD should allow the virtual machines to quit before the ESXi host powers down:



Virtual machines take different amounts of time to shut down and shut down properly.

The exact time, how long a machine needs, is very individual and depends strongly on the task and the promised hardware. To prevent data loss or damage to the virtual machine, the host can be instructed to give the machines a proper time window to shut themselves down before shutting down itself.

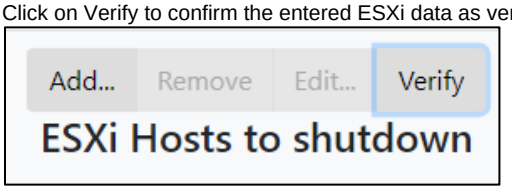
Shutdown delay indicates the time in seconds that the host waits before being turned off.

The Default setting is 90 seconds - virtual machines taking more will be turned off due to the fact the ESXi host powers down.

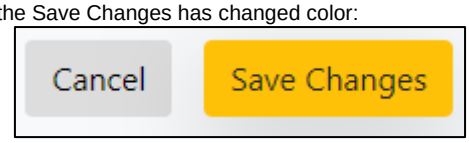
You can check the access data with Check Values:

If the test was successful, press Save Changes to exit the configuration dialog.

Click on Verify to confirm the entered ESXi data as verified server.



You will notice that at the bottom right the Save Changes has changed color:



You have made a change that requires RCCMD to be restarted to permanently save the inputs and apply them to the active configuration. This process is indicated by the green button.

7.2.3. vSAN

Before starting, please read the following configuration notes carefully to prevent shutdown issues caused by a wrong configuration of RCCMD.

RCCMD can handle vSAN VMware environments. Due to the fact, a vSAN is very complex and the operating conditions of a vSAN differs when compared with a single host or a standard cluster, there are some pre-conditions that must met before RCCMD can shut down a vSAN:

The RCCMD client that handles the vSAN cannot be installed inside a vSAN

Due to the fact, each host of a vSAN must be set to in maintenance mode before the can be switched off. As long as one virtual machine is running, it is not possible to switch off the hosts.

The vCenter that handles the vSAN is the first virtual machine that starts and the last virtual machine that shuts down.

The vCenter is the control unit of a vSAN. It is allowed to install the vCenter inside the vSAN as well as running it on a single host that is not part of the cluster. The essential function of the vCenter is managing the all data synchronization inside a vSAN after all other virtual machines are down. You need to ensure that the vCenter can complete this operation.

If you run a Witness-Server as a virtual machine inside a vSAN

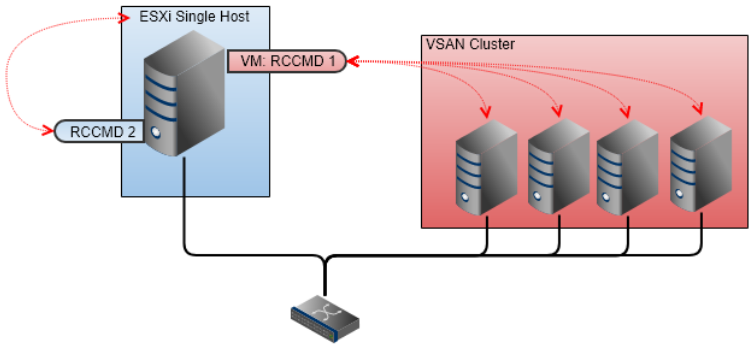
The Witness Server has a special task If two hosts do not match which host holds the most recent data, they ask the witness server. The witness server acts like a complete host, but cannot maintain virtual machines.

Due to this fact, the witness server can also be virtualized in the vSAN and still acts as a stand-alone host. In that case, you need to differ between the Witness server's IP address and the host's virtual machine where the witness server's virtual machine is located:

The witness server is shut down regularly within the vSAN cluster.

The host that maintains the virtual machine that contains a witness server, needs a second RCCMD client for enabling the maintenance mode after the witness server is switched off.

Technically, an RCCMD client can only handle the vSAN or the host it runs on



As a consequence, if you have single hosts AND a VSAN cluster, you will need at least 2 RCCMD clients: RCCMD 1 manages the shutdown of the VSAN cluster and RCCMD 2 manages the shutdown of the single host. The shutdown routine is then divided into 2 different commands for the CS141:

- o Shutdown the VSAN cluster
- o Shutdown of the single host

Since the two RCCMD clients run side by side:

When choosing the correct time window for shutdown tasks, ensure the VSAN has turned off all hosts completely before turning off the last remaining single host - otherwise the RCCMD client that manages the shutdown of the VSAN may not be able to complete the shutdown routine because the second RCCMD client performs a local virtual machine shutdown.

Note

Appliance vs Appliance - What is the Virtual Machine and what is "the RCCMD client"

Basically, the two appliances do not differ from each other: Both are virtual machines. However, because you use two appliances, the name of the virtual machine they run themselves on, will differ. Entering the name of the virtual machine will prevent that an RCCMD client will shut down itself first. So, if you tell RCCMD 2 the name of his own virtual machine, it will consider that RCCMD 1 is just another "guest VM" and will shut down it. When using a vSAN, the shutdown commands of the CS141 will harmonize the shutdown behavior of both appliances.

if you use a vSAN, take care for the time windows required by the modified shutdown sequence

The reason for using a vSAN is to combine a maximum data redundancy with a most possible availability of servers:
Basically, there is no reason for a regular vSAN cluster shut down.
A complete shutdown is an emergency issue, and should be handled accordingly:
It is difficult to predict how much time the vCenter will take within a vSAN to bring the hosts into maintenance mode.
In principle, the vSAN shutdown will be performed in three steps:

Shutdown of all virtual machines

In this step, all virtual machines will shut down.

Post synchronization phase

At this stage, all hosts synchronize their current datasets.

Switching into maintenance mode

All virtual machines are shut down and the datasets are up to date. The hosts can be switched off.

The critical system stage is the post synchronization phase. This process is difficult to assess:

The maintenance mode can only be assumed as soon as the synchronization of the data between all hosts has been completed. Unfortunately, this process is dynamic and the time needed to fulfill this process depends an the level of used hardware, the number of virtual machines as well as the amount and type of data that exists within the virtual machines.

To make it trickier, this process takes place within the VSAN without any information about the current data synchronization state - at some point, the hosts are in maintenance mode, which means that the process is complete.

However, available time is determined by the maximum operating time of the UPS:

RCCMD needs validated timer settings that not only use the calculated times for a shutdown but also respects the granted uptime of the UPS:

Ensure this time window …

allows to shut down the vSAN in good times.

contains some extra time if the post synchronization phase suddenly needs more time than expected

stays within the security range of the UPS's uptime,

ensures a shut down of other hosts and clusters, too.

System critical note:

Before you start to configure the shutdown of your vSAN, the following information are mandatory:

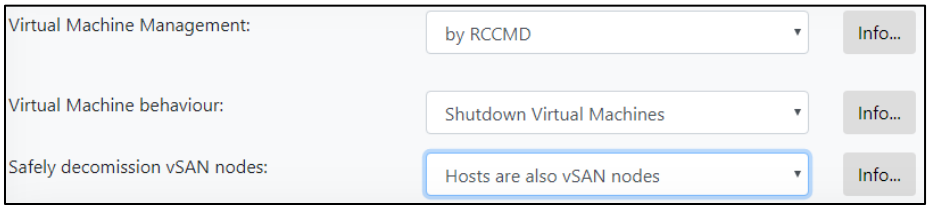
1. an overview of the time window that a UPS can grant for an orderly shutdown?
2. How long do you need for a manual shutdown?

Please note:

Due to the fact a vSAN is sensitive to shut down fails a vSAN is technically a very system critical process that needs your attention.

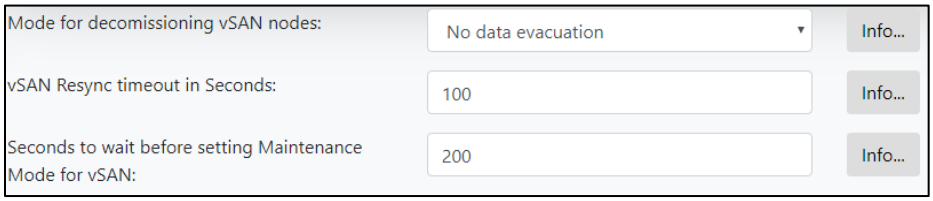
Preparing RCCMD for the vSAN

At vmware settings, enable "Hosts are also vSAN nodes"



To manage the shutdown routine, ensure that the RCCMD appliance must be located outside the VSAN cluster.

Once you have activated the vSAN mode, you will get additional menus:



Mode for decommissioning vSAN nodes

Leave the decommissioning mode on No data evacuation - this mode is the fastest method to shut down a vSAN cluster:
The virtual machines are shut down in a structured way and then all data will be synchronized on all affected hosts.

Definition of the vSAN Resync timeout

Unlike the default procedure, the vCenter becomes active after the virtual machine shut down and start synchronizing all records within the cluster.

This post synchronization phase defines the critical phase of the shutdown procedure:

All datasets from the virtual machines must be in sync with mirrored data stored on other hosts.
As long as this synchronous system state is not reached, the Maintenance mode cannot be taken by any host.

Note:

This process is very dynamic and depends on the type of data that needs to be synchronized. You may have created several new virtual machines and the synchronization time will only change marginally. However, it can also happen that you create a virtual machine and thus radically increase the post-sync time. In other scenarios, the data within the virtual machine may grow organically cause by the usage, which in turn affects the time required:

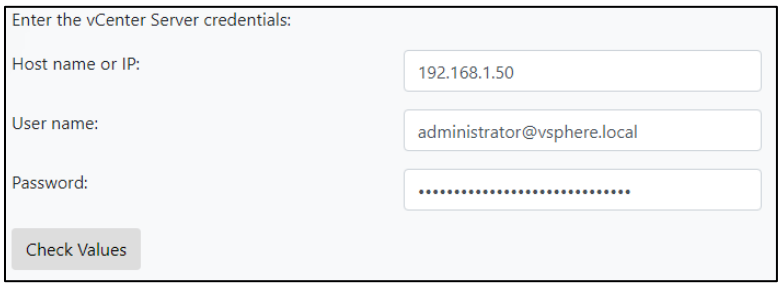
This value cannot be determined once during the first installation as a fixed value, it must be regularly checked for up-to-datedness and adjusted if necessary.

The vCenter takes all the time needed for this process. Unfortunately, this relative amount of time is in direct contrast to a clearly defined time window that can be provided by the UPS during an emergency power operation. You need to calculate a sufficiently large time window to give the vCenter a time reserve in case of the calculated period is insufficient.

Defining maintenance mode for the vCenter.

This setting defines how much time the vCenter has to shut itself down after synchronizing data. If the vCenter runs as a virtual machine within the vSAN, this point in time becomes interesting: After this time window, the hosts are put into maintenance mode and the vCenter is switched off by its host.

Enter data for the vSAN managing vCenter



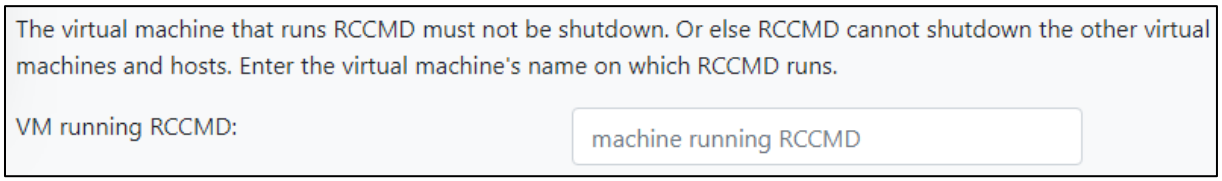
Since RCCMD must coordinate with the vCenter over the entire process, the access data for the vCenter, which manages the vSAN, is mandatory.

At this configuration dialog, do not enter credentials for individual host.

Define the vSAN managing RCCMD client:

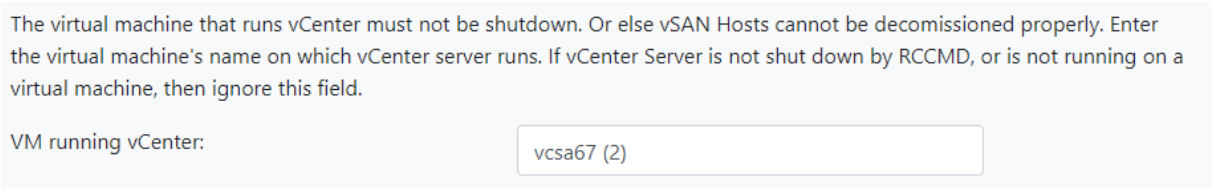
RCCMD has the task of shutting down all virtual machines and turning off the hosts at the end. Since within a vCenter not only a vSAN but further hosts can be mapped, RCCMD can shut them down, too. There are two exceptions that need more attention:

Information about the virtual machine running RCCMD



Although RCCMD itself cannot run in the vSAN that should be shut down, the vCenter that manages the vSAN may include additional hosts in its list. The RCCMD appliance is a virtual machine that must comply with the control commands of the host on which it is running itself - if the host advices a shutdown, the appliance will do it. To prevent RCCMD from inadvertently giving itself a shutdown command, enter the name of the virtual machine you chose for RCCMD. When entered, the virtual machine that holds this name will be excluded from the shutdown process.

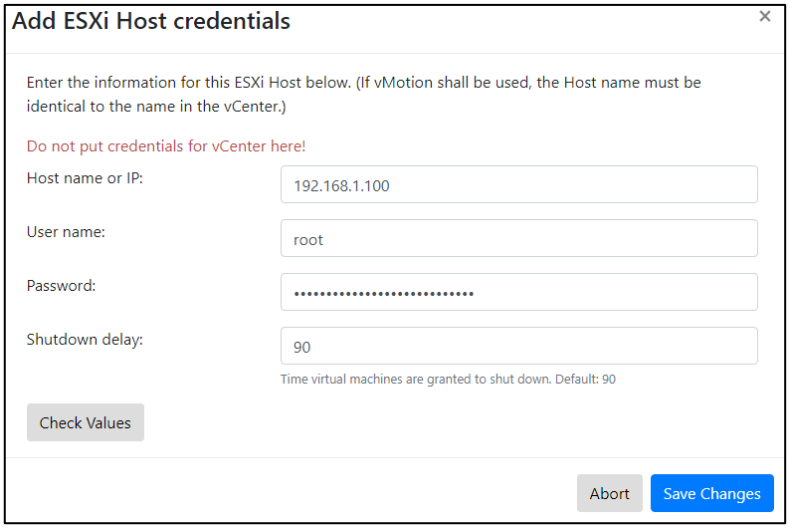
Define the virtual machine that contains the vSAN managing vCenter



Within the vSAN system, the vCenter performs special administrative tasks, but is also a virtual machine. During the shutdown, RCCMD first gets an overview of active virtual machines and then shuts them down, migrates them, etc. With this setting, RCCMD will know which of the virtual machines is the vCenter and will shut down it exclusively as the last machine in the vSAN shutdown procedure.

Definition of the vSAN ESXi host nodes

Define the hosts to be shut down by RCCMD. The virtual machines can be moved to other hosts via the vCenter. To shut down a host, RCCMD requires the following information:



HOST / IP name

We recommend using the IP address of the host at this point to avoid addressing problems when parts of the IT infrastructure are down.

Due to the fact RCCMD supports host names, you may enter a host name, too.

User

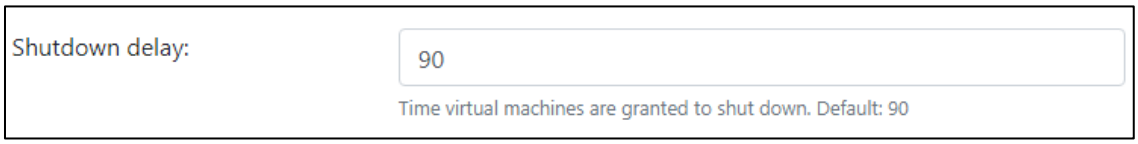
A user with the appropriate system rights to shut down the VM Ware environment accordingly. Normally, it is the local host administrator

Password

The password assigned to the user that allows RCCMD to authenticate itself as authorized.

Shutdown delay

The next step is to determine how much time RCCMD should allow the virtual machines to shut down before the before the ESXi host will quit all operation and switches off:



The vSAN has a special feature compared to other operating modes:

The shutdown duration typically defines the time window that a host grant the operating systems within virtual machines before the virtual machine is simply powered off. Thereby it does not matter if a vCenter has previously tried to migrate machines or not.

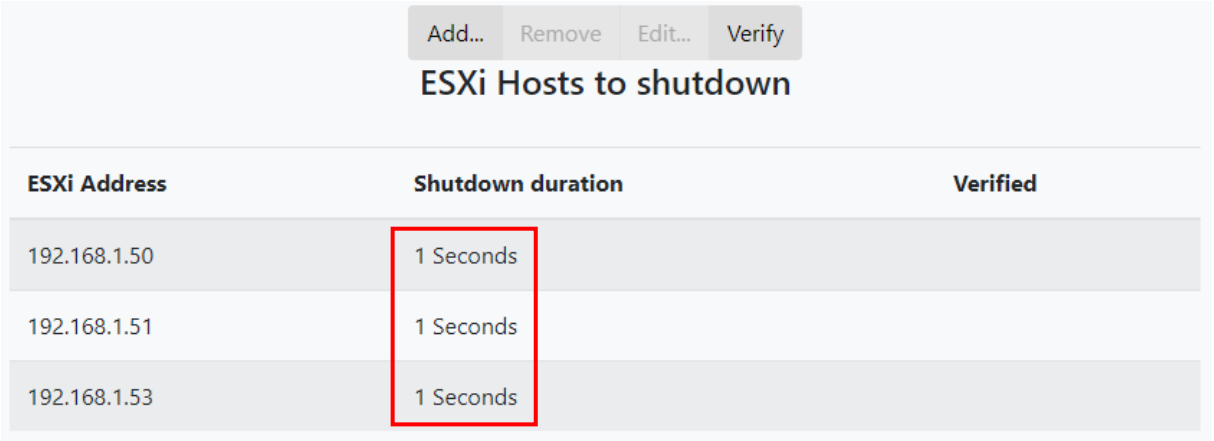
When this command is issued to the hosts running in a vSAN, there are no more virtual machines that need to be powered off:

- All hosts must be in maintenance mode

- A host can only be in maintenance if all virtual machines are moved or switched off.

For the hosts in vSAN, this means that the shutdown time of virtual machines can be set to 1 second:

The shutdown routine on a vSAN has already brought all hosts into maintenance mode. Consequently, no time window is required to grant operating systems within a virtual machine for a shut down.



Special role: The witness server

Small vSAN systems lack the necessary resources to be able to independently adjust all data stocks.

To prevent problems with data synchronization in minimalist vSAN systems, a witness server is used:

This witness server acts as a stand-alone host in vSAN, but is not responsible for hosting and managing virtual machines - as soon as hosts are unable to agree with the timeliness of their datasets, the witness server decides which host has to synchronize the data.

The witness server can be both, a real physical machine with it's own hardware as well as a acting like physical host but running within a virtual machine. The vSAN knots cannot see the difference between the different setup strategies of a witness server.

But this difference affects the RCCMD configuration:

If running a real witness server as a standalone machine:

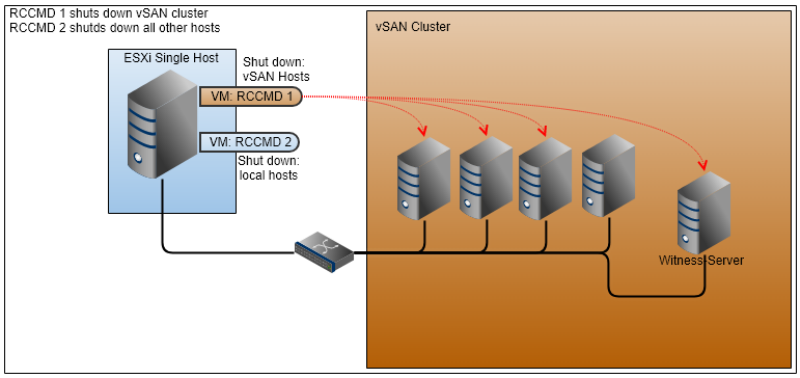
In this case, assign the witness server and any hosts that you want to shut down. The hosts will go into maintenance mode accordingly:

- Shut down virtual machines

- The vCenter will perform the reSynch

- The hosts switch into maintenance mode

- The hardware can be switched off.



When using a virtual machine to run a witness server

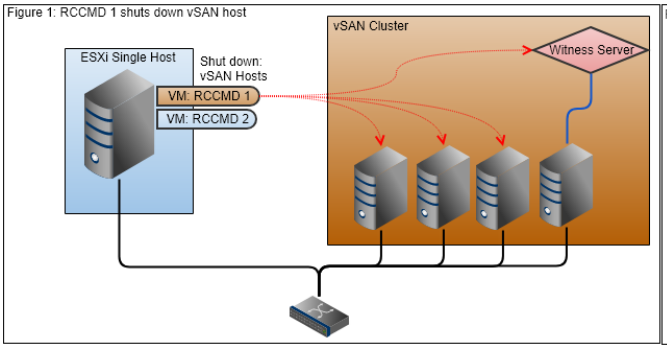
If you run the witness server as a virtual machine in the vSAN, you must differ between the host on which the witness server is stored and the witness server as a stand-alone host. Since the witness server acts like a host within the vSAN, it is perceived and treated accordingly - The installation type does not matter:

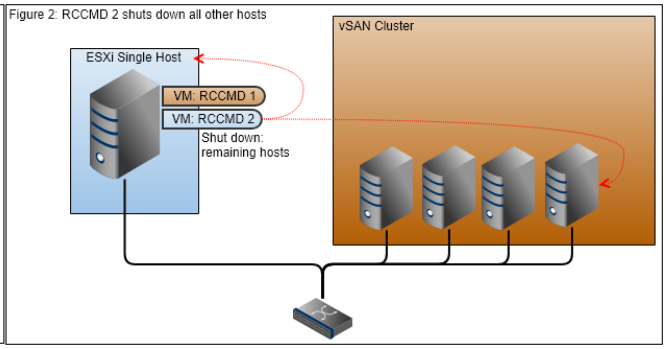
While the host that maintains the virtual machine of the witness internally perceives only one virtual machine running "some kind of system", it accepts the witness server as a standalone host and network node on the network. If the wrong IP address has now been specified, the host responsible for the virtual machine will respond correctly:

- The host will stop running the virtual machine

- The host changes to Maintenance Mode

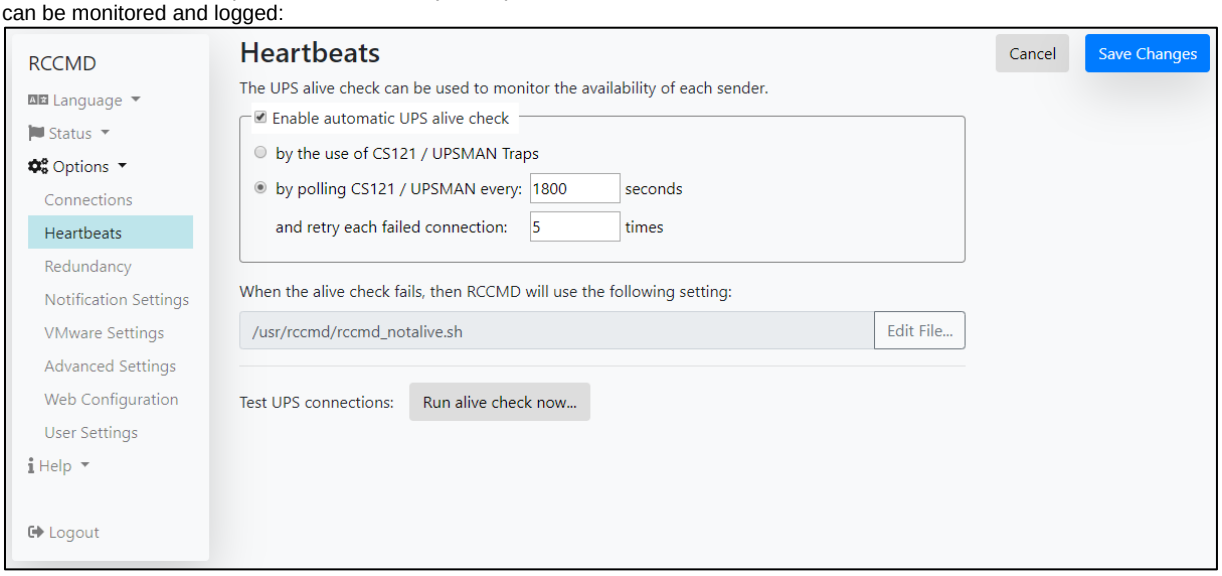
However, since the (albeit virtualized) witness server represents a full-fledged host and network node, it must consequently be treated as a real host and put into maintenance mode before being turned off. Formally, you need two RCCMD appliances to shut down a vSAN. If you use a virtualized witness server, you can use the second RCCMD to regularly switch off the host that manages the virtual witness server





7.3. Heartbeats

The heartbeats function provides an availability lookup. The communication between RCCMD client and the associated server can be monitored and logged:



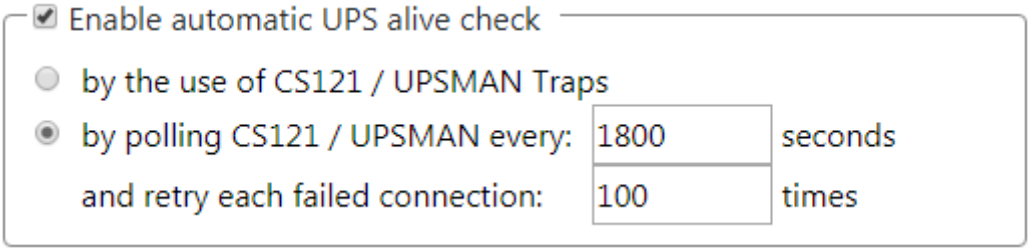
In principle, two basic sources of interference are checked:

1. The general network accessibility
2. The UPSMan service of the CS141

This test is not designed to run complex network diagnostics. RCCMD can use this test to find out if the RCCMD signal sending device is available and as well as working properly.

The RCCMD client offers two basic options:

- Automatic mode



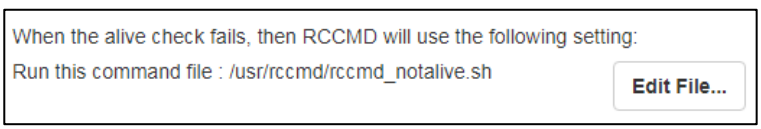
You can choose between two different options:

UPSMAN Traps

An RCCMD server sends a trap message to the RCCMD client. The receipt of this message is logged accordingly.

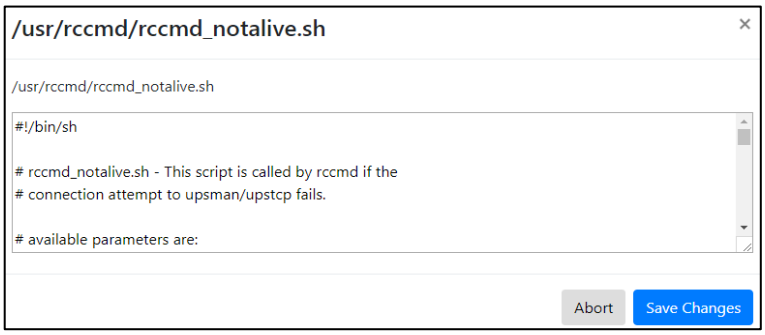
By Polling

The RCCMD client cyclically requests a message from the RCCMD server and logs the reachability of the remote station. In case of connection lost, the queries can be repeated as often as configured. If polling ends unsuccessful, an automatic script can be started.



This script can be customized freely to your needs. With Edit File ... you can directly edit and adapt the file in the web browser..

To edit this file, Linux scripting knowledge is mandatory.



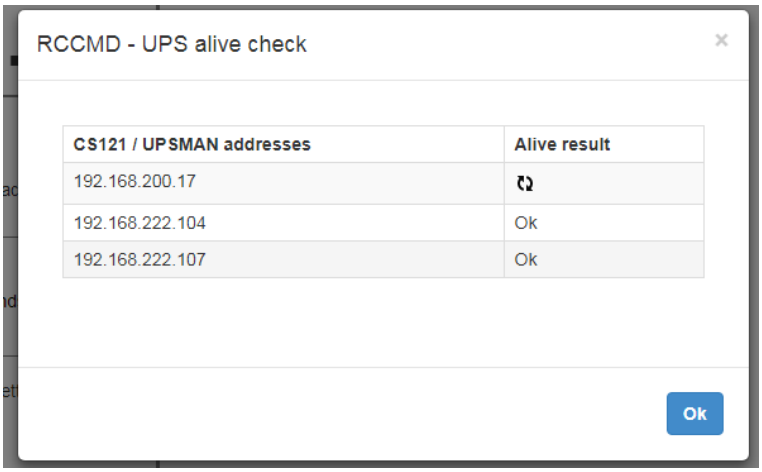
The Manual mode

With Test UPS connections, RCCMD provides a tool that enables quick accessibility lookup test.

Run alive check now ...

opens an additional window. All RCCMD devices entered at Connections are listed and will be queried.

Lack of communication readiness and missing availability will be displayed accordingly:



🗘 … Testing in progress

Ok … Testing complete, device is available und UPSMan service is running

Not Ok … Testing complete, device not found.

Please note: RCCMD will show the result for information and troubleshooting purposes.

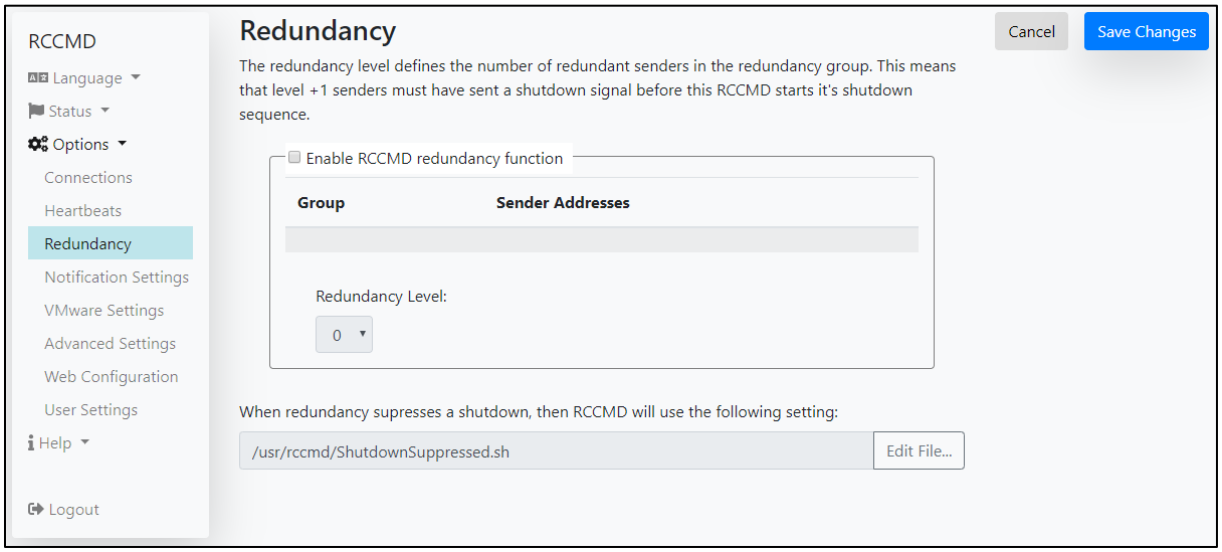
An Alive Check may fail under the following conditions:

- Network failure or broken infrastructure
- Target device is switched off
- Locked or misconfigured ports
- incorrect routing
- UPSMan service does not answer

Unlike automatic polling, no automatic script is executed on failure, as RCCMD assumes that an authorized administrator is monitoring this manual lookup process.

Please note that the configuration will only take effect after you have pressed the green Save Changes, as the RCCMD Client must be restarted for this function

7.4. Redundancy



The redundancy behavior depends on the settings of Connections and Heartbeats:

For the redundancy behavior to work properly, two preconditions must be met:

1. Two valid IP addresses must be specified under Connections.

At least two IP addresses must be stored and allow inbound RCCMD commands.
Redundancy means, RCCMD should not shutdown the server until at least two transmitters have instructed to power down the host.

2. The heartbeats must be set to "Automatic UPS alive check by polling"

RCCMD is instructed by the heartbeats to automatically check the availability of registered IP addresses:
Should a registered UPS become unreachable and the redundancy system shuts down, RCCMD will assume that there is a serious problem and shut down the system ignoring the redundancy setting.

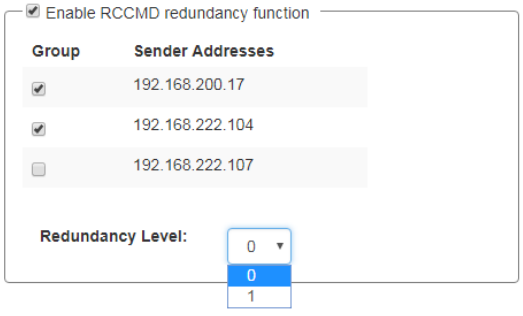
Note:
Keep in mind that the intervals between lookups can be crucial for a shutdown.

Note: The redundancy behavior refers exclusively to the RCCMD command shutdown

Other commands are handled individually and logged accordingly. With the ability to run your own scripts, RCCMD offers options to bypass the standard procedures in case of an emergency.

Defining redundancy levels

First activate the RCCMD redundancy function.
Then select the IP addresses that are allowed to send a shutdown signal.



The Redundancy Level is depending on the number of selected devices:

Number of selected units X -1

By using two devices, both need to send an RCCMD shutdown signal. Since only two systems have been selected, only a maximum of one additional system can send this command. Thereby it is not important, which device is the first sender - this may change dynamically.

For 3 selected systems, the maximum value is 2:

If 1 unit + 2 other units instruct the shutdown, it will be executed. RCCMD does not differ which of the three systems sends the first shutdown.

Using 3 systems, you can also change the Redundancy Level to 1:

As a consequence, two out of three systems are needed for RCCMD to shut down the server. The combination may change dynamically. If you just want to pair 2 of 3 UPS systems, it is recommendable to select them and set the redundancy level to 1. By doing so, the shut down will only be done if both selected UPS's will send a shutdown command.

Keep in mind:

With redundance, you combine several devices. Under connections, you allow general incoming shut down signals. As a consequence, it is possible to configure one redundancy shutdown as well as several single shutdown sender.

Note
Please keep in mind that a shutdown instruction remains active until the system which has instructed the shutdown explicitly withdraws it. This is controlled via the RCCMD Custom Command *wakeup*.

Shutdown behavior with two UPS systems

In case of a shutdown signal, The redundancy will check the connectivity and the availability of the second UPS system are. If it answers properly, the shutdown signal will be suppressed with reservation until further notice:

As soon as the second system instructs a shutdown, this command is executed and the system shuts down. If a shutdown signal is sent by the first system and the second system is not reachable, RCCMD shuts down the system - in this case, RCCMD assumes that the second system is not available.

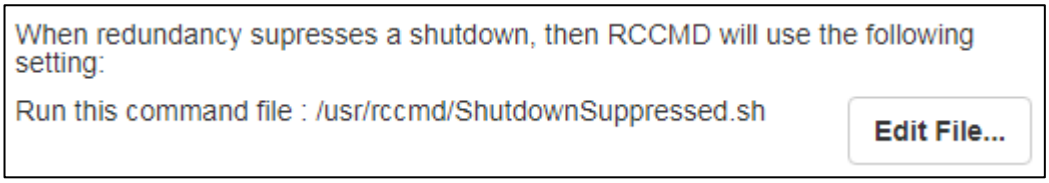
Shutdown behavior with three valid devices

From three devices onwards, the redundancy behavior can be individually adjusted to necessary conditions:

1. If one of three systems send a shutdown
2. When two out of three systems send a shutdown
3. All three systems must decide the shutdown together.

Each system can individually instruct and withdraw its shutdown via the RCCMD Custom command wakeup. In general, RCCMD will not execute the shutdown until the exact shutdown condition is met.
Redundancy-related scripting

If you use redundancy behavior, the RCCMD client waits to execute the shutdown until the appropriate number of devices also instruct the shutdown.



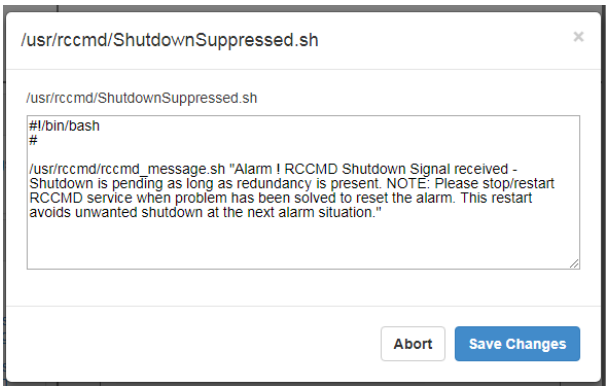
.

Because this process has a direct impact on the operation of the servers being monitored by RCCMD, a script will be launched to indicate an incident.

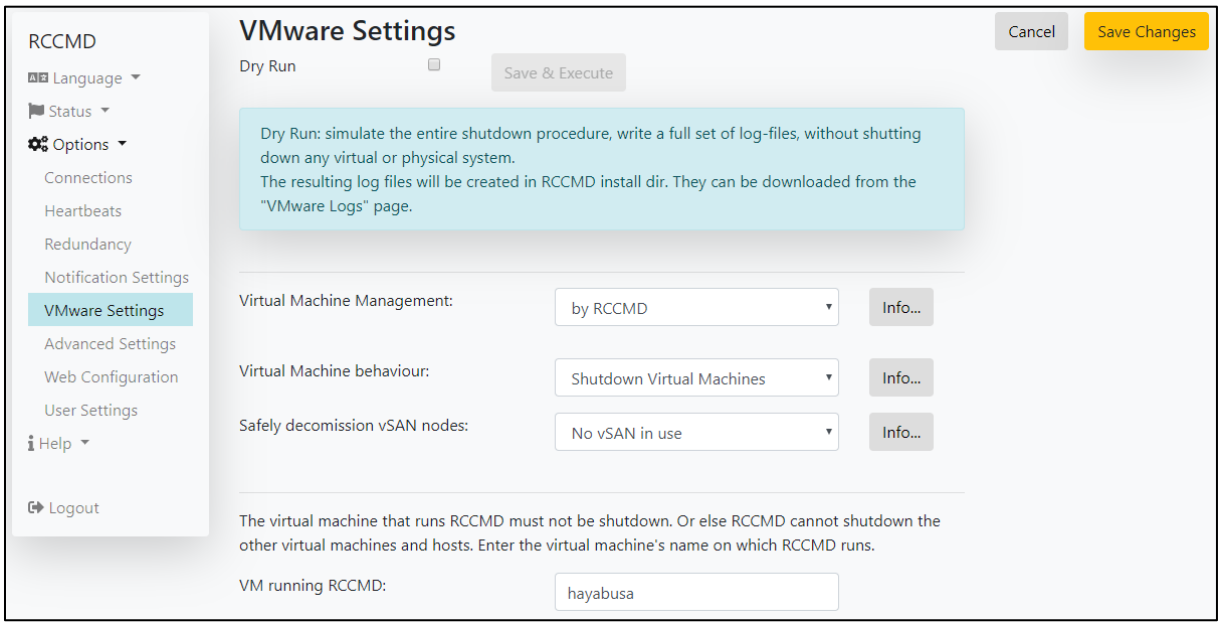
Use Edit File ... to customize and adapt this script to your individual requirements.

Abort will close the editor and withdraw all changes you made.

As a default, a text notification is pre-defined to indicate a redundancy-based shutdown behavior



7.5. VMware settings



The VMWare settings control the overall shutdown behavior of servers and hosts within VMware. Depending on the configuration level and configuration type, different types of configuration are necessary in order to manage a VMware based infrastructure. In addition to the mandatory basic data like IP addresses user credentials, you may need, among other things, more specific knowledge about the shutdown behavior of your IT landscape.

Please note, some data are not static. Values may change and should be adjusted during regular system checks..

➔ RCCMD evaluates and displays estimated shutdown times according to entered data.

Part 1: Basic setup

The basic settings assume that you are running hosts without vCenter. You can shut down as many hosts as you want with one RCCMD appliance:

Virtual Machine Management

This menu defines whether you want the hosts and virtual machines to be managed by RCCMD or by a vCenter. If you operate the hosts in lock-down mode, e.g. the control commands are exclusively approved by a vCenter. Even if you enter the credentials correctly, the host will deny command execution.

In the default setting, "from RCCMD" is preset.

Virtual machine behavior

Use this setting to define whether you want to use vMotion or just shut down your machines. A virtual machine shutdown will be controlled directly by the host:

the virtual machines are shut down normally, and then the host is turned off.

If you enable vMotion, local shutdown of virtual machines is the secondary protocol. First, the vCenter will try to move the virtual machines to another host.

The default setting is "Shut down virtual machines".

➔ If maintenance mode is selected, additional information are required like credentials of the vCenter as well as a time window that should be available for the vCenter to move virtual machines to another host.

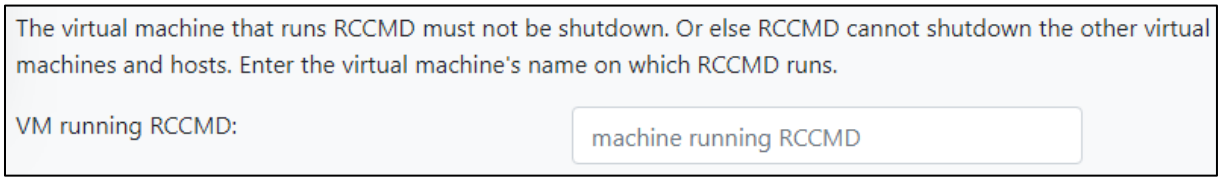
Safely decommission vSAN nodes auf no vSAN in use

This setting defines the shutdown behavior in case of a vSAN is in use - The vCenter provides different basic settings, to be selected at this configuration point. If you want to use an RCCMD-managed vSAN, refer to the basic requirements that must be met.

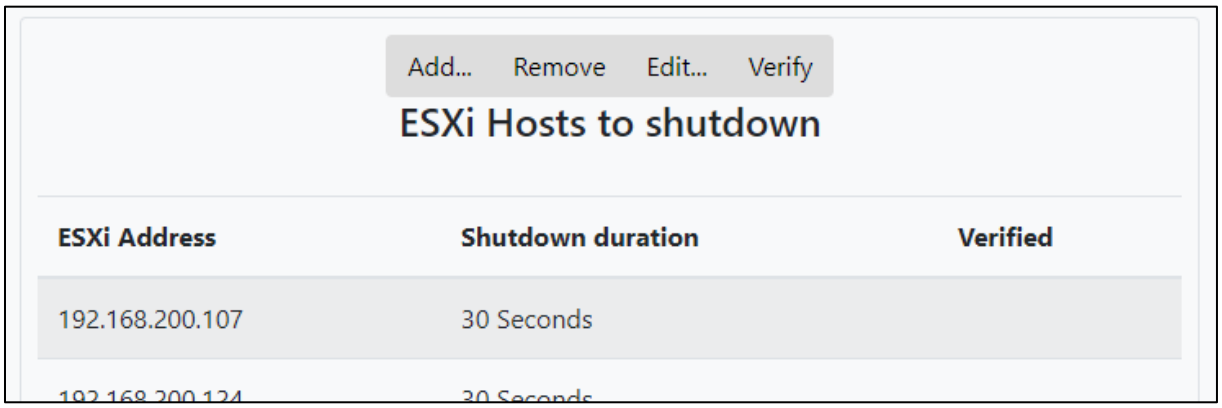
The default setting is "No vSAN in use".

VMware running RCCMD

RCCMD needs to know the name of the virtual machine that contains the RCCMD appliance. This setting prevents a shutdown of the RCCMD Client.



Tell RCCMD all ESXi Hosts to shut down



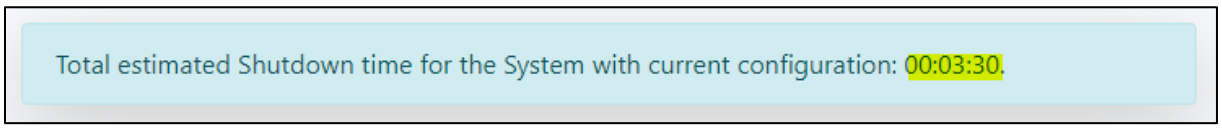
With this configuration dialog, declare which ESXi hosts has to be shut down by RCCMD:

The menu bar provides several functions:

- Add: Add another host. To remove a host
- Remove: Select a host and click Remove to remove it from the current list
- Edit: Select a host. With Edit you can edit the access data.
- Verify: If you press this button, the current configuration will be saved and the login data will be validated. At verified, RCCMD shows the connection attempt.

Estimated shutdown time

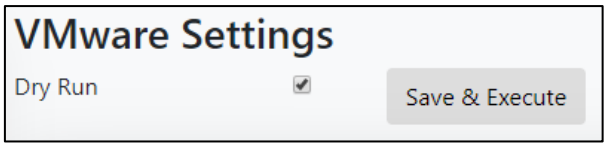
After the configuration job is done, RCCMD shows an estimated shutdown time:



This is the current average shut down time of your IT infrastructure. Please note, this shut down time is calculated and can be used to compare it with the he emergency power time granted by the UPS.

Due to the fact this is a calculated value: Please test you shutdown setting before activating!

Dry run (tests):

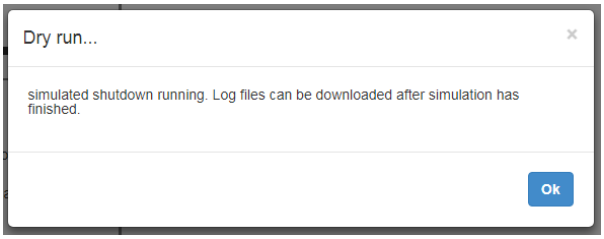


With the Dry Run RCCMD offers a unique function within the VMware settings:

The Dry Run is a simulation mode, in which your RCCMD installations simulate the behavior, but do not physically execute.

This feature is useful when installing an RCCMD installation on a production server:

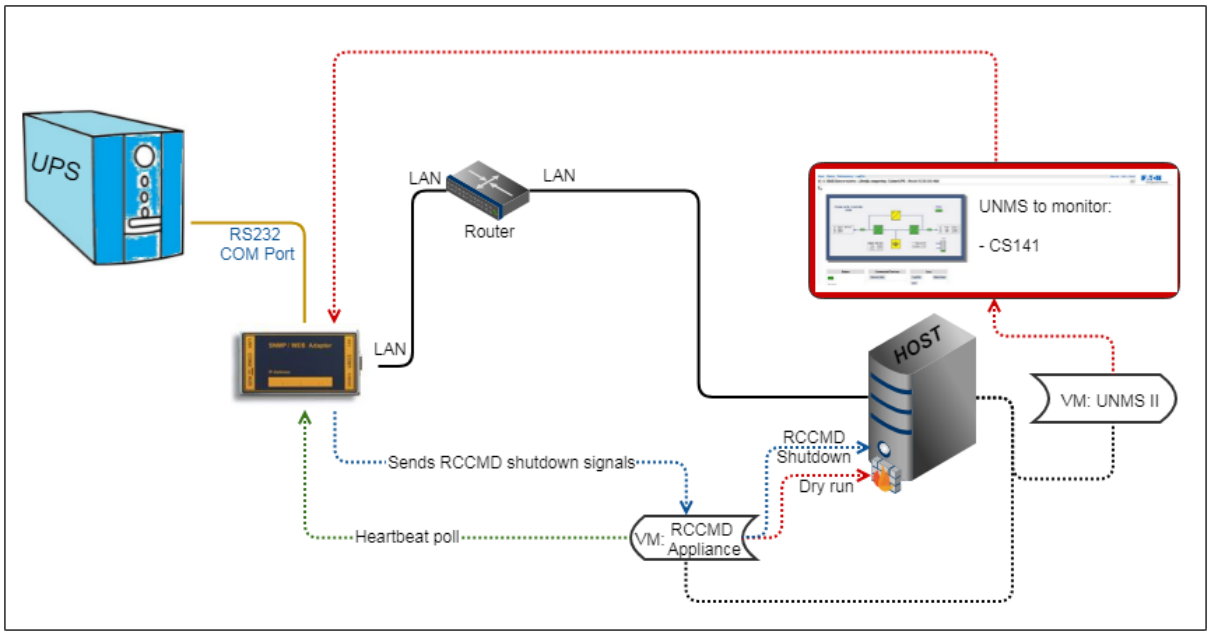
Accidental shutdown is prevented in this way. With Save and Execute, this feature is enabled, protecting your future configuration from accidental shutdown.



Note

Some configuration menus are locked during testing and cannot be adjusted "in between".

What a "Dry run" does …



Normally, a CS141 is the RCCMD server that sends a valid RCCMD command to an RCCMD client - the RCCMD software. The command and what to trigger with it depends on the final operating scenario. Due to the fact you can use the event handling from the CS141 for sending individual commands in order to start very delicate and complex scripts, it is possible to automate a server via scripts in many parts - you do not necessarily just have to shut down a server with RCCMD.

With VMware, the RCCMD appliance differs from normal client installation:

It is designed to ensure a structured shut down sequence for all hosts within a VMware environment-

To fulfill this task, RCMMD needs access data coming with system rights to allow a shutdown. The problem that RCCMD cannot differ between a real emergency situation and a user who press the test job - button at CS141. During testing, this is could be a problem. As soon as RCCMD will accept a valid signal, it will start the shutdown procedure - It is comparable with the quiet "OK" - console command of any normally shown „Are you sure " - Dialog inside an operating system.

Of course, you cannot simply shut down "all servers" during operation because you want to test your configuration - shutting down a real-time system with 100% availability is just for real emergency issues....

The dry run is a build-in self-running simulation mode

1. All configured hosts will be contacted
2. Credentials for the hosts will be tested
3. a protocol log will be written to log configuration issues as well as successful login tests.
4. The standard RCCMD shutdown signal is suppressed as long as simulation mode is active.

As long as dry run is active, no emergency shutdown is possible via any valid RCCMD server device.

Note:

If you change or adjust the standard scripts coming with a default installation or add new scripts, they will be executed consequently. The Dry Run only suppress its own standard scripted shutdown sequence - it does not check the changes you added manually.

This behavior contains advantages as well as disadvantages

1. Due to the fact your "sharp" scripts are executed mercilessly, the Dry Run test should take place beforehand!

2. By adding your own scripts that trigger harmless actions, you can check if your "sharp" scripts would work and all administrative shares on the target system are met.

Part 2: Advanced settings

If Maintenance Mode (vMotion) is selected

RCCMD will present two addition menu entries:

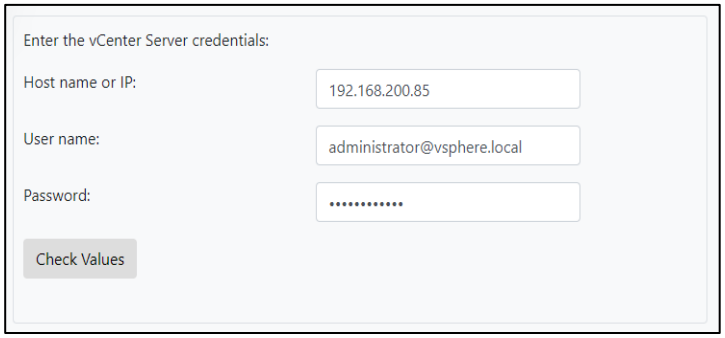
Maintenance Mode Timout in Seconds

This value defines the time window that RCCMD grants the vCenter to move virtual machines to host that are not going down into maintenance mode.

Virtual machines that have not been migrated within this time window will be left for shut down by the ESXi host.

vCenter credentials

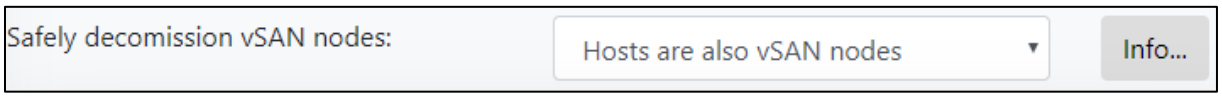
In order to use vMotion, RCCMD need valid vCenter credentials. Please note, an RCMD client can shut down many hotsts, but technically only maintain one vCenter. if you need to configure several different configuration types, it may be necessary to use 2 RCCMD appliances that work together.



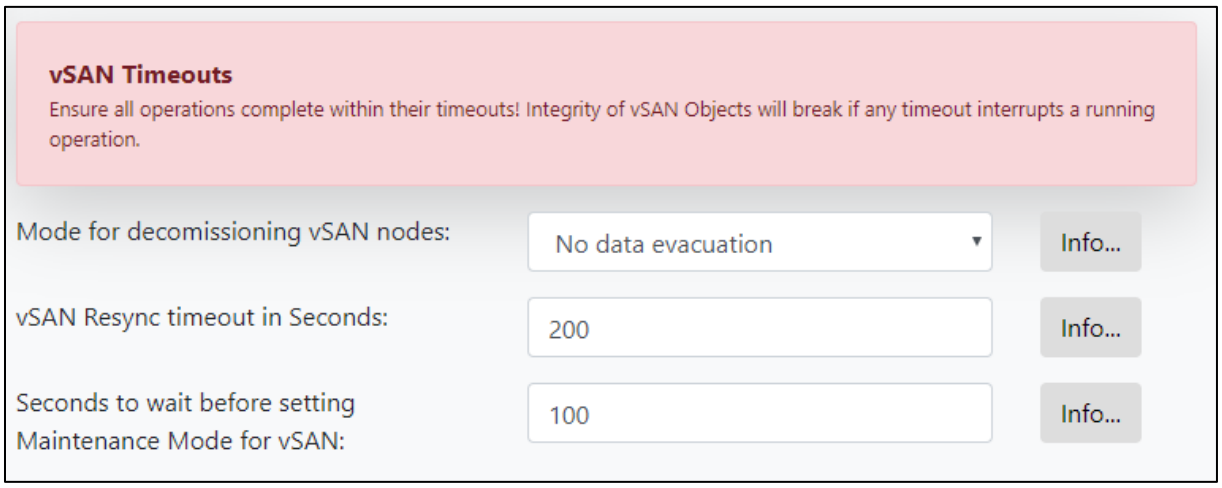
Check values

Test the vCenter credentials. RCCMD will try to log into the vCenter and give a feedback including a reason why the login attempt failed.

Part 3: Selecting "Host are also vSAN nodes" at vSAN Safely decommission vSAN nodes



This setting enables several sub menus and a vSAN time out warning.



Keep an eye on this warning message!

A vSAN is a little bit tricky when running a shutdown routine and the vSAN has been terminated incorrectly. It is even possible that a wrong configured shutdown routine leads into data corruption or even total data loss.

vSAN shutdown options

No data evacuation

This is the fastest way to ensure system shutdown. It shuts down the virtual machines, and then the vCenter synchronizes all the hosts that are inside the vSAN. There will be no data migration or virtual machines to be moved to other hosts.

Evacuate all data to other hosts

In principle, it is the same function that triggers vMotion. A vSAN can also be spanned across different sites, so you can also offload virtual machines to external hosts that are not in the vSAN cluster you are about to shut down. if you use vMotion, it will be executed first. Due to this fact it is possible that your vSAN host has no virtual machines that need a migration. But you may use it as "second try" to move machines away from your vSAN...

Ensure data accessibility

If larger vSAN systems provide enough capacities for redundancies, no data will be moved. Data migration will only be done for data without redundancy.

Note

With vSAN extensions, RCCMD introduces solution to allow you performing an emergency shut down of the entire vSAN system as fast as possible - virtual machines that have been previously migrated to another location via vMotion are not affected.

Due to the fact you want to stop and shut down the vSAN because there is an emergency, selecting "No data evacuation" is the best choice.

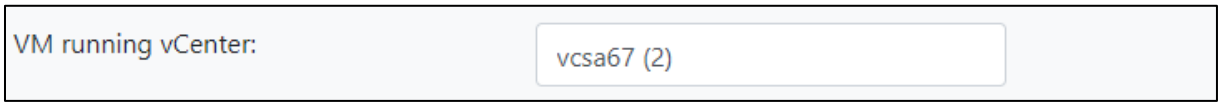
vSAN Resync timeout in Seconds

This setting is the basic time window RCCMD grants the vCenter synchronize the databases between the hosts before starting the next point in the shutdown sequence. This time window is a little bit tricky, because the resync time is a very relative value - in principle you can say it lasts as long as it takes ... the vCenter does not tell you an estimated resync time, you need to test it during a manual shut down. If your vCenter announces the job is done, you have the minimum time window for your emergency shutdown. Please calculate some extra time for this time window because the measured time during a manual shutdown is just a snapshot and not a general value.

Seconds to wait before setting Maintenance Mode for vSAN

Once the resync is completed, the vCenter is the last surviving virtual machine that needs to be shut down. With this setting, you define how long the vCenter has time to shut itself down before RCCMD starts the next step of the shutdown sequence.

Determine which VM is running the vCenter



Inside a vSAN, the vCenter is more:

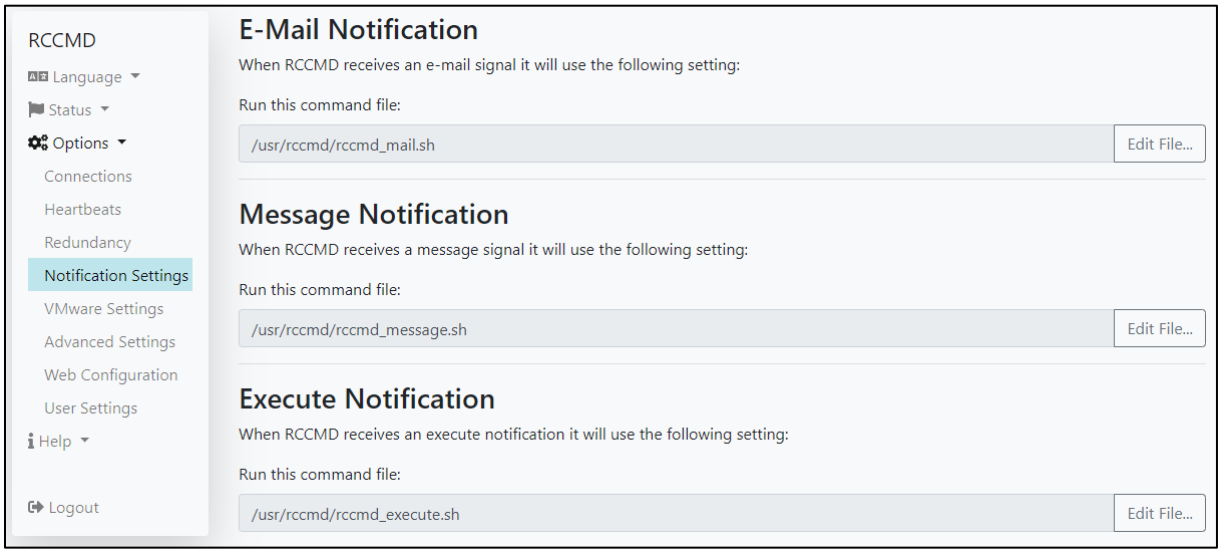
The vCenter manages the complete data transfer within a vSAN and handles the complete post synchronization phase during a vSAN shut down. This means:

If the vCenter runs inside a vSAN or runs on a host that will be shut down to fast, the complete vSAN hung up. If the vCenter is located as a virtual machine within the vSAN, RCCMD needs to know the name of the virtual machine in order to exclude it from virtual machine shutdown.

Note:

The vCenter that handles a vSAN is not always inside this cluster – it may be installed somewhere and handled separately. If the virtual machine with the vCenter is not inside the list of the hosts to be shut down, you do not need to enter it at this point. But you need to take an eye on it if when using different RCCMD appliances – Without it's vCenter, a vSAN cannot shut down as expected.

7.6. Notification settings



Depending on which command is received by a valid RCCMD transmitter, three basic scripts are executed automatically. Each script triggers an RCCMD functions. The RCCMD routines are preconfigured and normally there is no need to edit them.

However, if you want to execute your own scripts by RCCMD,

you can either write these scripts directly to the appropriate .sh - script and execute them as a custom command or you may edit these basic files.

Warming:

If you modify, customize, or extend these scripts, you change the overall behavior of RCCMD within your system. Be sure to make a backup before editing the scripts to find back to the original system state. Changes to the original configuration may result in unpredictable behavior of RCCMD and may cause system-wide problems.

Edit these scripts at your own risk!

When will these scripts be executed?

RCCMD differs between three different scripts:

Email notification

The CS141 will normally rely on its own mail client - this is also the recommended way. However, in some high-security networks, it may not be desirable for the web manager to be able to send their own mails. The RCCMD client can be used as an interface to forward short mail messages.

You can also use this script to trigger additional scripts:

Send an email AND execute the following script ...

for this function, the freeware Linux tool send mail is installed, which allows RCCMD to send e-mails. You can configure the tool at any time by logging in via a console on the Linux interface of the RCCMD client.

To forward an email from a CS141, use the Custom Commands and enter the following command by entering the IP address:

Mail targetmailaddress@targedmailserver.com <Text message>

At the Cs141, you will enter:

mail Kirk@enterprise.de Jean-Luc Picard was here

RCCMD would take over and write a mail to kirk@enterprise.de with the topic „Jean-Luc Picard was here“.

Is the only function of this script the trigger of an email?

No, this script can be edited to do everything. …

- ➔ changing the complete script will cause changing the behavior and may cause RCCMD will not run as expected.
- ➔ Edit it at your own risk.

Message Notification

This script controls the receipt of messages and is responsible for displaying them on the monitor. Because the RCCMD appliance is a non-graphical server program that runs without permanent a permanent monitoring, you should leave this script simple as it is:

Since it is triggered by each incoming RCCMD notification signal, additional content would also be executed each time.

Due to the fact, this is mostly without a function (no graphical interface) you may use it for routine scripting

- ➔ changing the complete script will cause changing the behavior and may cause RCCMD will not run as expected.
- ➔ Edit it at your own risk.

Execute Notification

This script is interesting:

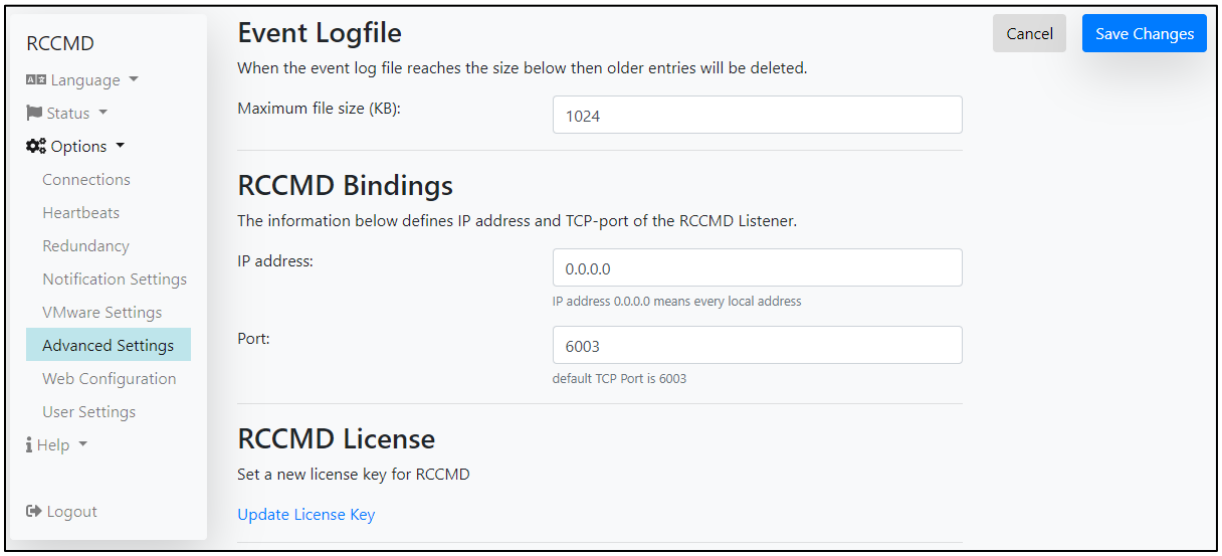
This script executes all valid incoming commands a CS141 may send. This script triggers the complete shut down routine RCCMD provides

With this script, RCCMD will provide you the unique option to add and trigger your very own customized shutdown scripting solution and even program an additional non-standard routine that specifically met exactly your network.

- ➔ This script is a very powerful option as well as dangerous because changes directly interfere with all functions of the RCCMD. Any changes and enhancements you make will directly affect the shutdown behavior.

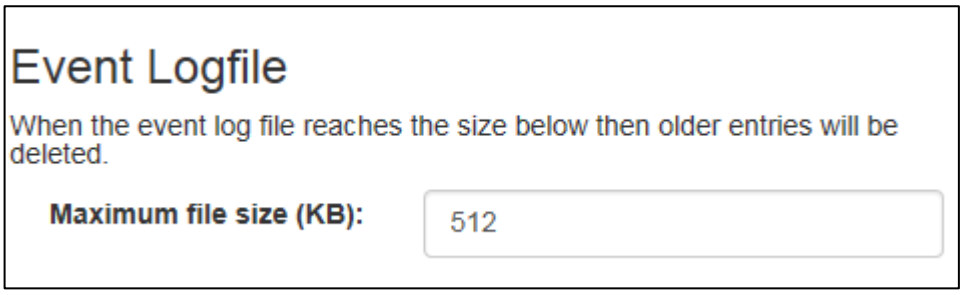
Advanced scripting skills in Linux are essential for changes to this script!

7.7. Advanced settings



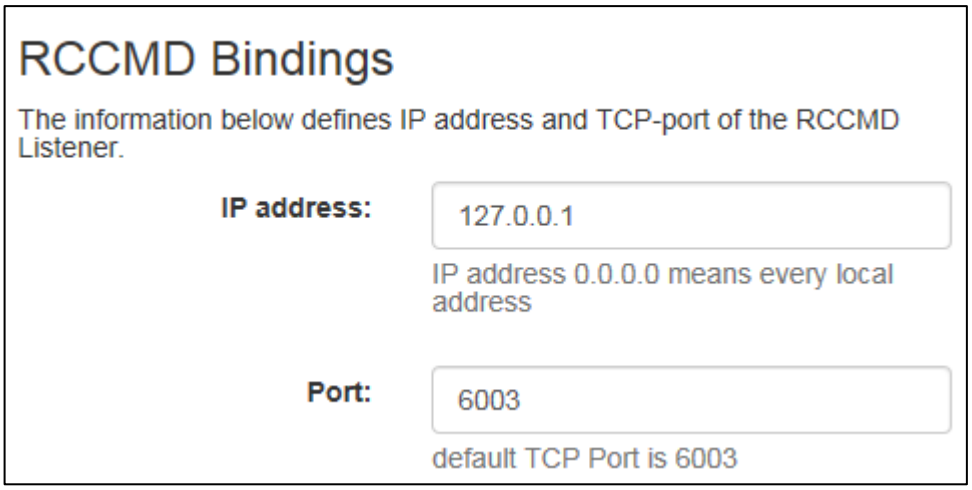
Use Advanced Settings for additional settings to configure RCCMD. The menu is divided into three parts:

Event Logfile

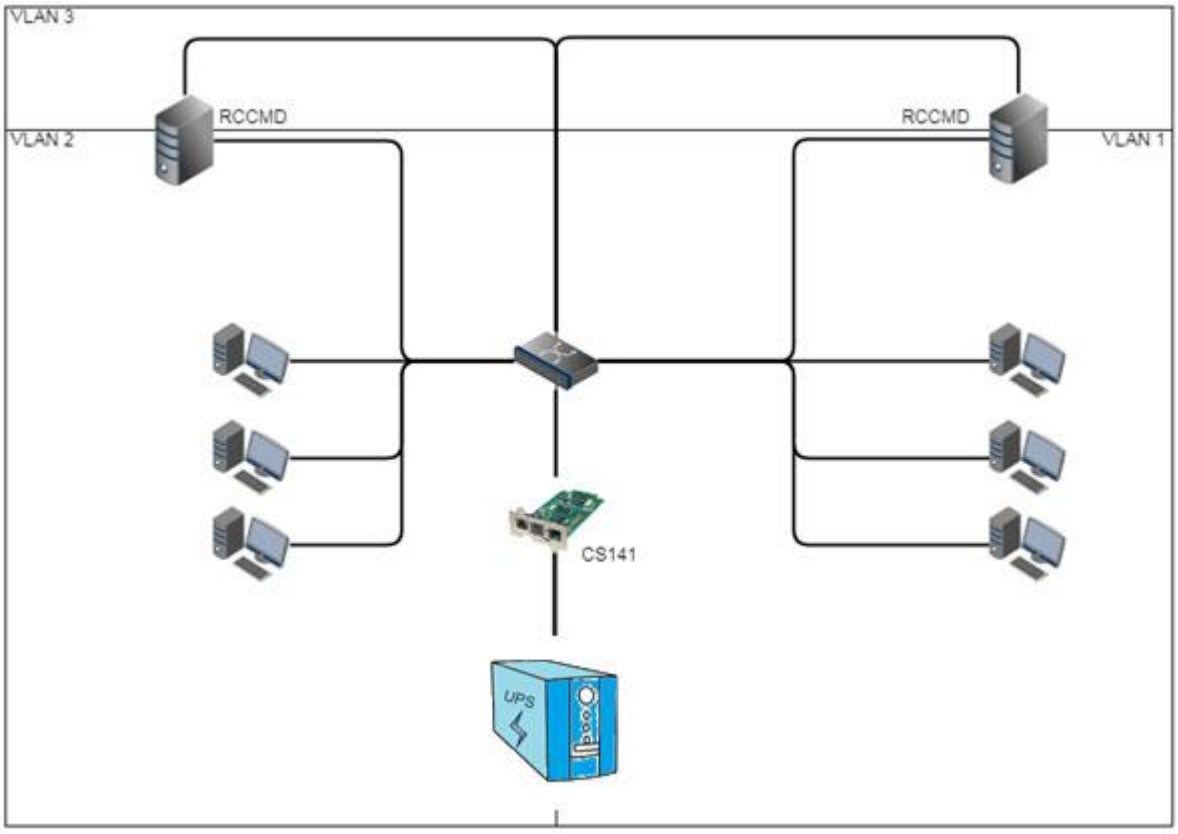


In general, any RCCMD Signal affecting the client will be logged. Due to the fact server systems may provide limited memory resources for log files, it may be necessary to limit the size of the log file to a maximum size to consume. In case the maximum file size is reached, the oldest entry is replaced by a new entry.

RCCMD Bindings

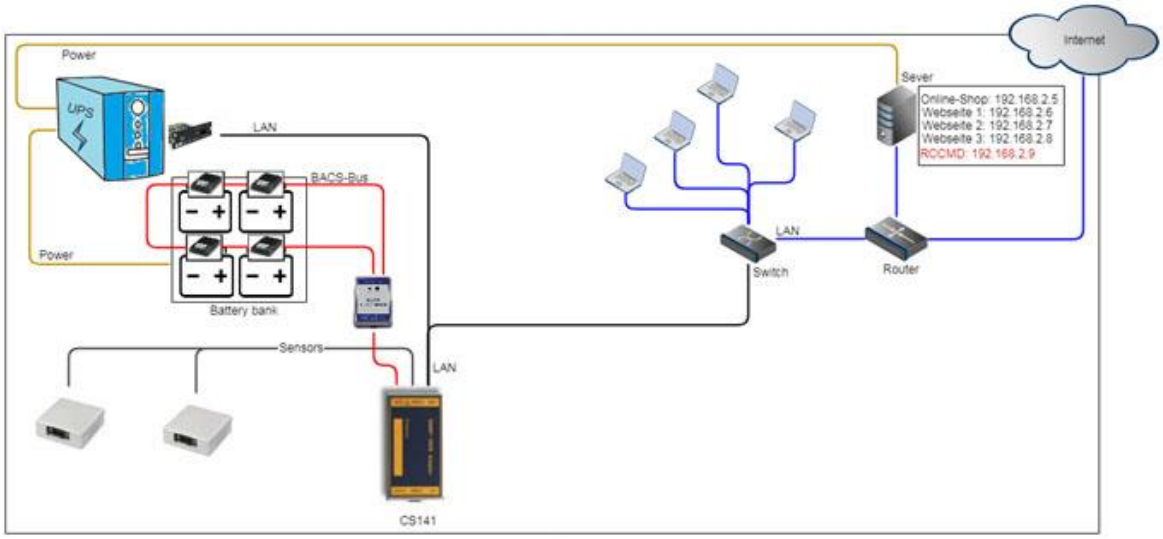


RCCMD Bindings is a sophisticated tool that helps you to limit traffic. Since this setting deeply affects your network setting, it should be used with caution. The bindings allow forcing RCCMD to listen on a specific network card. In case of multihoming is in use, the listener can be configured to a specific IP address within one network card. As an example, this will be used if there is a necessity to divide the network logically into a production network and an infrastructure network via VLAN:



In this example scenario, two or more network adapters can be installed. Binding RCCMD to one specific network card will prevent users to access the RCCMD client and accidentally shut down a server - this is only possible via devices that are located in VLAN 3 or have been properly enabled via a router.

Another scenario is the so-called multihoming:

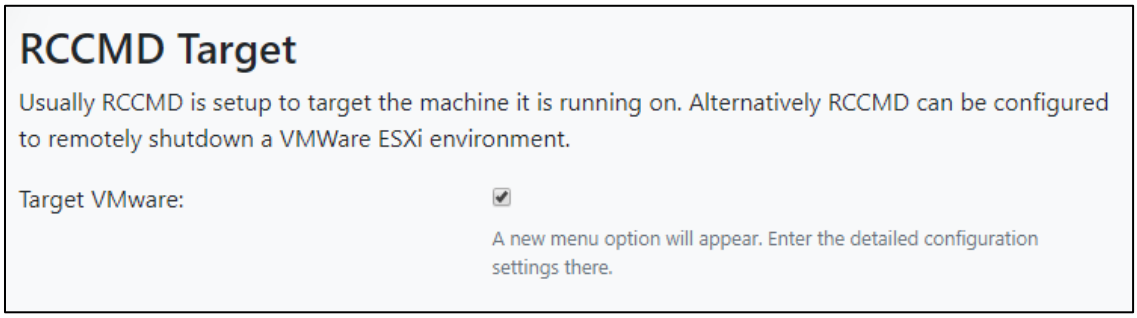


It is not absolutely necessary for modern network devices that an IP address is firmly linked to one network interface. In fact, multiple IP addresses can be connected via a network interface - they share hardware, but otherwise form self-contained instances. As an example, this could be a web server that manages different websites with a unique IP address: the server is connected by a router that determines between incoming signals and signals provided by local network. Bindings will instruct RCCMD to listen for incoming RCCMD signals only at a specific IP address that is assigned to the local network only.

Note

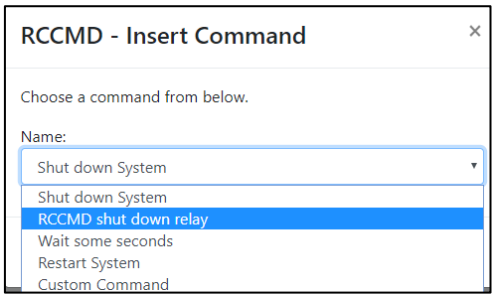
These configurations are used in special scenarios. Normally you can leave the setting 127.0.0.1 / local host, port 6003. In that case, RCCMD will listen on all available IP addresses for a valid incoming signal. Since you have defined the valid sender address at the menu Connections, RCCMD will notice the signal but deny execution and log this fact as an invalid RCCMD command.

Change RCCMD Target



The RCCMD appliance is more than just a small tool to handle just VMware hosts. On unchecking the checkbox and pressing Save changes, RCCMD changes to the local mode:

All VMware menus will be disabled and the Shutdown settings will switch to local options:



Due to the fact, RCCMD can not just receive, but also send RCCMD shutdown signals, it is possible to use an RCCMD appliance as a central RCCMD relay that runs with complete customized additional scripting.

When local mode is active, RCCMD provides the following command sequences:

Shut down system

RCCMD will shut down the server it runs on.

RCCMD shut down relay

With this option, RCCMD will forward a valid RCCMD shutdown to

- Single IP addresses
- An IP address range

With this option, it is possible to get advanced redundancy options - as an example, you may combine a CS141 and a second RCCMD client – if both advice a shutdown, the target RCCMD system will execute the command.

Wait some seconds

RCCMD will wait a customizable time window until the next command in the list will be executed.

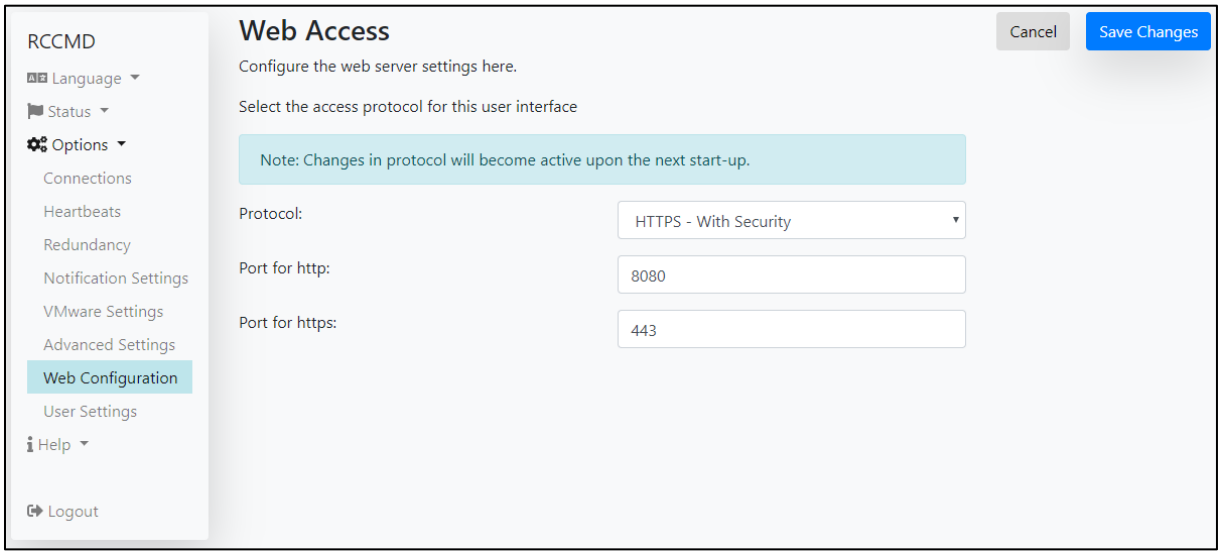
System restart

RCCMD will restart the complete RCCMD server that runs within a virtual machine

Custom command

Start programs, run kill-commands, run your own scripts, just enter the command and mandatory extensions and RCCMD will do the rest.

7.8. WEB configuration



Set the availability of the RCCMD web console.

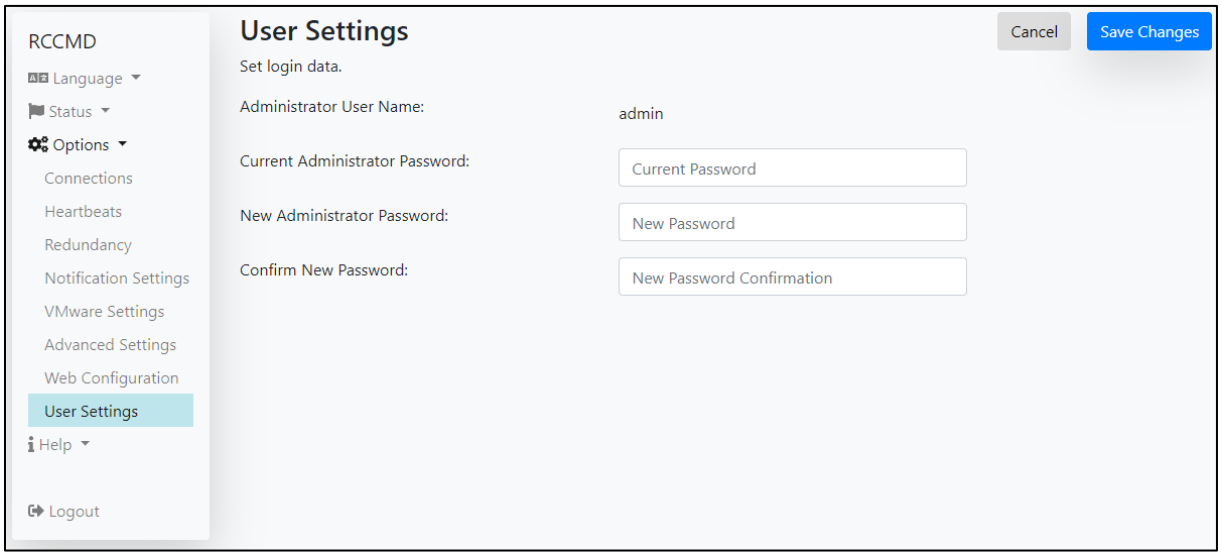
The default for web access is:

http: port 8080

https: port 8443

Please note changing the default values will cause the web console of RCCMD can only be reached via the ports you manually set.

7.9. User settings



Customize the administrator password according to your ideas and company policies. Please note that this password also applies to the admin user on the console. The appendix contains instructions how to set up an emergency user for password recovery

Administrator User Name: admin
This user name is hard-coded and cannot be changed.

Current Administrator Password:
This is the currently assigned password.

New Administrator Password
Assign the new password.

Confirm New Password
Repeat the password you have assigned. Please note that Copy and Paste will repeat typing errors and may lock up your RCCMD client.

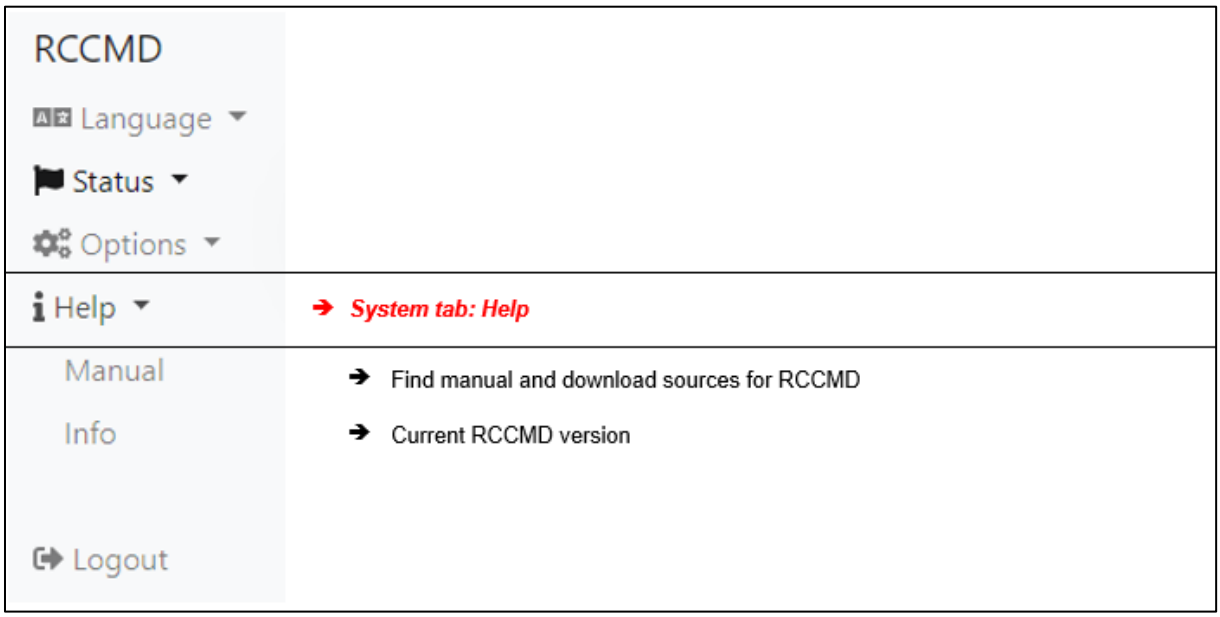
Note

Depending on the program version, there are two default passwords that can be assigned.

Program versions until 5/2018: cs121-snmp
Program versions from 5/2018: RCCMD

Due to the fact RCCMD comes with two years update authorization, it is possible that you need these two default passwords.

7.10. Help

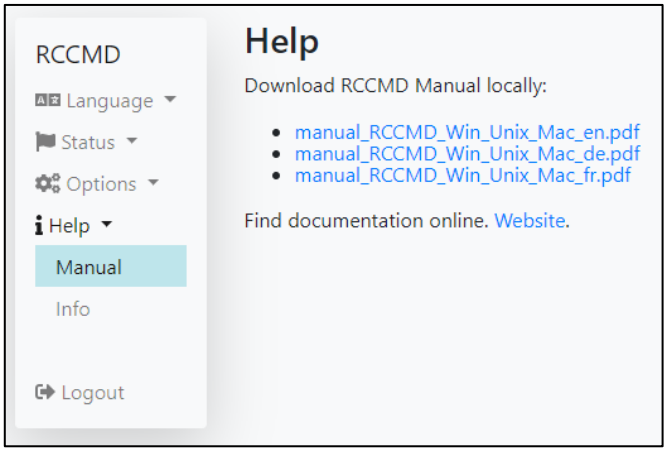


Manual

You need help?

The manuals are available inside RCCMD – you do not need any additional network connection.

Due to the fact the manual is a pdf-file you may need additional software tools to open the according file.

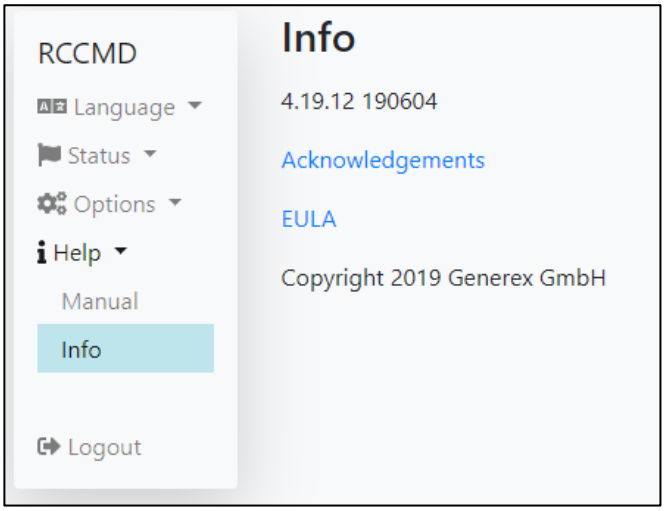


Info

Need additional information about your copy of RCCMD?

The info button will show

- Acknowlegdements
- EULA
- Copyrights



8. Appendix

RCCMD FAQ's

8.1. Static IP addressing

In some cases, a network design may not provide a DHCP server:

The carrier system starts, but without receiving a valid IP address RCCMD may use. Since the 100% availability of a DHCP server can never be given, it is advisable to assign a static IP address here. Search for the file interfaces – this file is responsible to manage dynamic or static IP address entries.

You need two commands to find required files:

Command: cd /etc/network

Command: ls

```
admin@rccmdAppliance:/etc/network$ ls
if-down.d  if-post-down.d  if-pre-up.d  if-up.d  interfaces  interfaces.d
admin@rccmdAppliance:/etc/network$
```

The RCCMD appliance uses nano - a small and handsome editor to help viewing and editing files.

Command: nano interfaces

The editor opens and displays the contents of the file Interfaces:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp
# iface ens33 inet static
#       address 192.168.200.223/24
#       gateway 192.168.200.1
#       # dns-* options are implemented by the resolvconf package, if installed
#       dns-nameservers 192.168.200.3 192.168.200.5 192.168.200.1
#       dns-search local
```

8.2. RCCMD network settings

Search for this crucial entry:

- ➔ iface ens33 inet dhcp
- ➔ iface ens33inet static

Basically, these two configuration lines decide whether to use a static IP address or the appliance asks for a DHCP server.

```
Source /etc/network/interfaces.d/*

# The loopback network interface
Auto lo
Iface lo inet loopback
#The primary network interface
alllow-hotplug ens33

#Iface ens33 inet dhcp                          <- use # to disable DHCP
iface ens33 inet static                         <- Remove # to enable manual IP address settings
address 192.168.200.99                          <- Enter static IP-address
subnet 255.255.255.0                            <- Enter subnet mask
gateway 192.168.200.1                           <- Enter IP address of the gateway

# dns-* options are implemented by the resolvconf package, if installed

dns-namservers 192.168.200.3 192.168.200.5 168.168.200.1    <- Enter DNS Server Ip address data
# dns-search local
```

After reboot (use command « init 6 » for reboot, the appliance should use and display a static IP address.

Note

If you choose to enter the IP address assigned by the DHCP server during startup as a static IP, ensure this IP address will be removed from the pool of dynamically assignable IP addresses. Alternatively, you can assign a fixed IP address via DHCP server and enter it statically in the appliance. By doing so, RCCMD will definitely be assigned an accessible IP address, which greatly increases resilience

8.3. Parametring a security user (VMware)

Setting up an emergency user

Note

You do not want it, but passwords can be lost - unfortunately always in company of big trouble:

For complex systems, a lost password can be very cumbersome and expensive, e.g. if complex scripts neet to be completly rebuild from scratch. The emergency user is not an all-in-one Solution for these problems, but it may be very useful if something unexpected occurs. You can configure the emergency user at any time - it is no need to do it right before initial configuration of RCCMD.

You may skip this part in case of not using an emergency user or if you wish to configure it later.

It happens again and again that passwords are lost due to adverse circumstances:

- e.g. no proper documentation about the installed systems,
- systems and passwords have been forgotten
- systems are inherited from other companies

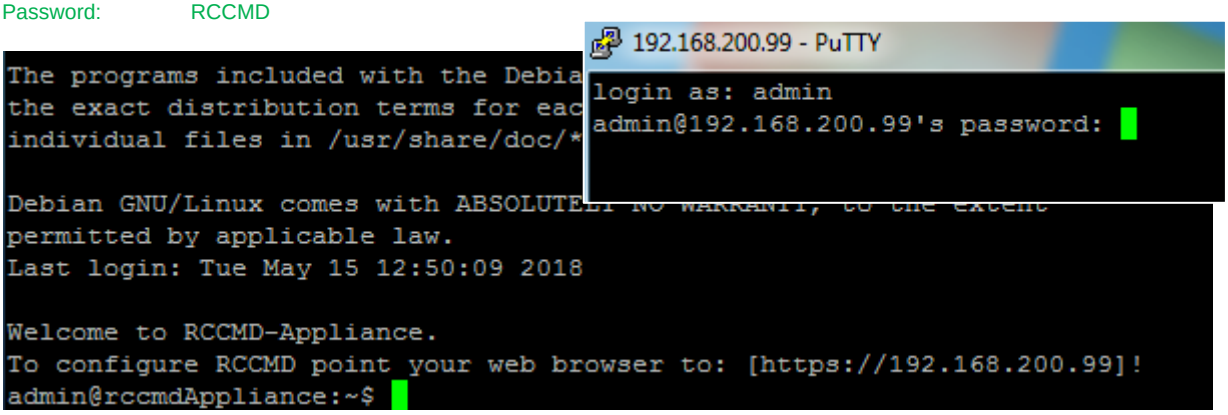
For safety reasons, RCCMD has no backdoors installed by default.

If you assign a new password to user admin, ensure it will be documented!

Otherwise you are damned to set up the complete RCCMD appliance again and reassemble all shutdown scripts. To prevent this incident, it is recommended to set up a backup user to ensure resetting passwords.

After installing the appliance, it is possible to access the console with a freeware tool like Putty:

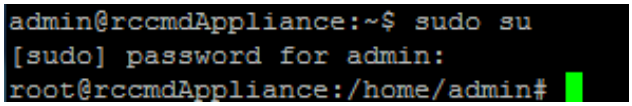
User: admin
Password: RCCMD



Requesting root privileges

Command: sudo su

Note the user "admin" not yet has been granted the necessary rights to set up a corresponding emergency user. This command will enable the superuser for advanced rights



Creating user and password

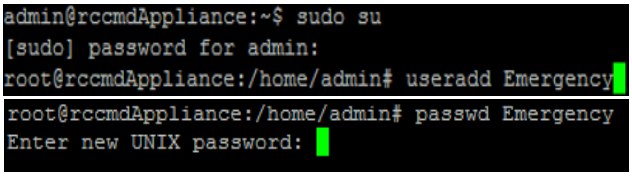
This step requires two commands

Command 1: useradd <Username>

This command will deploy a new user.

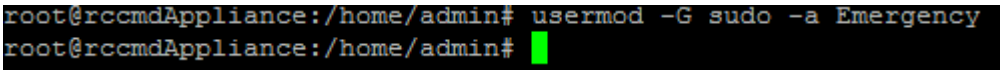
Command 2: passwd <Username>

This command sets up a valid password.



Adding to administrative user group

Command: usermod – G sudo -a Emergency



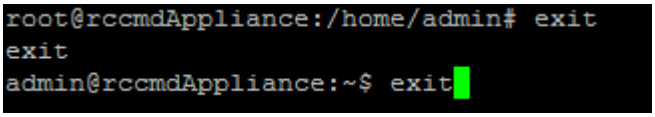
In order for the newly created user to be granted the necessary rights, he must be assigned to the appropriate user group

Logging off

Command: exit

Note: Enter exit twice:

The *first* exit will close up the SuperUser, the *second* exit will quit the connection to RCCMD and clos the console.



Performing an emergency password reset

Start the session using the credentials of the emergency user.

Requesting extended system rights

Command: sudo su

```
Welcome to RCCMD-Appliance.
To configure RCCMD point your web browser to: [https://192.168.200.99]!
$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for Emergency:
root@rccmdAppliance:/#
```

The user Emergency has basically no authorization to administer the RCCMD appliance. Since this user is listed in the group of superusers, *sudo su* enables extend the system rights.

Navigating to required directory

Command: cd /usr/rccmd/webconfig/resources

This directory contains the configuration scripts you need to edit the password of the user admin.

```
root@rccmdAppliance:/# cd /usr/rccmd
root@rccmdAppliance:/usr/rccmd# cd webconfig/resources/
root@rccmdAppliance:/usr/rccmd/webconfig/resources#
```

Using a text editor to change passwords

Command: nano realm.properties

nano is a very handy and well laid-out editor for viewing and editing files and scripts within the RCCMD operating system. The file realm.properties itself contains the encrypted password for the web interface of RCCMD.

```
#RCCMD realm.properties
# username: password [,rolename ...]
admin: CRYPT:adg.Dq8TXmNZI, admin
```

Following changes have to be made:

#RCCMD realm.properties	
# username: password [,rolename ...]	
#admin: CRYPT:adg.Dq8TXmNZI, admin	-> Use # to disable this line
admin: Notfall, admin	-> Add this line

In this example, the user admin would now be assigned the password "*Notfall*":

Saving settings.

Command: CTRL X

Save the file and exit the text editor. Be sure to overwrite the original file. Changing file name will not work.

Restarting RCCMD Web Interface

Command: /etc/init.d/rccmdConfig restart

```
root@rccmdAppliance:/usr/rccmd/webconfig/resources# /etc/init.d/rccmdConfig restart
stopping RCCMD-Configurator...
RCCMDConf has been stopped.
Starting RCCMD-Configurator...
RCCMDConf has been started.
```

This command will restart the web interface and set the new password.

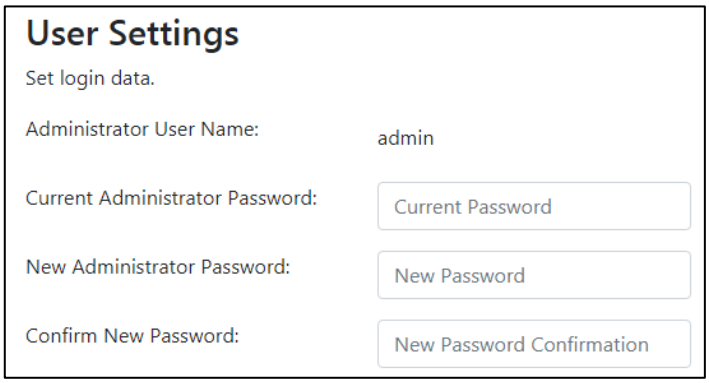
Synchronizing passwords

For the moment, the user admin uses two different passwords:

- The old password is valid inside the console of the RCCMD Appliance
- The new password is valid for the web interface of RCCMD

Furthermore, your password changes are not encrypted.

To synchronize and encrypt the credentials for user admin, open a web browser and enter the IP address of you RCCMD installation. After Login, navigate to User Settings and change password.



Press *Save changes* to synchronize and encrypt the password.

9. Copyright and licences

The copyright authorization from Generex and other relevant software suppliers must be respected. Generex and their suppliers reserve the rights to the software components. In particular the following are prohibited:

- *copying and distribution,*
- *modifications and derivations,*
- *decompilation, reverse engineering,*

Components which fall under GNU General Public License and further Open Source licenses are integrated into the software. An overview of the integrated Open Source components and a copy of the current license can be obtained at www.generex.de/legal/sla.

Generex will provide the source code for all components of software licensed under the GNU General Public License and comparable Open Source licenses.

For source code requests, please email info@generex.de