RCCMD – Multiple Server Shutdown Software

Benutzerhandbuch

Inhalt:

6. Schnellabsicherung unter Windows, Linux und MAC

Die Schnellabsicherung erfasst alle grundlegenden Konfigurationsschritte, die Ihre neue RCCMD-Installation unter Linux, Windows und MAC gegen versehentliches Herunterfahren absichern. Achten Sie bitte darauf, dass nach den Änderungen unter Systemstatus RCCMD auf „läuft“ steht.

7. Die RCCMD Screens im Detail erklärt

Dieser Abschnitt geht noch einmal auf alle Screens im Detail ein und erklärt Ihnen, wann Sie wo welche Screens finden und konfigurieren können. Beachten Sie bitte, dass eventuelle Skriptbeispiele generell für Windows-Maschinen gültig sind und ggfs. an Ihr verwendetes Betriebssystem angepasst werden müssen.

7.1: Windows / Linux /MAC - The RCCMD client configuration interface im Detail

In diesem Kapitel werden alle *CLIENT*-Konfigurationsbildschirme erläutert, die bei Verwendung einer Linux-, Windows- (Desktop, Server, Hyper-V, Core usw.), MAC/OS- oder Unix-basierten Version angezeigt werden.

7.2: Das RCCMD Appliance for VMware Configuration Interface

Dieses Kapitel erklärt alle Funktionsmenüs der RCCMD Appliance, wie sie in jeder VMware-Umgebung zu sehen sind. Beachten Sie, dass es unter „Erweiterte Optionen“ eine spezielle Funktion namens „RCCMD-Ziel ändern“ gibt. Mit dieser Funktion ist es möglich, je nach Bedarf zwischen VMWARE-Modus und Client-Modus umzuschalten.

8. Anhang

Dieses Kapitel widmet sich unter anderem speziellen Funktionen von RCCMD, die in der Standard-Anwendung keinen Platz finden und eine gewisse Erläuterung verdienen oder benötigen.

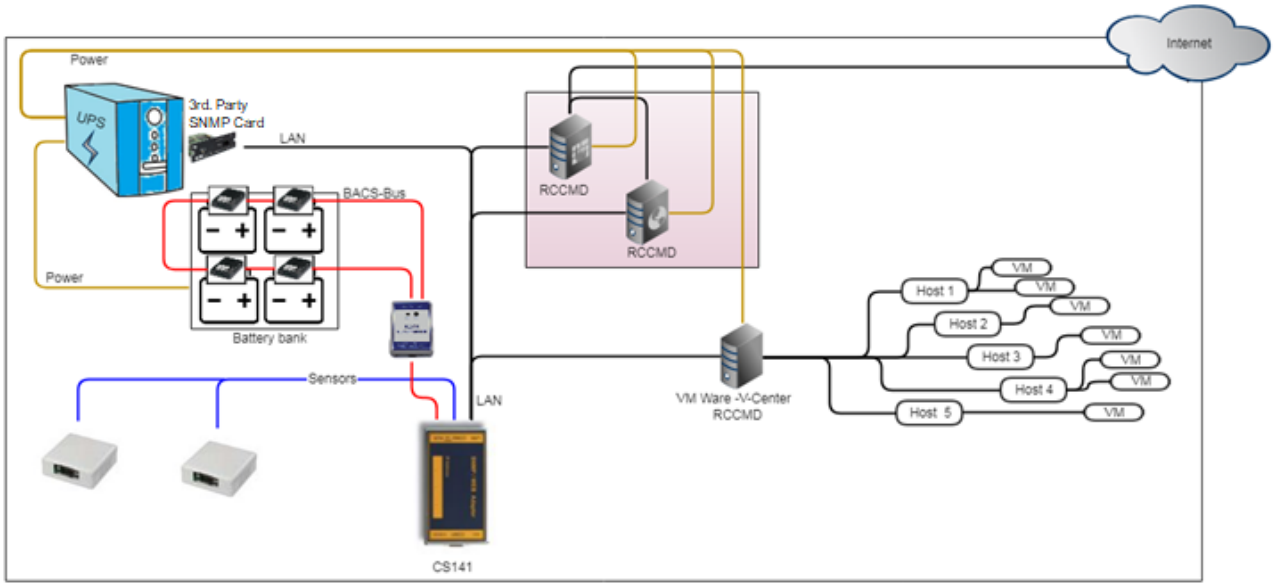
- Windows only: Das RCCM_NF Configuration Tool: RCCMD ohne Webbrowser konfigurieren
- RCCMD Security Guide
- Warum funktionieren die Heartbeats nicht mit SSL/TLS Verschlüsselung?
- Redundanzverhalten einrichten – eine Fallstudie
- Ich lese immer “Java”, ist das nicht unsicher?
- TLS ON / OFF – Warum ein RCCMD Shutdown nicht richtig kommunizieren will
- Einstieg in RCCMD mit Windows PowerShell und Hyper-V
- Glossar – wichtige Abkürzungen

9. Lizenzbedingungen und rechtliches

Dieser Abschnitt beschäftigt sich nur mit den Dingen, die sowieso niemand liest…

- Urheberrechtserklärung
- Copyrights

Allgemeine Informationen und Systemanforderungen über RCCMD



RCCMD ist darauf ausgelegt, im Notfall Ihre Systeme individuell herunterfahren. In diesem Fall wird von einem RCCMD Server – in der Regel ein UPSMan oder CS141 - ein Shutdown-Kommando an die Clients gesendet und von dem Client entsprechend umgesetzt.

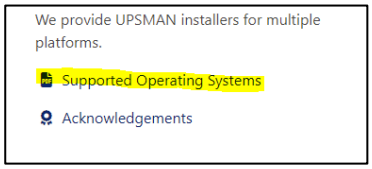
Die folgenden Ports müssen in Ihrem Netzwerk offen sein:

Port 8080	Über diesen Port wird die lokale RCCMD Weboberfläche aufgerufen
Port 8443	Über diesen Port wird die RCCMD Weboberfläche auf einem anderen Computer/Server aufgerufen
Port 6003	Über diesen Port kommuniziert der RCCMD Client

Der RCCMD Client benötigt eine feste IP-Adresse

Diese IP-Adresse muss dem RCCMD Server mitgeteilt werden, damit ein eindeutiges Kommando gesendet werden kann. Wenn sich die IP-Adresse dynamisch ändert oder in Notsituationen kein DHCP-Server vorhanden ist, kann auf diese Weise RCCMD auch direkt angesprochen werden.

Generell Unterstützte Betriebssysteme



RCCMD unterstützt mit wenigen Ausnahmen nahezu jedes am Markt verfügbare Betriebssystem auf Basis von Unix / Linux, Windows und zahlreiche Versionen von MAC/OS und ist als spezielle Version für AS400 verfügbar. Eine genaue Liste aller unterstützten Betriebssysteme finden Sie im Downloadbereich bei der Auswahl des jeweiligen Installers. Sollte Ihr Betriebssystem oder Derivat nicht aufgeführt sein, wenden Sie sich bitte an unseren technischen Support unter support@generex.de – Unser technischer Support beantwortet gerne alle Ihre Fragen.

Benötigte VMware Version für die Appliance:

VMware 6.7 - 7.X – basierte Systeme

Die offiziell zum Download verfügbare Appliance benötigt die VMware Version 6.7 oder höher. Ältere Versionen werden vom offiziellen Download nicht unterstützt. Die Appliance können Sie im Downloadbereich unter www.generex.de direkt herunterladen.

Auf Anfrage verfügbare Legacy-Versionen der Appliance für VMware:

VMware 6.x

Für diese Systeme gibt es eine spezielle Legacy-Version der Appliance, welche speziell auf die Bedürfnisse für den Betrieb ab VMware 6.5 zugeschnitten sind. Die Appliance unterstützt ebenso die mit 6.7 eingeführte vSAN – Funktion von VMware. Installation und Konfiguration sind wie unten beschrieben ausführbar (ggfs. kommt es zu leichten Abweichungen .in der Menüsteuerung.

VMware 5.x / 6.0

Diese älteren Systeme verwenden noch den Virtual Media Assistant von VMware, welcher exklusiv im Downloadbereich von VMware verfügbar ist. Nach dem Ausrollen der VMA kann per ftp eine spezielle RCCMD Version für VMware hochgeladen und installiert werden.

Sollten Sie eine ältere Version von RCCMD benötigen, hilft Ihnen unser technischer Support unter support@generex.de gerne weiter.

Installation: RCCMD für VMware 6.5 - 8.X

Installation auf einem ESXi Host

Some typical installation Problems:

During testing, everything worked very well, but now …

Überprüfen Sie die Lizenz Ihres ESXi-Hosts. Wenn Sie bei der Einrichtung einen Evaluierungsschlüssel für den ESXi-Host verwendet haben, haben Sie möglicherweise einige kommerzielle Funktionen konfiguriert. Hat man den kostenlosen Key dann importiert, kommen plötzlich seltsame Fehlermeldungen oder der Host fährt nicht mehr herunter.

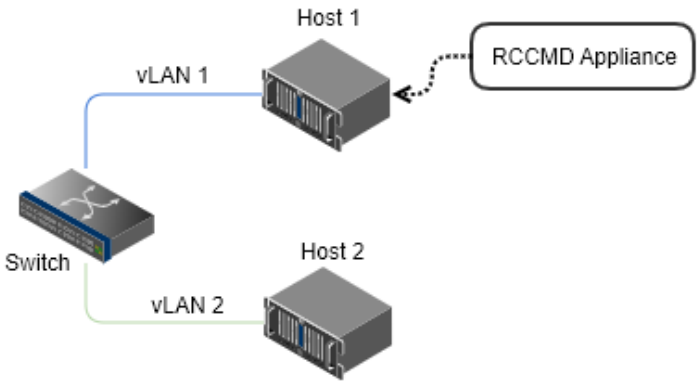
Prüfen Sie auch, ob Sie im RCCMD den richtigen Schlüssel eingetragen haben. Grundsätzlich ist die RCCMD Appliance mit einem Evaluierungsschlüssel ausgestattet, der jederzeit über das Webinterface geändert werden kann. Wenn der Testzeitraum abgelaufen ist, wird RCCMD den Dienst einstellen. Wenn Sie einen falschen oder ungültigen Schlüssel eingeben, wird automatisch die Evaluierungsphase aktiviert.

Manchmal läuft der eine RCCMD, dann er andere, …

Dies passiert immer dann, wenn Sie versehentlich einen RCCMD-Keys mehrfach eingegeben haben: In diesem Fall wird beim Start des Netzwerks der erste RCCMD, der mit einem betroffenen Schlüssel startet, diesen für sich beanspruchen. Nachfolgende RCCMD-Clients werden jedoch wieder mit einem entsprechenden Protokolleintrag „Licence fraut <IP-Adresse>“.

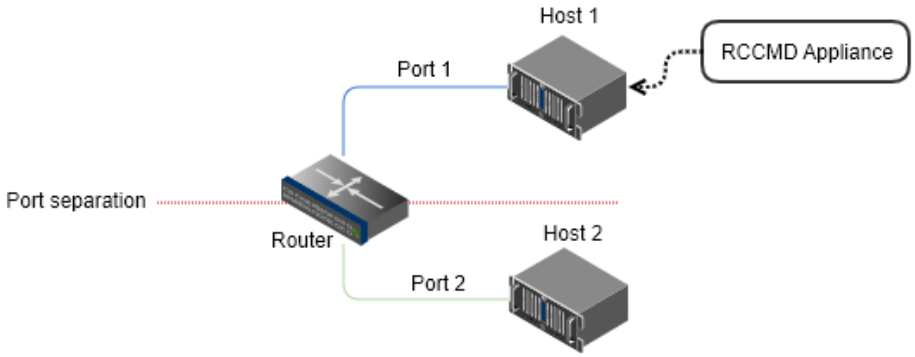
Typische Netzwerkprobleme, …

vLAN in use:

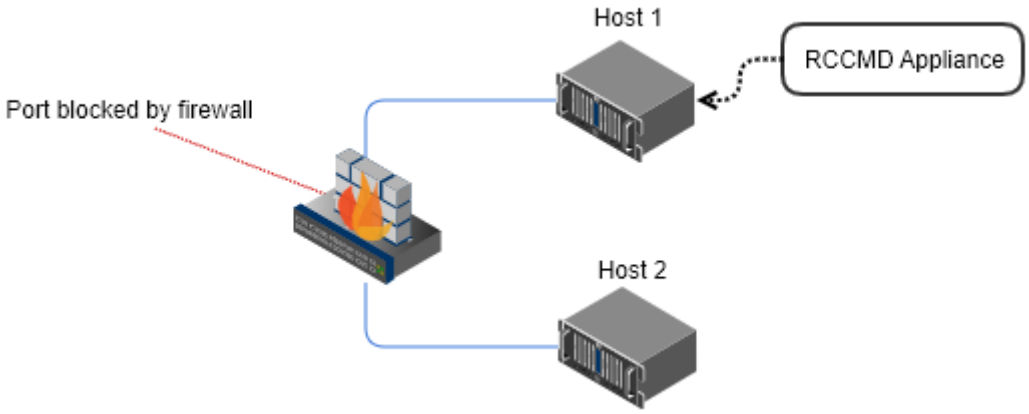


Auch wenn sich beide Hosts auf demselben Switch befinden, müssen sie, da die Ports über vLAN getrennt sind, als zwei separate Netzwerke betrachtet werden.

Port separation and/or missing routing:



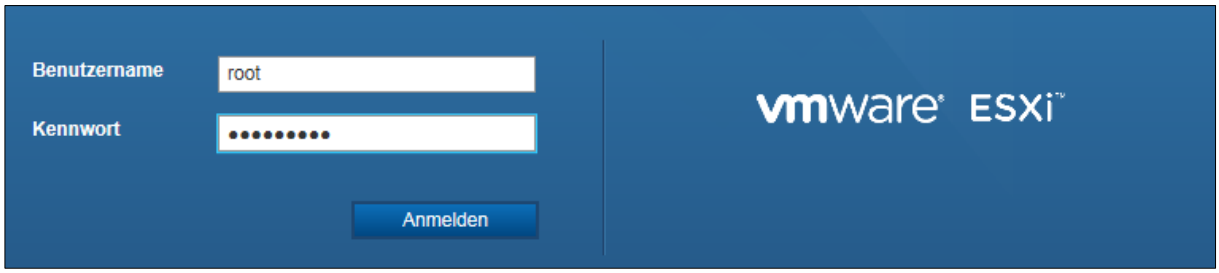
Diese Konfiguration ist durchaus üblich, wenn sich Server in unterschiedlichen Netzwerksegmenten befinden, und z. B. eine Uplink-Leitung zu einem neutralen dritten Netzwerksegment mit Internetanbindung besteht. Der Router benötigt spezielle Routing-Einträge, um zwischen den Netzen vermitteln zu können.



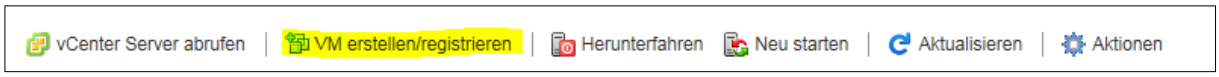
Eine Firewall oder intelligente Intrusion Detection kommt zum Schluss, dass RCCMD keine interne Freigabe hat, und lehnt die Kommunikation ab. Folglich kann RCCMD Host 2 nicht erreichen. Sehr große Netzwerke verwenden hier gerne auch mehrstufige oder modulare Firewall-Konzepte. Prüfen Sie, ob die Firewall-Einstellungen angepasst werden müssen. Kleinere Systeme hingegen können diese Probleme bekommen, wenn z. B. gleichzeitig eine lokale Firewall und eine zusätzliche Internet-Sicherheitssoftware im Einsatz sind.

RCCMD – Die VM aufsetzen:

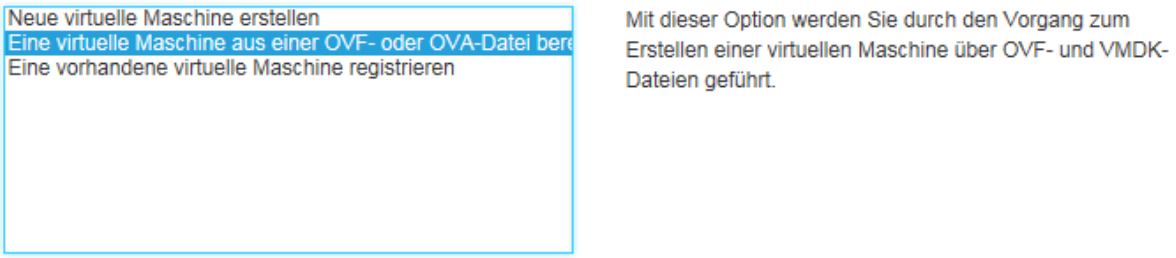
Melden Sie sich mit entsprechenden Rootrechten bei Ihre ESXi Host an:



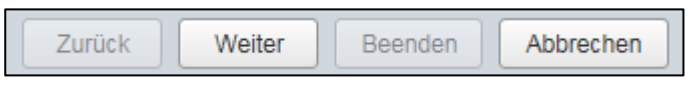
Nach dem erfolgreichen Anmelden erstellen Sie eine neu VM – Bei ESXi 6.5 finden Sie den dazugehörigen Reiter in der Regel in der oberen Leiste:



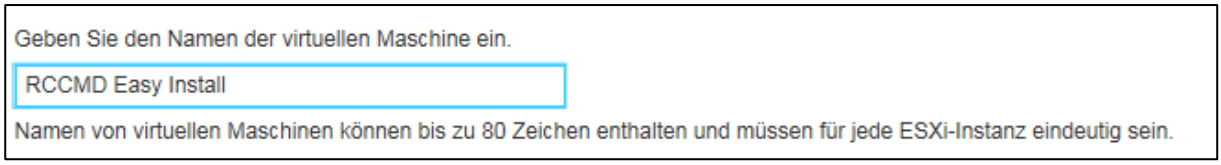
Wählen Sie anschließen die folgende Option:
Eine virtuelle Maschine aus einer OVF- oder OVA-Datei bereitstellen:



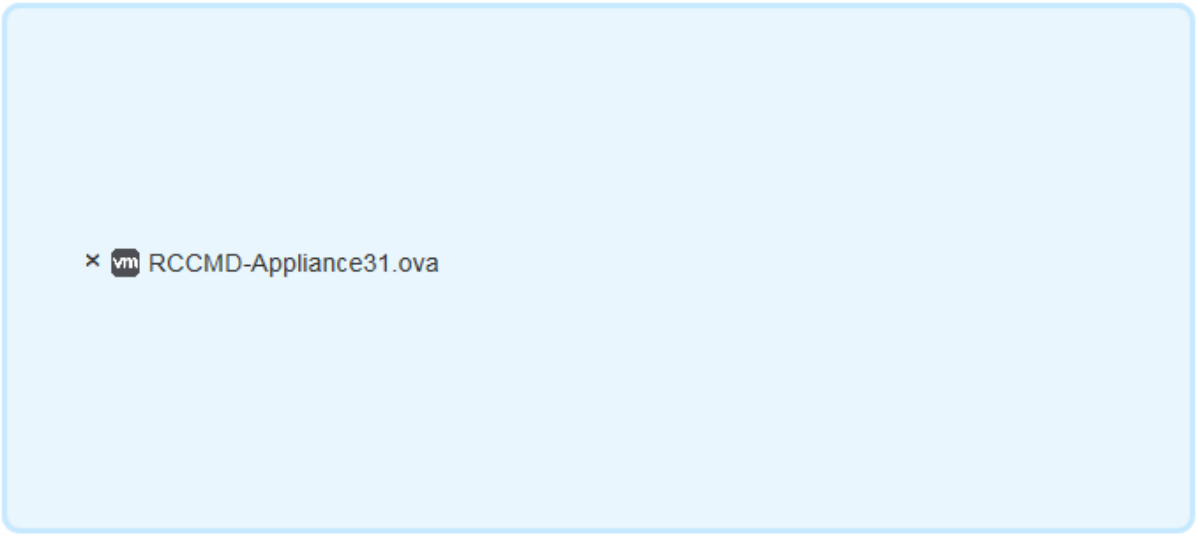
Klicken Sie anschließend unten auf weiter:



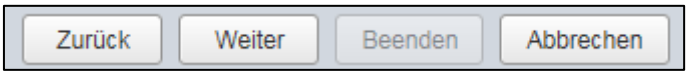
Geben Sie anschließend Ihrer neuen RCCMD – Maschine einen eindeutigen Namen:



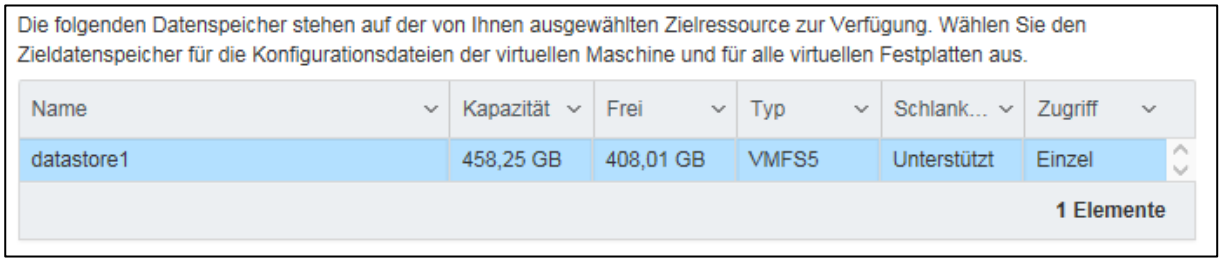
Ziehen Sie anschließend die OVA – Datei per Drag'n'Drop in das notwendige ESXi – Host Fenster…



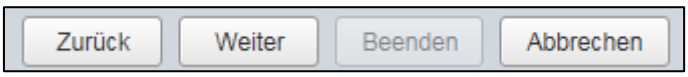
… und klicken Sie auf weiter:



Die OVA-Datei ist vorkonfiguriert, dass bedeutet, sie müssen keine weiteren Einstellungen vornehmen:

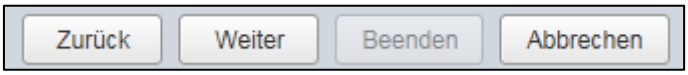


Daher klicken Sie einfach auf weiter:



Die Netzwerkzuordnung ist für RCCMD wichtig, da die Verwaltung von einem RCCMD-Server aus geht, welche den RCCMD-Client über das lokale Netzwerk erreichen können muss. In der Regel können Sie die Einstellungen „so“ übernehmen:

Gleiches gillt für Festplattenzuordnung. Die RCCMD OVF – Datei ist so vorkonfiguriert, dass in der Regel keine Änderungen in den Einstellungen vorgenommen werden muss.
Wenn Sie die Einstellungen gemäß Ihren Vorstellungen vorgenommen haben, klicken Sie auf weiter, um zum nächsten Schritt zu gelangen:



Im letzten Schritt wird Ihnen noch einmal die von Ihnen getroffenen Einstellungen angezeigt:

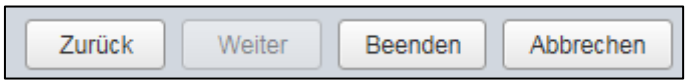
Produkt	RCCMD-Appliance
VM-Name	RCCMD Easy Install
Festplatten	RCCMD-Appliance31-disk1.vmdk
Datenspeicher	datastore1
Bereitstellungstyp	Thin
Netzwerkzuordnungen	bridged: VM Network
Name des Gastbetriebssystems	Unbekannt

Beachten Sie ins Besondere diesen Hinweis:

Aktualisieren Sie Ihren Browser nicht während der Bereitstellung dieser VM.

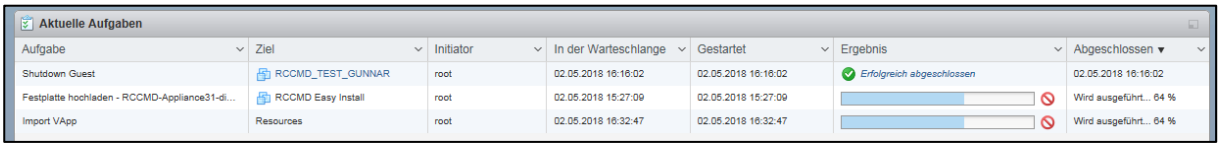
VMware reagiert auf Browseraktualisierungen sehr empfindlich. Sollten Sie den Browser zu früh aktualisieren, wird die Installation abgebrochen, was die virtuelle Maschine unbrauchbar macht.

Mit Beenden starten Sie den Installationsvorgang:



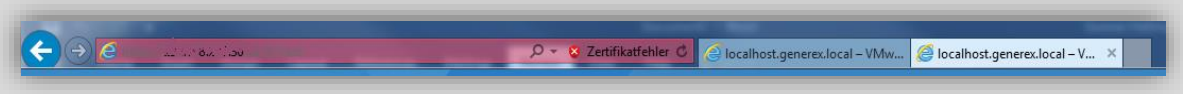
Die automatische Installation

Im unteren Statusfenster können Sie unter Aktuelle Aufgaben nun beobachten, wie RCCMD installiert wird:



Warten Sie, bis die Installation vollständig abgeschlossen ist, bevor Sie dieses Browserfenster aktualisieren.

Tipp:

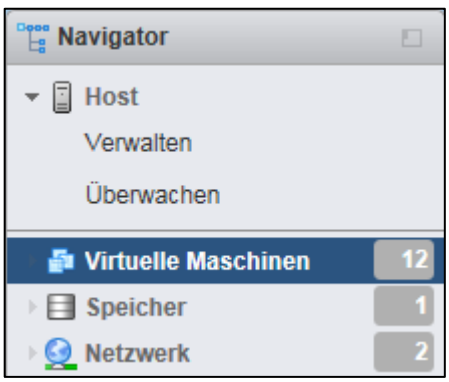


Um weiterarbeiten zu können, verwenden Sie sog. Tabbed Browsing, das System wird Sie automatisch als root anmelden. Das erlaubt Ihnen am System weiterzuarbeiten, während Sie auf die Installation warten.

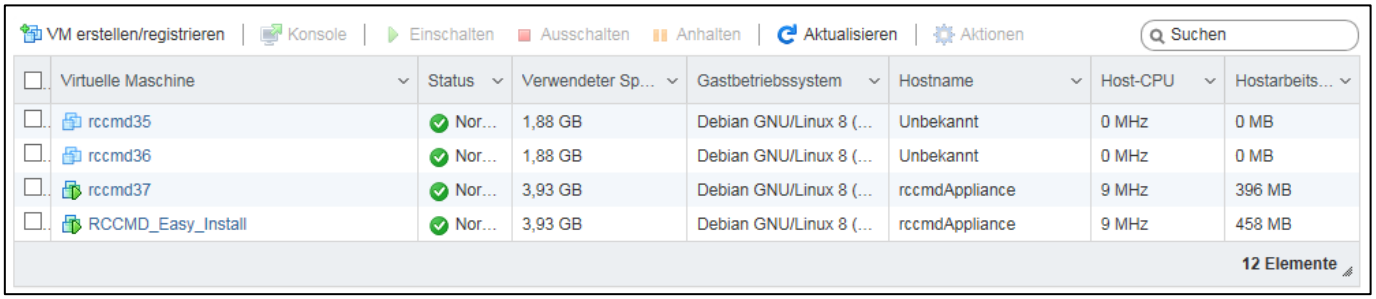
Installationsfortschritt verfolgen

Öffnen Sie den Navigator auf der linken Seite und klicken Sie auf Virtuelle Maschinen. Die von Ihnen erstellte Maschine sollte hier aufgeführt sein.

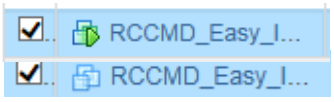
In diesem Installationsbeispiel hat die Maschine den folgenden Namen:



Die virtuellen Maschinen werden entsprechend aufgelistet. Als Grundeinstellung ist die von Ihnen zuletzt eingerichtete Maschine der letzte Eintrag am unteren Ende der Liste:



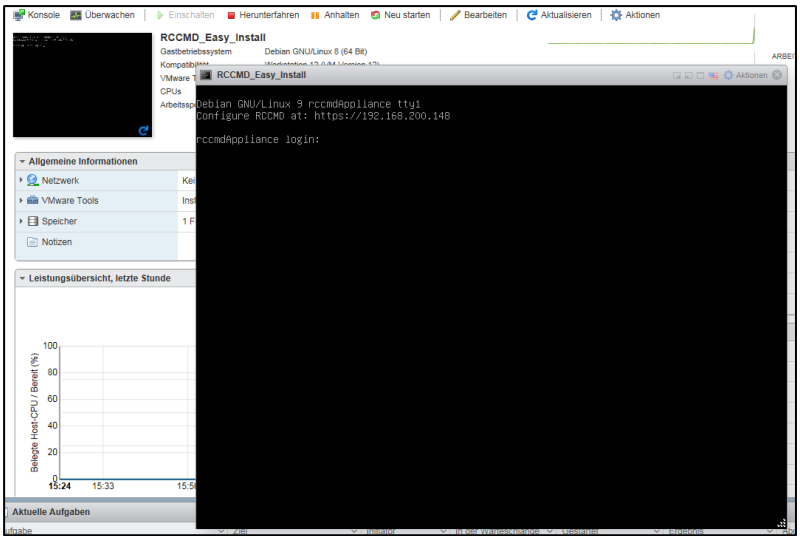
Vergewissern Sie sich, dass die virtuelle Maschine gestartet ist. Sie erkennen den aktuellen Zustand an den Symbolen:



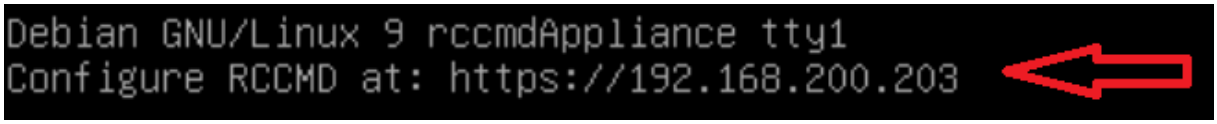
Die Maschine eingeschaltet und läuft

Die Maschine ist ausgeschaltet

Klicken Sie auf die von Ihnen installierte virtuelle Maschine, um genauere Informationen zu erhalten. Wenn Sie auf den Konsolenscreenshot drücken, öffnet sich die Webkonsole für die virtuelle Maschine erhalten:



Wenn Ihr System einen DHCP-Server verwendet, wird Ihnen an dieser Stelle bereits die IP-Adresse angezeigt, die Ihre neue RCCMD-Installation erhalten hat:



Sollte dies nicht der Fall sein, ist es notwendig, manuell eine IP-Adresse zu zuweisen. Hinweise hierzu finden Sie im Anhang unter IP-Adresse manuell zuweisen.

Konsolen-Login nach der Installation:

Sie können sich direkt über die Webkonsole an der RCCMD Appliance anmelden:

Nutzer: admin

Passwort: RCCMD

Rootrechte erlangen

Die VMware Appliance basiert auf einem Linux Debian 9 - Die Rootrechte erlauben das manuelle Nachinstallieren von offiziellen Packen sowie die Konfiguration der Netzwerkschnittstelle.

Befehl: sudo su

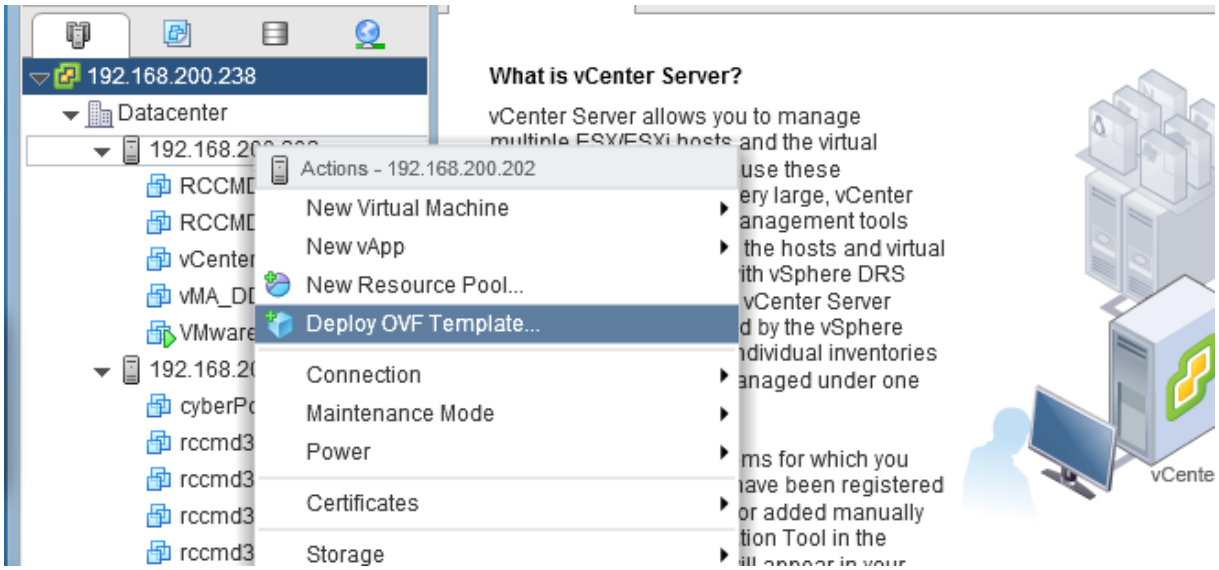
Beachten Sie, dass der Nutzer admin in der Grundeinstellung keine erhöhten Systemrechte bekommen hat, um Änderungen durchführen zu können – Sie müssen mit sudo su sich erhöhte Systemrechte zuweisen.

```
admin@rccmdAppliance:~$ sudo su
[sudo] password for admin:
root@rccmdAppliance:/home/admin#
```

Die Installation der RCCMD Appliance ist hiermit abgeschlossen. Weitere Konfiguration wird über das Webinterface durchgeführt. Informationen über die manuelle Vergabe einer IP-Adresse finden Sie im Anhang dieses Handbruchs.

Installation bei einem vCenter

Starten Sie mit Deploy OVF Template… die Installation der RCCMD Appliance über ein VCenter:



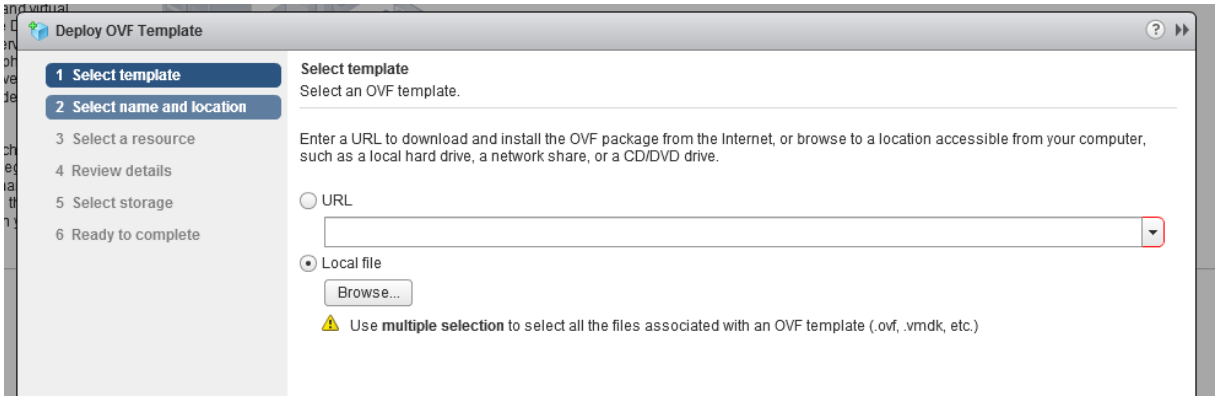
Im ersten Schritt wählen Sie die notwendige Datei aus. Hierzu stehen zwei Möglichkeiten zur Verfügung:

URL:

Sollte die OVF-Datei über eine Web-Ressource zur Verfügung stehen, geben Sie den entsprechenden Pfad an.

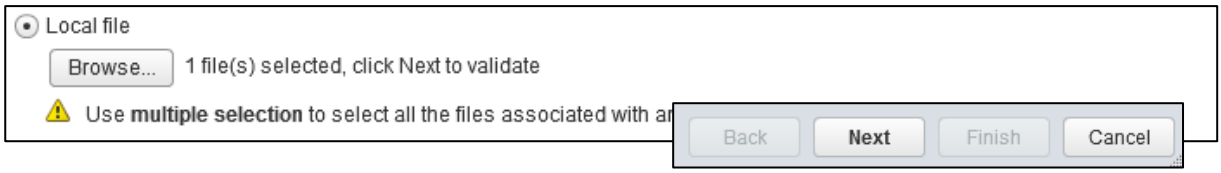
Local File

Sollten Sie die OVF-Datei als lokale Datei gespeichert haben, wählen Sie die die Datei direkt aus.

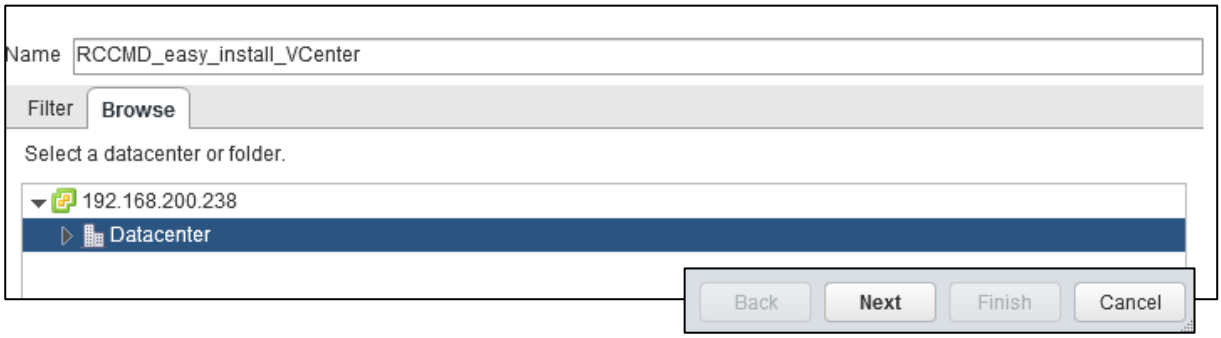


In diesem Installationsbeispiel wird die lokal gespeicherte Datei verwendet:

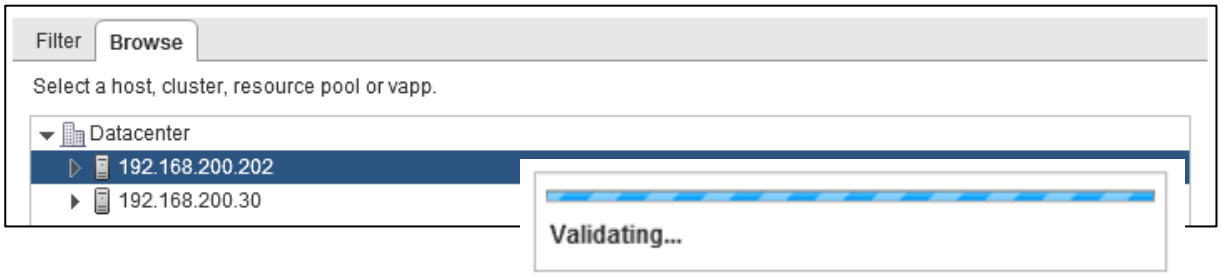
Nachdem Sie die lokale Datei ausgewählt haben, drücken Sie Next, um zum nächsten Installationsschritt zu gelangen:



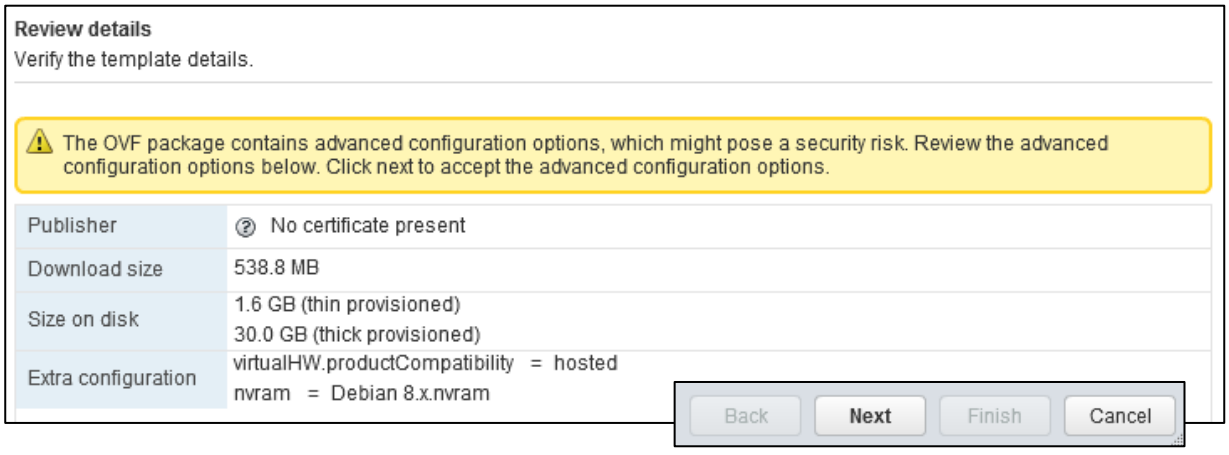
Im nächsten Schritt werden Sie aufgefordert, der VM einen eindeutigen Namen zu geben. Dieser Name wird bei der späteren Konfiguration von RCCMD benötigt. Mit Next schließen Sie diesen Konfigurationsschritt ab.



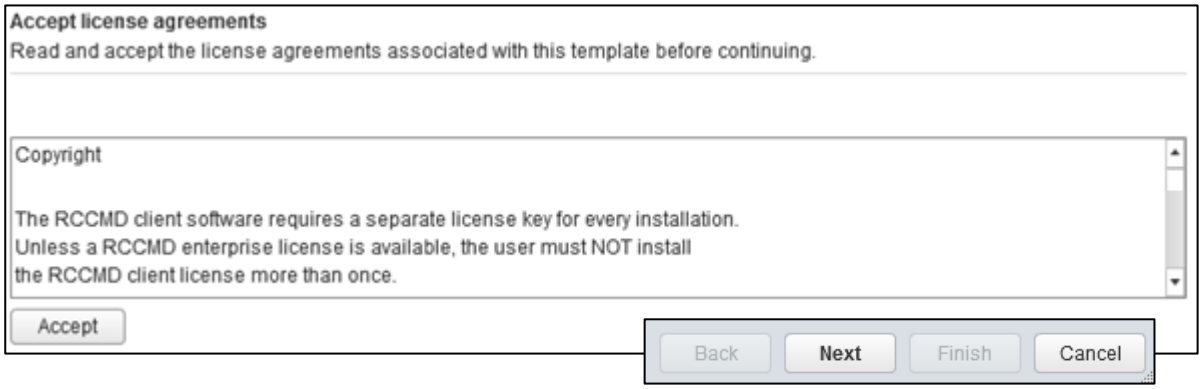
Wählen Sie in diesen Schritt den Zielhost aus, auf dem die VM installiert werden soll.



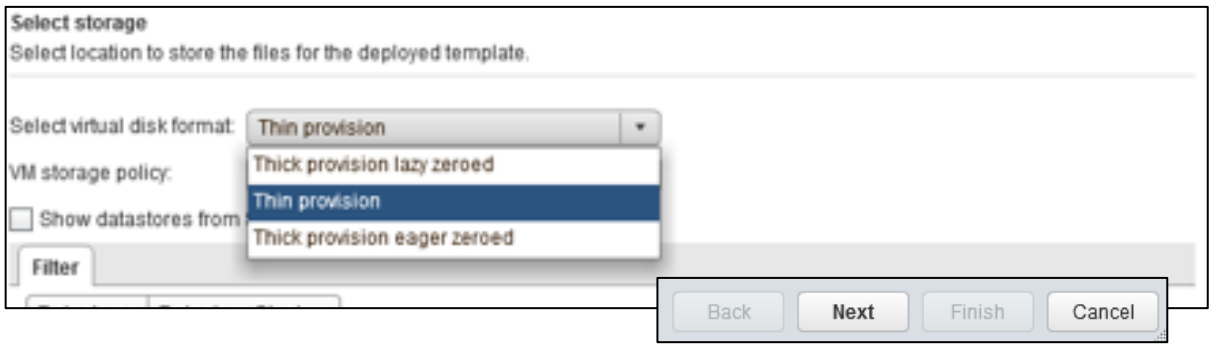
Im nächsten Schritt wird Ihnen noch einmal eine Übersicht der von Ihnen gewählten Einstellungen gezeigt.



Bitte beachten Sie, dass Sie die Copyright-Bedingungen mit Accept bestätigen müssen, bevor Sie die mit der Installation fortfahren können. Der Next-Button wird nicht funktionieren, solange dies nicht geschehen ist.

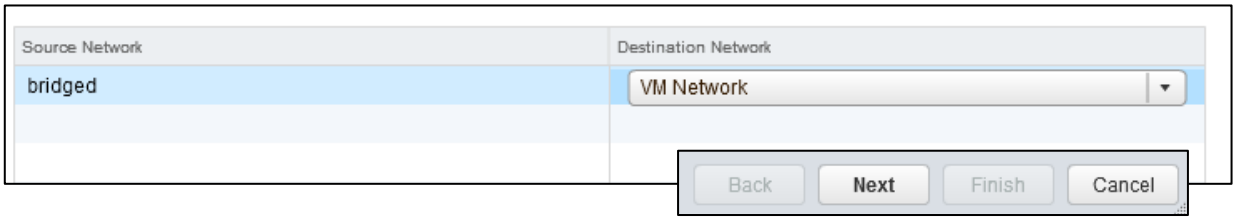


Die Festplattennutzung kann je nach Konfiguration Ihres Systems abweichen: Wenden Sie sich für die korrekte Angabe an Ihren lokalen Systemadministrator.



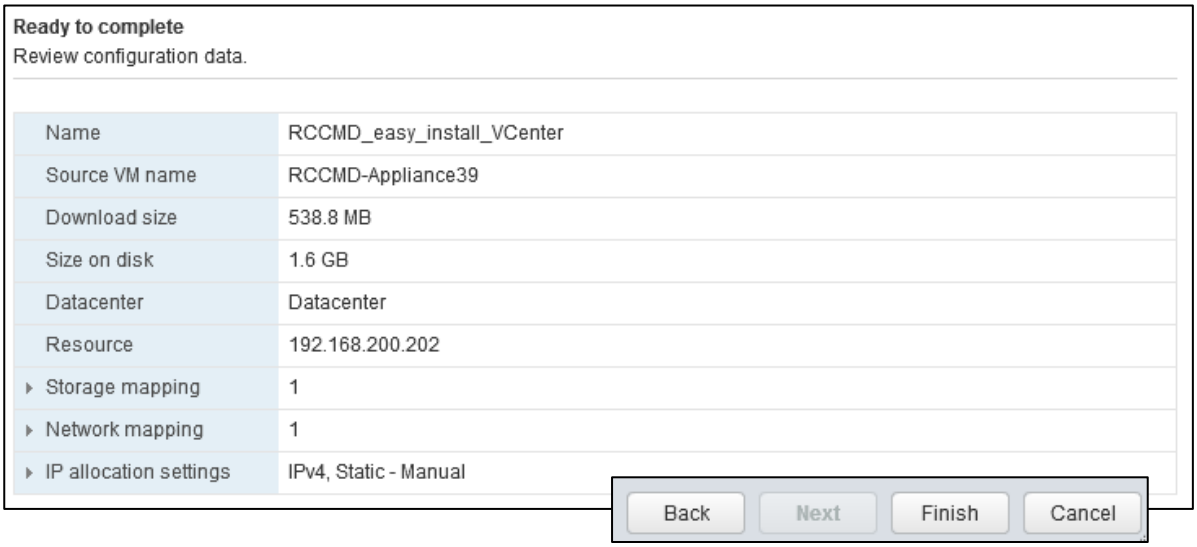
Wenn Sie sich bei den Einstellungen nicht sicher sind und keinen Administrator konsultieren können, wählen Sie bitte Sie bei der Festplattenbelegung Thin und none aus.

Die Appliance benötigt einen Zugang zum Netzwerk. Die korrekte Einstellung erfahren Sei von Ihren lokalen Systemadministrator.



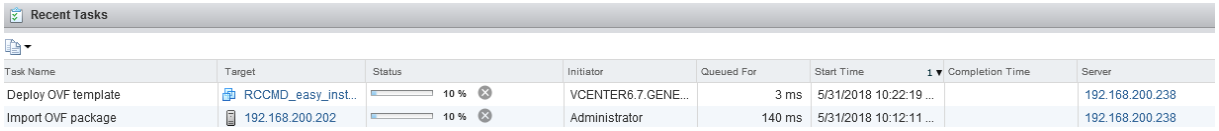
Im Zweifelsfall wählen Sie zunächst VM Network im bridged mode aus. In diesem Installationsbeispiel ist VM Network gewählt, um die VM mit dem Netzwerk korrekt zu verbinden.

Im letzten Schritt wird Ihnen noch einmal eine Übersicht über Ihre Konfiguration gezeigt. Wenn die Einstellungen Ihren Vorstellungen entsprechen, beenden Sie mit Finish den Konfigurationsdialog und RCCMD wird automatisch die Installation beginnen.

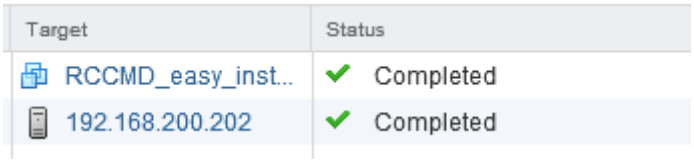


Installationsfortschritt verfolgen:

Unter Recent Tasks können Sie den aktuellen installationsfortschritt verfolgen:

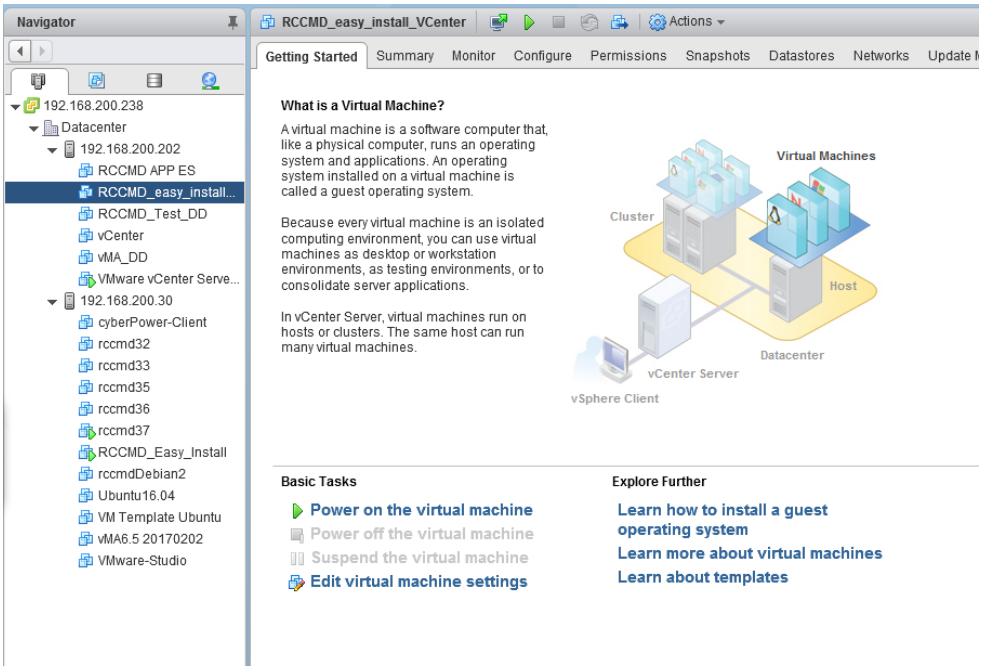


Warten Sie, bis der Status mit Completed beendet wurde:



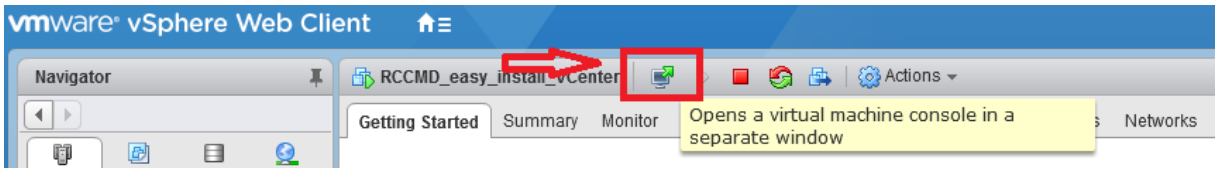
Starten der VM und Konsolenzugriff über VCenter

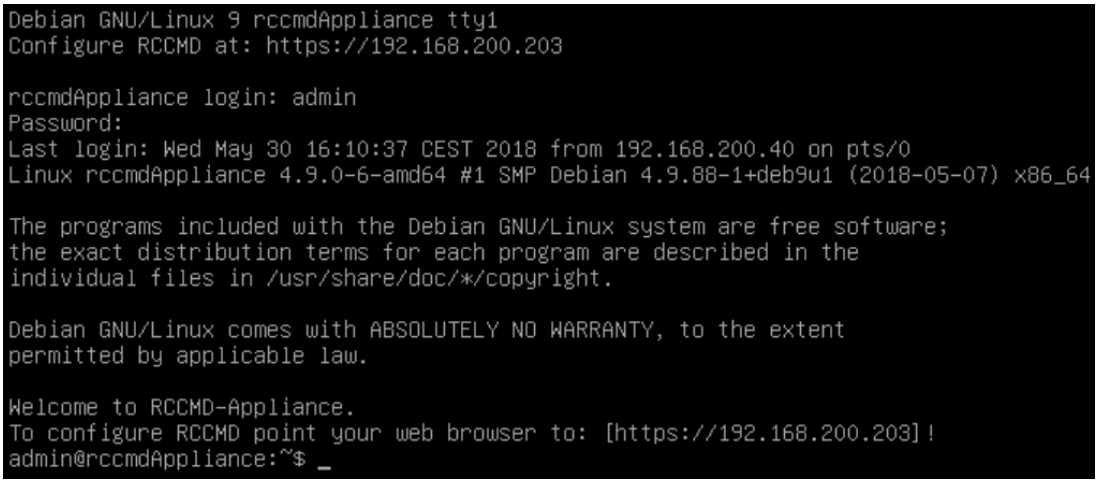
Suchen Sie im Navigator die entsprechende VM und betätigen Sie Power on the virtual machine:



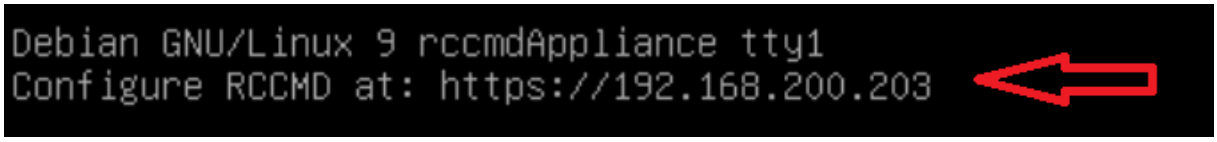
Konsolenlogin nach der Installation

Nachdem die VM erfolgreich gestartet ist, können Sie über das Konsolenmenü von VCenter direkt auf die Konsole zugreifen:





RCCMD benötigt für den Webzugriff und die Konfiguration über den Webclient eine gültige IP-Adresse. Sollte DHCP zur Verfügung stehen, wird diese IP-Adresse Ihnen am oberen Konsolenfenster direkt nach dem Öffnen präsentiert:



Sollte die IP-Adresse nicht angezeigt werden, ist eventuell eine manuelle Konfiguration der IP-Adresse notwendig, eine Konfigurationsanleitung finden Sie als Tutorial in diesem Kapitel.

Konsolen-Login nach der Installation:

Sie können sich direkt über die Webkonsole an der RCCMD Appliance anmelden:

Nutzer: admin

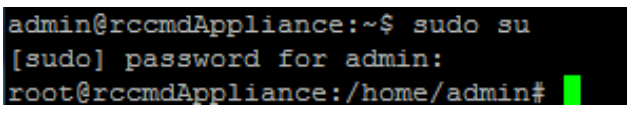
Passwort: RCCMD

Rootrechte erlangen

Die VMware Appliance basiert auf einem Linux Debian 9 - Die Rootrechte erlauben das manuelle Nachinstallieren von offiziellen Packen sowie die Konfiguration der Netzwerkschnittstelle.

Befehl: sudo su

Beachten Sie, dass der Nutzer admin in der Grundeinstellung keine erhöhten Systemrechte bekommen hat, um Änderungen durchführen zu können – Sie müssen mit sudo su sich erhöhte Systemrechte zuweisen.



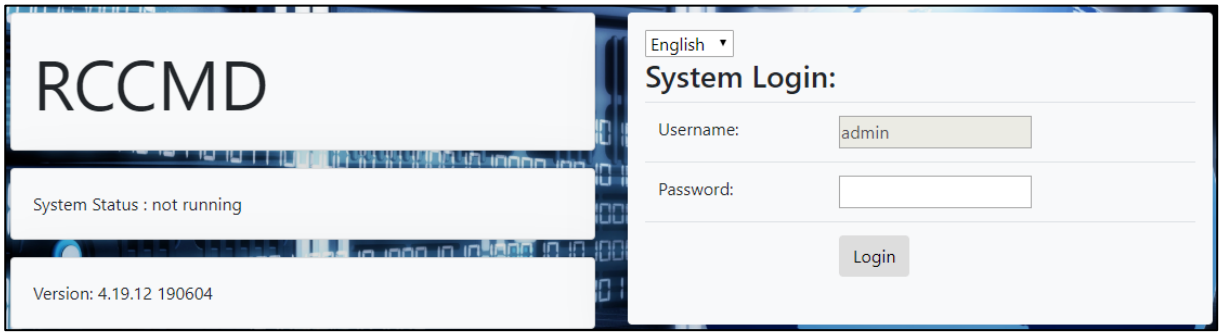
Die Installation der RCCMD Appliance ist hiermit abgeschlossen. Weitere Konfiguration wird über das Webinterface durchgeführt. Informationen über die manuelle Vergabe einer IP-Adresse finden Sie im Anhang dieses Handbuchskapitels.

Schnellkonfiguration von RCCMD

Dieser Abschnitt gibt Ihnen einen Überblick über die wesentlichen Einstellungen, welche für den Betrieb von RCCMD benötigt werden, wenn Sie einen oder mehrere Hosts betreiben. Voraussetzung für diesen Konfigurationsabschnitt ist, dass die Appliance erfolgreich ausgerollt wurde.

Login auf der Webkonsole

Öffnen Sie einen Webbrowser und geben Sie dort folgendes ein:
https://<IP-Adresse aus dem Konsolenfenster>



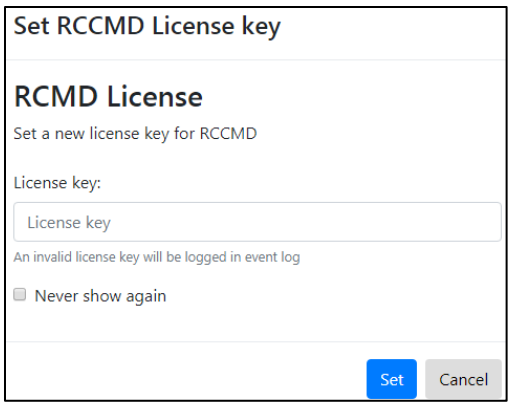
Die Standard-Zugangsdaten lauten:

Nutzer: admin
Passwort: RCCMD

Bevor Sie mit der Konfiguration beginnen können, müssen Sie die Nutzungsbedingungen akzeptieren, da diese für die Verwendung dieser Software zwingend notwendig sind:

Lesen Sie sich die Endnutzerbedingungen durch und klicken Sie im Anschluss auf den Accept-Button.

Im nächsten Dialog werden Sie aufgefordert, Ihren Lizenz Key einzugeben:



Sollten Sie keinen Key zur Verfügung haben, können Sie diesen später über die Weboberfläche nachträglich unter *Adcanced Settings* aktualisieren. Ohne Key startet RCCMD zunächst mit einem eigenen 30-tägigen Evaluations-Key, so dass Sie Ihre Installation zunächst konfigurieren können.
Beachten Sie bitte folgendes:

1. Es kann nur einen Key geben

   Sie können innerhalb einer Installation beliebig viele RCCMD-Keys verwenden. Ein Key darf jedoch nur einmal in der Installation vorkommen. Sollten Sie einen Key doppelt vergeben haben, wird bei einem Systemstart die Installation aktiv, welche den RCCMD-Client zuerst online gebracht hat. Der nächste RCCMD Client, der diese Lizenz verwenden will, wird sich mit einem entsprechenden Logeintrag beenden:

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

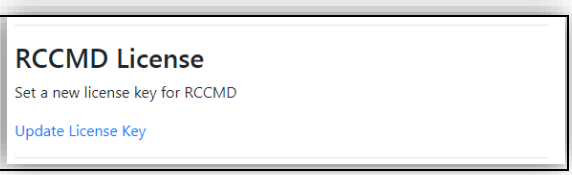
   Sollten Sie einen Key verwenden, welcher für eine bestimmte Anzahl von Installationen gültig ist, werden mit dem entsprechenden Key so viele Installationen aktiv, bis diese Zahl erreicht wurde.

2. Kein Key startet die Testversion

   Wenn Sie jetzt den Key nicht zur Hand haben oder das Produkt testen möchten, lassen Sie den Key einfach weg. In diesem Fall wird RCCMD davon ausgehen, dass es sich zunächst um eine voll funktionsfähige Testinstallation handelt und auf einen 30 Tage Evaluations-Key zurückgreifen.

Tipp

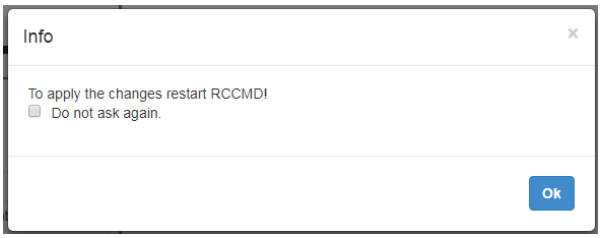
RCCMD bietet Ihnen innerhalb der Webkonsole einen Dialog an, über den Sie zu einem späteren Zeitpunkt den Key ändern oder anpassen können: Öffnen Sie hierzu das Menü *Advanced Settings* und klicken Sie auf *Update License Key*



Hinweis: Neustart des RCCMD-Clients nach wesentlichen Änderungen:

Während der Konfiguration von RCCMD ist immer wieder ein Neustart des Dienstes notwendig:

Wann Immer eine Änderung an der Konfiguration durchgeführt wurde, ist es zwingend notwendig, den RCCMD Service neu zu starten, da ansonsten die Daten zwar gespeichert, jedoch nicht in die aktive Konfiguration übernommen werden. Wenn Sie *Do not ask again* – Funktion aktivieren, wird RCCMD Sie künftig nicht mehr über einen notwendigen Restart informieren.



Absichern der RCCMD Appliance

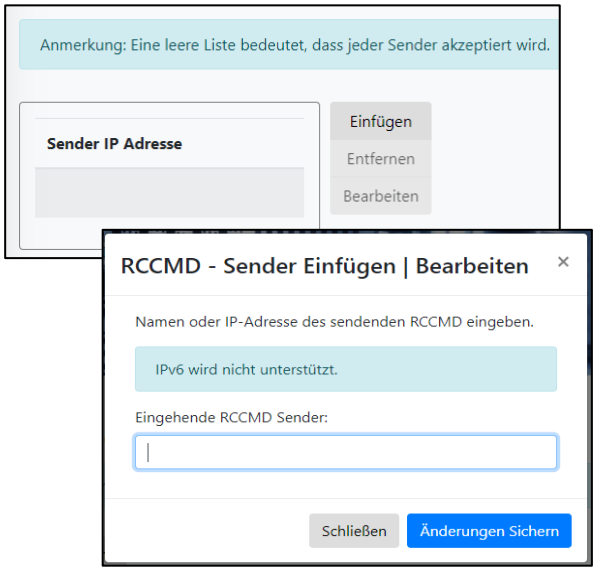
Menü: Verbindungen

Absichern gegen versehentliches Herunterfahren

Aktuell kann jeder RCCMD-Sender einen Shutdown auslösen, der eingeleitet nicht mehr zurückgenommen werden kann. Der RCCMD Client bietet Ihnen daher an, diese Befehle auf bestimmte Sender einzugrenzen.

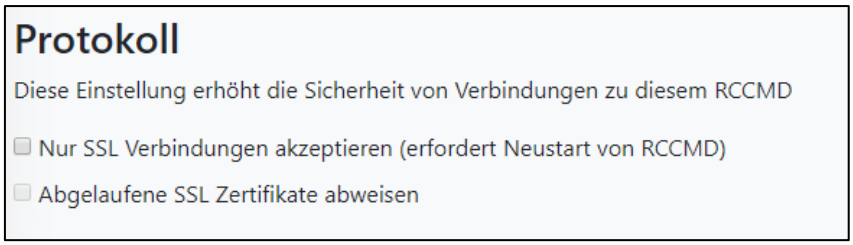
Klicken Sie hierzu unter Optionen auf *Connections*, um den entsprechenden Dialog zu öffnen. Mit *Insert* können Sie eine neue IP-Adresse hinzufügen:

Geben Sie anschließend eine IP-Adresse an, welche ausdrücklich berechtigt ist, einen RCCMD
Shutdown zu senden.



Verschlüsselung aktivieren

Wenn Sie in Ihrem Netzwerk ausschließlich SSL-Verschlüsselung verwenden, können Sie RCCMD anweisen, ausdrücklich SSL-Verschlüsselung zu benutzen.



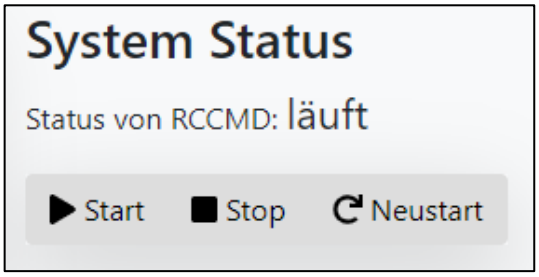
Aktivieren Sie hierzu Accept only SSL connections.

Wenn Sie nur aktuelle Zertifikate verwenden, können Sie zudem RCCMD anweisen, veraltete Zertifikate generell abzulehnen. Mit Save Changes wird die IP-Adresse in die
Liste übernommen:

RCCMD Status überprüfen

Menü: Status

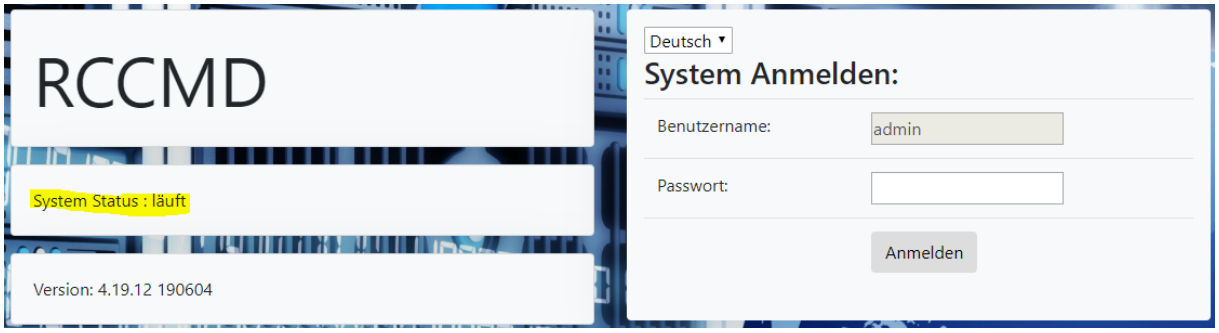
Klicken Sie anschließend auf Systemstatus und betätigen Sie noch einmal Restart. Unter *Current status of RCCMD* können Sie den aktuellen Betriebszustand erkennen.



Folgende Statusmeldungen zeigen den aktuellen RCCMD-Zustand:

angehalten	RCCMD-Dienst ist aktuell nicht aktiv.
läuft	RCCMD-Dienst ist aktiv

RCCMD Status auf der Anmeldemaske

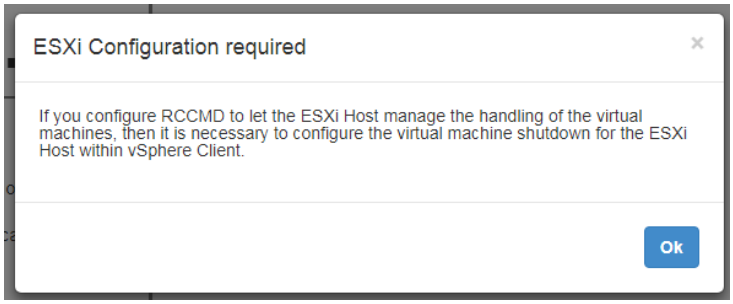


Der aktuelle Systemstatus wird nach dem Abmelden auf der Anmeldeseite von RCCMD angezeigt. So können Sie ohne Anmeldung überprüfen, ob RCCMD grundsätzlich richtig funktioniert.

Übergeben der Shutdownkontrolle an RCCMD bei der Verwendung eines Single Hosts

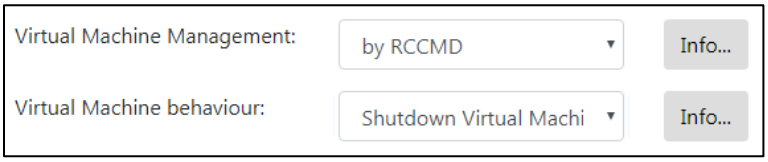
Menü: VMware Settings

Klicken Sie auf *VMware Settings*: Wenn Sie noch keine Einstellungen vorgenommen haben, werden Sie von RCCMD darauf hingewiesen, dass RCCMD zusätzliche Informationen benötigt:



RCCMD ist zwar als virtuelle Maschine installiert und bereits einsatzbereit, kann jedoch noch nicht seine eigentliche Funktion erfüllen, da die notwendigen Zugangsberechtigungen noch nicht hinterlegt sind. Bestätigen Sie diesen Hinweis mit OK, um die VMware Einstellungen zu öffnen:

Wenn ein Single Host im Einsatz ist, können virtuelle Maschinen ausgeschaltet werden, bevor der ESXi-Host selber heruntergefahren wird.

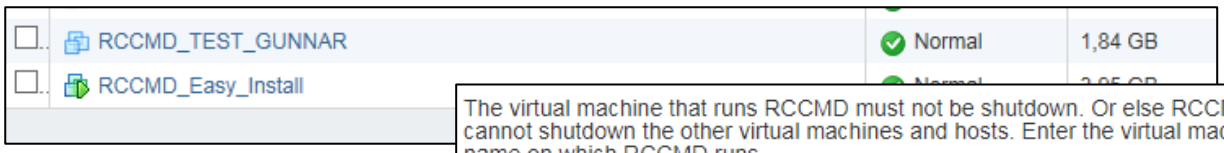


Tipp

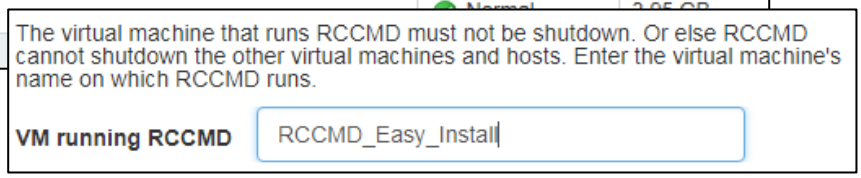
Die reguläre Shutdownroutine sieht vor, dass die virtuellen Maschinen beendet werden und der Host selber danach herunterfährt.

Dabei wird in der Shutdown duration lediglich das Zeitfenster definiert, dass die virtuellen Maschinen haben, um unmittelbar nach dem Eingang des RCCMD Shutdown Signals herunterzufahren. Der Maintenance Mode timeout definiert das Zeitfenster, die RCCMD vMotion einräumt, bevor die reguläre Shutdownroutine der Hosts greift. Der Maintenance Mode im shutdown behaviour kann somit auch verwendet werden, um unterschiedliche Hosts zeitverzögert herunterzufahren.

Wählen Sie hierzu bei Virtual Machine Management by RCCMD aus und als Virtual Machine behaviour Shutdown Virtual Machines- Um zu verhindern, dass RCCMD sich selber herunterfährt, muss der VMware-Host wissen, wie die Maschine heißt, auf dem der RCCMD Client selber läuft:



… auf dem ESXi …



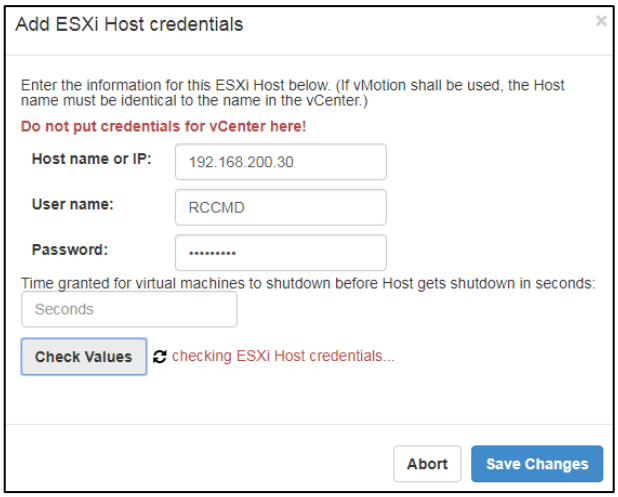
… im RCCMD Client

RCCMD benötigt zudem folgende Informationen:

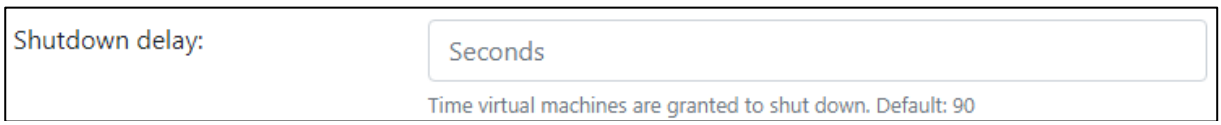
HOST/IP-Name
Im Normalfall empfehlen wir hier die IP-Adresse des ESXi - Hosts zu verwenden. Siekönnen jedoch auch den Hostnamen selber eintragen.

User
Ein Nutzer mit den entsprechenden Systemrechten, um die VM-Ware-Umgebung entsprechend herunterfahren zu können.

Password
Das dem Nutzer zugeordnete Passwort, mit dem sich RCCMD als berechtigt authentifizieren kann.

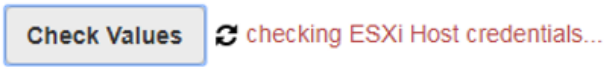


Im nächsten Schritt bestimmen Sie, wie viel Zeit RCCMD dem Host einräumen soll, bevor der ESXi-Host sich selber herunterfährt:



Virtuelle Maschinen benötigen unterschiedlich lange, um sauber herunterzufahren und sich zu beenden. Die genaue Zeit, wie lange eine Maschine hierbei benötigt, ist sehr individuell und hängt stark von der Aufgabe und der zugesicherten Hardware ab. Um einen Datenverlust oder eine Beschädigung der virtuellen Maschine zu verhindern, kann der Host angewiesen werden, vor dem eigenen Herunterfahren den Maschinen ein entsprechendes Zeitfenster zu geben, sich selber sauber zu beenden. Der an dieser Stelle eingestellte Wert gibt die Zeit in Sekunden an, die der Host wartet, bevor er ausgeschaltet wird. Ein guter Richtwert ist 90 Sekunden – virtuelle Maschinen, die länger benötigen, werden ausgeschaltet.

Die Zugangsdaten können Sie mit Check Values überprüfen:



st, beenden Sie die Prozedur mit *Save Changes*.

Klicken Sie im Anschluss auf *Verify*, um die eingegebenen ESXi-Daten als verifizierte Server zu bestätigen.

Sie werden bemerken, dass unten rechts das Save Changes die Farbe gewechselt hat:

Der Hintergrund ist, dass Sie eine Änderung vorgenommen haben, bei der RCCMD neu gestartet werden muss, um die Eingaben permanent zu speichern und in die aktive Konfiguration zu übernehmen. Dieser Vorgang wird übe die grüne Schaltfläche angezeigt.

Menü: VMware Settings

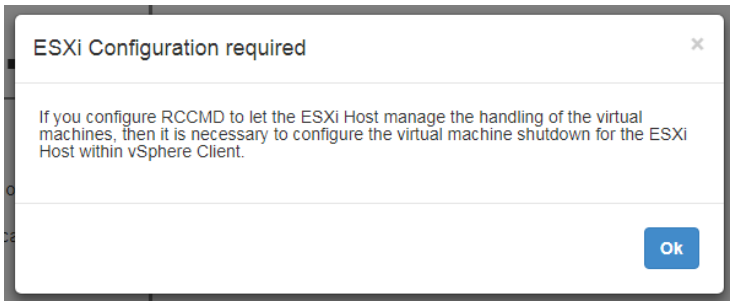
Das vCenter unterscheidet sich mit seinen Betriebsmodi von einem Standalone Host. Während der Standalone Host für sich alleine arbeitet und bei Bedarf die virtuellen Maschinen herunterfährt und ausschalten kann, ist über das vCenter das sog. vMotion möglich. Im Rahmen der HA – der High Availability – können virtuelle Maschinen von einem Host zu einem anderen verschoben werden, bevor dieser Host gezielt abgeschaltet wird.

Bevor Sie die RCCMD Appliance mit vMotion verwenden können, muss der Distributed Ressouces Scheduler DRS im vollautomatischen Modus konfiguriert sein.

Tipp

Stellen Sie vor der Verwendung von RCCMD in Verbindung mit vMotion unbedingt sicher, dass jede virtuelle Maschine auf dem Host mit Wartungsmodus getestet wurde. Sollte im Notfall der Wartungsmodus fehlschlagen, werden nicht migrierte virtuelle Maschinen regulär heruntergefahren und der Host abgeschaltet.

Klicken Sie auf *VMware Settings*: Wenn Sie noch keine Einstellungen vorgenommen haben, werden Sie von RCCMD darauf hingewiesen, dass RCCMD zusätzliche Informationen benötigt:

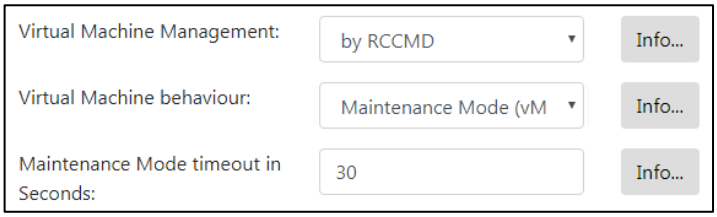


RCCMD ist zwar als virtuelle Maschine installiert und bereits einsatzbereit, kann jedoch noch nicht seine eigentliche Funktion erfüllen, da die notwendigen Zugangsberechtigungen noch nicht hinterlegt sind. Bestätigen Sie diesen Hinweis mit OK, um die VMware Einstellungen zu öffnen:

Wenn ein vCenter im Einsatz ist, können virtuelle Maschinen vor dem Abschalten eines Hosts auf einen anderen Host migrieren, um dort nahtlos weiterzuarbeiten.

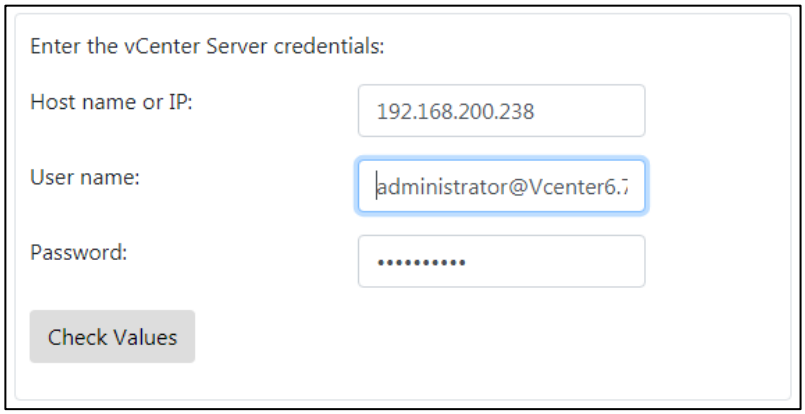
Beachten Sie bitte die abweichenden Zugangsdaten:

Wählen Sie Sie unter Virtual Machine behaviour den Maintenance Mode (vMotion) aus.

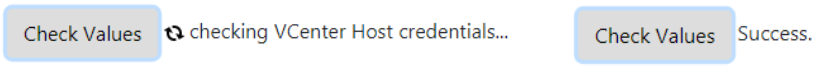


Der Maintenance ModeTimeOut in Seconds definieren Sie das Zeitfenster, welches Sie dem vCenter einräumen, eine virtuelle Maschine mittels vMotion auf einen anderen Host zu verschieben, bevor der betroffene Host heruntergefahren und physikalisch abgeschaltet wird. Dabei wird das Verhalten von vMotion im Rahmen der Hochverfügbarkeit (HA) innerhalb des vCenters konfiguriert.

Um das vCenter nutzen zu können, benötigt RCCMD abweichend zum Standalone Host Nutzerdaten mit den entsprechenden Berechtigungen des vCenters:

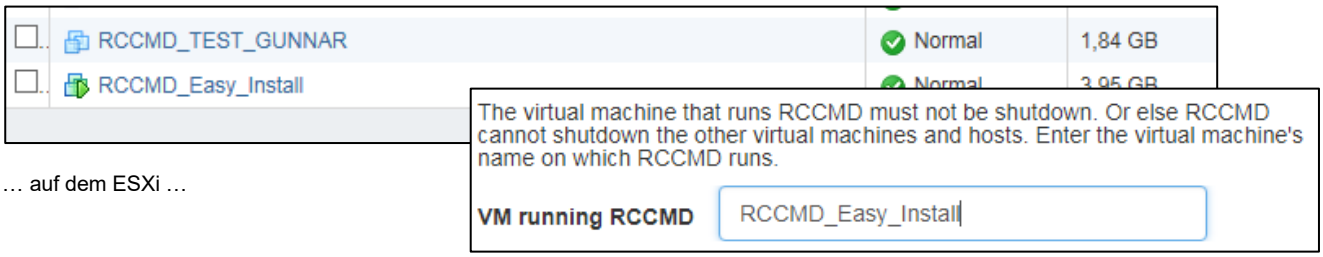


Mit Check Values können Sie überprüfen, ob das vCenter erreichbar ist und die Zugangsdaten korrekt eingetragen wurden:



Sollte das vCenter nicht erreichbar sein, werden Sie eine entsprechende Fehlermeldung erhalten.

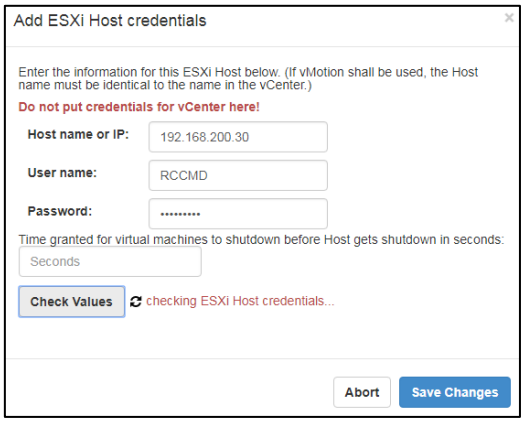
Um zu verhindern, dass RCCMD sich selber herunterfährt, muss der VMware-Host wissen, wie die Maschine heißt, auf dem der RCCMD Client selber läuft:



… auf dem ESXi …

… im RCCMD Client

Definieren Sie im Anschluss die Hosts, welche von RCCMD im Rahmen des vCenters heruntergefahren werden sollen. Die dort befindlichen virtuellen Maschinen können von vCenter entsprechend auf einen anderen Host verschoben werden:



RCCMD benötigt folgende Host Informationen:

HOST/IP-Name
Im Normalfall empfehlen wir hier die IP-Adresse des RCCMD-Hosts zu verwenden. Siekönnen jedoch auch den Hostnamen selber eintragen.

User
Ein Nutzer mit *Root-Rechten (ganz wichtig)*, um die VM-Ware-Umgebung entsprechend herunterfahren zu können.

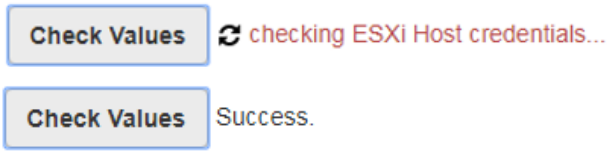
Password
Das dem Nutzer zugeordnete Passwort, mit dem sich RCCMD als berechtigt authentifizieren kann.

Im nächsten Schritt bestimmen Sie, wie viel Zeit RCCMD dem Host einräumen soll, bevor der ESXi-Host sich selber herunterfährt:

Virtuelle Maschinen benötigen unterschiedlich lange, um sauber herunterzufahren und sich zu beenden.

Die genaue Zeit, wie lange eine Maschine hierbei benötigt, ist sehr individuell und hängt stark von der Aufgabe und der zugesicherten Hardware ab. Um einen Datenverlust oder eine Beschädigung der virtuellen Maschine zu verhindern, kann der Host angewiesen werden, vor dem eigenen Herunterfahren den Maschinen ein entsprechendes Zeitfenster zu geben, sich selber sauber zu beenden. Der an dieser Stelle eingestellte Wert gibt die Zeit in Sekunden an, die der Host wartet, bevor er ausgeschaltet wird. Ein guter Richtwert ist 90 Sekunden – virtuelle Maschinen, die länger benötigen, werden ausgeschaltet.

Die Zugangsdaten können Sie mit Check Values überprüfen:



Wenn der Test erfolgreich verlaufen ist, beenden Sie die Prozedur mit *Save Changes.*

Klicken Sie im Anschluss auf *Verify*, um die eingegebenen ESXi-Daten als verifizierte Server zu bestätigen.

Sie werden bemerken, dass unten rechts das Save Changes die Farbe gewechselt hat:

.

Erweiterter Shutdown: Herunterfahren eines Clusters mit Abhängigkeiten

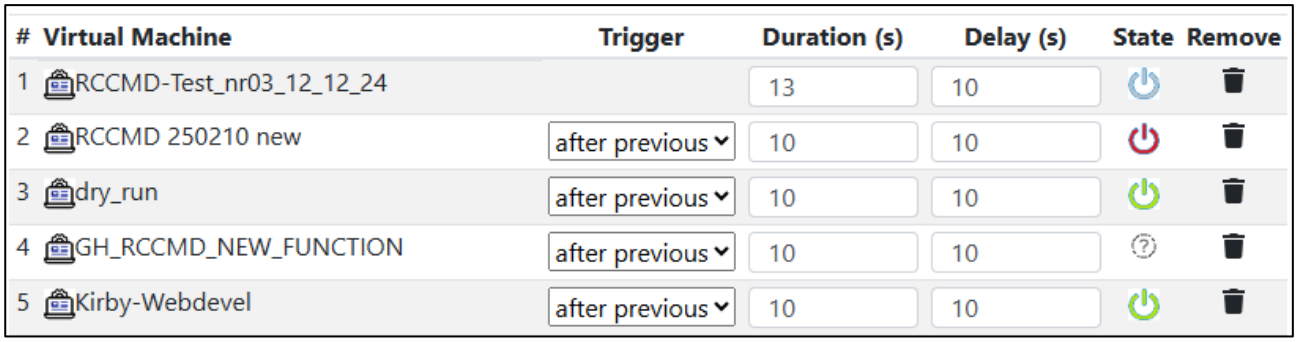
Menü 1: VMware Settings
Menü 2: VMware Shutdown Management

Unabhängig vom Standard-Shutdown über die VMware Settings bietet RCCMD Ihnen die Möglichkeit an, virtuelle Maschinen nicht nur in Shutdowngruppen zu organisieren, sondern auch im Vorfeld eine direkte Abhängigkeit zwischen einzelnen virtuellen Maschinen herzustellen. RCCMD geht dabei wie folgt vor:

Sequenz 1: Custom Shutdown Group

Die Custom Shutdown Group definiert die erste Gruppe von virtuellen Maschinen, welche heruntergefahren werden. Virtuelle Maschinen werden per Drag and Drop hinzugefügt oder in der Position zueinander geändert werden. Eine virtuelle Maschine, die hier abgelegt wurde, wird permanent aus der Liste der ESXi – Hosts entfernt und exklusiv unter der Custom Shutdown Group angezeigt.

- ➔ Im Fall eines Shutdowns wird RCCMD exklusiv alle unter VMware Settings kontaktieren und nach dieser virtuellen Maschine suchen.
- ➔ Sollte die virtuelle Maschine nicht gefunden werden, werden die eingetragenen Zeitfenster akribisch verfolgt, die virtuelle Maschine als solche jedoch nicht weiter beachtet.



Trigger, Duration (s) und Delay (s)

In der Custom Group abgelegte virtuelle Maschinen können in Relation zueinander individuell heruntergefahren werden. Die Einstellungen sind dabei nicht an die jeweiligen Zustände der virtuellen Maschine gebunden, und laufen in jedem Fall exakt in der vorgegebenen Reihenfolge ab, auch wenn die virtuelle Maschine weniger bzw. mehr Zeit für den Shutdownprozess benötigen.

Trigger: „after previous“*	Definiert, dass der individuelle Delay (s) restriktiv nach dem Ablauf der Duration (s) der vorangegangenen Maschine gestartet wird
Trigger: with previous“*	Definiert, dass der individuelle Delay (s) zeitgleich mit der Duration (s) der vorangehenden Maschine startet.
Duration (s)	Definiert die Zeit, in der eine virtuelle Maschine heruntergefahren sein sollte. Dieser Wert hat Auswirkung auf den Trigger der nachfolgenden virtuellen Maschine, sofern diese auf after previous gestellt ist.
Delay (s)	Definiert eine Zeitverzögerung, wann der Shutdown an die jeweilige virtuelle Maschine gesendet wird. Die Zeitverzögerung wirkt sich relativ zum Trigger aus.
State	Zeigt den aktuellen Betriebszustand der gefundenen virtuellen Maschine. Nur aktive virtuelle Maschinen können hierbei heruntergefahren werden.
Remove	Entfernt die virtuelle Maschine aus der Liste und fügt sie wieder dem jeweils bekannten ESXi – Host hinzu. Die virtuelle Maschine wird dann automatisch über Shutdown Sequenz 3: Default Gruppe heruntergefahren.

*) Die Duration (s) repräsentiert einen vom Administrator festgelegten Wert, den eine virtuelle Maschine zur Verfügung hat, bevor sie von RCCMD als heruntergefahren betrachtet wird:

Wenn ein Administrator weiß, dass ein vorgelagerter Managementserver insgesamt mit allen Routinen ca. 300 Sekunden zum Herunterfahren benötigt, aber die Netzwerkverbindungen innerhalb von 100 Sekunden schließt, muss ein nachgelagerte Backup- oder Datenbankserver nicht zwangsläufig die vollständige Duration (s) von 300 Sekunden des Management-Servers abwarten und über die Trigger definieren, ob die individuelle Delay (s) einer virtuellen Maschine gleichzeitig mit dem Shutdown der vorangegangenen Maschine startet, oder explizit erst nach dessen Ablauf.

Sequenz 2: General Shutdown Group

Diese statische Shutdowngruppe wird gestartet, sobald der Delay (s) des letzten Eintrags der Custom Group (Sequenz 1) ausgelaufen ist. Alle hier abgelegten virtuellen Maschinen werden gleichzeitig heruntergefahren. Der individuelle Shutdown entfällt, es gelten Werksvoreinstellungen von 90 Sekunden, bevor die nächste Shutdown-Gruppe aufgerufen wird.

Sequenz 3: Default Gruppe: No Cathegory / General Shutdown Group

Jeder Host, der VMware Settings eingetragen wurde, wird während der Shutdownprozedur in Echtzeit auf aktuell laufende VM’s abgefragt:

Alle gefundenen virtuellen Maschinen, die in keiner Gruppe abgelegt wurden, werden dabei dynamisch erfasst und entsprechend heruntergefahren – inklusive der virtuellen Maschinen, welche nach der Konfiguration von RCCMD neu ausgerollt wurden bzw. zu einem späteren Zeitpunkt auf einen der unter VMware Settings definierten Host migrierten.

- ➔ Diese Gruppe ist eine dynamische Systemgruppe und kann nicht konfiguriert werden.

Sequenz 4: Host based Shutdown Group

Dies ist die letzte Gruppe, die heruntergefahren wird. Hier werden die essenziellen Infrastruktur-Server wie DHCP, DNS, RADIUS, Mailservices, virtuelle Telefonanlagen, oder auch die Appliance abgelegt. Der Shutdown erfolgt in diesem Fall nicht über das VMWare

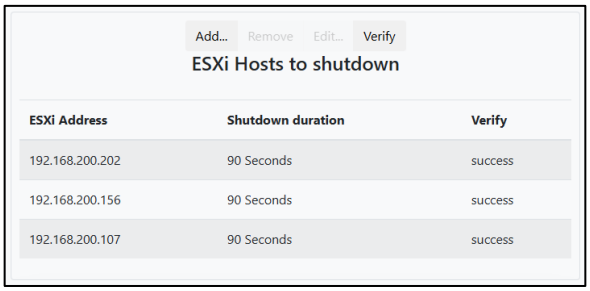
Shutdown Management, sondern wird an die VMware Settings mit der Shutdownduration für Hosts übergeben, welche die hier abgelegten virtuellen Maschinen und anschließend die physikalischen Hosts herunterfährt.

Schnellkonfiguration, erweitertes Shutdownszenario:

Schritt 1: Definition der Hosts

In diesem Konfigurationsschritt definieren Sie die ESXi – Hosts, welche von RCCMD heruntergefahren werden sollen.

Fügen Sie hierzu alle Hosts hinzu und bestätigen Sie mit Verify die Zugangsdaten.



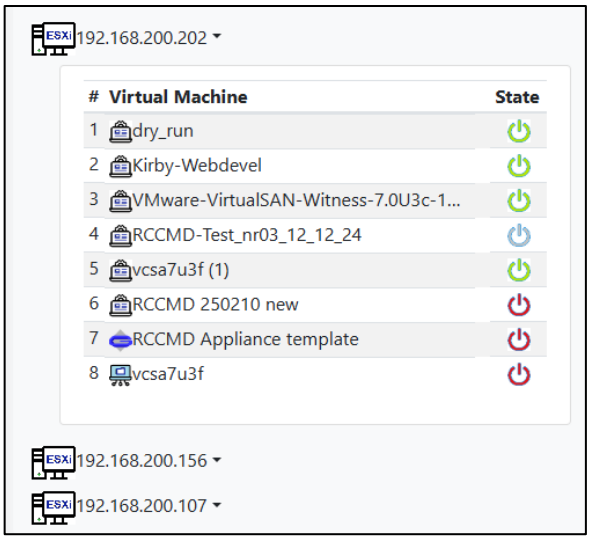
Schritt 2: Einrichten der Abhängigkeiten zwischen VMs

In diesem Konfigurationsschritt definieren Sie die gegenseitigen Abhängigkeiten und weisen Shutdowngruppen zu.

Öffnen Sie jetzt das Menü VMware Shutdown Management:

Alle unter VMware Settings angegebenen ESXi – Host inklusive der auf ihnen beheimateten virtuellen Maschinen werden Ihnen zusammen mit dem jeweiligen Betriebszustand angezeigt:

	Die virtuelle Maschine ist derzeitig ausgeschaltet. Alle Daten sind gesichert.
	Die virtuelle Maschine pausiert gerade bzw. befindet sich im Tiefschlaf Modus.
	Die virtuelle Maschine läuft und ist bei einem Stromausfall betroffen.
	Die in einer statischen Gruppe abgelegte virtuelle Maschine wurde nicht gefunden. RCCMD wird gem. den Einstellungen zum nächsten Eintrag springen.
	Gastsystem: Eine virtuelle Maschine mit diesem Ikon ist eine VM mit einer beliebigen Funktion.
	vCenter: Eine virtuelle Maschine mit diesem Ikon ist das vCenter für den jeweiligen Cluster.
	Die RCCMD Appliance: Dies ist der Name der virtuellen Maschine, der für die Appliance vergeben wurde.



Tipp: Ausnahme-Regelung vCenter und RCCMD Appliance

Alle virtuellen Maschinen werden gleichbehandelt – die einzige Ausnahme ist die virtuelle Maschine, in der RCCMD läuft sowie das vCenter, welches innerhalb von einem ESXi – Cluster auch als virtuelle Maschine auftreten kann. Je nach Konfiguration wird RCCMD diese gesondert behandeln, um einen strukturierten Shutdown zu ermöglichen.

Übergeben der Shutdownkontrolle an RCCMD bei Verwendung eines vSAN

Bevor Sie beginnen, lesen Sie bitte die folgenden Seiten aufmerksam durch:

RCCMD kann neben einzelnen Hosts auch VSAN-Systeme strukturiert herunterfahren. Da ein vSAN sehr komplex ist und teilweise in der Art des Betriebs sich von einem normalen ESXi unterscheidet, ist man in der Konsequenz bei der Konfiguration der Shutdownroutine durch RCCMD entsprechend an bestimmte Rahmenbedingungen gebunden.

- ✓ **Der RCCMD, der das vSAN betreuen soll darf nicht innerhalb des VSAN-Clusters laufen**

  Hintergrund ist, dass bei einem vSAN sich alle Hosts im Maintenance Mode befinden müssen, bevor Sie die Hosts ausschalten können. Solange eine virtuelle Maschine läuft, kann ein Host den Maintenance Mode nicht erreichen.

- ✓ **Das vCenter des vSANS muss als erstes starten und als letztes herunterfahren**

  Das vCenter ist die Steuereinheit für die Gesamtverwaltung des vSANS. Dabei kann das vCenter sowohl auf einem eigenen Host außerhalb des Clusters abgelegt sein als auch auf innerhalb des vSAN als VM laufen. Wichtig ist, dass ohne das vCenter die Datenysnchronisation nach dem Herunterfahren aller VM's koordiniert und nicht vor Abschluss dieser Aufgabe beendet werden darf.

- ✓ **Der Witness – Server des vSAN muss exklusiv heruntergefahren werden**

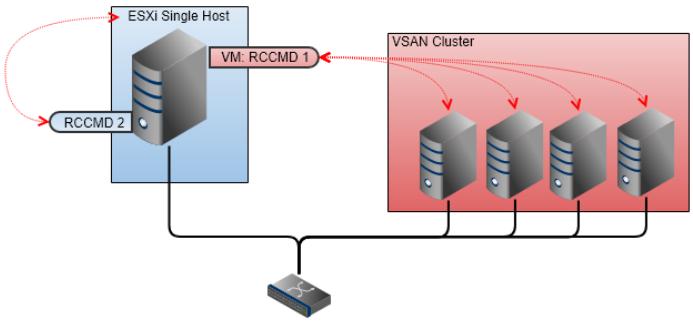
  Der Witness-Server ist eine weitere besondere Rolle innerhalb eines vSAN. Wenn sich zwei Hosts uneinig sind, welcher Host die aktuelleren Daten hat, entscheidet der Witness-Server. Der Witness Server tritt selbst als Host auf, kann aber keine eigenen virtuellen Maschinen aufnehmen oder halten.

  Beachten Sie bitte, dass der Witness-Server auch virtualisiert, im vSAN liegen kann und dennoch als eigenständiger Host auftritt. In dem Fall müssen Sie zwischen der IP-Adresse des Witness-Servers und des Hosts, auf dem die virtuelle Maschine des Witness-Servers liegt, differenzieren: Während der Witness-Server innerhalb des vSANs regulär heruntergefahren wird, muss der Host, auf dem der Witness-Server läuft von einem anderen RCCMD-Client exklusiv zu einem späteren Zeitpunkt in den Maintenance Mode gefahren werden.

- ✓ **Ein RCCMD Client kann entweder den vSAN-Cluster betreuen oder den Host, auf er selbst läuft**

  Wenn Sie also Single Hosts UND ein VSAN-Cluster haben, benötigen Sie in der Konsequenz mindestens 2 RCCMD-Clients:

  Dabei Übernimmt RCCMD 1 die Betreuung des VSAN-Clusters und RCCMD 2 kümmert sich im Anschluss um das Herunterfahren des Single Hosts. Die Shutdownroutine wird beim CS141 dann entsprechend in 2 unterschiedliche Kommandos aufgeteilt:

  - Shutdown des VSAN-Clusters
  - Shutdown des Single Hosts

  Da die beiden RCCMD-Clients nebeneinander laufen, achten Sie bei der Wahl des korrekten Zeitfensters unbedingt darauf, dass der VSAN alle Hosts ausgeschaltet hat, bevor Sie den letzten verbliebenen Single Host ausschalten – Ansonsten kanne s passieren, dass Shutdownbefehle, die das VSAN betreffen, nicht mehr abgesetzt werden: Das VSAN wird nicht korrekt heruntergefahren.

Tipp

Appliance vs Appliance – was ist die Virtuelle Maschine und was ist „der RCCMD"

Grundsätzlich unterscheiden sich hier die beiden Appliances nicht voneinander. Beide sind virtuelle Maschinen. Sie geben jedoch den beiden Appliances mit auf den Weg, wie die virtuelle Maschine heißt, auf der sie selber laufen. Damit verhindern Sie, dass ein RCCMD sich aus Versehen selbst als erstes beendet. Wenn Sie also RCCMD 2 mitteilen, wie ihre virtuelle Maschine heißt, wird sie RCCMD 1 als „Gast-VM" betrachten und entsprechend beenden, bevor diese ihre Aufgaben erfüllen kann.

✓ **Beachten Sie benötigte Zeitfenster durch die veränderte Shutdownsequenz, wenn Sie ein vSAN nutzen:**

Ziel bei der Verwendung eines vSAN ist maximale Datenredundanz in Verbindung mit maximaler Verfügbarkeit. Das System ist grundsätzlich nicht darauf ausgelegt, dass es regelmäßig heruntergefahren wird. Ein systemweiter Komplettshutdown ist hier eher eine Ausnahme, bei der nur schwer abschätzbar ist, wie viel Zeit das VCenter innerhalb eines vSAN benötigt, um die Hosts in den Maintenance Mode zu bringen.

Im Prinzip geht das vSAN dabei dreizügig vor:

Der zeitkritische Moment ist hierbei die Nachsynchronisationsphase, da diese Phase nur schwer einschätzbar ist: Der Maintenance Mode kann erst dann eingenommen werden, sobald die Synchronisation der Daten zwischen allen Hosts abgeschlossen ist.

Dieser Vorgang ist dynamisch und ändert sich je nach Ausbaustufe der Hardware, Anzahl der virtuellen Maschinen sowie der Menge und Art der Daten, die innerhalb der virtuellen Maschinen vorliegen, die letztendlich zwischen allen Hosts synchronisiert werden müssen. Erschwerend kommt hinzu, dass dieser Vorgang innerhalb des VSAN abläuft - Irgendwann sind die Hosts im Maintenance Mode, was bedeutet, dass der Vorgang abgeschlossen ist.

Dem steht allerdings die maximale Betriebsdauer der USV gegenüber

RCCMD brauch für den Shutdown die Angabe von klaren Zeitfenstern, die sich neben den berechneten Zeiten für einen Shutdown auch an der Betriebsdauer der USV orientieren müssen - RCCMD benötigt daher für die Ausführung des Shutdowns ein reserviertes Zeitfenster, das

- weit genug gefasst ist, um die EDV rechtzeitig herunterfahren zu können,
- einen Zeitpuffer enthält, falls sich die Nachsynchronisationsphase ändert,
- innerhalb des Sicherheitsbereiches der Laufzeit der USV liegt,
- genug Zeit für den Host außerhalb des Clusters zum Herunterfahren gibt.

✓ **DRS innerhalb des vSAN-Clusters beachten**

DRS und vCenter sind entgegen den oft angeführten Darstellungen *unabhängige Systemdienste*, welche lediglich miteinander kommunizieren. Man kann sogar ein HA-Cluster ohne DRS aufspannen, auch wenn es nicht unbedingt Sinn macht, da der HA-Cluster selbst eigentlich DRS impliziert.

DRS ist im Unterschied zu einem HA-Cluster in einem vSAN ein wesentlicher Bestandteil, da dieser Dienst im Hintergrund nicht genutzte Speicherressourcen aufspüren kann und diese für eine virtuelle Maschine bündelt. Diese intelligente Ressourcenverwaltung in Echtzeit erlaubt den Betrieb von mehr virtuellen Maschinen im Vergleich zu einem normalen Cluster:

Virtuelle Maschinen, welche jetzt diesen verteilten Zustand annehmen sind bei einem Host-basierten Cluster-Shutdown besonders gefährdet, weil das vCenter und das DRS nur dann sauber miteinander den Cluster-Shutdown umsetzen, wenn er über das vCenter von einem Administrator explizit angewiesen wurde.

VMware gibt zwar Empfehlungen über eine Cluster-Shutdown – Prozedur über den Maintenance-Mode, wenn jedoch die Hosts zu schnell in den Maintenance-Mode gefahren werden, kann es passieren, dass der DRS-Service die notwendigen Ressourcen für eine interne Migration von VM-Daten nicht unmittelbar ermitteln kann, und es nach einer Art Warteschleife wieder versucht. Virtuelle Maschinen, denen in diesem Fall der zugesicherte Festplattenspeicher inzwischen entzogen wird, weil die Hardware nicht mehr verfügbar ist, sind akut vom Ausfall betroffen. Ob und inwieweit das Betriebssystem und die Daten dabei beschädigt werden, hängt stark vom Speicherzustand und der Verwendung durch ein Betriebssystem ab.

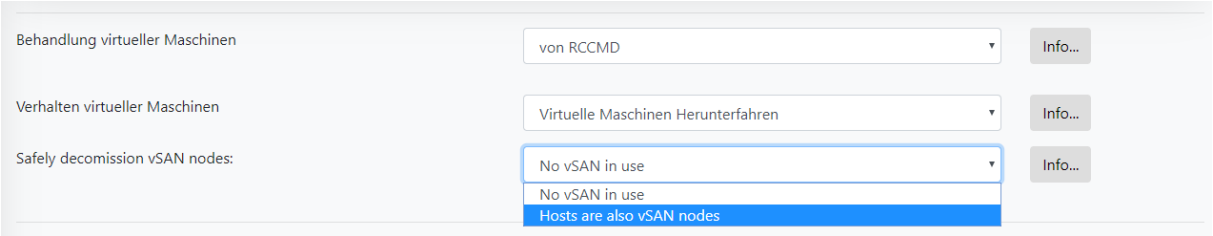
Das neue RCCMD Shutdown Management mit individualisierter Shutdownprozedur kann hier nicht nur die empfindlichen Systeme in Abhängigkeit zueinander herunterfahren, sondern auch wertvolle Systemressourcen einsparen, sobald der generelle Shutdown durchgreift.

Wichtig:

Bevor Sie mit der Konfiguration des vSAN-Shutdowns beginnen, müssen Sie einen Überblick haben, welches Zeitfenster eine USV für einen geordneten Shutdown bereitstehen kann. Daraus ergibt sich neben dem konkreten Ablaufplan auch der Zeitpunkt, an dem Sie mit dem Systemshutdown spätestens beginnen müssen:

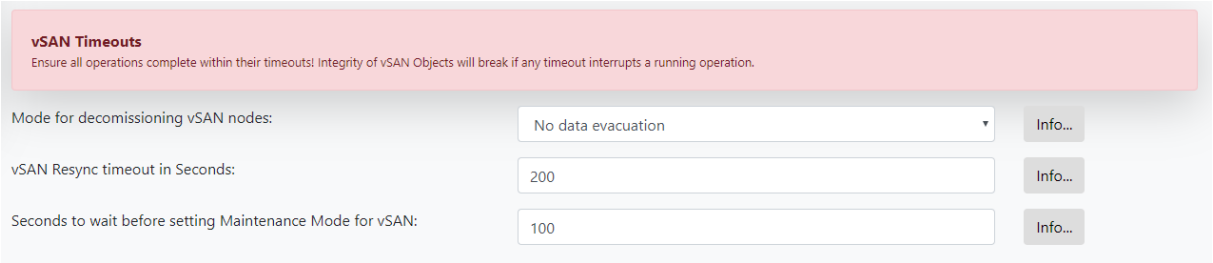
Das Herunterfahren eines vSAN ist technisch bedingt ein sehr systemkritischer Vorgang. Ein vSAN reagiert empfindlich, wenn es nicht ordentlich heruntergefahren wurde.

RCCMD für den VSAN-Modus vorbereiten:



Bitte beachten Sie, dass der RCCMD Client sich außerhalb des VSAN Clusters befinden muss, da anonsten die Shutdownroutine nicht korrekt angestoßen werden kann.

Sobald Sie den vSAN-Modus aktiviert haben, erhalten Sie zusätzliche Menüs:



Belassen Sie den decomissioning Mode auf *No data evacuation* – dieser Modus ist der schnellste Weg, einen vSAN Cluster herunterzufahren:

Die virtuellen Maschinen werden strukturiert heruntergefahren und im Anschluss die Datenbestände auf allen betroffenen Hosts synchronisiert.

Definition des *vSAN Resync timeout*

Anders als bei der Standardprozedur wird nach dem Herunterfahren der virtuellen Maschinen das vCenter aktiv und beginnt, alle Datensätze, die sich aus dem Betrieb der virtuellen Maschinen ergeben haben, zwischen den Hosts innerhalb des Clusters zu synchronisieren.

Diese Nachsynchronisationsphase definiert die kritische Phase innerhalb der Shutdownprozedur:

Alle Datensätze aus den virtuellen Maschinen müssen synchron zu Spiegeldaten sein, die auf anderen Hosts abgelegt wurden. So lange dieser synchrone Systemzustand nicht erreicht ist, kann der Maintenance Modus nicht eingenommen werden.

Tipp

Dieser Vorgang ist sehr dynamisch und ist stark von der Art der Daten abhängig, die synchronisiert werden müssen. Es kann durchaus sein, dass Sie mehrere neue virtuelle Maschinen erstellt haben und die Synchronisationszeit ändert sich nur marginal. Es kann jedoch auch passieren, dass Sie eine virtuelle Maschine erstellen und damit die Nachsynchronisationszeit eklatant verlängern. In einem anderen Szenario kann es sein, dass die Daten innerhalb der virtuellen Maschine durch das Nutzungsprofil organisch wachsen, was wiederum Einfluss auf die benötigte Zeit hat:

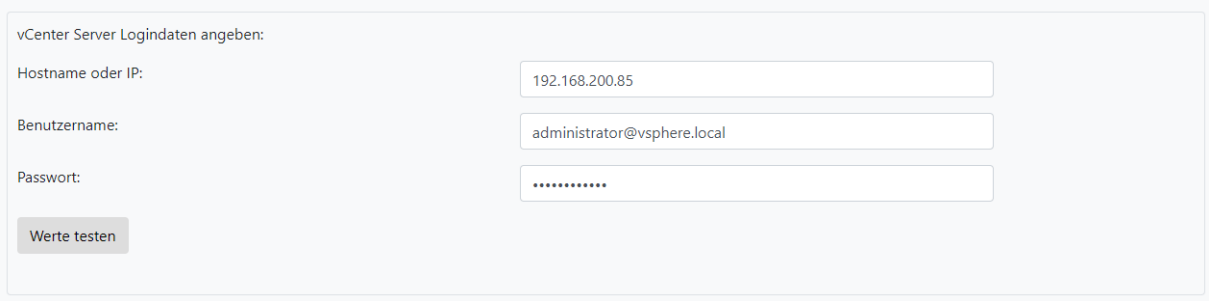
Dieser Wert kann nicht bei der Erstinstallation einmalig ermittelt und fest definiert werden, er muss regelmäßig auf Aktualität überprüft und ggfs. angepasst werden.

Das vCenter nimmt sich die Zeit, die für diesen Vorgang individuell benötigt wird. Dieser relative Zeitraum, der benötigt wird, steht leider in direktem Kontrast zu einem klar definierten Zeitfenster, die im Notfall von der USV zur Verfügung gestellt werden kann. Planen Sie also an dieser Stelle ein genügend großes Zeitfenster ein, um dem vCenter Reserve zu geben, fass der berechnete Zeitraum nicht reicht.

Maintenance Mode für das vCenter definieren.

Diese Einstellung definiert, wie viel Zeit das vCenter hat, sich selber nach dem Synchronisieren von Daten herunterzufahren. Sollte das vCenter innerhalb des vSAN als virtuelle Maschine laufen, wird dieser Zeitpunkt interessant: Nach Ablauf dieses Zeitfensters werden die Hosts in den Maintenance Mode versetzt und das vCenter von seinem Host ausgeschaltet.

Daten für das zuständige vCenter eingeben



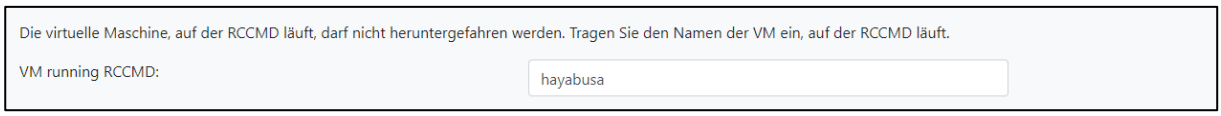
Da sich RCCMD mit dem vCenter über den ganzen Vorgang abstimmen muss, werden die Zugangsdaten für das vCenter benötigt, welches den vSAN betreut. Geben Sie hier keine Zugangsdaten für einzelne Hosts an.

Die virtuellen Maschinen für das vSAN RCCMD definieren:

RCCMD hat die Aufgabe, alle virtuellen Maschinen herunterzufahren und am Ende die Hosts abzuschalten. Da innerhalb eines vCenters nicht nur ein vSAN, sondern auch weiterführende Hosts abgebildet werden können, kann RCCMD diese auch herunterfahren.

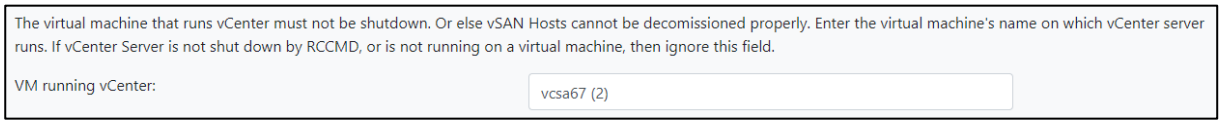
Dabei gibt es zwei Ausnahmen, die besonders beachtet werden müssen:

Angaben über die virtuelle Maschine, auf der RCCMD läuft



RCCMD kann zwar selber nicht im vSAN laufen, das heruntergefahren werden soll, aber das vCenter, dass den vSAN betreut kann durchaus auch weiterführende Hosts in seiner Liste enthalten. Die RCCMD Appliance ist letztendlich eine virtuelle Maschine, die sich an die Steuerbefehle des Hosts, auf dem sie selber läuft halten muss. Um zu verhindern, dass sich RCCMD versehentlich selber als erstes einen Shutdownbefehl erteilt, geben Sie hier den Namen der virtuellen Maschine an, die sie für RCCMD eingegeben haben. Diese wird dann zunächst aus dem Shutdownprozess ausgenommen.

Angabe der virtuellen Maschine auf der das vCenter für vSAN läuft

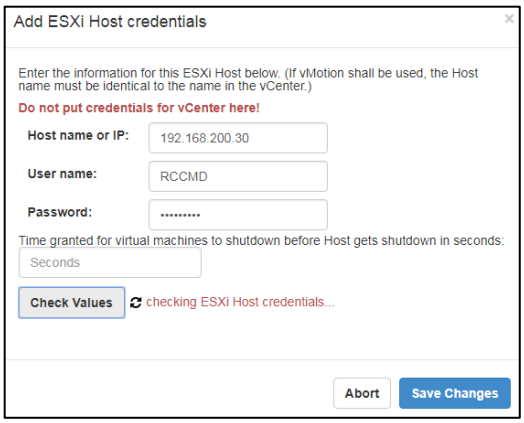


Innerhalb des vSAN-Systems übernimmt das vCenter besondere Verwaltungsaufgaben, ist jedoch auf der anderen Seite jedoch auch eine virtuelle Maschine. Beim Shutdown verschafft sich RCCMD im sich zunächst einen Überblick über aktiven virtuellen Maschinen, um diese dann entsprechend herunterzufahren, zu migrieren, etc.

Mit dieser Einstellung geben RCCMD bekannt, welche der virtuellen Maschinen das vCenter ist – diese wird als letzte Maschine im vSAN exklusiv heruntergefahren.

Definition der ESXi Hosts bei einem vSAN

Definieren Sie im Anschluss die Hosts, welche von RCCMD im Rahmen des vCenters heruntergefahren werden sollen. Die dort befindlichen virtuellen Maschinen können von vCenter entsprechend auf einen anderen Host verschoben werden:



RCCMD benötigt folgende Host Informationen:

HOST/IP-Name

Im Normalfall empfehlen wir hier die IP-Adresse des RCCMD-Hosts zu verwenden. Siekönnen jedoch auch den Hostnamen selber eintragen.

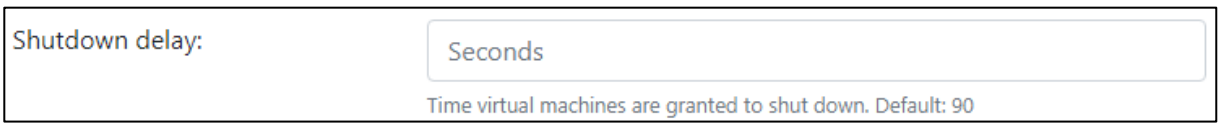
User

Ein Nutzer mit den entsprechenden Systemrechten, um die VM-Ware-Umgebung entsprechend herunterfahren zu können.

Password

Das dem Nutzer zugeordnete Passwort, mit dem sich RCCMD als berechtigt authentifizieren kann.

Im nächsten Schritt bestimmen Sie, wie viel Zeit RCCMD dem Host einräumen soll, bevor der ESXi-Host sich selber herunterfährt:



Hier hat das vSAN eine Besonderheit im Vergleich zu anderen Betriebsarten:

Die Dauer zum Herunterfahren definiert im Normalfall das Zeitfenster, dass ein Host zur Verfügung hat, um die Betriebssysteme innerhalb der virtuellen Maschinen herunterzufahren, bevor die virtuelle Maschine unabhängig vom Inhalt einfach ausgeschaltet wird. Hierbei ist es unerheblich, ob ein vCenter im Vorfeld versucht hat, Maschinen zu migrieren oder nicht.

Wenn dieser Befehl an die Hosts, die in einem vSAN laufen, ausgegeben wird, gibt es keine virtuellen Maschinen mehr, die noch ausgeschaltet werden müssen, da

- *Alle* Hosts im Maintenance Mode sein müssen
- Ein Host nur im Maintenance sein kann, wenn alle virtuellen Maschinen aus oder wegmigriert sind

Für die Hosts im vSAN bedeutet das, dass die Dauer zum Herunterfahren von virtuellen Maschinen auf 1 Sekunde gestellt werden kann. Die Shutdownroutine bei einem vSAN hat alle Hosts bereits in den Maintenance Mode gebracht. Konsequenterweise wird hier kein Zeitfenster benötigt, die RCCMD zum Herunterfahren garantieren muss.

Sonderrolle Witness-Server

Kleinen vSAN-Systemen fehlt es an nötigen Recourcen, um alle Datenbestände selbstständig abgleichen zu können. Um Probleme beim Datenabgleich in minimalistischen vSAN-Systemen zu verhindern, kommt ein Witness Server zum Einsatz:

Der Witness-Server tritt im vSAN als eigenständiger Host auf, ist jedoch nicht für die Aufnahme und den Betrieb von virtuellen Maschinen zuständig - sobald sich Hosts über die Aktualität ihre Datenbestände nicht einig werden können, entscheidet der Witness-Server, welcher Host seine Daten zu synchronisieren hat.

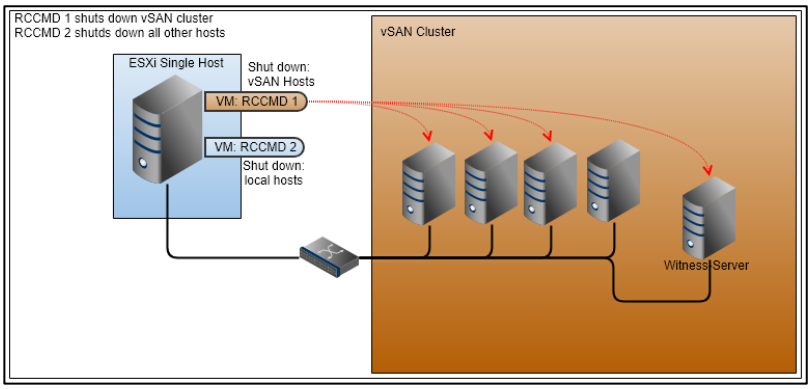
Dabei kann der Witness-Server sowohl eine physikalische Maschine sein als auch als innerhalb einer virtuellen Maschine einen physikalischen Host simulieren. Das hat Auswirkungen auf die RCCMD-Konfiguration:

Wenn der Witness-Server auf als echter Host betrieben wird

In diesem Fall geben Sie den Witness-Server und alle entsprechenden Hosts direkt an, die Sie herunterfahren möchten.

Die Hosts werden entsprechend in den Maintenance Mode gehen:

- virtuelle Maschinen herunterfahren
- Das vCenter wird den reSynch durchführen
- Die Hosts wechseln in den Maintenance Mode
- Das System wird ausgeschaltet.



Wenn der Witness-Server virtualisiert in einem vSAN liegt

Sollten Sie den Witness-Server als virtuelle Maschine im vSAN betreiben, müssen Sie zwischen dem Host, auf dem der Witness-Server abgelegt wurde und dem Witness-Server als eigenständiger Host unterscheiden:

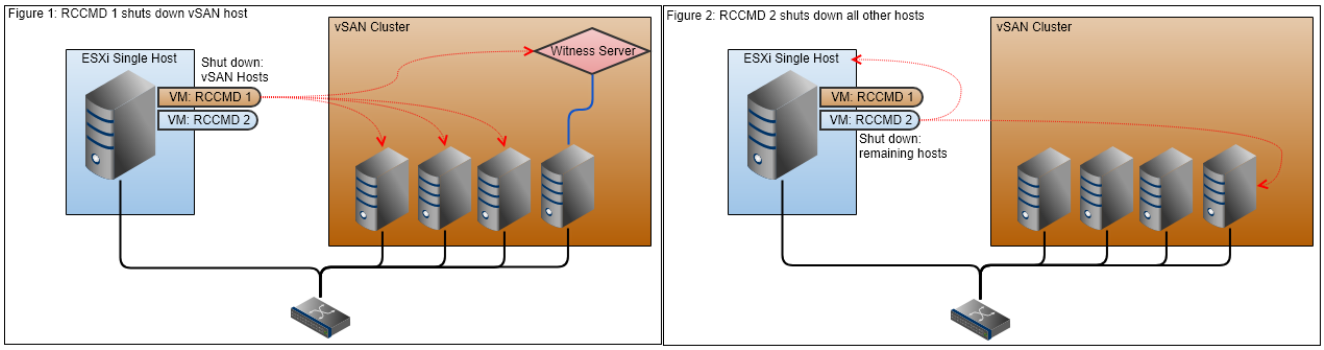
Da der Witness-Server innerhalb des vSAN selber als Host auftritt, wird er unabhängig von seiner Installationsart entsprechend wahrgenommen und behandelt:

Während der Host, auf dem der Witness-Server virtualisiert läuft, intern lediglich eine virtuelle Maschine, auf er „irgend so ein System“ läuft, wahrnimmt, akzeptiert er im Netzwerk den Witness-Server als eigenständigen Host und Netzwerkknoten.

Wenn jetzt die falsche IP-Adresse angegeben wurde, wird der Host, der für die virtuelle Maschine zuständig ist, richtig reagieren:

- Die virtuelle Maschine wird beendet
- Der Host wechselt in den Maintenance Mode

Da jedoch der (wenn auch virtualisierte) Witness-Server funktionsbedingt einen vollwertigen Host und Netzwerkknoten darstellt, muss dieser als Konsequenz wie ein echter Host behandelt und vor dem Ausschalten in den Maintenance Mode gebracht werden. Im Anschluss kann von dem zweiten RCCMD Der Host, der die virtuelle Maschine betreut, regulär ausgeschaltet werden:



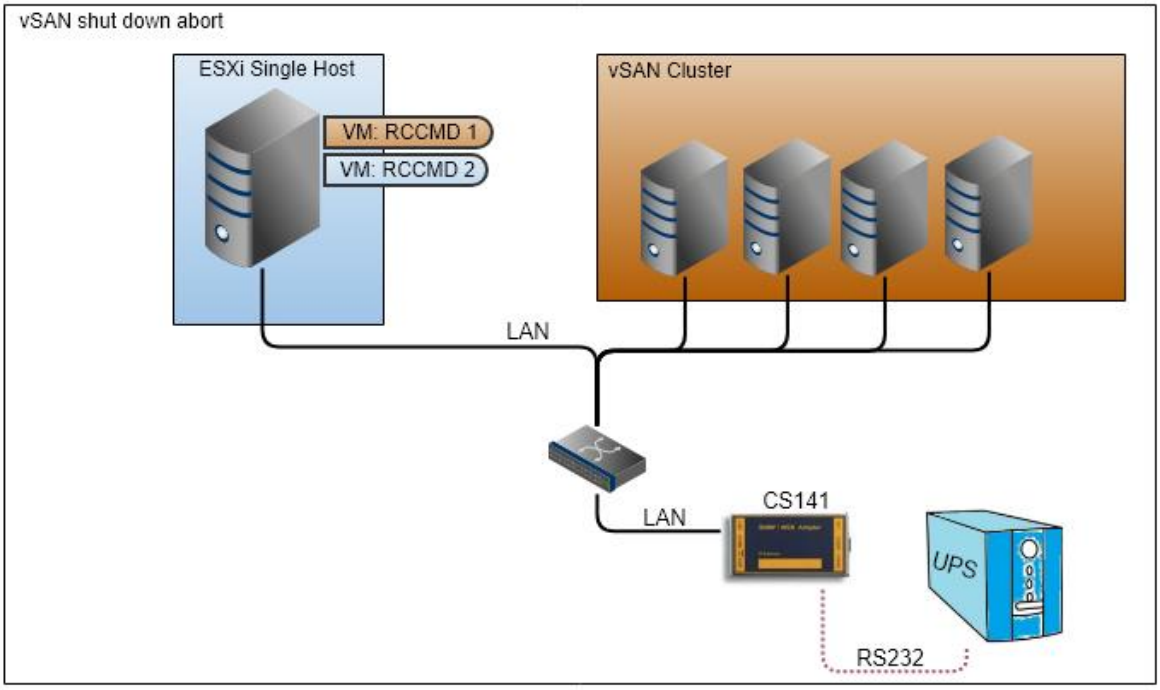
Tutorial: Wenn der Shutdown bei einem vSAN einmal abgebrochen werden muss...

Ein normaler ESXi – Cluster mit vCenter unterscheidet sich hier von einem vSAN:

Während ein normales Cluster mit einzelnen Hosts letztendlich auch in Eigenregie seine virtuellen Maschinen herunterfahren und ausschalten kann sollte der Maintenance Mode nicht möglich sein, kann ein vSAN nur dann ausgeschaltet werden, wenn keine virtuellen Maschinen auf dem vSAN mehr läuft. Der zweite große Unterschied ist, dass der RCCMD Client, der das vSAN betreut, logischerweise nicht innerhalb halb des vSANS Clusters laufen kann, sondern diesen von außen steuern muss. Als dritten Punkt hat benötigt vSAN nach dem Herunterfahren aller virtuellen Maschinen noch eine Nachlaufzeit, bei der alle Bestandsdaten synchronisiert werden, erst danach dürfen die Hosts gefahrlos ausgeschaltet werden.

Dadurch ergeben sich logische Abschnitte, zwischen denen eine Abbruch-Sequenz durchaus möglich ist. Dieses Tutorial zeigt eine Möglichkeit, wie ein automatisierter Shutdown abgebrochen werden könnte:

In diesem Beispiel sind die Rahmenbedingungen erfüllt sind, die den Betrieb ohne einen Witness-Server erlauben.



Problematik:

Sobald ein Stromausfall vorliegt, wird RCCMD 1 aktiv und beginnt rechtzeitig mit dem Shutdownprozess. Messungen haben ergeben, dass der gesamte Shutdown irgendetwas bei 38 Minuten dauern wird. Da die USV insgesamt bis zu 45 Minuten abdecken kann, muss also spätestens nach 5 Minuten der Shutdown eingeleitet werden, da ansonsten das System nicht korrekt heruntergefahren werden kann.

Bei Zeitfenster 20 Minuten ergibt es sich nun, dass die Hauptstromversorgung wieder zurückkehrt und ein weiterführen des Shutdowns nicht mehr notwendig ist.

Da die RCCMD Appliance per Definition des Softwarezwecks die Shutdownsequenz nicht wieder zurückzunehmen oder stoppen kann, wird RCCMD 1 dieses auch bis zum Ende durchführen und das vSAN sauber herunterfahren. Der CS141 kann in diesem Fall keine „Entwarnung“ an RCCMD 1 senden.

Grundsatzentscheidung treffen

Da die USV 20 Minuten lief, dürfte ein erneuter Netzausfall fatale folgen haben, sollte in Betracht gezogen werden, ob ein Shutdown und eine Wartezeit bis die Mindestvorhaltezeit von 40 Minuten oder ein Abbruch des Shutdowns eine Option ist. Der Unterschied ist. Die Befehle, die gegeben werden, sind hier identisch, das Ereignis ändert sich. In diesem Beispiel wurde sich für ein Abbruch des Shutdowns entschieden. Wie auch der Shutdown wird der Abbruch über den CS141 eingeleitet, nur eben bei dem Ereignis für Power Restored.

Dabei gilt zu beachten: Der Shutdown selber ist bereits eine Notfallmaßnahme – über einen erzwungenen Abbruch der Notfallmaßnahme nachzudenken ist zwar legitim, jedoch immer mit zusätzlichen Risiken verbunden.

Shutdownabbruch einleiten

Bei dem Ereignis Power restored wird ein Shutdownsignal auf RCCMD 2 gelegt – dieser Sollte ja den letzten Single Host herunterfahren – was das sofortige Beenden aller virtuellen Maschinen einschließt. RCCMD 1 wird sich als virtuelle Maschine an diese Vorgabe halten und entsprechend herunterfahren und sich ausschalten – und dabei vergessen, dass noch offiziell Steuerbefehle ausstehen, die das vSAN betreffen.

Das vCenter wird die letzten Befehle abarbeiten und entsprechend dann auf weitere Anweisungen warten. Da die Steuerbefehle an Zeitfenster gebunden sind, die im RCCMD 1 hinterlegt wurden, lässt sich auf diese Weise schnell herausfinden, was bereits gemacht wurde.

1. vMotion ist aktiv und versucht, die virtuellen Maschinen standardmäßig zu verschieben
2. vSAN – shutdown ist aktiv und die virtuellen Maschinen werden heruntergefahren oder verschoben.
3. Die Nachsynchronisationsphase läuft gerade

Dabei wird die aktuelle laufende Phase beendet und wenn danach kein neuer Befehl eingeht, wird das vSAN in diesem Zustand stehen und warten.

Strukturierter Restart: RCCMD -Schutz reaktivieren

Senden Sie WOL-Signal auf den ESXi Single Host – dieser wird über das WOL- Signal wieder gestartet und dem entsprechend starten auch die RCCMD-Appliances und gehen in ihre Startposition. Damit steht die RCCMD -Verbindung wieder.

Anfahren ausgeschalteter Hosts

Senden Sei nun auf *jeden* Single Host ein WOL-Signal – es ist unerheblich, ob dieser Host bereits ausgeschaltet wurde oder nicht:

Wenn der Host läuft, fällt das WOL-Signal ins Leere und wird an seinem Zielort ignoriert.

Anfahren der vm’s

Je nach Konfiguration können virtuelle Maschinen, die ausgeschaltet wurden, über ein WOL-Signal wieder angeschaltet werden. Senden Sie hierzu ein WOL-Signal auf die MAC-Adresse der jeweiligen virtuellen Maschine.

Tipp

Beachten Sie bitte, dass WOL-Signale auf die MAC-Adresse gesendet werden, der CS141 muss im selben Netzwerksegment liegen bzw. das Signal entsprechend durchgeroutet werden.

Da Sie das Timing frei definieren können, ist sogar möglich, eine spezielle Reihenfolge festzulegen, in der virtuelle Maschinen anlaufen. Dadurch können Sie das Basis-Netzwerk automatisch anfahren lassen.

Abbruch eines vSAN Shutdowns

RCCMD verfügt über einen Schutzmechanismus, der einen gültigen Shutdown auch dann ausführt, wenn jemand nach dem Auslösen des Shutdowns den RCCMD – Dienst über der Weboberfläche stoppt. Das System wird dennoch sauber herunterfahren und ausgeschaltet. Das Shutdownmanagement wird vom CS141 übernommen – dort werden auch die optimalen Zeitfenster zum Shutdown definiert:

Normalerweise wird der Shutdown daher möglichst knapp an das Ende der Überbrückungszeit gelegt, um maximale Funktionsbereitschaft und Kontrolle über die Daten zu gewährleisten.

Durch das vSAN können sich die Zeitparameter stark verschieben:

Je nach aktueller Datenlage und Ausbaustufe des vSAN kann dieser Shutdown sehr in die Länge ziehen und es muss entsprechend frühzeitig mit der Prozedur begonnen werden. Sollte die Hauptstromversorgung oder ein Notfallgenerator in dieser Zeit verfügbar werden,

ändert das nichts an der Shutdownroutine –RCCMD verfolgt eine Anweisung und organisiert die Umsetzung.

Sollten Sie einen Shutdown zurücknehmen wollen, der gerade umgesetzt wird:

Dieser Vorgang kann nicht automatisiert werden, da RCCMD zwar die Anweisungen und ihre Zeitfenster koordiniert, jedoch vom vCenter kein Feedback über logische Sinnabschnitte bekommt. Daraus resultiert, dass ein Administrator sich überlegen muss, ob er den Shutdown bis zum Ende laufen lässt und das System wieder anfährt oder aber innerhalb einer Shutdownroutine einen Abbruch provoziert:

Beides hat seine jeweiligen Vor- und Nachteile.

Um den Shutdownprozess zu beenden und die dazugehörigen Skripte wieder auf 0 zu setzen, beenden Sie auf dem Host die virtuelle Maschine der Appliance. Sobald dies geschieht, werden keine weiteren Befehle mehr an die Hosts übertragen und das System stoppt den Shutdownprozess nachdem der letzte Befehl erfolgreich übermittelte Befehl durchgeführt wurde.

WICHTIG:

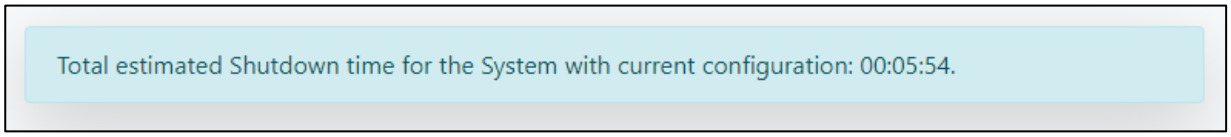
Achten Sie in diesem Fall darauf, dass die virtuelle Maschine mit der Appliance beendet wird. Auch wenn Sie im Webinterface RCCMD auf „Stopp“ stellen und der Dienst laut Webinterface angehalten wurde:

Die Shutdownsequenz wird weiterhin ausgeführt.

Wie lange wird die geschätzte Shutdownzeit dauern?

Grundlegende Shutdownzeit

Wenn Sie alle Daten eingegeben haben, erscheint unterhalb der Herunterzufahrenden ESXi Hosts eine Schätzung wie lange ein vollständiger Shutdown dauern würde:



Beachten Sie bitte, dass dieser Wert ein Richtwert ist, welcher auf Basis der eingetragenen Daten ermittelt wurde. Dieser Wert soll Ihnen helfen, zu ermitteln, wann spätestens ein Shutdown ausgelöst werden muss, damit das System korrekt herunterfährt.

Tipp

Die USV hat maximales absolutes Zeitfenster, in der sie eine Notstromversorgung garantieren kann. Es würde nichts bringen, wenn Sie so lange an den Zahlen innerhalb von RCCMD spielen, bis die Werte zur USV passen. Ein falsches Zeitfenster führt eher dazu, dass der Shutdown nicht richtig ausgeführt oder im schlimmsten Fall sogar komplett verweigert wurde.

Dieser Wert ist eine Momentaufnahme Ihres Systems, der auf den von Ihnen eingegeben Daten basiert!

Überprüfen Sie bitte regelmäßig, ob die eingegebenen Werte dem realen Anforderungsprofil eines Notfallshutdows entsprechen.

Planen Sie in jedem Fall bei der Berechnung Ihrer persönlichen Shutdownzeit einen Zeitpuffer ein, sollte sich durch die Regelnutzung das Zeitfenster zwischen zwei Routinetests geändert haben.

Die Konfiguration von RCCMD unter VMware ist hiermit beendet und RCCMD wird Ihr System im Notfall herunterfahren können. Bitte beachten Sie, dass RCCMD im Normalfall nicht selbstständig aktiv wird, sondern auf ein entsprechend gültiges Eingangssignal wartet.

Der Sender ist hierbei in der Regel eine SNMP-Karte, welche RCCMD – Shutdownsignale verwenden kann.

Weiterführende Informationen sowie alle Screens im Detail finden Sie in Kapitel 7 in diesem Handbuch!

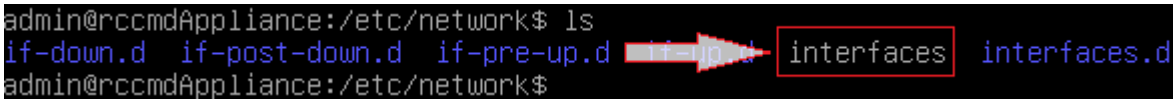
Tutorial: Netzwerkinterface von Hand zuweisen

Unter bestimmten Umständen kann es passieren, dass kein DHCP-Server zur Verfügung steht. In dem Fall startet zwar das Trägersystem, jedoch ohne IP-Adresse, die RCCMD verwenden kann. Da die 100%ige Verfügbarkeit eines DHCP-Servers niemals gegeben sein kann, ist es ratsam, hier eine statische IP-Adresse zu vergeben.

Die dafür zuständige Datei findet sich in dem folgenden Verzeichnis:

/etc/network

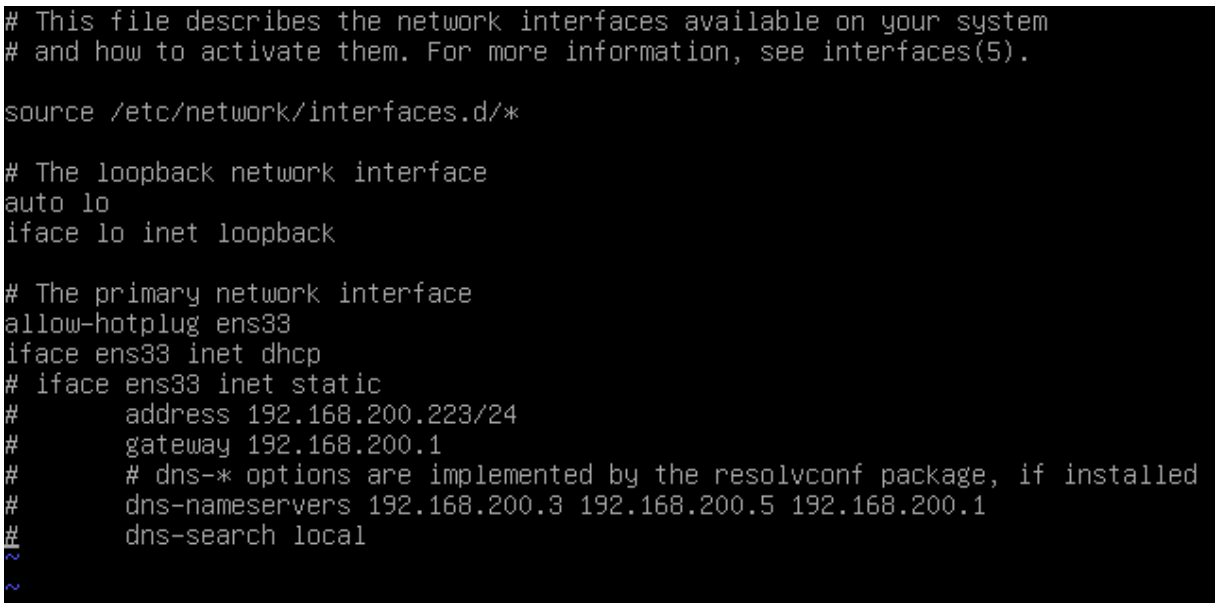
Die für einen statischen IP-Adresseintrag zuständige Datei lautet „interfaces“



Die Appliance hat mit nano einen Texteditor integriert, welcher das Betrachten und Editieren von Dateien erlaubt. Um die Datei editieren zu können, benötigen Sie zunächst erhöhte Systemrechte. Diese erhalten Sie mit dem Befehl *sudo su*. Danach starten Sie nano mit folgendem Kommando:

nano /etc/network/interfaces

Der Editor wird Ihnen folgende Datei anzeigen:



Der entscheidende Eintrag ist

➔ Iface ens33 inet dhcp

Dieser Eintrag entscheidet, ob die Appliance die IP-Adresse über DHCP oder statisch zugewiesen bekommen hat.

Passen Sie folgende Einstellungen an Ihre lokalen Gegebenheiten an:

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 <- Auskommentieren mit #
iface ens33 inet static <- Die Raute entfernen
Address 192.168.200.223/24 <- Vergeben Sie IP-Adresse und Subnetzmaske
Gateway 192.168.200.1 <- Vergeben Sie das 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 <- Passen Sie den DNS-Server an.
dns-search local

Spätestens beim nächsten Neustart sollte eine feste IP-Adresse vergeben sein.

Tipp

Sie können auch die vom DHCP-Server beim Start statisch vergebene IP-Adresse eintragen, müssen jedoch sicherstellen, dass diese im Anschluss aus dem Pool dynamisch vererbbarer IP-Adressen entfernt wird.

Alternativ können Sie eine feste IP-Adresse über DHCP-Server vergeben und diese statisch in der Appliance eintragen. In dem Fall wird RCCMD auf jeden Fall eine erreichbare IP-Adresse zugewiesen bekommen, was die Ausfallsicherheit enorm erhöht.

Tipp

Man wünscht es sich nicht, aber Passworte können verloren gehen. Bei komplexen Anlagen kann das sehr umständlich und teuer werden, sollte in dem Fall eine VM komplett neu aufgesetzt und konfiguriert werden müssen. Der Aufwand richtet sich hier stark nach der Komplexität der RCCMD-Konfiguration. Der Notfall-User sollte daher eingerichtet werden, bevor Sie mit der eigentlichen Konfigurationsarbeit beginnen.

Es kommt immer wieder vor, dass auf Grund widriger Umstände Passworte verloren gehen, z.B. weil es keine richtige Dokumentation über die installierten Systeme gibt, Passworte vergessen wurden, weil sie so selten gebraucht werden, IT-Systeme von anderen Unternehmen geerbt werden etc.

RCCMD hat als Grundeinstellung keine Hintertüren installiert.

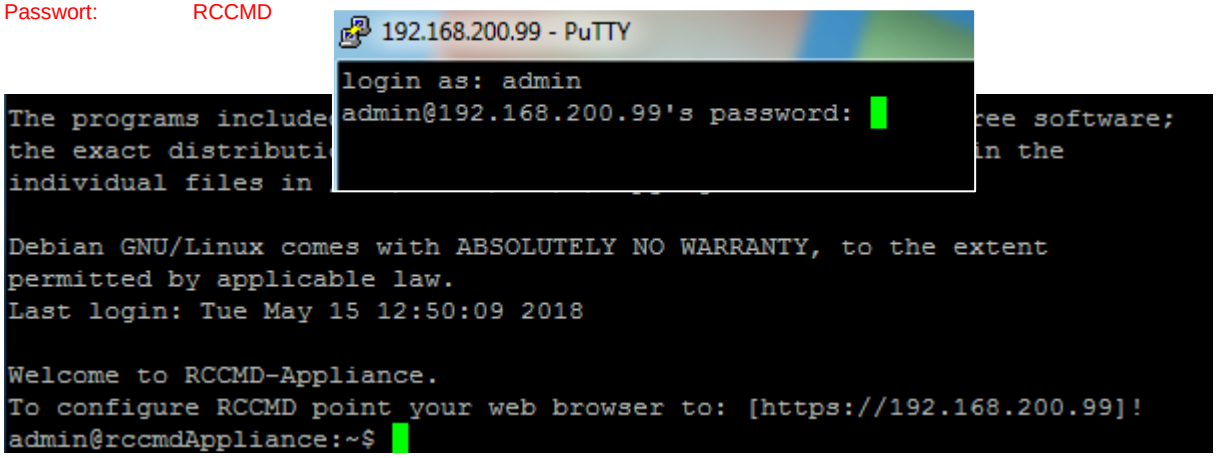
Wenn Sie den Standard Benutzer Admin ein anderes Passwort zuweisen und dieses verloren geht, müssen Sie grundsätzlich den RCCMD-Client neu aufsetzen. Dieses könnte in einigen Fällen ein sehr komplexes Problem werden, etwa, wenn spezielle Skripte hinterlegt sind, die neu erstellt werden müssen.

Um das zu verhindern, empfiehlt es sich, einen Backup-User mit Administratorrechten einzurichten.

Nachdem Sie die Appliance installiert haben, können Sie mit einem Freeware Tool wie Putty auf die Konsole zugreifen:

Nutzer: admin

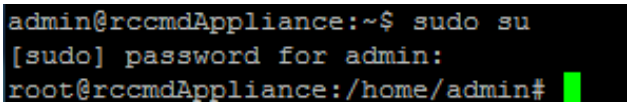
Passwort: RCCMD



Rootrechte erlangen

Befehl: sudo su

Beachten Sie, dass Sie nach dem Login noch nicht die benötigten Rechte eingeräumt bekommen haben, um einen entsprechenden Notfallnutzer einzurichten.



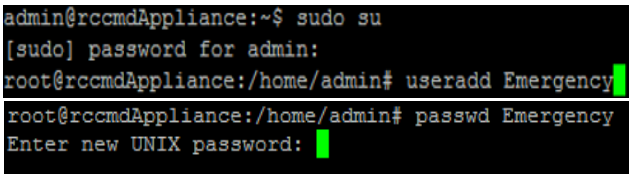
Benutzer und Passwort anlegen

Befehl 1: useradd <Benutzername>

Mit diesem Befehl legen Sie einen neuen Benutzer an.

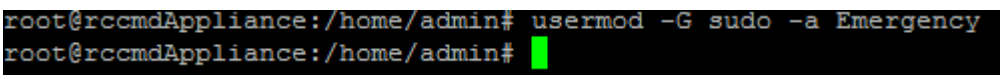
Befehl 2: passwd <Benutzername>

Vergeben Sie als nächstes ein gültiges Passwort.



Nutzergruppe zuweisen

Befehl: usermod – G sudo -a Emergency

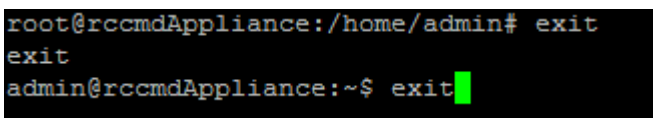


Damit der neu angelegte Nutzer auch die notwendigen Rechte wie su erhalten kann, muss er der passenden Nutzergruppe zugewiesen werden

Ausloggen

Befehl: exit

Geben Sie zwei Mal exit ein. Das erste Mal beenden Sie den SuperUser, das zweite Mal die Konsole selber.



Notfall Passwort Reset durchführen

Starten Sie die Session verwenden Sie die Zugangsdaten des Notfallbenutzers.

Mit dem Befehl sudo su erhalten Sie die notwendigen Rootrechte für den Notfall:

```
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:/#
```

Bitt beachten Sie:

Der Nutzer Emergency hat keine Berechtigung, die Webkonsole zu administrieren. Dieser Nutzer dient dazu, im Notfall das Passwort des Benutzers admin neu zu setzen.

Navigieren Sie zum richtigen Verzeichnis

Befehl: cd /usr/rccmd/webconfig/resources

In diesem Verzeichnis liegen die für die Passwortabfrage notwendigen Konfigurations-skripte.

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

Texteditor öffnen und Passwort ändern

Befehl: nano realm.properties

Es öffnet sich der Texteditor nano, mit dem Sie die Datei öffnen und editieren können. Diese Datei entscheidet, mit welchen Passwort sich der Nutzer admin auf der Weboberfläche anmelden kann.

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

Führen Sie folgende Ändeurngen durch

#RCCMD realm.properties
username: password [,rolename ...]
#admin: CRYPT:adg.Dq8TXmNZI, admin -> Mit # die Zeile deaktivieren
admin: Notfall, admin -> Diese Zeile hinzufügen

In diesem Beispiel würde der Nutzer admin jetzt das Passwort Notfall zugewiesen bekommen.

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

Speichern Sie die Datei und beenden Sie den Texteditor. Achten Sie darauf, dass der orginale Dateiname überschrieben wird und nicht Ihre Änderungen mit einem anderen Dateinamen gespeichert wird.

RCCMD Konfiguration neu einlesen

Befehl: /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.
```

Durch diesen Befehl wird das von Ihnen eben vergebene Passwort eingelesen und aktiv geschaltet. Alternativ starten Sie die Appliance neu.

Gehen Sie nun auf die Weboberfläche Ihrer RCCMD- Installation und melden Sie sich mit dem neuen Passwort an. Von dort aus können Sie im Anschluss direkt unter User Settings ein neues Passwort vergeben.

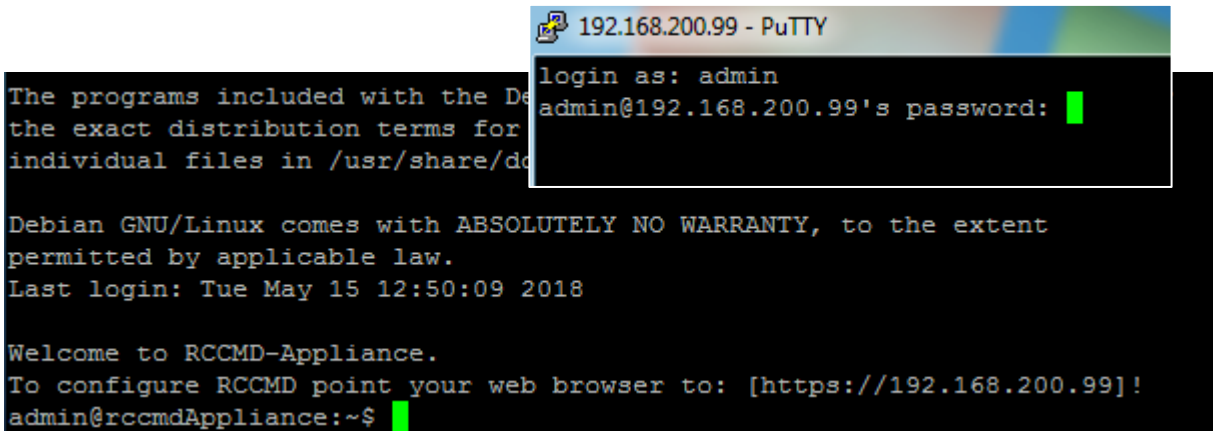
Tutorial: Login über ein externes Tool

Nach der Installation erlaubt die RCCMD Appliance einen direkten Zugriff über ein entsprechendes Tool. Sofern eine gültige und erreichbare IP-Adresse zur Verfügung steht.

Nachdem Sie die Appliance installiert haben, können Sie mit einem Freeware Tool wie zum Beispiel Putty direkt auf die Konsole zugreifen:

Nutzer: admin

Passwort: RCCMD



Tutorial: Tastaturlayout hinzufügen

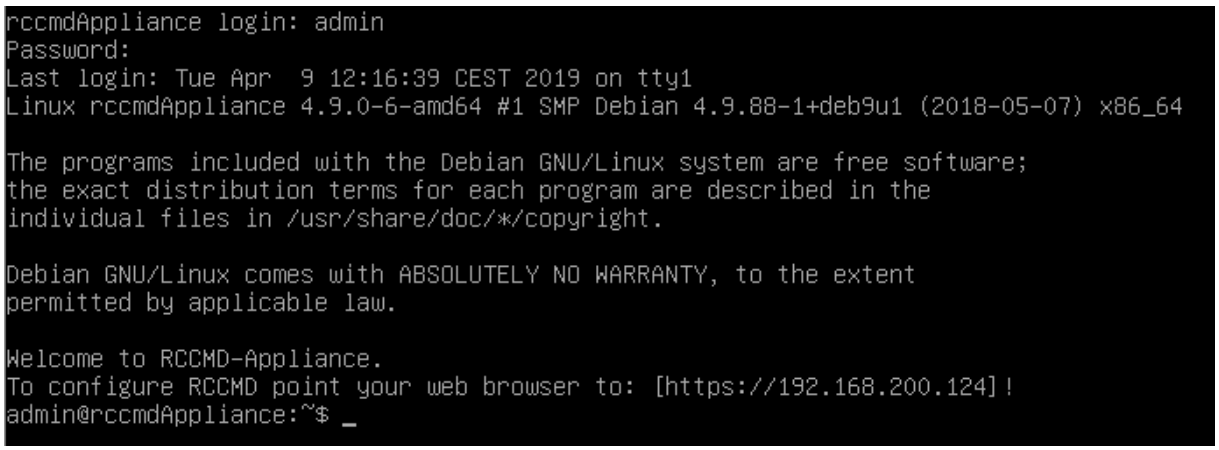
Da es viele Weltsprachen und entsprechende Tastaturbelegungen gibt, kann es sein, dass Sie unter bestimmten Umständen mit einem falschen Tastaturlayout arbeiten müssen. Da wird aus dem „Ö“ schnell ein Doppelpunkt, etc. Schwierig wird es, wenn man spezielle Sonderzeichen sucht und diese einfach nicht finden kann.

Sollten speziellere Einstellungen innerhalb der Konsole vornehmen wollen, empfiehlt sich daher, das Tastaturlayout auf die von Ihnen präferierte Sprache anzupassen

Melden Sie sich hierzu zunächst mit dem Nutzer admin und dem aktuellen RCCMD-Passwort an und verschaffen Sie sich die Systemrechte eines Super-Users. In diesem Beispiel ist das Standardpasswort RCCMD gesetzt:

Schritt 1: Anmelden an der RCCMD Konsole

Anmeldename: admin
Passwort: RCCMD



Schritt 2: Super-User aktivieren

Befehl: sudo su
Passwort: RCCMD

```
Welcome to RCCMD-Appliance.
To configure RCCMD point your web browser to: [https://192.168.200.124]!
admin@rccmdAppliance:~$ sudo su
[sudo] password for admin:
root@rccmdAppliance:/home/admin#
```

Wenn es geklappt hatm steht dort statt *admin* das Wort *root@rccmdAppliance*

Im nächsten Schritt installieren Sie das entsprechende Tool, welches Ihnen die Konfiguration der Tastaturlayouts ermöglicht:

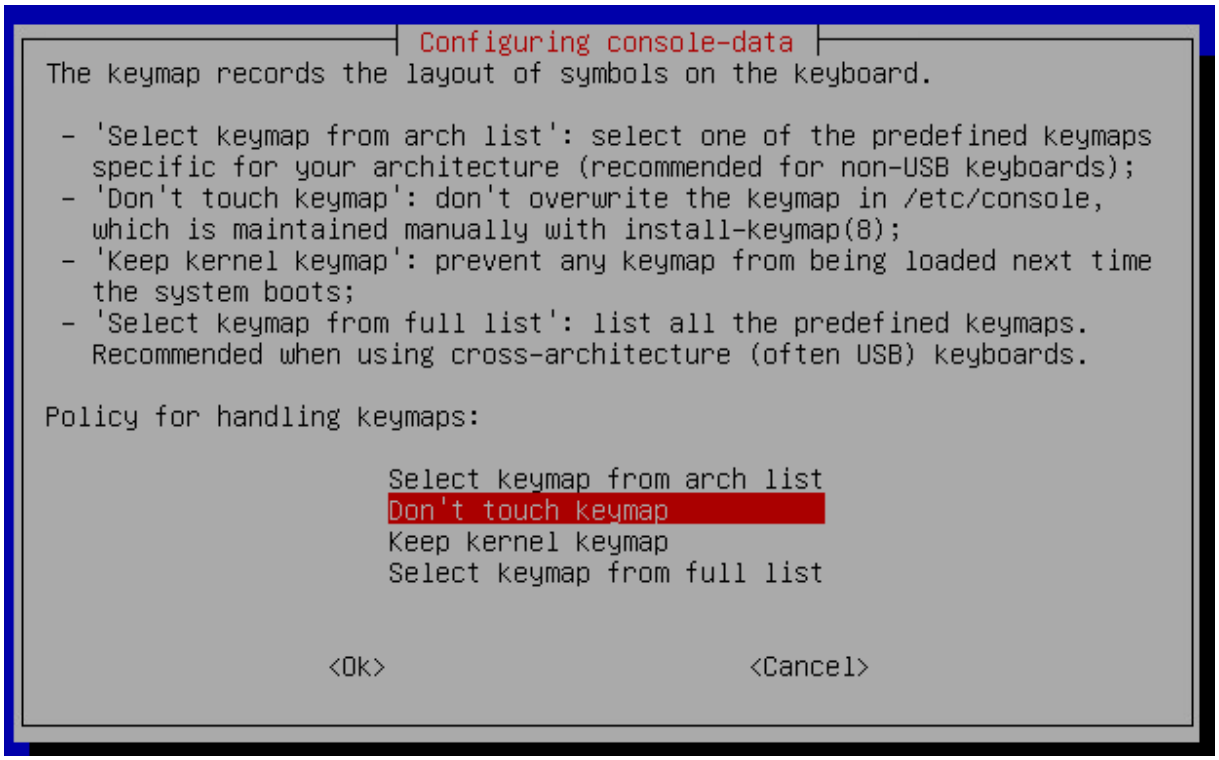
Befehl: apt-get install console-data

```
root@rccmdAppliance:/home/admin# apt-get install console-data
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  console-common
Suggested packages:
  unicode-data
The following NEW packages will be installed:
  console-common console-data
0 upgraded, 2 newly installed, 0 to remove and 1 not upgraded.
Need to get 0 B/1,270 kB of archives.
After this operation, 2,996 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

Bestätigen Sie die Installation.

Schritt 3 – Der Konfigurationsdialog

Nach der Installation startet automatisch der Konfigurationsdialog



Wählen Sie „Select keymap from full list" und betätigen Sie die Eingabetaste.

Wählen Sie im Anschluss aus der Liste verfügbarer Tastaturlayouts die von Ihnen gewünschte Tastatur aus und bestätigen Sie die Auswahl mit der Eingabetaste.

Das Tool installiert und aktiviert automatisch die gewünschte Tastatur.

Ändern des Tastaturlayouts

Da das Programm bereits installiert ist, können Sie den Dialog nicht mit dem install-Befehl erneut aufrufen – daher ändert sich in dem Fall auch der Befehl, den Sie verwenden müssen:

Befehl: dpkg-reconfigure console-data

Damit starten Sie den Konfigurationsdialog erneut, über den Sie die Tastatur auswählen können.

Tipp:

Der Befehl *sudo su* gibt Ihnen so lange administrative Rechte, bis Sie diesen Modus mit „exit“ wieder beenden. Als alternative können Sie natürlich auch sudo [befehl] direkt eingeben, müssen dann jedoch jedes Mal das Passwort erneut eingeben.

Tutorial: RCCMD Installation auf einem public ESXi Host

Wichtig:

Diese Anleitung beschreibt die Installation von RCCMD auf einem public domain ESXi Host.
Bitte beachten Sie, dass die Installation auf einem nicht lizenzfreien Host von Generex nicht offiziell unterstützt wird (die Warnung im RCCMD WebConfigurator verschwindet also nie).

Hier gibt es mehrere Möglichkeiten – welche Anleitung für Sie zutrifft entscheidet sich, ist von zwei Faktoren abhängig:

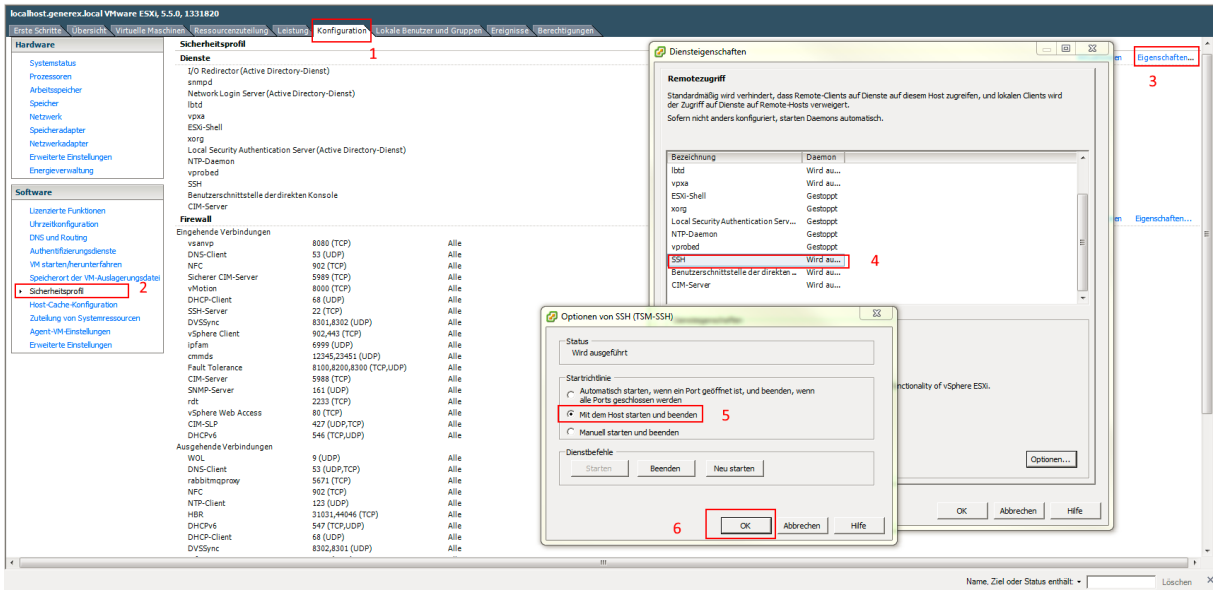
1. welche ESXi – Version wird verwendet
2. Welche RCCMD Version ist im Einsatz

RCCMD mit VMware 5.x verwenden

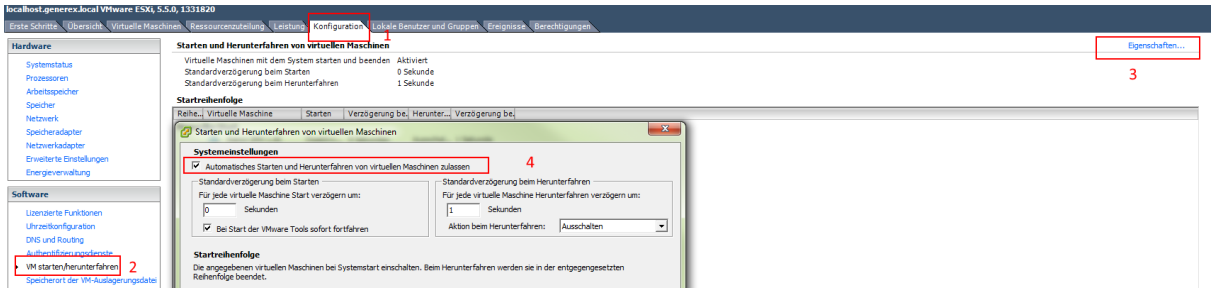
Für die Version 5.x wurde ein (schon lange abgekündigten) Media Assistant, von VMware selber angeboten, auf dem ein RCCMD für VMware installiert wurde. Für die Verwendung eines Free Hosts mit der Version 5.x müssen daher folgende Schritte durchgeführt werden:

1. Aktivieren Sie SSH im vSphere Client:

Wechseln Sie in der ESXi Host Konfiguration -> Software/Sicherheitsprofil -> Dienste -> Eigenschaften -> SSH -> Mit dem Host starten und beenden aus. Starten Sie den Dienst, und bestätigen Sie mit Ok.



2. Aktivieren Sie das automatische Starten und Herunterfahren von virtuellen Maschinen im vSphere Client.
-> Wechseln Sie in der ESXi Host Konfiguration -> VM starten/herunterfahren -> Eigenschaften, und aktivieren Sie den Haken für das automatische Starten und Herunterfahren von VMs zulassen.

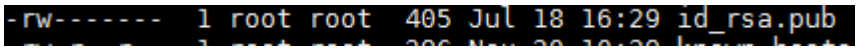


3. Stellen Sie sicher, dass auf allen VMS VMware Tools installiert sind.

4. Verbinden Sie sich via SSH mit der vMA, und kopieren Sie den Inhalt der Datei /root/.ssh/id_rsa.pub

5. Verbinden Sie sich via SSH mit den ESXi Host direkt, und hängen Sie den Inhalt von id_rsa.pub in die Datei /etc/ssh/keys-root/authorized_keys an.

Stellen Sie sicher, dass die Zugriffsberichtigung für die Datei authorized_key auf 600 steht!

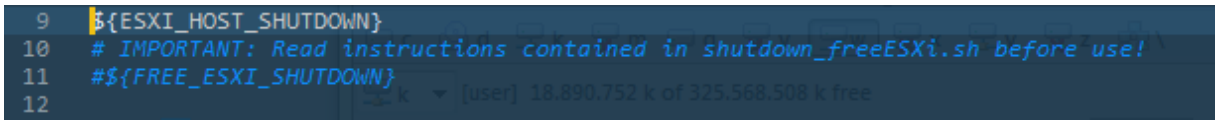


Der Befehl hierzu lautet: "chmod 600 /root/.ssh/id_rsa.pub "

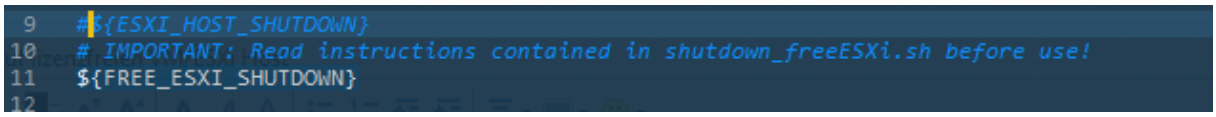
6. Verbinden Sie sich von der vMA via SSH auf den ESXi Host. Beim ersten Mal werden Sie aufgefordert, den Host Key zu den bekannten Hosts hinzuzufügen.

7. Überprüfen Sie die Konfiguration, indem Sie via SSH von der vMA mit den ESXi Host eine Verbindung aufbauen. Es sollte nun keine Passwortabfrage mehr erscheinen.
Wird dennoch ein Passwort verlangt, überprüfen Sie, ob die beiden Dateien wirklich 100% identisch sind. Wenn dies nicht der Fall ist, wiederholen Sie die Schritte 4-7.

8. Aktivieren Sie das FREE_ESXI_SHUTDOWN Skript in der rccmd_shutdown.sh.



Kommentieren Sie die Zeile ${ESXI_HOST_SHUTDOWN} mit # aus, und entfernen Sie in der Zeile #${FREE_ESXI_SHUTDOWN} den Kommentar am Anfang der Zeile.



Nun können Sie RCCMD testen.

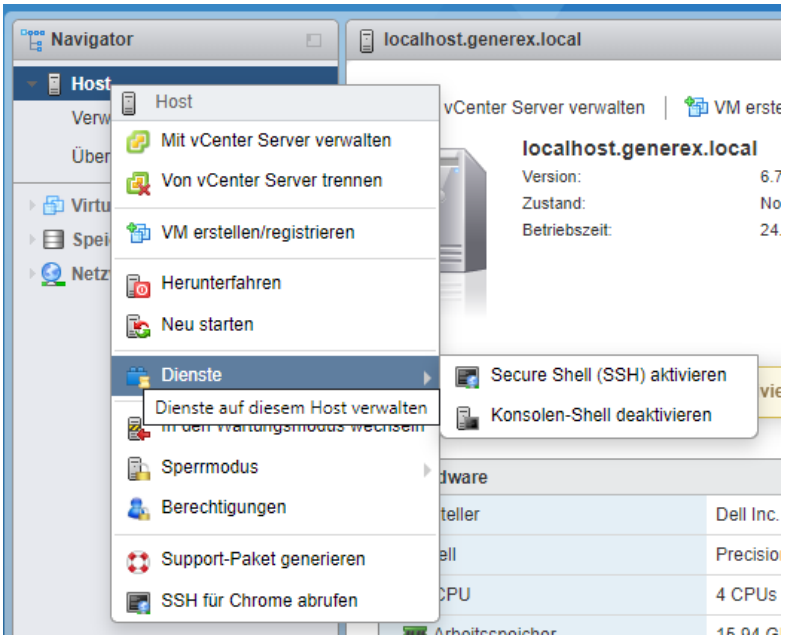
RCCMD mit vmware 6.7 und neuere Versionen verwenden

Die Version 6.7 geht ein wenig andere Wege, vor allem wurde mit der ESXi v. 6.5 die vma abgekündigt. RCCMD wird daher seit der ab Version 6.5 aufwärts dem entsprechend mit einer eigenen Appliance ausgeliefert, welche eine vorinstallierte und vorkonfigurierte RCCMD – Installation enthält.

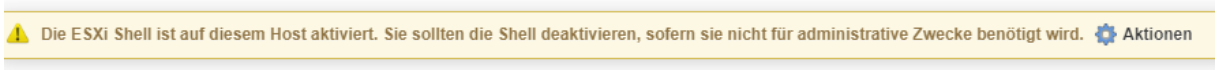
Hier entscheidet das Alter der jeweils verwendeten Appliance, welcher Konfigurationsweg notwendig ist.

Konfiguration für die RCCMD Appliance bis Version 4.54.12 231129

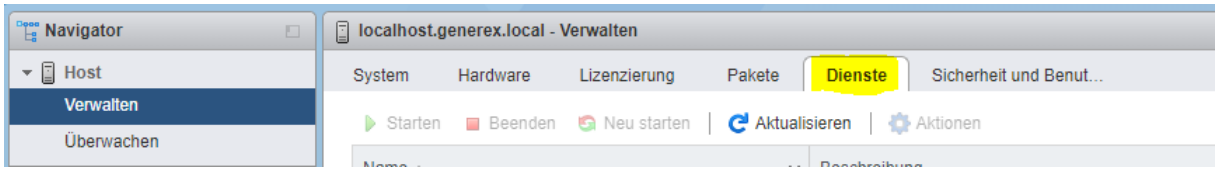
Gehen Sie hierzu wie folgt vor:
Aktivieren Sie die SSH -Konsole auf dem ESXi-Host



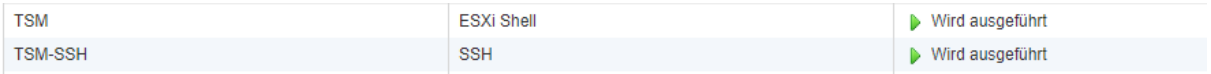
Klicken Sie hierzu am Einfachsten im Navigator mit der rechten Maustaste auf den Host und gehen Sie unter Dienste auf „Secure Shell (SSH) aktivieren. Wenn es funktioniert hat, wird Ihnen vmware eine entsprechende Meldung ausgeben:



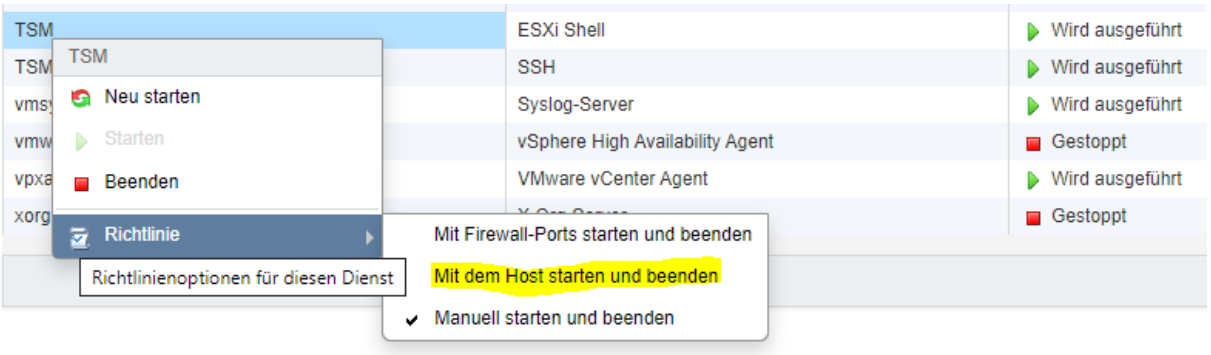
Stellen Sie sicher, dass die Dienste nicht nur temporär gestartet werden



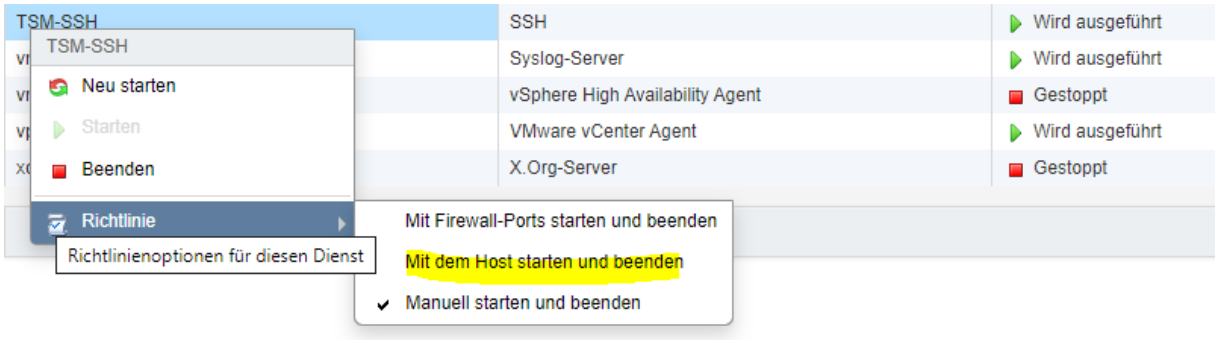
Klicken Sie hierzu im Navigator auf „Verwalten“ und öffnen den Reiter Dienste. Suchen Sie in der Liste vorhandener Dienste diese beiden Einträge:



Standardmäßig werden diese Dienste manuell gestartet und beendet. Als Konsequenz würde der Host den Dienst nach einem Neustart des Servers deaktiviert lassen. Klicken Sie zunächst mit der rechten Maustaste auf TSM und gehen Sie im Kontextmenü auf „Richtlinie“:



Ändern Sie den Eintrag von Manuell starten und beenden auf „Mit dem Host starten und beenden“. Wiederholen Sie den Schritt mit dem Dienst TSM-SSH:



Verbinden Sie die Appliance per SSH mit dem entsprechenden Host

Diesen Schritt können Sie nicht über das Webinterface machen, Sie müssen auf die Konsole der RCCMD Appliance wechseln. Nehmen Sie hierzu ein entsprechendes Tool wie das Freewareprogramm putty und loggen sich direkt auf der Konsole von RCCMD ein.

Alternativ können Sie auch über die Konsolenfunktion des Hosts die Konsole von RCCMD öffnen.

```
Debian GNU/Linux 9 rccmdAppliance tty1
Configure RCCMD at: https://192.168.81.138

Hint: Num Lock on

rccmdAppliance login: admin
Password:
Last login: Mon Oct 14 14:14:59 CEST 2019 on tty1
Linux rccmdAppliance 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Welcome to RCCMD-Appliance.
To configure RCCMD point your web browser to: [https://192.168.81.138]!
admin@rccmdAppliance:~$
```

Folgende Standardnutzer sind auf sshder Konsole vorgegeben:

Nutzer: admin
Passwort: RCCMD

Tipp:

Achten Sie darauf, unter welchen Nutzer Sie den Key erstellen, da dieser mit dem Nutzer, unter dem Sie selbigen erstellt haben, verknüpft ist. RCCMD versendet die Steuerbefehle an den Host mit dem Nutzer „root“, Sie melden sich jedoch bei RCCMD mit dem Nutzer Admin an. Wenn Sie nur den Nutzer „Admin“ einrichten, wird der ESXi-Host mit dem Nutzer Admin wie beschrieben funktionieren, aber den Shutdown ablehnen, da das Zertifikat für den RCCMD-internen Nutzer „root“ ungültig ist.

Um Verwirrung zwischen den Nutzern zu vermeiden, führen Sie die Prozedur sowohl mit dem Nutzer „admin“ als auch mit dem Nutzer root durch. Zum Aktivieren des Nutzers root geben Sie „sudo su“ ein.

Dadurch funktioniert der Zugriff sowohl mit dem Nutzer „admin“ als auch mit dem Nutzer „root“.

Erstellen Sie sich zunächst einen entsprechenden SSH Key, den Sie auf den ESXi-host übertragen können.

Befehl: ssh-keygen

```
admin@rccmdAppliance:~$ ssh-keygen
```

Folgen Sie den Anweisungen des Konfigurationsdialogs:

a. Wo soll der Key gespeichert werden?

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
```

Drücken Sie die Eingabetaste, um die Originaleinstellung zu belassen und zum nächsten Schritt zu gelangen.

Wenn Sie diesen Schritt schon einmal durchgeführt haben, existiert bereits ein entsprechender Key. In diesem Fall wird Sie ssh-keygen fragen, ob die Datei überschrieben werden soll:

```
/home/admin/.ssh/id_rsa already exists.
Overwrite (y/n)? y
```

b. Erweiterte Passwortsicherheit

In einigen Hochsicherheitsbereichen ist es notwendig, die Datei zusätzlich mit lokalen Passworten zu verschlüsseln. ssh-keygen gibt Ihnen hier die Möglichkeit zu. Wenn Sie keine zusätzliche Passwortsicherheit benötigen, um die Datei selber zu schützen, können Sie einfach mit der Eingabetaste bestätigen:

➔ Ein zusätzliches Passwort ist bei diesem Schritt optional.

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

c. Die Erstellung der Keys abschließen

```
Your identification has been saved in /home/admin/.ssh/id_rsa.
Your public key has been saved in /home/admin/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:rubVkhjMLzlXQAds8z708PagHW6UQsacuv9iYpdfdN8 admin@rccmdAppliance
The key's randomart image is:
+---[RSA 2048]----+
|        .o..     |
|        .+.      |
|        ..= .    |
|     o    .X     |
|      + S*.+ .. .|
|       *.++ O. .o|
|      = B..X +. E|
|       .*+.* +..  |
|     oo. =.=o    |
+----[SHA256]-----+
```

ssh-keygen teilt Ihnen mit, wohin genau die Key-Datei gespeichert wurde.

Übertragen des Keys an den ESXi Host, Teil 1

In diesem Schritt müssen Sie den eben erstellten Authentifizierungsschlüssel an den ESXi-Host übertragen, damit dieser entsprechend die RCCMD Appliance als permanent berechtigt einstufen kann.

Befehl: ssh-copy-id root@<Ihre IP-Adresse>

```
admin@rccmdAppliance:~$ ssh-copy-id -f root@192.168.200.107
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/id_rsa.pub"
Password:
```

Als Passwort benötigen Sie das root-Passwort Ihres ESXi hosts.

Da der Host derzeitig nicht authentifiziert werden kann, gibt die Appliance eine entsprechende Warnung aus und fragt, ob die Verbindung dennoch hergestellt werden soll:

```
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/id_rsa.pub"
The authenticity of host '192.168.200.107 (192.168.200.107)' can't be established.
RSA key fingerprint is SHA256:rbII6HjWaSPUcYUVfdiYttQurCL/1cjb2Ioveb/336c.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alr
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
Password:
```

Beantworten Sie die Frage mit „yes“ (nicht einfach y eingeben)

Wenn die Übertragung erfolgreich war, meldet die RCCMD Appliance folgendes Feedback:

```
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.200.107'"
and check to make sure that only the key(s) you wanted were added.

admin@rccmdAppliance:~$ _
```

Übertragen des Keys an den ESXi Host, Teil 2

Die Datei ist zwar standardmäßig korrekt übertragen worden, es gibt jedoch eine VMware-spezifische Abweichung in den Standard-Verzeichnissen, die noch korrigiert werden muss. Deshalb benötigen Sie nach wie vor das Passwort für den Nutzer root.

Geben Sie folgenden Befehl ein:

Befehl: ssh root@<IP-Adresse des Hosts>

```
admin@rccmdAppliance:~$ ssh root@192.168.200.107
Password:
```

Bei der Passwortabfrage geben Sie das Passwort des Nutzers root ein.

```
The time and date of this login have been sent to the system logs.

WARNING:
   All commands run on the ESXi shell are logged and may be included in
   support bundles. Do not provide passwords directly on the command line.
   Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~]
```

Beim ersten Mal werden Sie eventuell aufgefordert, den Host zu den bekannten Hosts hinzuzufügen – bestätigen Sie diesen Vorgang einmalig. Wenn es richtig funktioniert hat, sind Sie jetzt per SSH auf dem local host des ESXi-Servers verbunden.
Wechseln Sie jetzt in das ssh-Verzeichnis, in das der Befehl ssh-copy-id in Schritt 5 die Datei abgelegt hat und kontrollieren Sie, ob die Keydatei tatsächlich vorliegt:

Befehl 1: cd /.ssh
Befehl 2: ls
Die Konsole wird Ihnen die Datei authorized_keys anzeigen.

```
[root@localhost:~] cd /.ssh
[root@localhost:/.ssh] ls
authorized_keys
[root@localhost:/.ssh] _
```

Der Inhalt dieser Datei muss jetzt an die „scharfe“ authorized_keys des ESXi-Hosts angehängt werden:

Befehl: cat 43uthorized_keys >> /etc/ssh/keys-root/authorized_keys

```
[root@localhost:/.ssh] cat authorized_keys >> /etc/ssh/keys-root/authorized_keys
```

Verlassen Sie anschließend mit exit die SSH-Konsole und loggen Sie sich aus der RCCMD Appliance aus:

Befehlssequenz: exit, exit, exit…

```
[root@localhost:/.ssh] exit_
```

So überprüfen Sie, ob die SSH-Konsole richtig eingerichtet wurde:

```
Debian GNU/Linux 9 rccmdAppliance tty1
Configure RCCMD at: https://192.168.81.138

rccmdAppliance login: _
```

Ob Sie das Zertifikat richtig eingebunden haben können Sie überprüfen, indem Sie sich noch einmal mit SSL bei dem Host-Server einwählen. Wenn das Zertifikat richtig hinterlegt wurde, sollten Sie nun nicht mehr nach einem Passwort gefragt werden.

Melden Sie sich an der RCCMD-Appliance in der Konsole an

Nutzer: admin
Passwort:RCCMD

Und wechseln anschließend direkt per SSH auf den RCCMD host

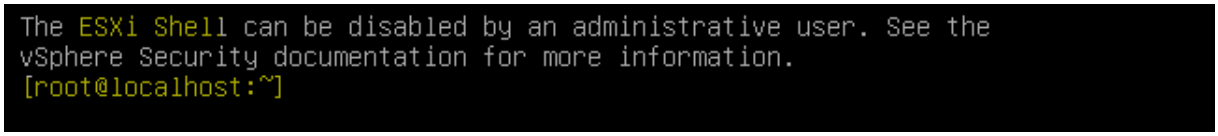
Befehl: ssh root@<IP-Adresse des Hosts>

Sie sollten jetzt als Nutzer root auf den ESXi-Host gelangen, ohne dass Sie ein Passwort eingeben müssen:

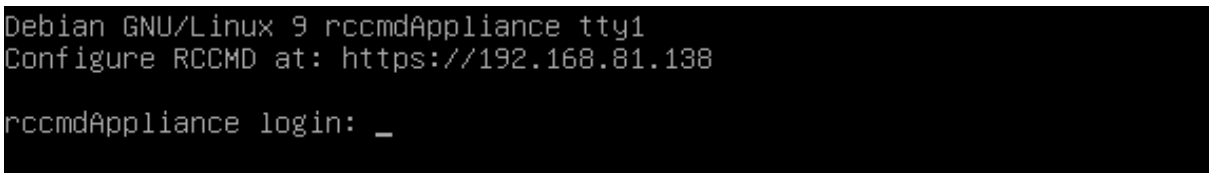
Lokaler login bei der RCCMD Appliance:

SSH-Befehl zu Ihrem ESXi-Host

Welcome-Screen des ESXi-Hosts:



So überprüfen Sie, ob die SSH-Konsole richtig eingerichtet wurde:



Ob Sie das Zertifikat richtig eingebunden haben können Sie überprüfen, indem Sie sich noch einmal mit SSL bei dem Host-Server einwählen. Wenn das Zertifikat richtig hinterlegt wurde, sollten Sie nun nicht mehr nach einem Passwort gefragt werden.

Melden Sie sich an der RCCMD-Appliance in der Konsole an

Nutzer: admin
Passwort: RCCMD

Und wechseln anschließend direkt per SSH auf den RCCMD host

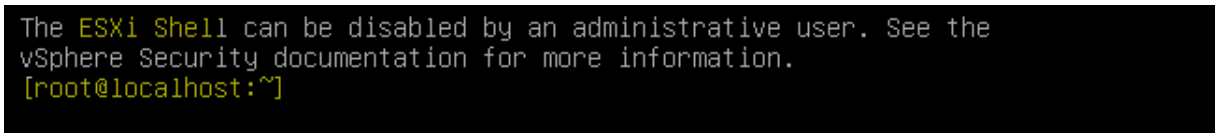
Befehl: ssh root@<IP-Adresse des Hosts>

Sie sollten jetzt als Nutzer root auf den ESXi-Host gelangen, ohne dass Sie ein Passwort eingeben müssen:

Lokaler login bei der RCCMD Appliance:

SSH-Befehl zu Ihrem ESXi-Host

Welcome-Screen des ESXi-Hosts:



RCCMD auf public ESXi Server Script umstellen

Im letzten Schritt müssen Sie nur noch RCCMD mitteilen, dass es sich um einen Public Server (bzw. eine Community Edition) handelt. Hierzu müssen Sie das spezielle Shutdownscript von Hand anpassen.

Melden Sie sich in der Konsole der RCCMD Appliance mit dem User „admin“ an und wechseln Sie mit folgendem Befehl in das Skriptverzeichnis und lassen sich den Inhalt anzeigen:

Befehl 1: cd /opt/rccmd/remoteHostScripts/
Befehl 2: ls

```
admin@rccmdAppliance:~$ cd /opt/rccmd/remoteHostScripts/
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$ ls
bash_tools.sh                                pltmp.pl
cache_host_dns_names.sh                      rccmd_shutdown.sh
checkESXipwd.pl                              registerGXPlugin.sh
checkESXiVersion.pl                          registerPlugin.pl
get_ESXi_Hosts_from_vCenter.pl               shutdown_ESXI.pl
getESXiVersionNumber.pl                      shutdown_ESXI.sh
is_ESXI_in_maintenancemode.pl                shutdown_freeESXi.sh
listESXiLicenses.pl                          shutdown_Vms.pl
maintenancemode_ESXi_direct.pl               verify_hosts.pl
maintenancemode_vcenter.pl                   vsanHostMaintenanceMode.pl
noBlockSendOneHostIntoMaintenanceMode.pl
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$
```

Bitte beachten Sie, dass es hier Abweichungen geben kann: Ältere Versionen von RCCMD verwenden hier das Verzeichnis /usr/rccmd, wogegen neuere Versionen als Verzeichnis /opt/rccmd verwenden.

Das Script, welches Sie editieren müssen, heißt rccmd_shutdown.sh. Die RCCMD Appliance bietet Ihnen hierzu den nutzerfreundlichen Editor nano an, welcher bereits vorinstalliert ist. Da dieses Skript Systemrelevant ist, können Sie diese Datei nur als Super User editieren:

Befehl: sudo nano rccmd_shutdown_sh

```
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$ sudo nano rccmd_shutdown.sh
[sudo] password for admin:
```

Ändern Sie das Skript wie folgt:

Mit STRG + X beenden Sie den Editor.
Beantworten Sie die Frage, ob gespeichert werden soll, mit Y

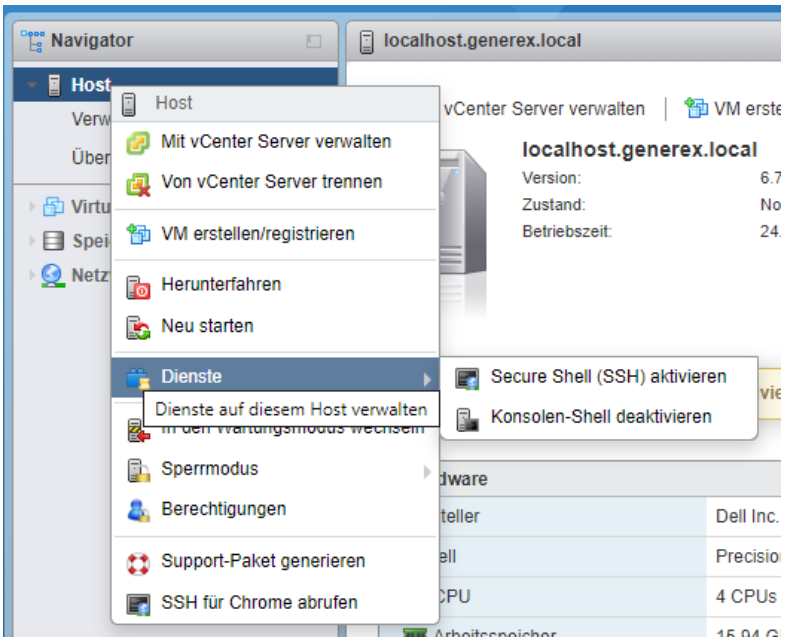
```
Save modified buffer?  (Answering "No" will DISCARD changes.)
 Y Yes
 N No           ^C Cancel
```

RCCMD kann fehlerfrei mit Ihrem Free ESXi Host verwendet werden.

Konfiguration für die RCCMD Appliance an Version 4.54.12 231129

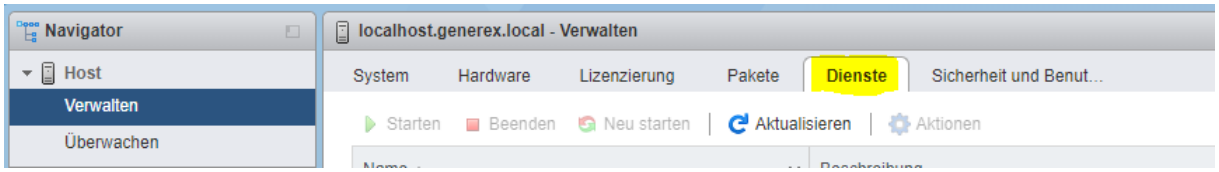
Mit der Version 4.45.12 231129 entfallen ein paar wesentliche Schritte, was die Konfiguration erheblich einfacher gestaltet:

Aktivieren Sie die SSH -Konsole auf dem ESXi-Host



Klicken Sie hierzu am einfachsten im Navigator mit der rechten Maustaste auf den Host und gehen Sie unter Dienste auf „Secure Shell (SSH) aktivieren. Wenn es funktioniert hat, wird Ihnen VMware eine entsprechende Meldung ausgeben:

Stellen Sie sicher, dass die Dienste nicht nur temporär gestartet werden



Klicken Sie hierzu im Navigator auf „Verwalten“ und öffnen den Reiter Dienste. Suchen Sie in der Liste vorhandener Dienste diese beiden Einträge:

TSM	ESXi Shell	Wird ausgeführt
TSM-SSH	SSH	Wird ausgeführt

Standardmäßig werden diese Dienste manuell gestartet und beendet. Als Konsequenz würde der Host den Dienst nach einem Neustart des Servers deaktiviert lassen. Klicken Sie zunächst mit der rechten Maustaste auf TSM und gehen Sie im Kontextmenü auf „Richtlinie“:

Ändern Sie den Eintrag von Manuell starten und beenden auf „Mit dem Host starten und beenden“. Wiederholen Sie den Schritt mit dem Dienst TSM-SSH:

Verbinden Sie die Appliance per SSH mit dem entsprechenden Host

Diesen Schritt können Sie nicht über das Webinterface machen, Sie müssen auf die Konsole der RCCMD Appliance wechseln. Nehmen Sie hierzu ein entsprechendes Tool wie das Freeware Programm putty und loggen sich direkt auf der Konsole von RCCMD ein.

Alternativ können Sie auch über die Konsolenfunktion des Hosts die Konsole von RCCMD öffnen.

```
Debian GNU/Linux 9 rccmdAppliance tty1
Configure RCCMD at: https://192.168.81.138

Hint: Num Lock on

rccmdAppliance login: admin
Password:
Last login: Mon Oct 14 14:14:59 CEST 2019 on tty1
Linux rccmdAppliance 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Welcome to RCCMD-Appliance.
To configure RCCMD point your web browser to: [https://192.168.81.138]!
admin@rccmdAppliance:~$
```

Folgende Standardnutzer sind auf sshder Konsole vorgegeben:

Nutzer: admin
Passwort: RCCMD

RCCMD auf Public ESXi Server Script umstellen

Im letzten Schritt müssen Sie nur noch RCCMD mitteilen, dass es sich um einen Public Server (bzw. eine Community Edition) handelt. Hierzu müssen Sie das spezielle Shutdownscript von Hand anpassen.

Melden Sie sich in der Konsole der RCCMD Appliance mit dem User „admin“ an und wechseln Sie mit folgendem Befehl in das Skriptverzeichnis und lassen sich den Inhalt anzeigen:

Befehl 1: cd /opt/rccmd/remoteHostScripts/
Befehl 2: ls

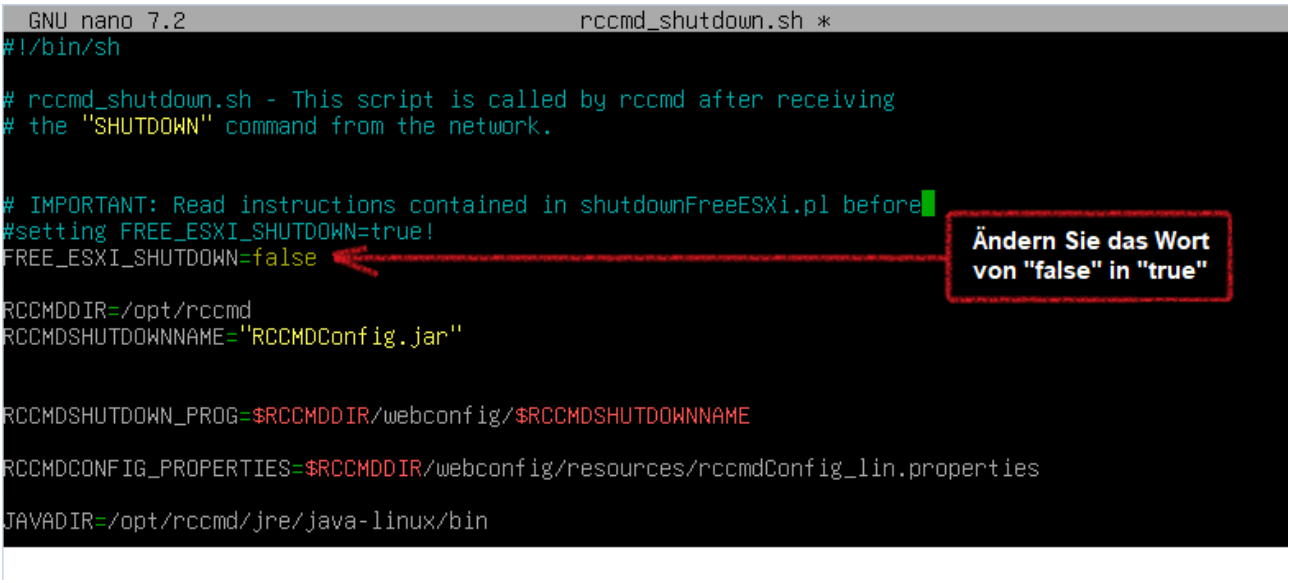
```
admin@rccmdAppliance:~$ cd /opt/rccmd/remoteHostScripts/
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$ ls
bash_tools.sh                                  pltmp.pl
cache_host_dns_names.sh                        rccmd_shutdown.sh
checkESXipwd.pl                                registerGXPlugin.sh
checkESXiVersion.pl                            registerPlugin.pl
get_ESXi_Hosts_from_vCenter.pl                 shutdown_ESXI.pl
getESXiVersionNumber.pl                        shutdown_ESXI.sh
is_ESXI_in_maintenancemode.pl                  shutdown_freeESXi.sh
listESXiLicenses.pl                            shutdown_Vms.pl
maintenancemode_ESXi_direct.pl                 verify_hosts.pl
maintenancemode_vcenter.pl                     vsanHostMaintenanceMode.pl
noBlockSendOneHostIntoMaintenanceMode.pl
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$
```

Das Script, welches Sie editieren müssen, heißt rccmd_shutdown.sh. Die RCCMD Appliance bietet Ihnen hierzu den nutzerfreundlichen Editor nano an, welcher bereits vorinstalliert ist. Da dieses Skript Systemrelevant ist, können Sie diese Datei nur als Super User editieren:

Befehl: sudo nano rccmd_shutdown_sh

```
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$ sudo nano rccmd_shutdown.sh
[sudo] password for admin:
```

Ändern Sie das Skript wie folgt:



1. Suchen Sie nach der Zeile FREE_ESXI_SHUTDOWN=**false**
2. Ändern Sie die Zeile wie folgt: FREE_ESXI_SHUTDOWN=**true**

Mit STRG + X beenden Sie den Editor.
Beantworten Sie die Frage, ob gespeichert werden soll, mit Y

```
Save modified buffer?  (Answering "No" will DISCARD changes.)
 Y Yes
 N No           ^C Cancel
```

RCCMD kann mit Ihrem Free ESXi Host verwendet werden.

A - Vorgehensweise bis Version 4.54.12 231129:

Wichtig: Manuell erstellte Backups aus älteren Programmversionen können nicht eingespielt werden, Ab der Version 4.54.X.231129 muss einmalig RCCMD neu konfiguriert werden.

1. Update von Bestanddsystemen

Ein generelles Update von RCCMD innerhalb der bestehenden Appliance ist nicht möglich – für ein Update rollen Sie bitte eine neue Appliance wie beschrieben aus.

Backup & Restore

Wichtig bei älteren RCCMD – Installationen:

A. Wenn Sie von einer älteren RCCMD-installation auf die aktuelle Version wechseln, dann befinden sich die für das Backup notwendigen Dateien abweichend im Verzeichnis ***/usr/****rccmd*, wogegen die neue Appliance als Speicherort standardmäßig **/opt/**rccmd verwendet.

B. Mit der Version 4.54.12 231129 bietet Ihnen RCCMD die Möglichkeit an, über das Webinterface via Drag'n'Drop durchzuführen.

A – Sollten Sie eine ältere Version von RCCMD aktualisieren wolle

Das Backup & Restore muss in diesem Fall händisch durchgeführt werden, indem Sie die notwendigen Dateien über die Konsole direkt sichern, und späte rwieder zurückspielen.

Achten Sie bei den Arbeiten darauf, dass Sie sich im Vorfeld mit dem Befehl **sudo su** die notwendige administrative Freigabe erhalten haben.

1. Erstellen eines Backups
2. Ausrollen der neuen Appliance
3. Einspielen der Backupdateien

Punkt 1: Erstellen eines Backups:

a. Wechseln Sie in das Verzeichnis /opt/rccmd
Sichern Sie folgende Dateien:
   - Die Datei „rccmd.cfg"

b. Wechseln Sie in das Verzeichnis /opt/rccmd/webconfig/resources
Sichern Sie die folgenden Dateien:
   - rccmdConfig_eclipse.properties
   - ream.properties

c. Sichern Sie Ihre eigenen Skripte.

Punkt 2.Installationsarbeiten durchführen

Rollen Sie wie beschrieben die neue Appliance aus.

Punkt 3: Backup einspielen:

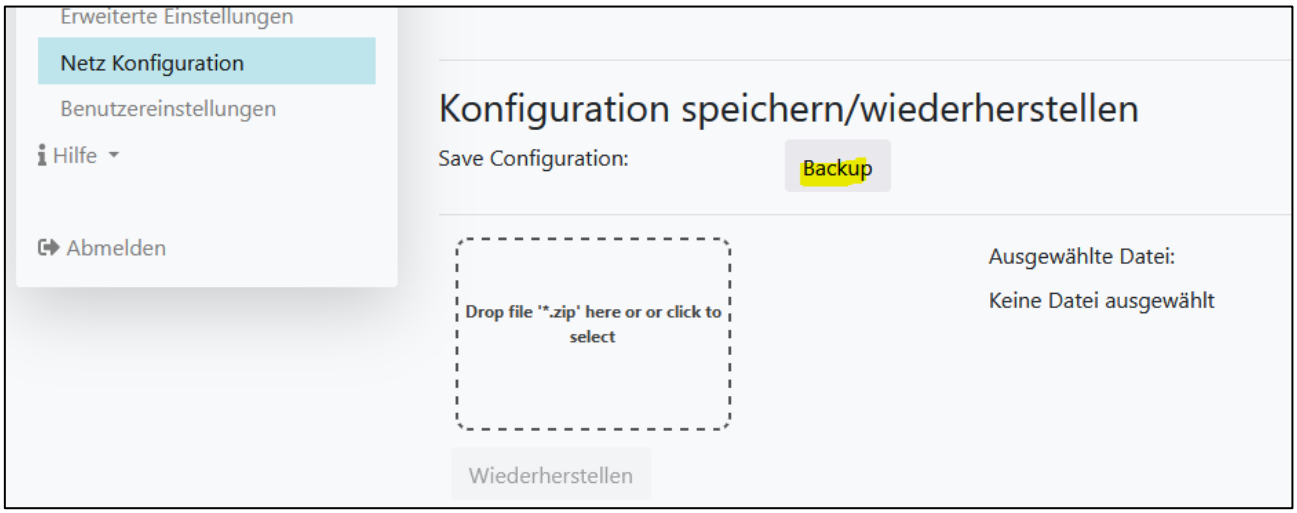
Das Einspielen des Backups wird ähnlich wie die Sicherung durchgeführt:

- Kopieren Sie Ihre Skripte wieder zurück in die entsprechenden Verzeichnisse.
- Wechseln Sie in das Verzeichnis /opt/rccmd
  - Legen Sie hier Ihre gesicherte rccmd.cfg ab und überschreiben Sie die existierende Datei
- Wechseln Sie in das Verzeichnis /opt/rccmd/webconfig/resources
  Legen Sie hier die folgenden Dateien aus Ihrem Backup ab und überschreiben Sie eventuell existierende Dateien:
  - rccmdConfig_eclipse.properties
  - realm.properties
- Um das Datenbackup zu aktivieren starten Sie RCCMD neu.
- Überprüfen Sie die Einstellungen und Funktionen.

B – Backup/Restore über die Weboberfläche RCCMD ab Version 4.54.12 231129

Wichtig: Datensicherungen früherer Programmversionen sind nicht mit dieser Funktion kompatibel! Mit der Programmversion 4.54.X.231129 ist eine Erstkonfiguration von RCCMD zwingend erforderlich.

So führen Sie das Backup mit Hilfe des Webinterfaces durch:



1. Backup erstellen

   Klicken Sie unter Netz Konfiguration auf „Backup“, um ein Backupfile zu erstellen und automatisch herunterzuladen.

2. Ip-Adresse notieren und Appliance herunterfahren.
   Nachdem Sie die IP-Adresse notiert haben, fahren Sie die bestehende Appliance herunter und schalten Sie diese aus. Es ist nicht notwendig, die virtuelle Maschine gleich zu löschen.

3. Rollen Sie eine neue Appliance aus

   Wichtig: Um auf das Webinterface zugreifen zu können, benötigt die Appliance eine gültige IP-Adresse. Sollte diese nicht beim Ausrollprozess vergeben worden sein oder kein DHCP – Server zur Verfügung stehen, müssen Sie die IP-Adresse manuell über die Konsole zuweisen.

4. Spielen Sie das Backup ein

   Platzieren Sie das Backupfile wie heruntergeladen in der vorgegebenen Box und klicken Sie auf Wiederherstellen.

5. Testen Sie die Einstellungen

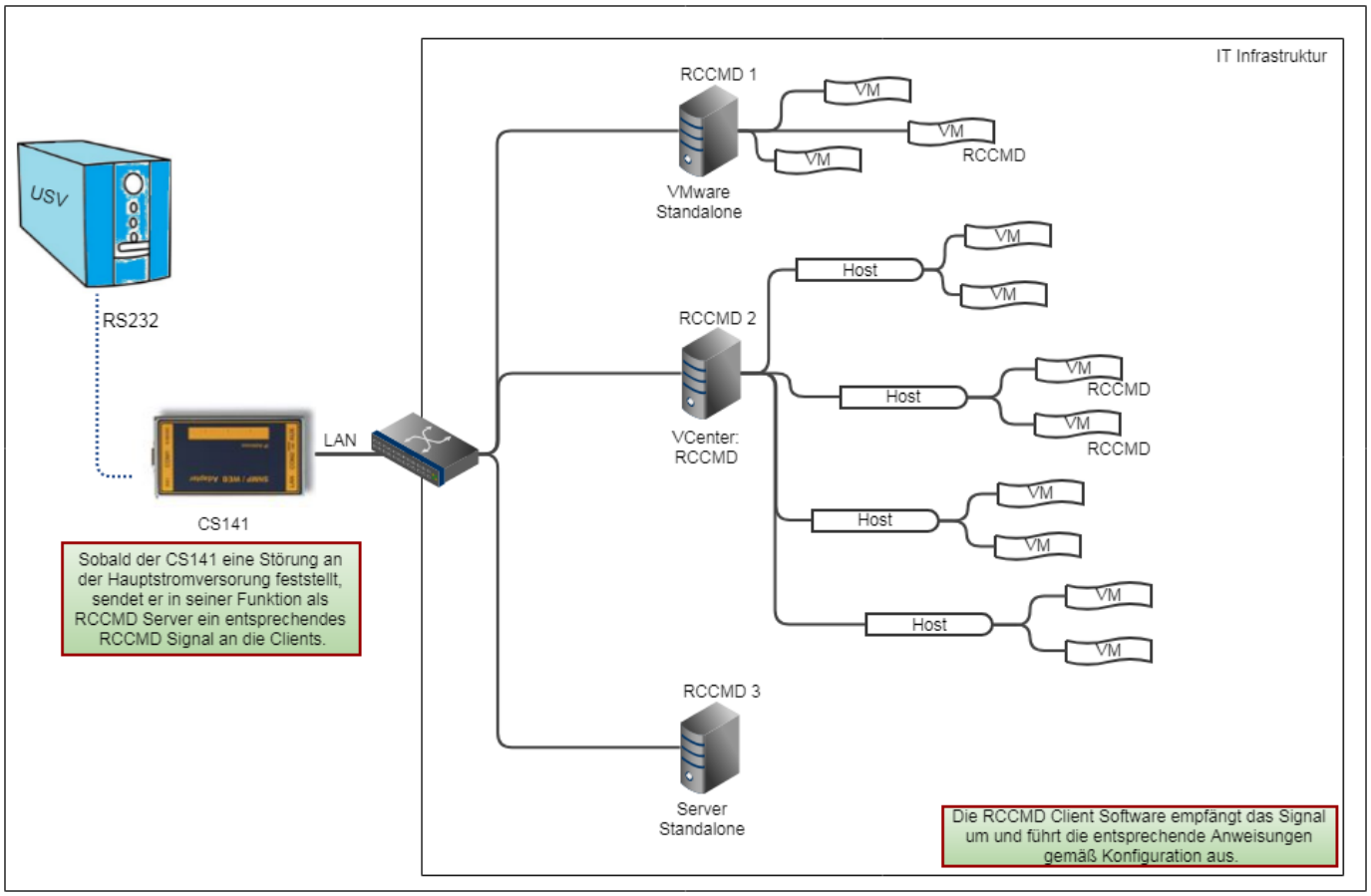
   Beachten Sie bitte, dass das Backup bei einigen Funktionen auf eine bestimmte IP-Adresse zugeschnitten wurde. Wenn Sie z.B. die IP-Adresse über einen DHCP-Server erhalten haben, kann es sein, dass sich diese geändert hat. Als Folge schickt ein CS141 ein Signal an die „alte“ IP-Adresse, wodurch der RCCMD Shutdown ins Leere laufen würde.

Installation – RCCMD für Microsoft Windows

Installation unter Windows Betriebssystemen

Der Unterschied zu VMware

Unter VMware funktioniert RCCMD ein anders:



Der CS141 sendet in der Regel in seiner Funktion als gültiger RCCMD Server Steuersignale an einen Client, welcher je nach Konfiguration die entsprechenden Befehle umsetzt. Dabei gibt es zwei grundsätzliche Möglichkeiten:

1. Das Signal ist gültig und der Sender ist berechtigt.
2. Das Signal ist gültig, aber der Sender ist unberechtigt

Der Unterschied zwischen VMware, Hyper-V und einem einzelnen Server zeigt sich im Detail:

Unter VMware laufen auf einem Host laufen Normalfall unterschiedliche virtuelle Maschinen. Wenn RCCMD auf einem Host installiert wird, kommuniziert RCCMD nicht mit den virtuellen Maschinen, sondern lediglich mit dem Trägersystem. Dabei ist sowohl die Größe des Hosts als auch die Anzahl der Hosts nicht von Bedeutung:

Sobald die IP-Adresse bekannt ist, kann die RCCMD Appliance mit dem entsprechenden Host kommunizieren. Sie können in einem Verbund RCCMD einfach die Zugangsdaten von weiteren Hosts mitteilen. Die virtuellen Maschinen, die auf dem entsprechenden Host installiert sind, werden von der RCCMD Appliance nicht angefasst. Das Herunterfahren oder Verschieben ist in diesem Zusammenhang eine Angelegenheit zwischen Host und ggfs. dem vCenter.

Windows Betriebssysteme und Hyper-V funktionieren hier anders:

Sie haben ein Windows Betriebssystem, auf dem Sie mit Hyper-V virtuelle Maschinen laufen lassen können. Wenn das Windows Betriebssystem heruntergefahren wird, übernimmt Hyper-V die Koordination von Verschieben und Herunterfahren einzelner virtueller Maschinen. Da RCCMD in diesem Fall keine eigene virtuelle Maschine, sondern ein laufendes Programm ist, bewegen Sie sich wie bei einem Standalone-System auf der Ebene des lokalen Administrators:

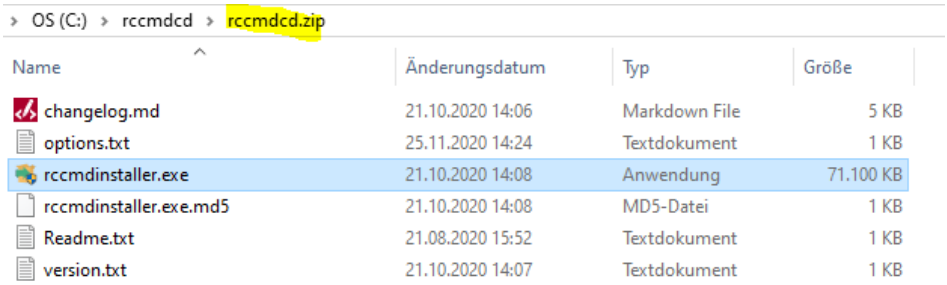
Sie können Jobs ausführen und lokale Skripte anstoßen, über Die sie alles, was sich auf dem Server befindet, automatisieren können. Bei einem Hyper-V Cluster können Sie einen Windows-PC herunterfahren, und Hyper-V kümmert sich um den Verbleib der virtuellen Maschinen.

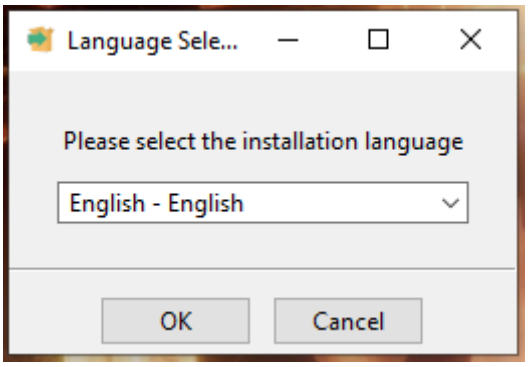
Dadurch fallen einige Menüs weg, die unter VMware wichtig sind, und werden durch andere Menüpunkte ersetzt, welche ausschließlich bei Standalone-Servern bzw. Einzelplatzinstallationen möglich sind, ohne dass sich das Konzept von RCCMD ändert.

Installation unter Windows mit GUI

Starten Sie das Setup, um die Installation zu beginnen:

Entpacken Sie zunächst die Datei vollständig (nicht mit der Preview von Windows verwechseln) und wechseln Sie in das Installationsverzeichnis:



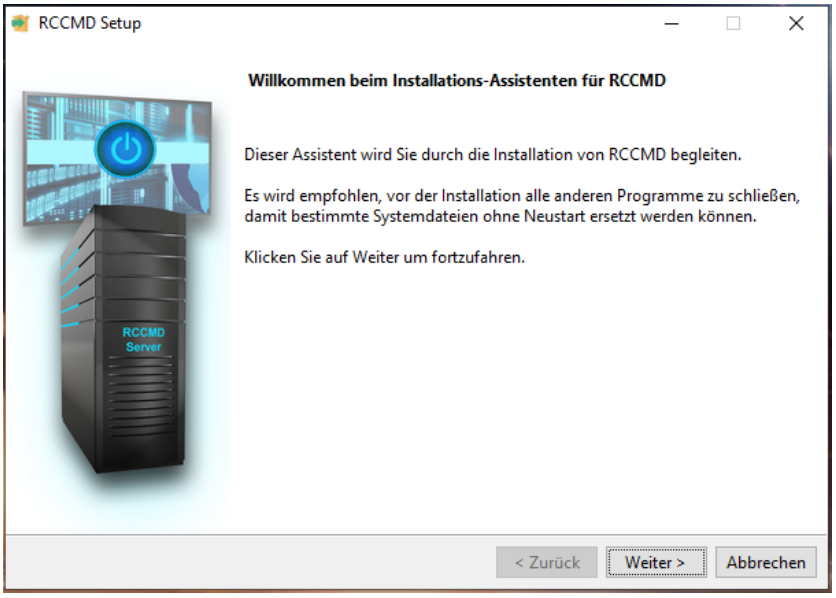


Wählen Sie zunächst die Sprache aus, in der Sie die Installation durchführen möchten. Beachten Sie bitte, dass diese Sprachauswahl keinen Einfluss auf den RCCMD Client selber hat – diese können Sie später bei der Konfiguration von RCCMD anpassen.

Wenn Sie Ihre Auswahl getroffen haben, betätigen Sie OK, um die Installation zu beginnen.

Der Installationsdialog

Der Installationsdialog, der Sie durch die Installation führt, ist in zwei unterschiedliche Bereiche unterteilt:

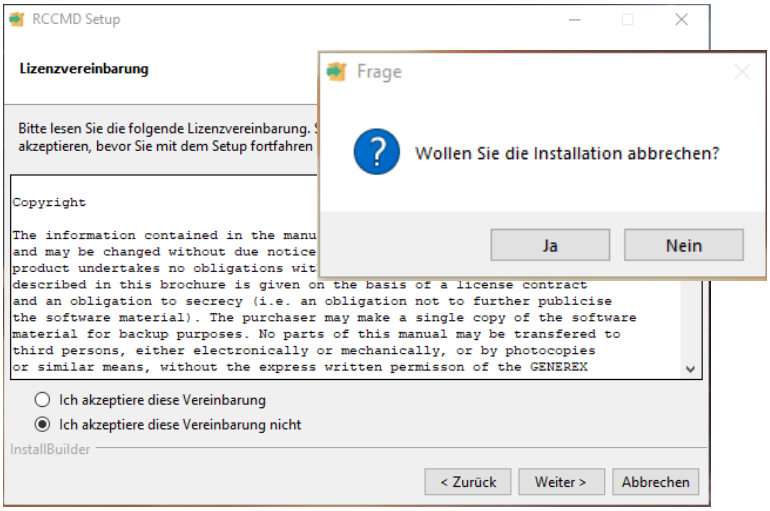


Der Dialog ist linear – Beantworten Sie einfach die Fragen und drücken Sie auf „Weiter“ ….

Tipp
Die eigentliche Installation wird erst durchgeführt, nachdem Sie alle für die Installation notwendigen Schritte durchlaufen haben und mit Fertig die Eingaben bestätigen.

Schritt 1: AGB's und Nutzungsbedingungen

In diesem Schritt dürfen Sie die Garantie- Copyright- und Nutzungsbedingungen lesen oder alternativ auch ohne zu lesen einfach für gut befinden und dafür sind. Sollten Sie nicht einverstanden sein, ist der Installationsprozess nach einer Rückfrage beendet und der Vorgang wird ohne Änderungen an Ihrem System *abgebrochen:*



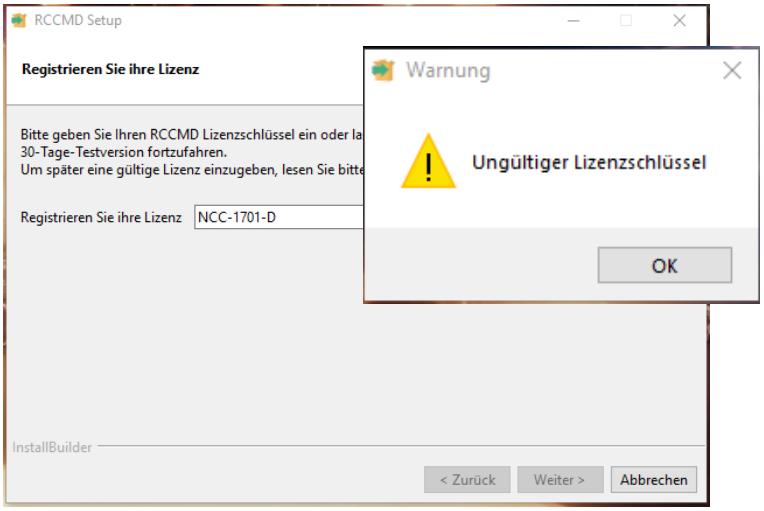
Schritt 2: Lizenzschlüssel eingeben

Der RCCMD Lizenzkey liegt entweder Ihrem CS141 bei oder Sie haben eine Mail erhalten, in der ein gültiger Key vorliegt.

Geben Sie den Lizenzschlüssel ein und klicken Sie auf „Weiter" – Der Installer überprüft automatisch die Gültigkeit und weist Sie bei Bedarf auf einen Fehler hin.

Wenn Sie keinen Lizenzschlüssel zur Hand haben, lassen Sie das Feld leer und klicken direkt auf „Weiter", RCCMD wird dann automatisch einen internen Evaluationskey verwenden, welcher für 30 Tage gültig ist.

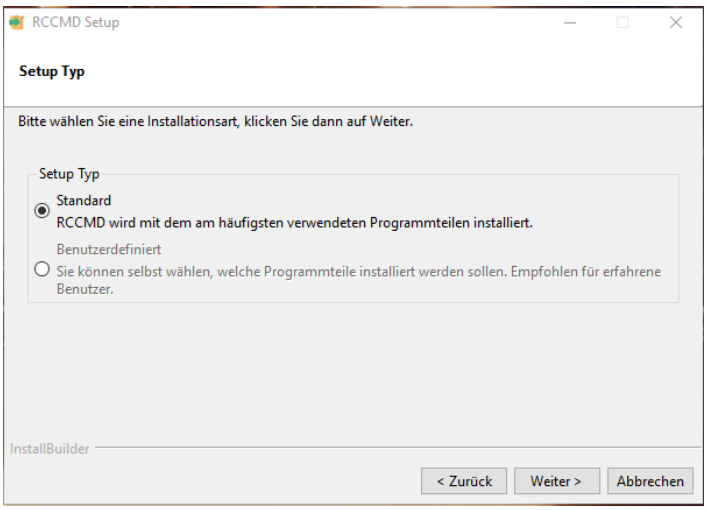
➔ Wenn Sie fertig sind, drücken Sie auf „Weiter"



Schritt 3: Setupmethode auswählen.

Die Standardinstallation installiert die empfohlene Startkonfiguration mit allen für den Betrieb empfohlenen Modulen und Standard Ports.

Die Benutzerdefinierte Installation richtet sich an erfahrene Benutzer und Systemintegratoren, die grundlegende RCCMD-Einstellungen bereits bei der Installation an das Zielsystem anpassen wollen.



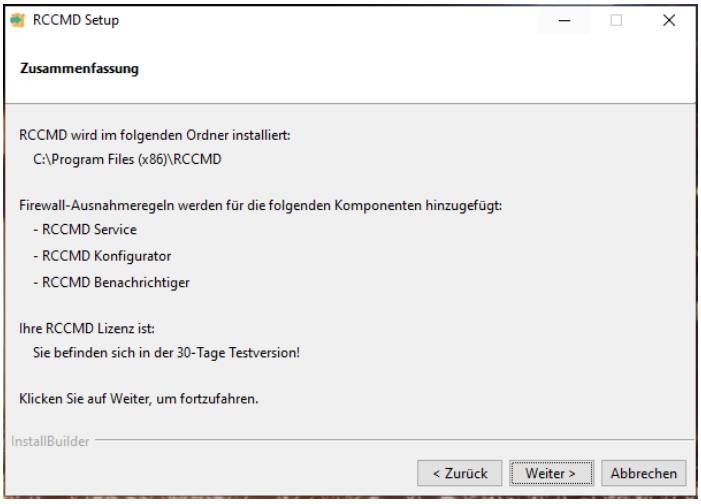
Schritt 3 - Standard

Die Installationsübersicht

Sie erhalten eine kurze Übersicht über die auszuführenden Installationsarbeiten. Wenn Sie mit den Vorgaben einverstanden sind, drücken Sie auf „Weiter“, um mit der Installation zu beginnen.

Wenn Sie Einstellungen an Ihr Zielsystem anpassen möchten, drücken Sie auf „Zurück“ und wählen die Option Benutzerdefiniert aus.

Mit „Abbrechen“ wird der Installationsdialog beendet, es werden keine Änderungen an Ihrem System durchgeführt.



➔ ***Klicken Sie „Zurück“ um Änderungen an Ihrer Einstellung durchzuführen.***

➔ ***Klicken Sie auf „Weiter“, um die Installation zu beginnen.***

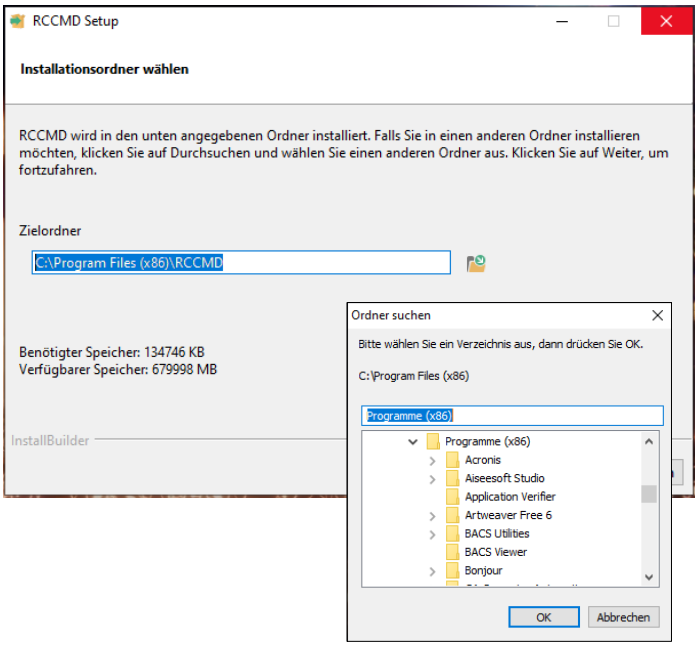
Schritt 3a – Benutzerdefiniert

Installationspfad angeben

Der Installationspfad bestimmt, wo RCCMD installiert werden soll. Üblicherweise verwendet RCCMD den Standardpfad für Programme, wie er in Windows Betriebssystemen vorgegeben ist.

Wenn Sie einen abweichenden Programmpfad verwenden möchten, können Sie hier das Installationsziel direkt angeben.

Für den grafischen Dateimanager klicken Sie neben dem Eingabefeld auf das Ordnersymbol:



➔ *Wenn Sie Ihre Einstellungen durchgeführt haben, klicken Sie auf „Weiter“*

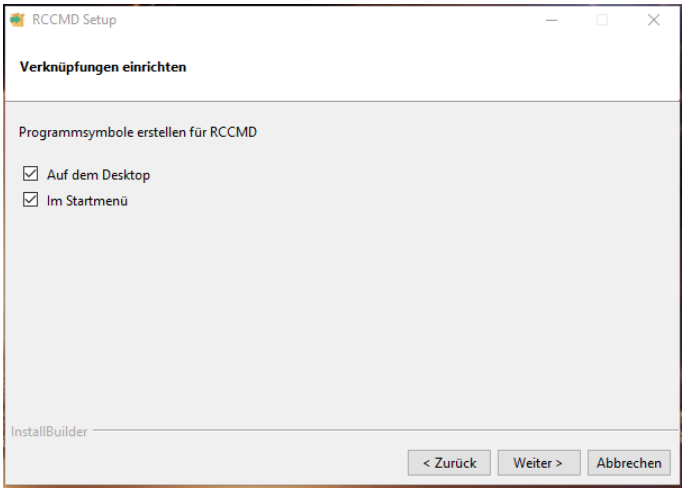
Schritt 3b – Benutzerdefiniert

Programmsymbole erstellen

Die Programmsymbole sind Schnellstarter, mit denen Funktionen von RCCMD von der Oberfläche des Betriebssystems aus direkt erreicht werden können.

Wenn Sie sich zu einem späteren Zeitpunkt remote auf den entsprechenden Computer verbinden, können Sie mit den Schnellstartsymbolen komfortabel RCCMD lokal konfigurieren.

Wenn Sie keine Programmsymbole haben möchten, können Sie die Haken entfernen.



➔ *Wenn Sie Ihre Einstellungen durchgeführt haben, klicken Sie auf „Weiter“*

Schritt 3c – Benutzerdefiniert

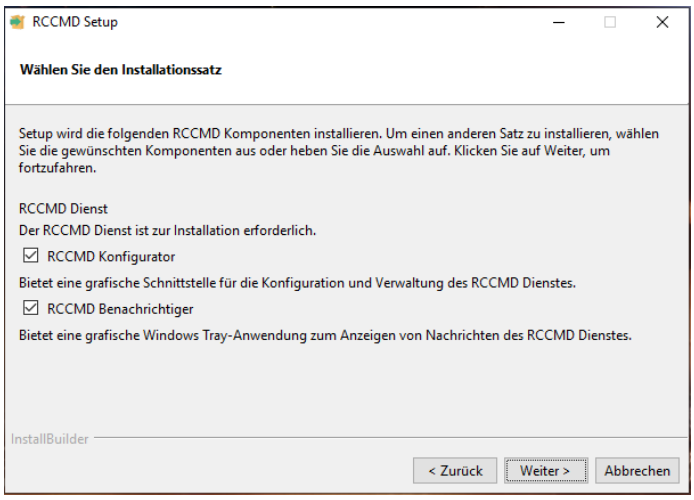
Module auswählen

RCCMD besteht aus mehreren Modulen, die aufeinander aufbauen.

RCCMD Dienst: Der zentrale Hintergrundprozess, über den Ihr System im Notfall heruntergefahren wird. Dieses Modul ist für den Betrieb zwingend notwendig.

RCCMD Konfigurator: Dieses Modul ist de webbasierter Konfigurationsdialog für RCCMD, über den Sie alle Funktionen einstellen können, die RCCMD übernehmen soll.

RCCMD Benachrichtiger: Der RCCMD Dienst ist ein Hintergrundprozess. Der Benachrichtiger ermöglicht neben ein Popup-Fenster, die RCCMD-Prozesse mit dem angemeldeten Nutzer Interaktiv laufen zu lassen. Wenn Sie eigene Skripte verwenden, wo das Betriebssystem eine Bestätigung für verlangt, kann dieses Modul sehr hilfreich sein.



➔ *Wenn Sie Ihre Einstellungen durchgeführt haben, klicken Sie auf „Weiter“*

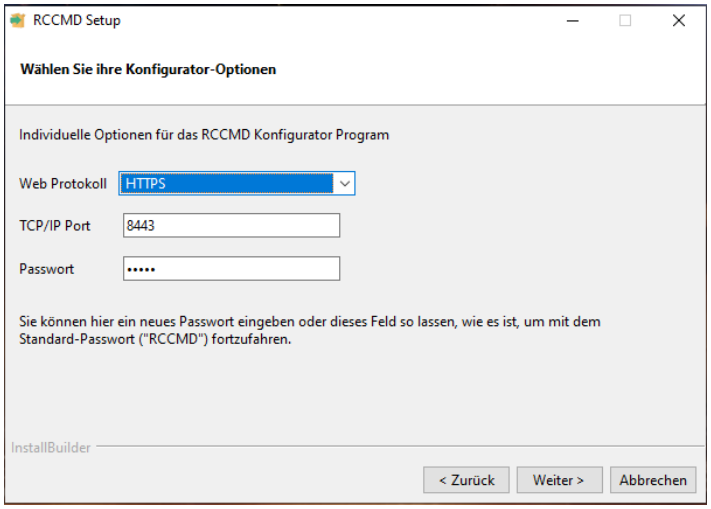
Schritt 3d – Benutzerdefiniert

HTTP / HTTPS und Passwort

Standardmäßig setzt RCCMD bei seinem Webinterface auf HTTPS. Hierfür steht ein integriertes Zertifikat zur Verfügung. Mit dieser Einstellung definieren Sie, ob als Standard HTTP oder HTTPS verwendet werden soll.

TCP/Port: RCCMD antwortet bei Anfragen auf das Webinterface nicht auf jeden Port. Standard ist hier der Port 8443. Sollten Sie abweichende Ports verwenden wollen, können Sie diesen hier angeben.

Passwort: Mit dem Passwort definieren Sie das Standardpasswort, mit dem Sie sich am RCCMD Webinterface anmelden. Wenn Sie das Passwort später einrichten möchten, lassen Sie das Feld wie es ist. RCCMD wird dann das Startpasswort „RCCMD“ verwenden.



➔ *Wenn Sie alle Einstellungen durchgeführt haben, klicken Sie auf „Weiter“*

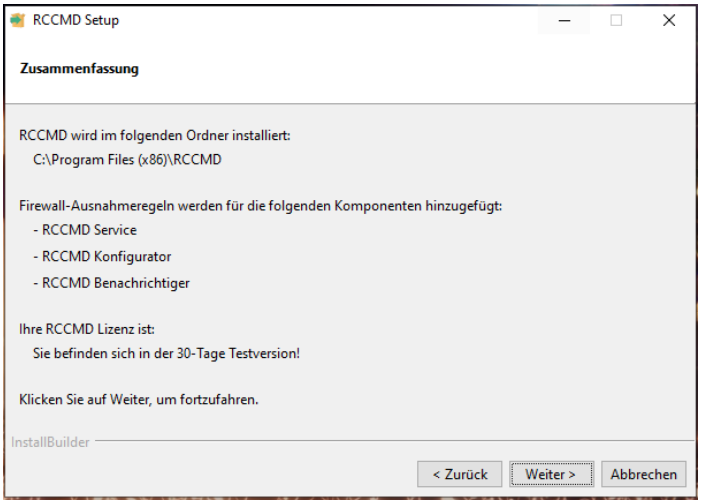
Schritt 3e – Benutzerdefiniert

Die Installationsübersicht

Die Übersicht zeigt Ihnen Ihre Auswahl an. Wenn Sie noch Änderungen durchführen möchten, können Sie mit „Zurück“ noch einmal den jeweiligen Konfigurationspunkt auswählen.

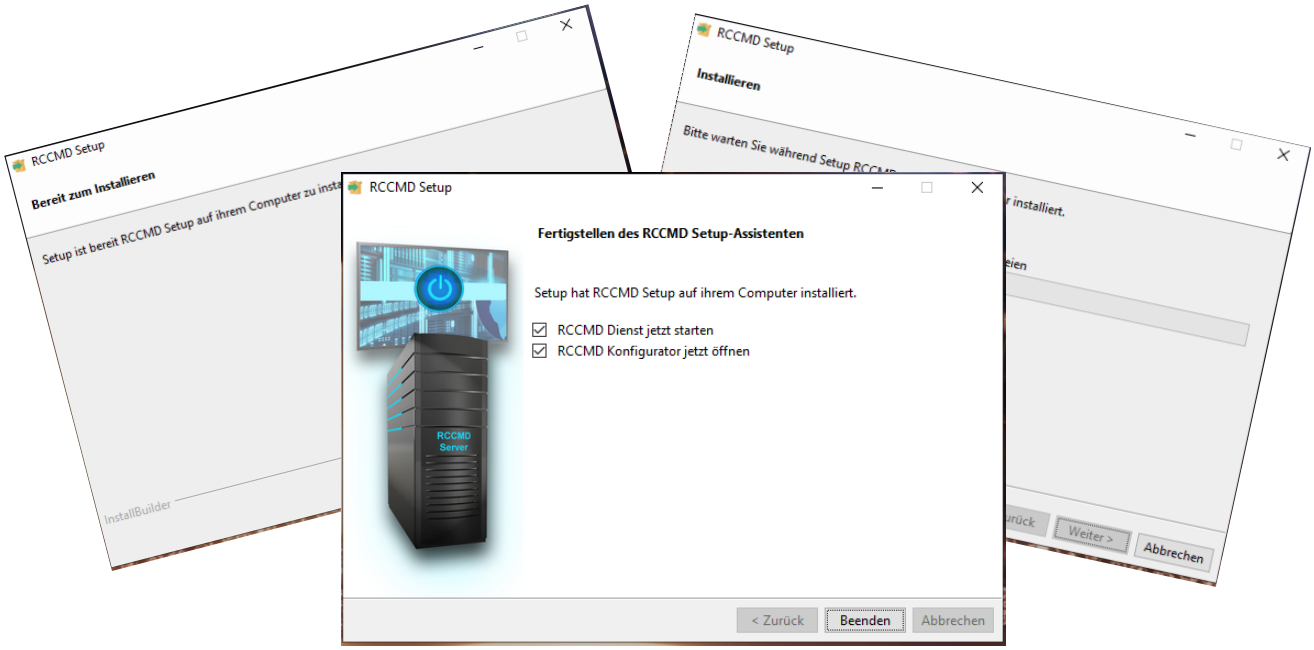
Mit „Weiter“ wird die eigentliche Installation von RCCMD angestoßen

Mit Abbrechen wird der Installationsdialog beendet und die von Ihnen eingestellten Parameter verworfen, ohne eine Änderung am Betriebssystem vorzunehmen.



➔ *Die Konfiguration ist abgeschlossen, klicken Sie auf „Weiter“, um die Installation zu beginnen.*

Schritt 4 – Abschluss der Installation



RCCMD installiert und konfiguriert automatisch alle notwendigen Komponenten. Im Anschluss können Sie das Webinterface unter Angabe der IP-Adresse des Rechners erreichen:

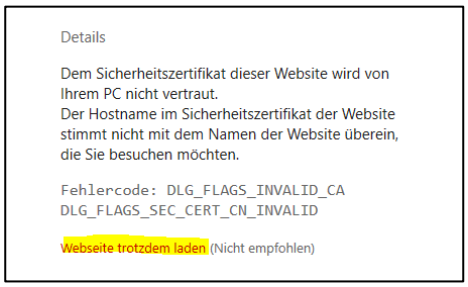
Zugang zum Webinterface:

- https://127.0.0.1:8443 ,
- https://[IP-Adresse des Computers]:8443,
- https://localhost:8443

Passwort: RCCMD bzw. das von Ihnen vergebene Passwort.

Die grafische Installation von RCCMD ist hiermit abgeschlossen. Bitte fahren Sie bei der Konfiguration von RCCMD über das Webmenü fort.

Tipp:



Im ersten Schritt werden Sie feststellen, dass Sie einen “Zertifikatsfehler” haben:

Das ist normal, da das Zertifikat zwar in sich durchaus gültig ist, RCCMD aber natürlich auf einem Server installiert wurde, für dessen Hardware das mitgebrachte SSL – Zertifikat logischerweise nicht signiert werden kann. Der Webbrowser merkt das und gibt folgerichtig zu bedenken, dass hier eventuell ein Problem vorliegen könnte.

Bei Edge klicken Sie auf „Details“ bei Crome auf „Erweiterte Optionen“, um zu der Startseite von RCCMD zu gelangen:

Befehl zum Ausführen: rccmdinstaller.exe --optionfile rccmd-answer.txt

Die Installation läuft im Hintergrund. Besuchen Sie anschließend das Webinterface Ihrer RCCMD-Installation um die notwendige Konfiguration durchzuführen**.**

Zugang zum Webinterface:

- https://127.0.0.1:8443 ,
- https://[IP-Adresse des Computers]:8443,
- https://localhost:8443

Passwort: RCCMD bzw. das von Ihnen vergebene Passwort.

Die Schnellkonfiguration für das Webinteface finden Sie in folgendem Kapitel:

RCCMD Schnellkonfiguration: Windows, Linux und MAC OS

Installation via Konsole

```
Select your preferred installation language
[1] English - English
[2] German - Deutsch
Please choose an option [1] : 2
```

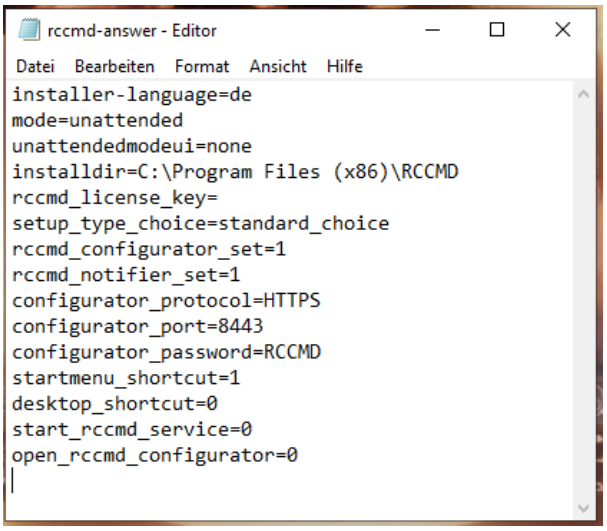
Core-Server oder Betriebssysteme via Konsolenzugriff bieten keine GUI an – RCCMD der Installer erkennt dieses automatisch und bietet in dem Fall einen alternativen Anzeigemodus für die Konfigurationsmenüs an. Das Setup-Programm wird Sie dabei genau wie bei der grafischen Installation durch den Installationsprozess begleiten.

Silent Install unter Windows

Der Silent Install ist ein besonderer Modus, bei dem alle für die Installation notwendigen Parameter in einer zentralen Antwortdatei hinterlegt sind.

Erstellen einer Silent Install Antwort-Datei

Öffnen Sie einen Texteditor und speichern Sie die Datei z.B. als rccmd-answer**.txt** ab. Der Aufbau der Datei ist ohne Sonderzeichen oder spezielle Formatsymbole.



Für eine vollständige Silent Install empfehlen wir folgende Einstellungen:

installer-language=de	Definieren Sie die Sprache des Installers
mode=unattended	Installationsmethode einstellen
unattendedmodeui=none	Darf der Installer interaktiv werden?
installdir=C:\Program Files (x86)\RCCMD	Standardinstallationsverzeichnis
rccmd_license_key=	RCCMD-Key für diese Installation. Wenn Sie keinen Key zur Hand haben, lassen Sie das Feld leer. RCCMD wird dann mit einem Evaluationskey installiert.
setup_type_choice=standard_choice	Setzt den Konfigurationsdialog auf “Standard”
rccmd_configurator_set=1	Installiert das Konfigurationsinterface*
rccmd_notifier_set=1	Installiert die Popup-Fenster innerhalb der GUI*
configurator_protocol=HTTPS	Definiert den Zugriffsstandard von RCCMD
configurator_port=8443	Definieren Sie den Port, auf dem RCCMD antworten soll.
configurator_password=RCCMD	Startpasswort für die RCCMD Benutzeroberfläche
startmenu_shortcut=1	Soll im Startmenü von Windows ein Shortcut abgelegt werden?*
desktop_shortcut=0	Sollen RCCMD Ikons auf dem Desktop hinterlegt werden?*
start_rccmd_service=0	Definieren Sie, ob RCCMD nach der Installation direkt gestartet werden soll.
open_rccmd_configurator=0	Definieren Sie, ob nach dem Start lokal der RCCMD Konfigurator gestartet werden soll. Diese Einstellung macht nur Sinn, wenn Sie eine GUI installiert haben.*

* 1 = JA / 0= NEIN

Befehl zum Ausführen: rccmdinstaller.exe --optionfile rccmd-answer.txt

Die Installation läuft im Hintergrund. Besuchen Sie anschließend das Webinterface Ihrer RCCMD-Installation um die notwendige Konfiguration durchzuführen**.**

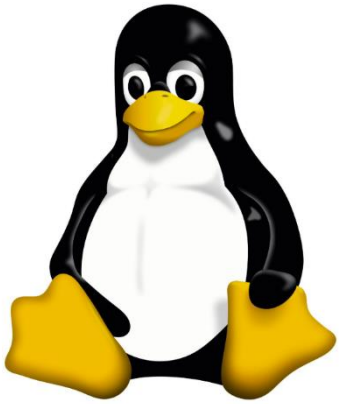
Zugang zum Webinterface:

- https://127.0.0.1:8443 ,
- https://[IP-Adresse des Computers]:8443,
- https://localhost:8443

Passwort: RCCMD bzw. das von Ihnen vergebene Passwort.

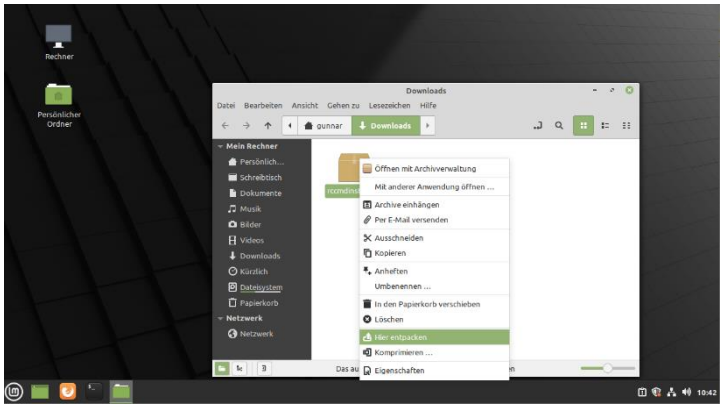
Installation - RCCMD für Linux

Installation unter Linux Betriebssystemen



Installation unter Linux mit GUI

In diesem Fall haben wir uns für ein Linux Mint „Ulaya 64 Bit“mit der Cinnamon-Oberfläche entschieden. Beachten Sie bitte, dass andere Distributionen, Derivate und Nutzeroberflächen ggfs. abweichende Anzeigen haben können.



Herunterladen und entpacken

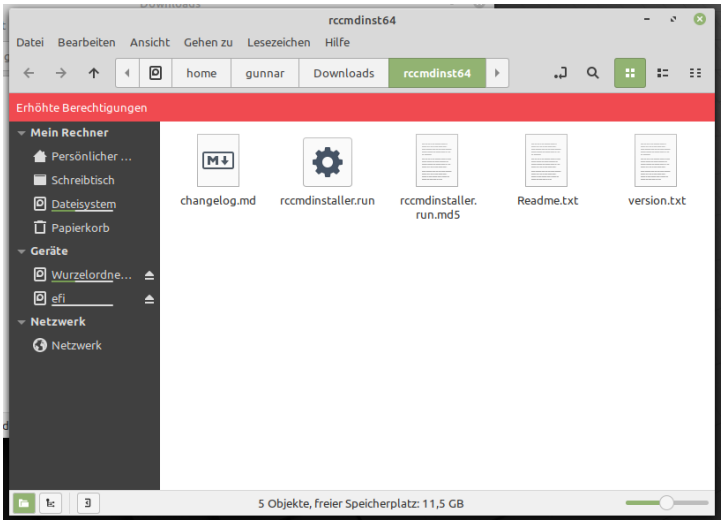
Nach dem Herunterladen entpacken Sie zunächst die RCCMD – Version:

Achten Sie darauf, dass Sie die gepackte Datei wirklich entpackt haben und nicht lediglich eine Vorschau der gepackten Dateien verwenden.

Installation durchführen

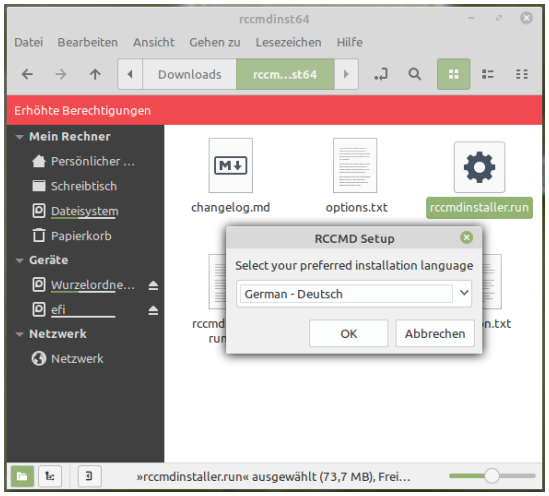
Für die Installation benötigen Sie erhöhte Rechte, achten Sie darauf, dass Sie den entpackten Ordner als Systemverwalter öffnen. Wenn Sie das Verzeichnis richtig geöffnet haben, steht dort der Hinweis, dass Sie innerhalb des Verzeichnisses mit erhöhten Rechten arbeiten.

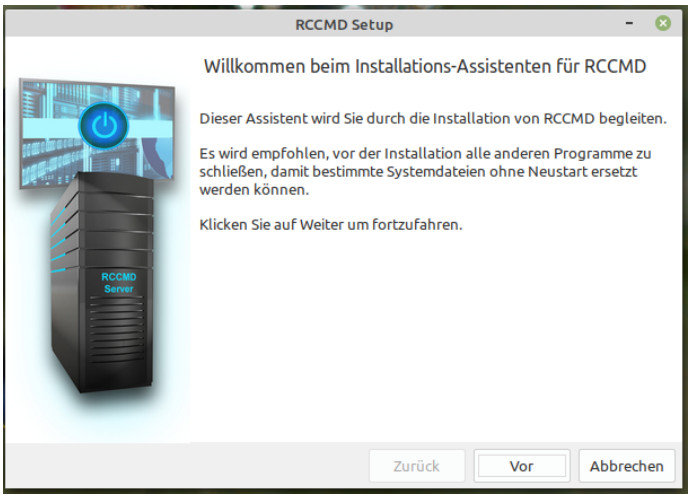
Mit einem Doppelklick auf Installer.run starten Sie die Installation



<u>Die Instalationsscreens in Kürze:</u>

Die Installation wird mit Doppelklick auf die Datei „rccmdinstaller.run“ gestartet.





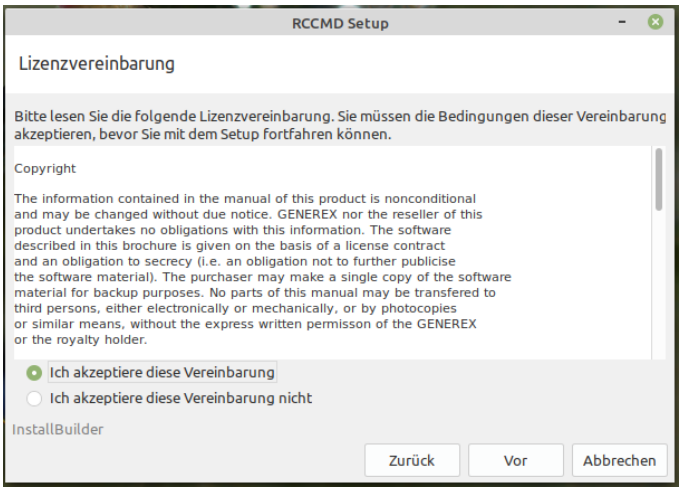
Sprache auswählen…

… „Vor“ klicken

Die Lizenzvereinbarung:

Wir wissen zwar, dass niemand diese Lizenzverienbarung wirklich liest, aber dennoch haben wir sie hier mit abgelegt. Um die RCCMD-Software nutzen zu können, ist es notwendig, die Lizenzbereinbarung zu bestätigen.

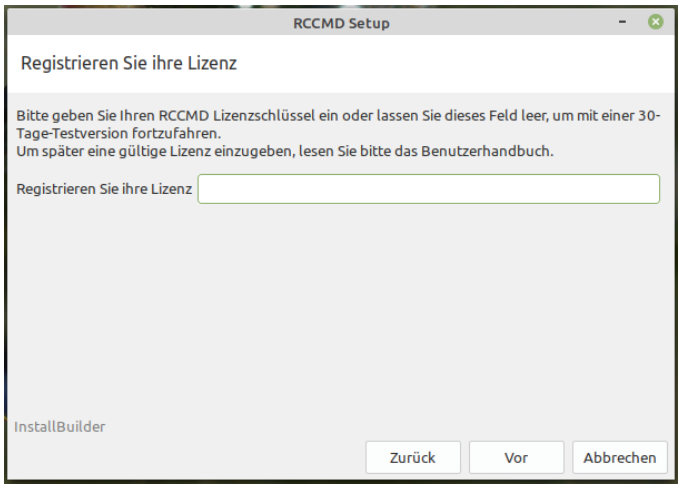
Wenn Sie nicht einverstanden sind, wird der Installer beendet und keine Änderungen an Ihrem Betriebssystem durchgeführt.



Der Lizenzkey

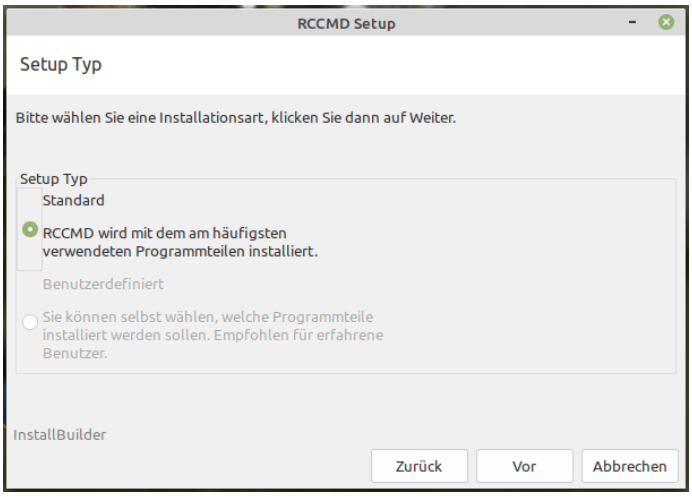
Geben Sie bitte den LIzenzkey ein, den Sie mit Ihrer Kopie von RCCMD erhalten haben. Wenn Sie keinen Key zur Hand haben, lassen Sie das Feld leer – RCCMD wird dann automatisch einen 31 Tage Evaluationskey verwenden, nach der sich der Client selber bis zur Eingabe einer gültigen Lizenz deaktiviert. Das Betriebssystem ist hiervon nicht betroffen. Beachten Sie bitte, dass Sie beliebig viele RCCMD Clients in Ihrem Netzwerk verwenden können, wobei jeder Lizenzkey nur einmal verwendet werden kann. Sobald ein Client mit dem Key gestartet ist, wird der nachfolgende Client seinen Service mit dem Hinweis „Licence Fraut“ einstellen. Die Ausnahme bildet hier der sog. Corporate Key – dieser ist für eine bestimmte Anzahl von Clients gültig und kann dem entsprechend auch mehrfach eingegeben werden.

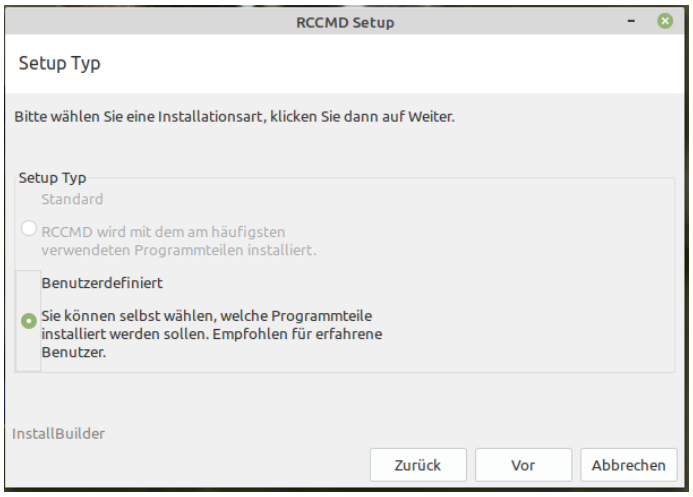
Die Keys sind nicht auf eine bestimmte Anzahl von „Aktivierungen“ begrenzt. Wenn Sie einen Key wiederverwenden möchten, deinstallieren Sie einfach die entsprechende RCCMD – Installation, die nicht mehr benötigt wird.



Tipp: Sie können den Lizenzkey jederzeit über die Erweiterten Einstellungen im RCCMD Konfigurationsmenü ändern.

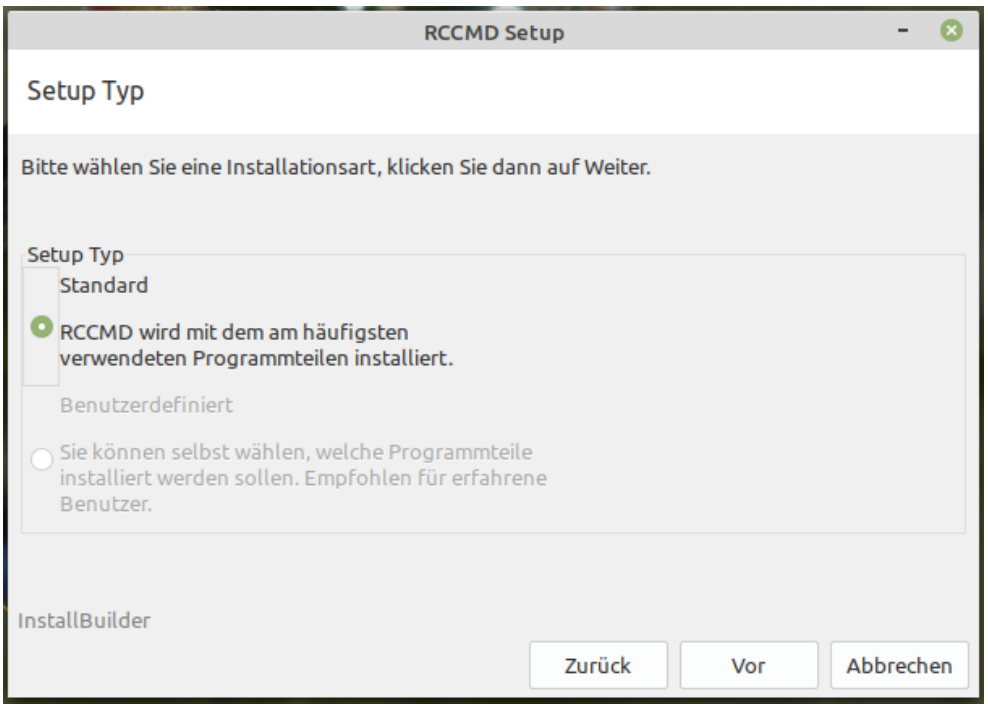
Setup Typ





Definieren Sie die Art der Installation. Es gibt zwei grundsätzliche Möglichkeiten, mit denen Sie die Installation durchführen können.:

Standardinstallation



Die Standard-Installation installiert RCCMD mit den empfohlenen Voreinstellungen, so dass Sie keine weiteren Einstellungen vornehmen müssen.

Für de Zugriff sind folgende Einstellungen vorgegeben:

https://127.0.0.1:8443	Der Local Host: RCCMD kann über den eigenen Webbrowser direkt aufgerufen werden
https://[IP-Adresse des Computers]:8443	Das Webinterface kann von einem beliebigen Computer kann aus dem Netzwerk erreicht werden.
Default Zugangspasswort:	RCCMD

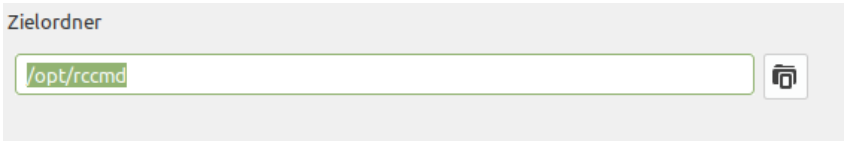
Benutzerdefinierte Installation

Diese Installation gibt Ihnen die Möglichkeit, die Installation genauer anzupassen. Bitte beachten Sie, dass die geänderten Parameter unter Umständen zusätzliche administrative Anpassungen im Betriebssystem erforderlich machen könnten. Diese Installationsart ist daher nur für erfahrene Anwender empfohlen.

RCCMD bietet Ihnen folgende weiterführende Anpassungsmöglichkeiten an:

Zielordner auswählen

Der Standardordner für die Installation ist /opt/rccmd. Wenn Sie möchten, können Sie hier einen anderen Ordnerpfad

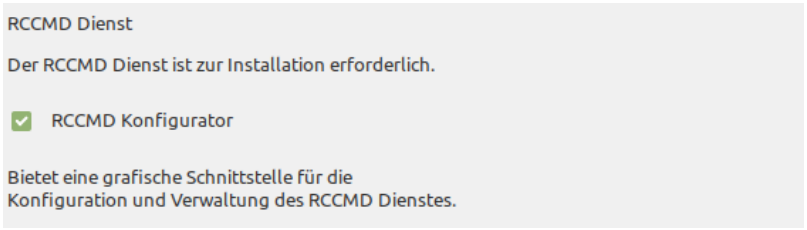


 Für einen grafischen Dateibrowser klicken Sie auf das Datei-Ikon auf der rechten Seite neben dem Textfeld.

Module anpassen

Der RCCMD Dienst wird für den Betrieb von RCCMD zwingend notwendig, daher kann er auch nicht an- bzw. abgewählt werden.

Der RCCMD Konfigruator stellt ein Webinterface bereit, über das Sie nach der Installation alle notwendigen Einstellungen vornehmen können. Das Webinterface ist im Anschluss erreichbar unter folgenden Adressen:



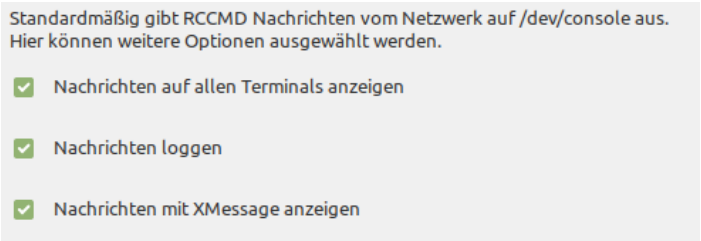
https://127.0.0.1:8443
Der Local Host: RCCMD kann über den eigenen Webbrowser direkt aufgerufen werden

https://[IP-Adresse des Computers]:8443
Das Webinterface kann von einem beliebigen Computer kann aus dem Netzwerk erreicht werden.

Benachrichtigungsverhalten

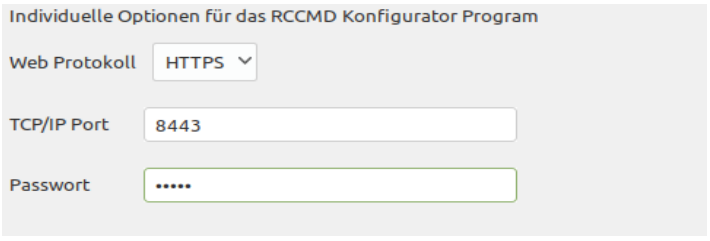
Standardmäßig werden alle Nachrichten, die RCCMD empfängt und weitergeben will direkt auf der Konsole ausgegeben. Mit dieser Einstellung können Sie das Alarmverhalten zusätzlich beeinflussen:

1. Auf allen Terminals anzeigen: Die Nachricht wird auf allen offenen Terminals ausgegeben
2. Nachrichten loggen: Die Nachrichten werden protokolliert
3. Nachrichten mit XMessage anzeigen: Wenn Sie eine grafische Benutzeroberfläche verwenden, erscheint ein Poup-Fenster, das die entsprechende Nachricht enthält.

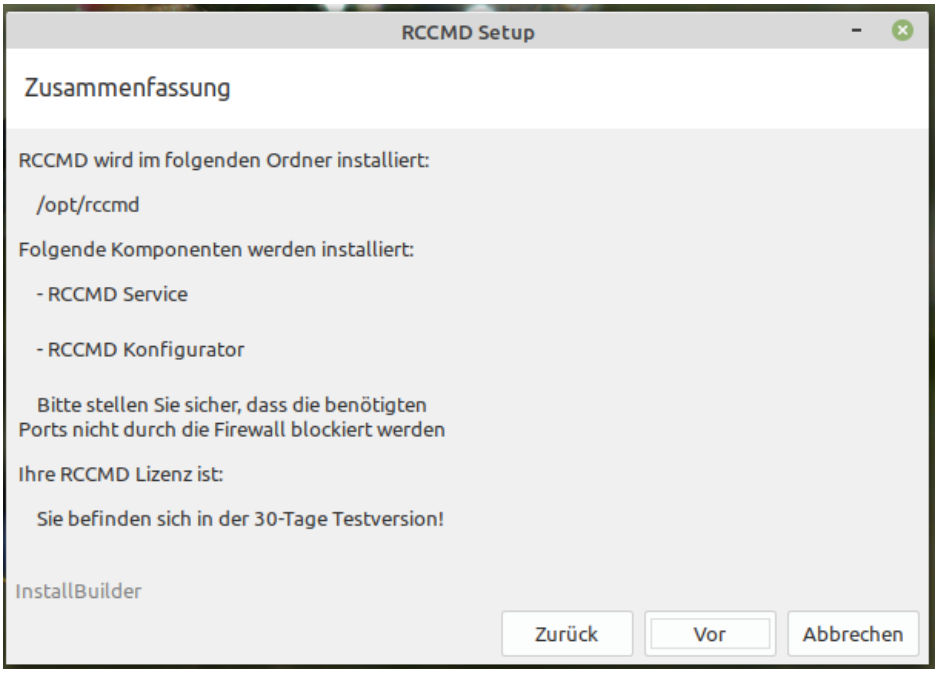


Zugriffsmöglichkeit auf das Webinterface

Standardmäßig wird das Webinterface von RCCMD mit https und dem TCP/Port 8443 angesprochen. Ändern Sie bei Bedarf die Einstellungen, um die RCCMD-Konfiguration an Ihre Bedürfnisse anzupassen. Das Standard-Passwort lautet generell zunächst RCCMD. Sie können es über die Weboberfläche zu einem späteren Zeitpunkt noch an Ihre Bedürfnisse anpassen.

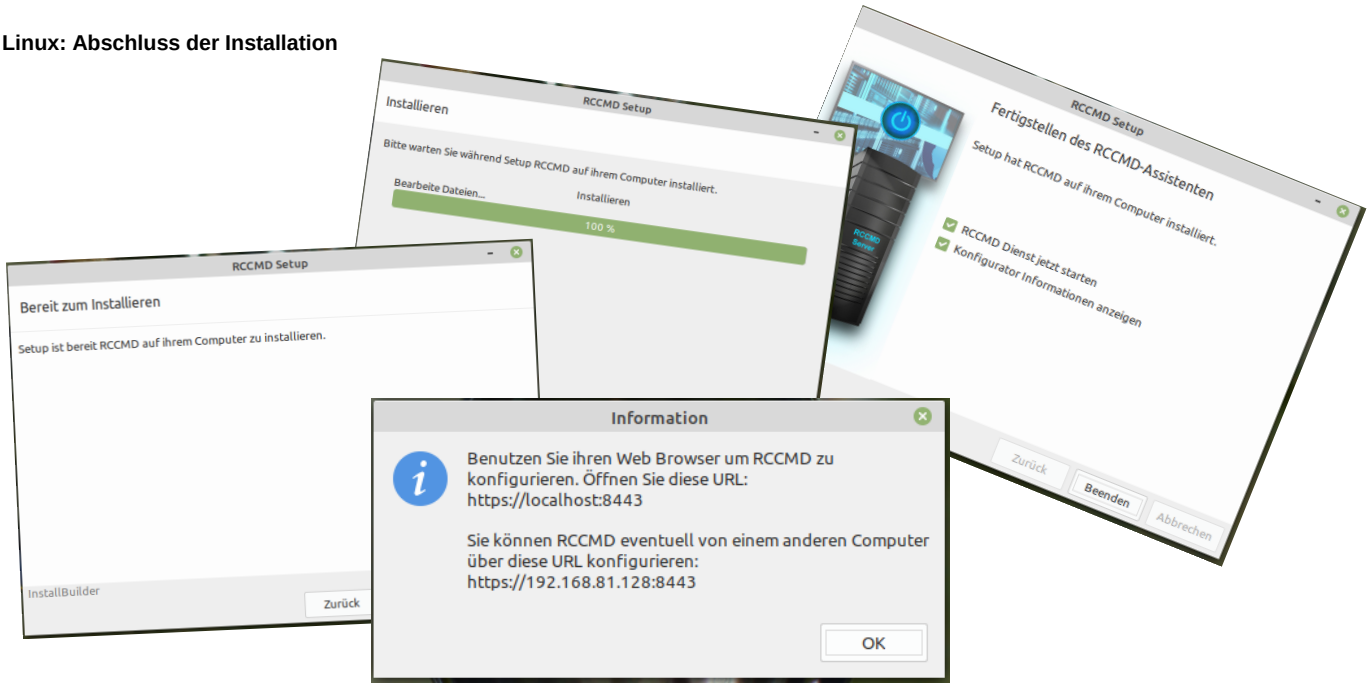


Zusammenfassung



Je nachdem, ob Sie die Standard-Installation oder die manuelle Installation ausgewählt haben, können Sie hier noch einmal übersichtlich Ihre Auswahl anzeigen lassen. Bis zu diesem Punkt hat RCCCMD noch keine Installationsarbeiten durchgeführt.

Linux: Abschluss der Installation



RCCMD installiert und konfiguriert automatisch alle notwendigen Komponenten. Im Anschluss können Sie das Webinterface unter Angabe der IP-Adresse des Rechers erreichen:

Zugang zum Webinterface:

- https://127.0.0.1:8443 ,
- https://[IP-Adresse des Computers]:8443,
- https://localhost:8443

Passwort: RCCMD bzw. das von Ihnen vergebene Passwort.

Die grafische Installation von RCCMD ist hiermit abgeschlossen. Bitte fahren Sie bei der Konfiguration von RCCMD über das Webmenü fort.

Konsoleninstallation

Mit der Konsoleninstallation durchlaufen Sie im prinzipiell die gleichen Schritte wie beim grafischen Installer. Das folgende Installationsbeispiel zeigt die Installation auf einem Linux Mint 20.1 „Ulyssa“. Bitte beachten Sie, dass der genaue Installationsbefehl in Ihrer Linux-Version abweichen könnte.

Wechseln Sie nach dem Anmelden und Herunterladen von RCCMD in das jeweilige Download-Verzeichnis und entpacken Sie zunächst die Datei rccmd64.tar.

```
Linux Mint 20.1 Ulyssa gunnar-virtual-machine tty1

gunnar-virtual-machine login: gunnar
Password:
Last login: Thu Apr 15 11:38:11 CEST 2021 on tty1
gunnar@gunnar-virtual-machine:~$ dir
Bilder  Dokumente  Downloads  Musik  Öffentlich  Schreibtisch  Videos  Vorlagen
gunnar@gunnar-virtual-machine:~$ cd Downloads
gunnar@gunnar-virtual-machine:~/Downloads$ dir
rccmdinst64  rccmdinst64.tar
gunnar@gunnar-virtual-machine:~/Downloads$ _
```

Wechseln Sie anschließend in das neu erstellte Verzeichnis mit den entpackten Installationsdateien.

Sysemrechte erweitern

Um RCCMD über die Konsole installieren zu können, müssen systemrelevante Änderungen durchgeführt werden, die einem Systemverwalter (Administrator) vorbehalten sind:

Befehl: sudo su

Mit dem Befehl sudo su verschaffen Sie sich bis auf Widerruf mit dem Befehl „exit“ die notwendigen erhöhten Systemrechte. Das ist daran zu erkennen, dass vor dem Nutzernahmen „root@“ steht.

```
Linux Mint 20.1 Ulyssa gunnar-virtual-machine tty1

gunnar-virtual-machine login: gunnar
Password:
Last login: Thu Apr 15 11:51:50 CEST 2021 on tty1
gunnar@gunnar-virtual-machine:~$ dir
Bilder  Dokumente  Downloads  Musik  Öffentlich  Schreibtisch  Videos  Vorlagen
gunnar@gunnar-virtual-machine:~$ cd Downloads
gunnar@gunnar-virtual-machine:~/Downloads$ dir
rccmdinst64  rccmdinst64.tar
gunnar@gunnar-virtual-machine:~/Downloads$ cd rccmdinst64
gunnar@gunnar-virtual-machine:~/Downloads/rccmdinst64$ sudo su
[sudo] Passwort für gunnar:
root@gunnar-virtual-machine:/home/gunnar/Downloads/rccmdinst64#
```

Damit sind die vorbereitenden Arbeiten erledigt und Sie können den Installatiosndialog starten.

Der Installationsdialog

Der Installer bietet in diesem Modus ein interaktives Setup, welches Sie komfortabel durch den Installationsprozess begleitet. Aufgerufen wird das Setup über die rccmdinstaller.run

Befehl: ./rccmdinstaller.run

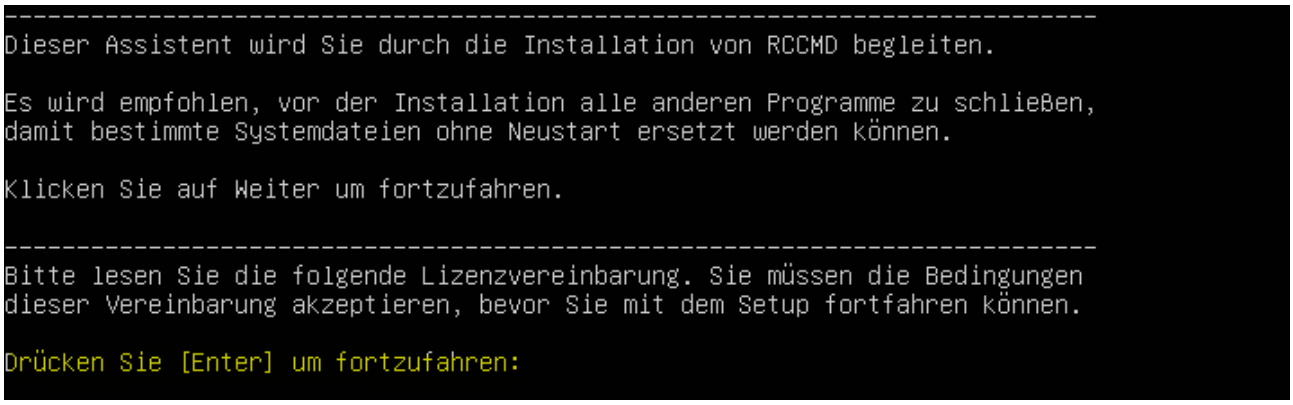
```
root@gunnar-virtual-machine:/home/gunnar/Downloads/rccmdinst64# ./rccmdinstaller.run
RCCMD Setup

Select your preferred installation language
```

Sprachauswahl

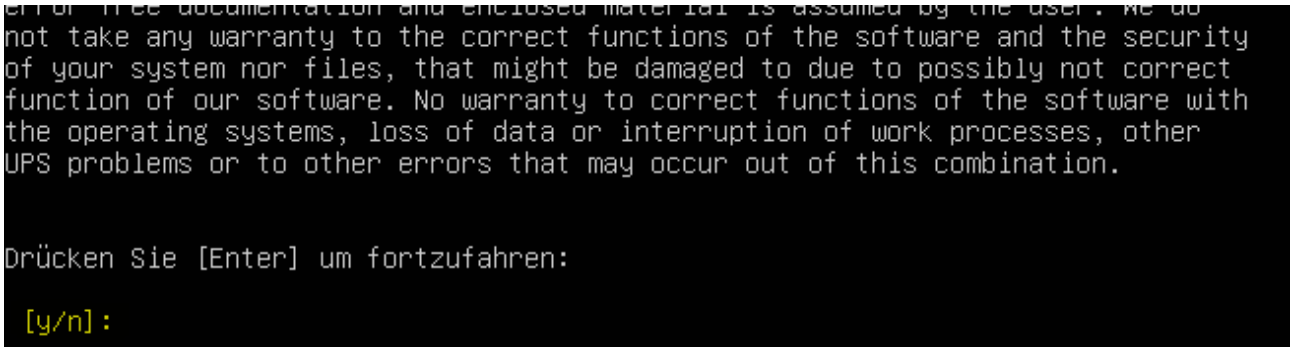
Mit der Sprachauswahl definieren Sie, welche Sprache der Installer verwenden soll. Sie können später innerhalb von RCCMD eine andere Sprache auswählen. Wählen Sie Ihre bevorzuge Sprache aus.

```
Select your preferred installation language
[1] English - English
[2] German - Deutsch
Please choose an option [1] : 2
```

Die Lizenzvereinbarungen



Wir glauben zwar nicht, dass jemand jemals diese Lizenzvereinbarung gelesen hat, aber um die RCCMD-Software nutzen zu können, ist es notwendig, die Nutzungs- und Lizenzvereinbarung zu bestätigen. Drücken Sie also entgegen der Empfehlung, aufmerksam zu lesen so lange die Eingabetaste, bis Sie die Lizenz- und Nutzungsbedingungen direkt annehmen können:



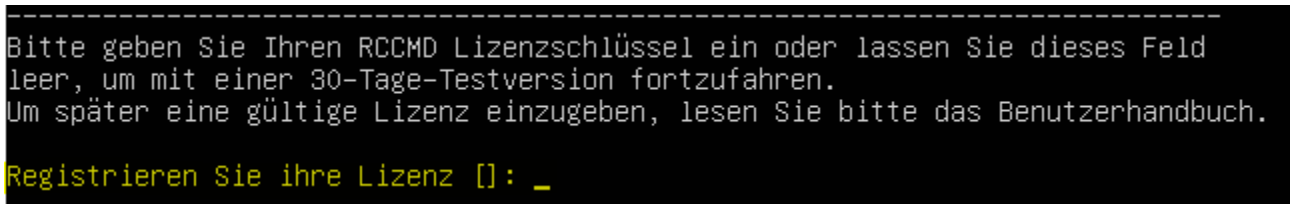
Wenn Sie nicht einverstanden sind, wird der Installer beendet und keine Änderungen an Ihrem Betriebssystem durchgeführt und der Installationsdialog beendet.

➔ ***Wenn Sie einverstanden sind, drücken Sie „y“ und bestätigen mit der Eingabetaste Ihre Entscheidung.***

Die Menüs des textbasierten Installers:

Schritt 1: Der Lizenzkey

Geben Sie hier den Lizenzkey Ihrer RCCMD-Software an. Den Lizenzkey erhalten Sie kostenpflichtig bei Ihrem USV-Anbieter. Wenn Sie mit Ihrer USV einen CS141 Webmanager erworben haben, ist eine Lizenz bereits enthalten. Sollten Sie den Key jetzt nicht zur Hand haben, lassen Sie dieses Feld leer, RCCMD wird dann automatisch einen Evaluationskey verwenden. Sie können zu einem späteren Zeitpunkt im Konfigurationsmenü von RCCMD den Key ändern und so Ihre Kopie dauerhaft aktivieren.



Schritt 2: Der Setup-Typ

Der Setup-Typ definiert, wie viel Sie im Verlauf der Installation

```
Setup Typ

[1] RCCMD wird mit dem am häufigsten verwendeten Programmteilen installiert.: Standard
[2] Sie können selbst wählen, welche Programmteile installiert werden sollen. Empfohlen für erfahren
e Benutzer.: Benutzerdefiniert
Bitte wählen Sie eine Option [1] :
```

Folgende Möglichkeiten stehen Ihnen zur Verfügung:

1. Empfohlende Einstellungen
   RCCMD wählt für Sie die benötigten Komponenten aus, die einen fehlerfreien Betrieb garantieren.
2. Angepasste Installation
   In diesem Installationsmodus können Sie entscheiden, welche Programmteile von RCCMD installiert werden sollen. Bitte beachten Sie, dass die einzelnen Module aufeinander abgestimmt sind. Wenn Sie einige Module nicht installieren, kann es dazu führen, dass RCCMD nicht ordungsgemäß funktioniert. Dieser Modus ist nur für erfahrene Benutzer empfohlen.

Wenn Sie Option 1 wählen:

Der Setup-Tool wählt die empfohlene Standardeinstellung für Sie aus und bereitet die Installation für Sie vor:

```
Ihre RCCMD Lizenz ist:

    Sie befinden sich in der 30-Tage Testversion!

--------------------------------------------------------------------------------
Setup ist bereit RCCMD auf ihrem Computer zu installieren.

Möchten Sie fortfahren? [Y/n]:
```

Sie erhalten eine Übersicht, welche Module installiert werden sowie den Ort. Auf Ihren Wunsch wird die eigentliche Installation von RCCMD gestartet. Sollten Sie an dieser Stelle die Installation abbrechen, werden Ihre Einstellungen verworfen.

Wenn Sie Option 2 wählen

Passen Sie die Installation an Ihre Vorstellungen an:

Der Zielordner

```
Zielordner

  [/opt/rccmd]:
```

Standardmäßig wird RCCMD unter /opt/rccmd abgelegt. Passen Sie bei Bedarf den Zielordner an Ihr Dateisystem an.

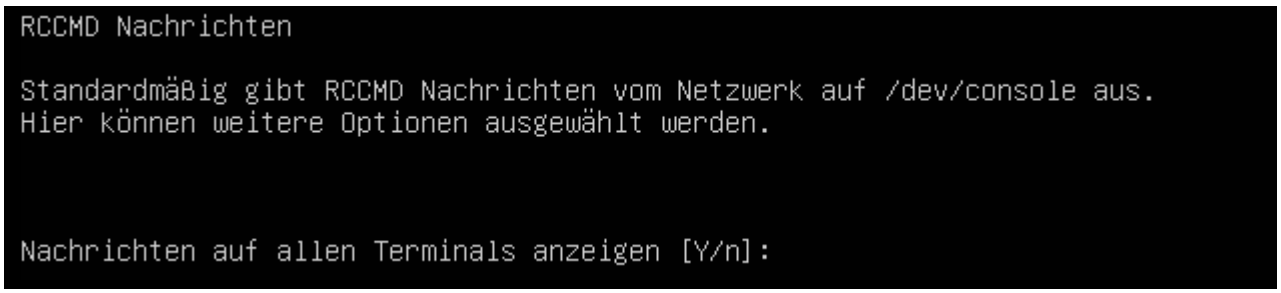
RCCMD Dienst und Konfigurator

```
RCCMD Dienst

Der RCCMD Dienst ist zur Installation erforderlich.


RCCMD Konfigurator [Y/n]: _
```

Der RCCMD Dienst ist für den Betrieb zwangsläufig notwendig, da dieser den Shutdown verwaltet.

Der RCCMD Konfigurator ist eine komfortable Weboberfläche über die Sie alle weiterführenden Einstellungen für Ihr Shutdownkonzept durchführen können. Die Konfiguration von RCCMD über einen Editor ist nur für sehr erfahrene Nutzer und Systemintegratoren mit weitreichenden Linux-Kenntnissen zu empfehlen.

RCCMD Nachrichten: Anzeigeort

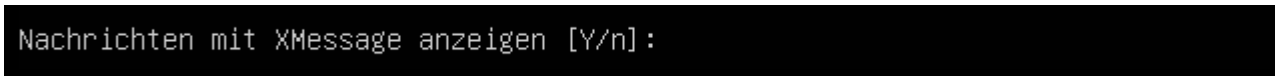


RCCMD kann von allen Geräten der CS121 und CS141 Produktfamilie sowohl automatisch generierte Statusnachrichten als auch von Ihnen konfigurierte Texte zu Systemereignissen innerhalb Ihrer USV empfangen und anzeigen. Mit dieser Einstellung können Sie definieren, wo die empfangenen Nachrichten angezeigt werden.

RCCMD Nachrichten: Mitloggen

Alle Geräte der CS121 und CS141 Produktfamilie fertigen zu den Systemereignissen automatisch ein Ereignisprotokoll mit Zeitstempel an. Von daher ist es im Normalfall nicht unbedingt notwendig, alle eingehenden Nachrichten mitzuschneiden. Wenn Sie einen Mitschnitt der eingegangenen Nachrichten erhalten möchten, aktivieren diese Funktion

RCCMD Nachrichten XMessage



Wenn Sie eine grafische Benutzeroberfläche zur Verfügung haben, können Sie die Nachrichten als Popup-Fenster anzeigen lassen.

Webprotokoll Port und Passwort

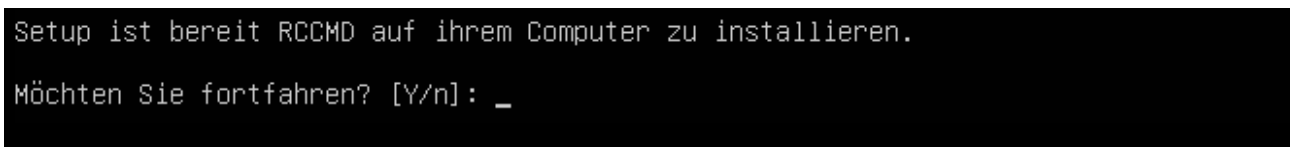
Das Webinterface kann sowohl über http als auch über https angesprochen werden, wobei RCCMD standardmäßig HTTPS aktiviert. Sie können diese Einstellung später über den Konfigurator an Ihre Vorstellungen anpassen. Für die korrekte Einstellung wenden Sie sich an den zuständigen Systembetreuer.

Die Portangabe definiert, auf welchem Port das Webinterface letztendlich erreichbar ist. RCCMD verwendet standardmäßig den Port 84443 für sein Interface. Bitte wenden Sie sich an den zuständigen Systembetreuer für die korrekte Einstellung, da dieser Port verfügbar und eventuell in Firewalls freigeschaltet werden muss.

Passwort

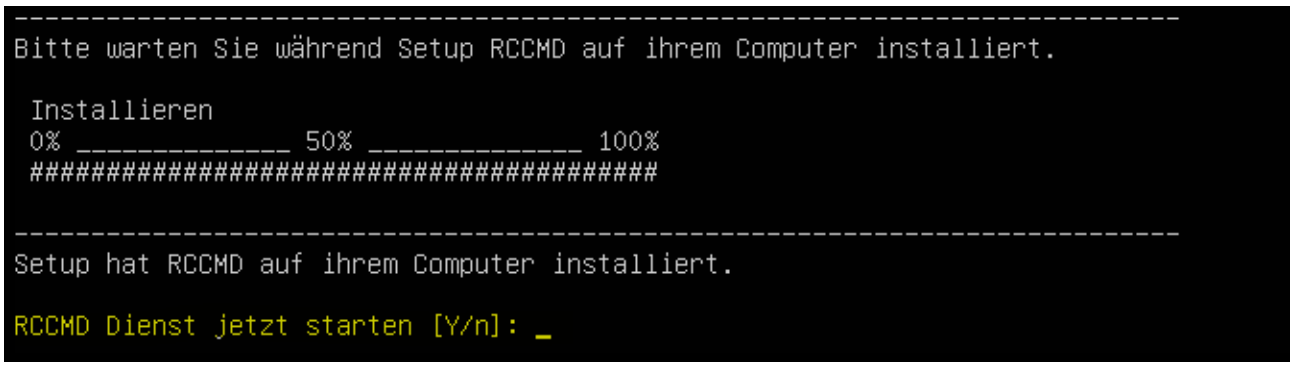
Definieren Sie das Login-Passwort von RCCMD. Dieses wird im späteren Verlauf beim Login auf der Weboberfläche benötigt. Wenn Sie das Passwort später vergeben möchten, drücken Sei die Eingabetaste und lassen das Feld leer. In dem Fall wird das Standard-Passwort „RCCMD“ verwendet.

Zusammenfassung und Beginn der Installation



Bis zu diesem Punkt sind noch keine Änderungen an Ihrem System durchgeführt worden. Wenn Sie die Installation abbrechen, werden Ihre Eingaben verworfen und Sie fallen zurück auf die Standardinstallation.

Abschluss der Installation:

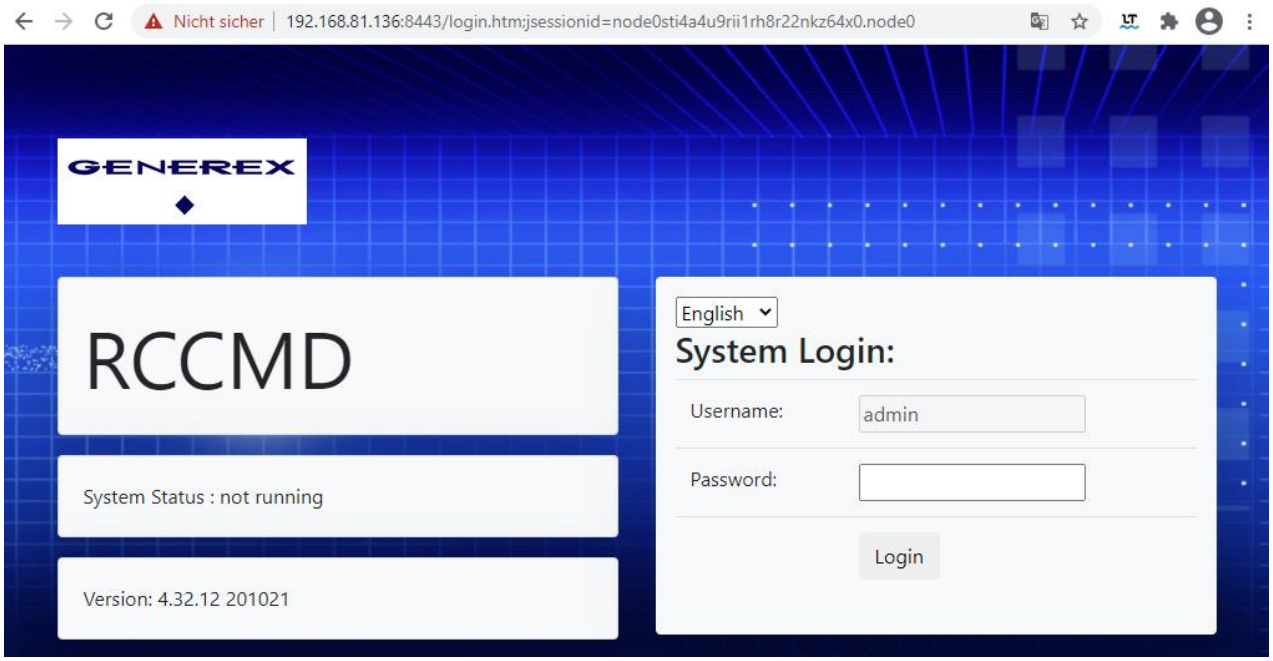


RCCMD führt automatisch die Installation durch.

Tipp:

Standardmäßig ist RCCMD so vorkonfiguriert, dass bei einem Eingehenden RCCMD Shutdown-Signal das Betriebssystem heruntergefahren wird. Da Sie aber noch nicht definiert haben, unter welchen Bedingungen ein Shutdownsignal gesendet werden soll bzw. welcher Sender bei mehreren Möglichkeiten berechtigt ist, könnte dies zu bösen Überraschungen führen, z.B. wenn Team-Mitglieder zeitgleich das Shutdownmanagement testen. Bevor Sie den Dienst innerhalb einer Produktionsoberfläche starten (und damit den Shutdown „scharf“ schalten), empfehlen wir eine schnelle Konfiguration über das komfortable Webinterface.

Die Installation ist abgeschlossen, die weitere Konfiguration wird über das Webinterface.



Zugang zum Webinterface:

- https://127.0.0.1:8443 ,
- https://[IP-Adresse des Computers]:8443,
- https://localhost:8443

Passwort: RCCMD bzw. das von Ihnen vergebene Passwort.

Die Schnellkonfiguration für das Webinterface finden Sie in folgendem Kapitel:

RCCMD Schnellkonfiguration: Windows, Linux und MAC OS

Update, Wartung und Deinstallation unter Linux

Tipp:

Die folgende Anleitung befasst sich mit der Deinstallation unter Linux MINT (!) mit einer Standardinstallation unter /opt/rccmd/ – Je nach Distributionen und Ihren Angaben während der Installation können Installationspfade, Vorgehensweisen und benötigte Parameter von dieser Anleitung abweichen.

Die genauen Befehle erhalten Sie in dem Fall im Hilfebereich Ihrer verwendeten Linux-Distribution.

Backup erstellen
Bevor Sie eine neue (aktualisierte) Version von RCCMD installieren können, müssen Sie die alte RCCMD – Version zunächst sauber deinstallieren. Je nach Konfiguration kann hier ein Datenbackup als vorbereitende Maßnahme viel Arbeit ersparen. Dabei sind folgende Schritte notwendig:

Bitte bedenken Sie, dass Sie je nach verwendetem User ggfs. sich mit dem Befehl *sudo su* erhöhte Systemrechte verschaffen müssen.

Wichtig bei älteren RCCMD – Installationen:

Wenn Sie von einer älteren RCCMD-installation auf die aktuelle Version wechseln, dann befinden sich die für das Backup notwendigen Dateien abweichend im Verzeichnis ***/usr/****rccmd*. Bedenken Sie bitte auch, dass RCCMD je nach verwendeter Version der RCCMD-Installer standardmäßig entweder das Installationsverzeichnis ***/usr/****rccmd* (ältere Versionen von RCCM) oder ***/opt/****rccmd* (neue Version) verwenden wird.

4. Erstellen eines Backups
5. Deinstallation des existierenden RCCMD Clients
6. Installation des neuen RCCMD Clients
7. Einspielen der Backupdateien

Punkt 1: Erstellen eines Backups:

d. Wechseln Sie in das Verzeichnis /opt/rccmd
Sichern Sie folgende Dateien:

   - Die Datei „rccmd.cfg“

e. Wechseln Sie in das Verzeichnis /opt/rccmd/webconfig/resources
Sichern Sie die folgenden Dateien:

   - rccmdConfig_eclipse.properties
   - ream.properties

f. Sichern Sie Ihre eigenen Skripte.

Punkt 2/3.Installationsarbeiten durchführen

Führen Sie die die Deinstallation der bestehenden RCCMD Software aus und installieren Sie im Anschluss die neue RCCMD Software.

Punkt 4: Backup einspielen:

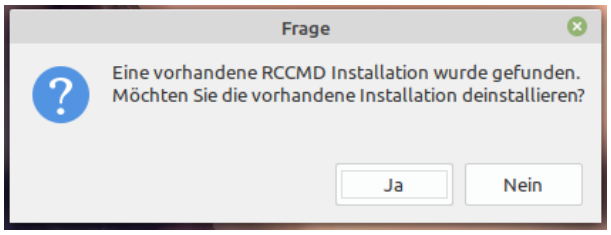
Das Einspielen des Backups wird ähnlich wie die Sicherung durchgeführt:

- Kopieren Sie Ihre Skripte wieder zurück in die entsprechenden Verzeichnisse.
- Wechseln Sie in das Verzeichnis /opt/rccmd
   - Legen Sie hier Ihre gesicherte rccmd.cfg ab und überschreiben Sie die existierende Datei
- Wechseln Sie in das Verzeichnis /opt/rccmd/webconfig/resources
Legen Sie hier die folgenden Dateien aus Ihrem Backup ab und überschreiben Sie eventuell existierende Dateien:
   - rccmdConfig_eclipse.properties
   - realm.properties
- Um das Datenbackup zu aktivieren starten Sie RCCMD neu.
- Überprüfen Sie die Einstellungen und Funktionen.

Deinstallation unter Linux

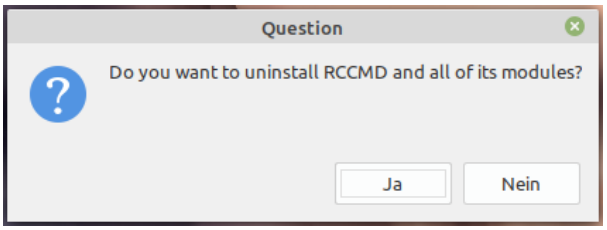
Möglichkeit 1: Über den Installer

Bei der Erstinstallation von RCCMD fällt dieses Feature nicht auf, weil es ja noch keine Installierte Version von RCCMD gibt. Bei einem Update auf eine höhere Programmversion jedoch muss zunächst die alte RCCMD-Version sauber deinstalliert werden. Hierzu liefert der Installer die entsprechende Routine gleich mit.

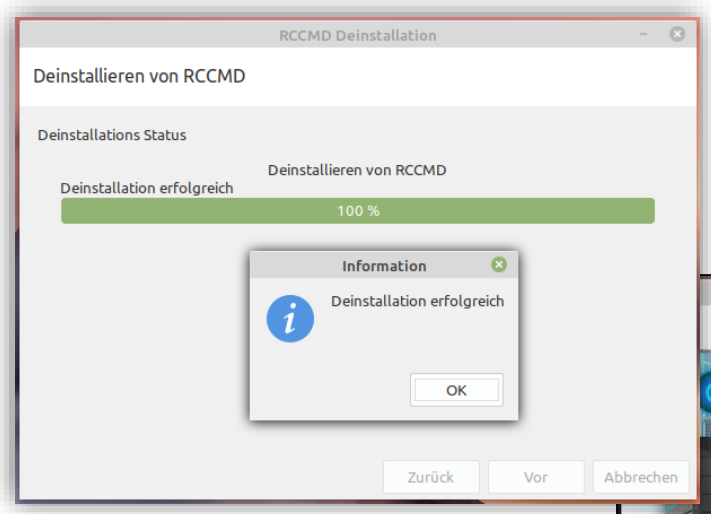


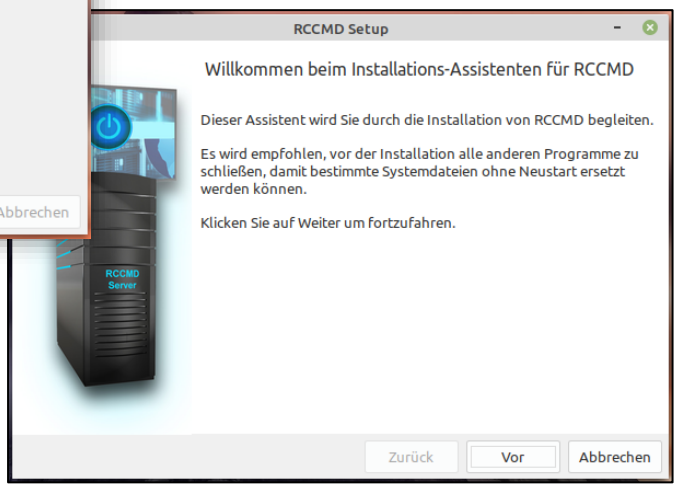
Öffnen Sie hierzu das RCCMD Installationspaket als Systembetreuer und starten Sie mit einem Doppelklick die Datei „rccmdinstaller.run“

Der Installer erkennt automatisch, dass RCCMD bereits installiert ist und bietet Ihnen die automatische Deinstallation an. Bestätigen Sie die Deinstallation mit „Ja“ und bestätigen Sie, dass Sie alle Module deinstallieren haben möchten.



Der weiterführende Deinstallationsprozess läuft voll automatisch:





Klicken Sie im Anschluss beim Installer auf „Abbrechen“, um den Installer zu beenden. Damit ist die Deinstallation abgeschlossen.

Tipp:

Die Deinstallation über die Packet- und Appvewaltung ist spezifisch für die jeweilige Linux-Distribution und hängt zudem vom persönlichen Geschmack des Systemverwalters ab. Wie Sie ein Programm über die Systemeinstellungen deinstallieren erfahren Sie im Nutzerhandbuch Ihrer jeweiligen Linux-Distribution

Vorgehensweise über die Konsole

RCCMD liefert einen eigenes Deinstallationsprogramm mit, dass Sie über das Installationsverzeichnis direkt aufrufen können.

Öffnen Sie hierzu zunächst ein Terminalfenster. Um auf das Installationsverzeichnis /opt/rccmd zugreifen zu können, benötigen Sie zunächst erhöhte Systemrechte:

Befehl: sudo su

```
gunnar@gunnar-virtual-machine:~$ sudo su
[sudo] Passwort für gunnar:
root@gunnar-virtual-machine:/home/gunnar#
```

Den Erfolg erkennen Sie daran, dass vor Ihrem Nutzernamen „root@“ steht.

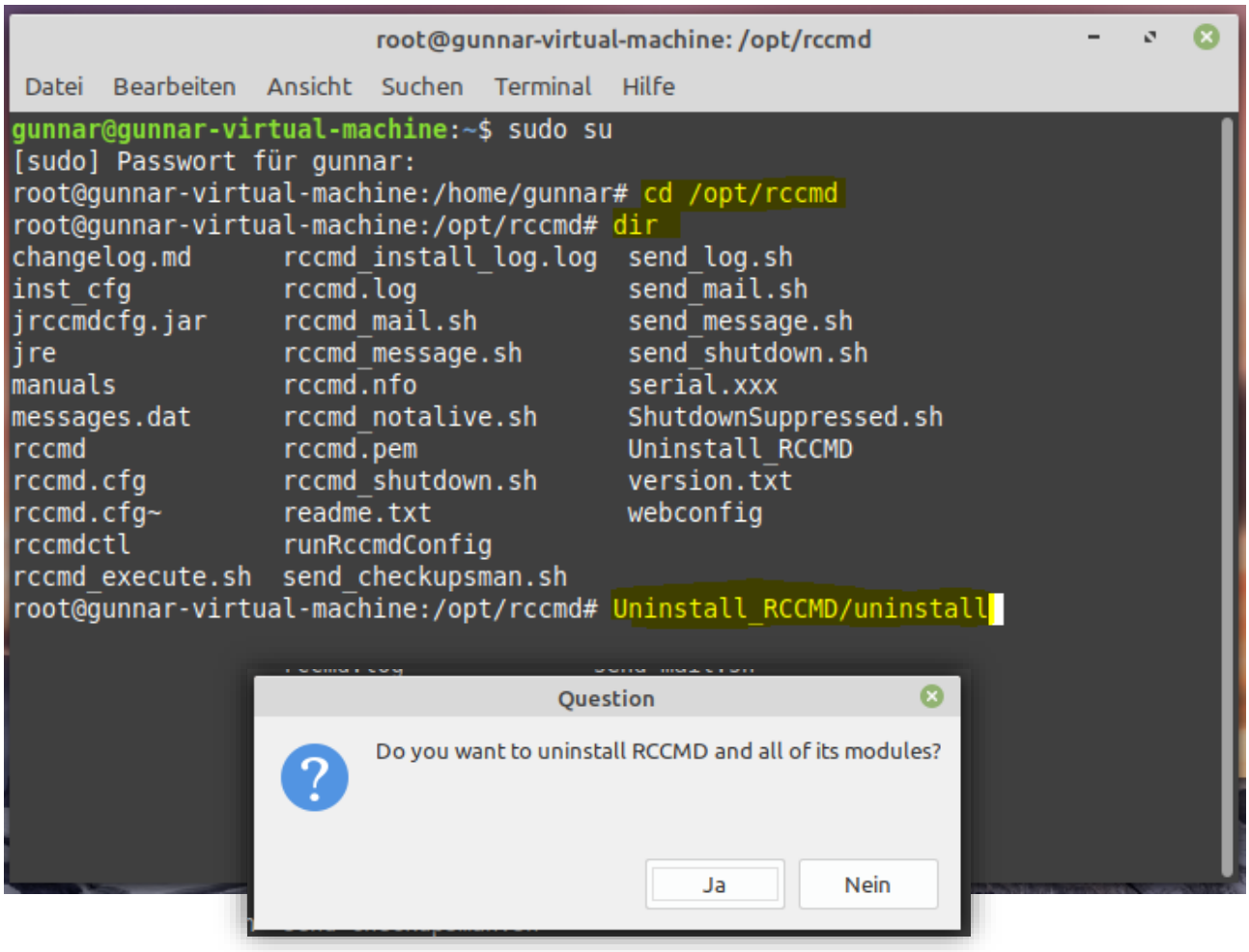
Deinstallation einleiten

Wechseln Sie jetzt in das Verzeichnis von RCCMD:

Befehl 1: cd /opt/rccmd

Befehl 2: dir

Befehl 3: Uninstall_RCCMD/uninstall



Wechseln Sie zunächst mit dem Befehl „cd /opt/rccmd“ in das Installationsverzeichnis von RCCMD und vergewissern Sie sich mit dem Befehl „dir“, dass Sie im richtigen Verzeichnis sind und die Datei Uninstall_RCCMD vorhanden ist.

Sobald Sie Uninstall_RCCMD/uninstall eingeben und mit Enter bestätigen, startet der Dialog für die Deinstallation, der Sie durch die Prozedur leiten wird:

Deinstallation bei Linux OHNE GUI

Möglichkeit 1: Über den Installer

Der Installer merkt, dass keine GUI zur Verfügung steht und wechselt daher in den Textmodus. Eine der Einschränkungen dabei ist, dass die Deinstallatinosroutine nicht parallel aufgerufen kann, von daher läuft es über die Konsole sehr viel direkter:

Wechseln Sie hierzu in das Downloadverzeichnis, in dem Sie RCCMD heruntergeladen und entpackt haben, sichern sich mit sudo su die erweiterten Systemrechte und starten anschließend mit ./rccmdinstaller.run die Installation.

Benötigten Befehle:

Befehl 1: cd Downloads

Befehl 2: cdrccmdinst64

Befehl 3: sudo su

Befehl4: ./rccmdinstaller.run

```
Linux Mint 20.1 Ulyssa gunnar-virtual-machine tty2

gunnar-virtual-machine login: gunnar
Password:
Last login: Fri Jul 30 13:47:18 CEST 2021 on tty2
gunnar@gunnar-virtual-machine:~$ cd Downloads
gunnar@gunnar-virtual-machine:~/Downloads$ cd rccmdinst64/
gunnar@gunnar-virtual-machine:~/Downloads/rccmdinst64$ dir
changelog.md  options.txt  rccmdinstaller.run  rccmdinstaller.run.md5  Readme.txt  version.txt
gunnar@gunnar-virtual-machine:~/Downloads/rccmdinst64$ sudo su
[sudo] Passwort für gunnar:
root@gunnar-virtual-machine:/home/gunnar/Downloads/rccmdinst64# ./rccmdinstaller.run
```

Damit startet der Installer, der Sie durch die Prozedur begleitet.

Nach der Sprachauswahl werden Sie aufgefordert, die Deinstallation des vorhandenen RCCMD-Clients zu bestätigen:

```
Select your preferred installation language
[1] English - English
[2] German - Deutsch
Please choose an option [1] : 2
Eine vorhandene RCCMD Installation wurde gefunden. Möchten Sie die vorhandene Installation deinstall
ieren? [Y/n]: _
```

Tipp

Anders als bei einem Linux mit GUI gibt es hier keine weitere Rückfrage, die Deinstallation wird von hier direkt ausgeführt. Das hängt technisch betrachtet damit zusammen, dass keine 2 Dialoge parallel auf derselben Konsole laufen können. Daher ist die Deinstallation automatisiert.

Nach diesem Schritt startet die Standard-Installationsroutine

```
--------------------------------------------------------------------------------
Dieser Assistent wird Sie durch die Installation von RCCMD begleiten.

Es wird empfohlen, vor der Installation alle anderen Programme zu schließen,
damit bestimmte Systemdateien ohne Neustart ersetzt werden können.

Klicken Sie auf Weiter um fortzufahren.

--------------------------------------------------------------------------------
Bitte lesen Sie die folgende Lizenzvereinbarung. Sie müssen die Bedingungen
dieser Vereinbarung akzeptieren, bevor Sie mit dem Setup fortfahren können.

Drücken Sie [Enter] um fortzufahren:
```

Brechen Sie wie bereits beschrieben die Installation ab, um den Assistenten zu verlassen.

RCCMD ist mit allen Komponenten deinstalliert.

Direkte Deinstallation ohne Installer und GUI

Die direkte Installation kann aus dem Installationsverzeichnis von RCCMD angestoßen werden. Standardmäßig liegt das unter /opt/rccmd. Um dorthin zu gelangen, benötigt man jedoch nach dem Login erweiterte Systemrechte:

Befehl: sudo su

```
Linux Mint 20.1 Ulyssa gunnar-virtual-machine tty2

gunnar-virtual-machine login: gunnar
Password:
Last login: Fri Jul 30 13:53:29 CEST 2021 on tty2
gunnar@gunnar-virtual-machine:~$ sudo su
[sudo] Passwort für gunnar:
root@gunnar-virtual-machine:/home/gunnar#
```

Deinstallation einleiten

Wechseln Sie jetzt in das Verzeichnis von RCCMD:

Befehl 1: cd /opt/rccmd

Befehl 2: dir

Befehl 3: Uninstall_RCCMD/uninstall

```
root@gunnar-virtual-machine:/home/gunnar# cd /opt/rccmd
root@gunnar-virtual-machine:/opt/rccmd# dir
changelog.md   rccmd.cfg             rccmd_message.sh   send_checkupsman.sh    Uninstall_RCCMD
inst_cfg       rccmd.cfg~            rccmd.nfo          send_log.sh            version.txt
jrccmdcfg.jar  rccmdctl              rccmd_notalive.sh  send_mail.sh           webconfig
jre            rccmd_execute.sh      rccmd.pem          send_message.sh
manuals        rccmd_install_log.log rccmd_shutdown.sh  send_shutdown.sh
messages.dat   rccmd.log             readme.txt         serial.xxx
rccmd          rccmd_mail.sh         runRccmdConfig     ShutdownSuppressed.sh
root@gunnar-virtual-machine:/opt/rccmd# Uninstall_RCCMD/uninstall
Möchten Sie RCCMD und alle verbundenen Module löschen? [Y/n]: _
```

Wechseln Sie zunächst mit dem Befehl „cd /opt/rccmd“ in das Installationsverzeichnis von RCCMD und vergewissern Sie sich mit dem Befehl „dir“, dass Sie im richtigen Verzeichnis sind und die Datei Uninstall_RCCMD vorhanden ist.

Sobald Sie Uninstall_RCCMD/uninstall eingeben und mit Enter bestätigen, startet der Dialog für die Deinstallation, der Sie durch die Prozedur leiten wird:

```
Möchten Sie RCCMD und alle verbundenen Module löschen? [Y/n]: y

------------------------------------------------------------------------------
Deinstallations Status

 Deinstallieren von RCCMD
 0% _____________ 50% _____________ 100%
 ########################################

Information: Deinstallation erfolgreich
Drücken Sie [Enter] um fortzufahren:_
```

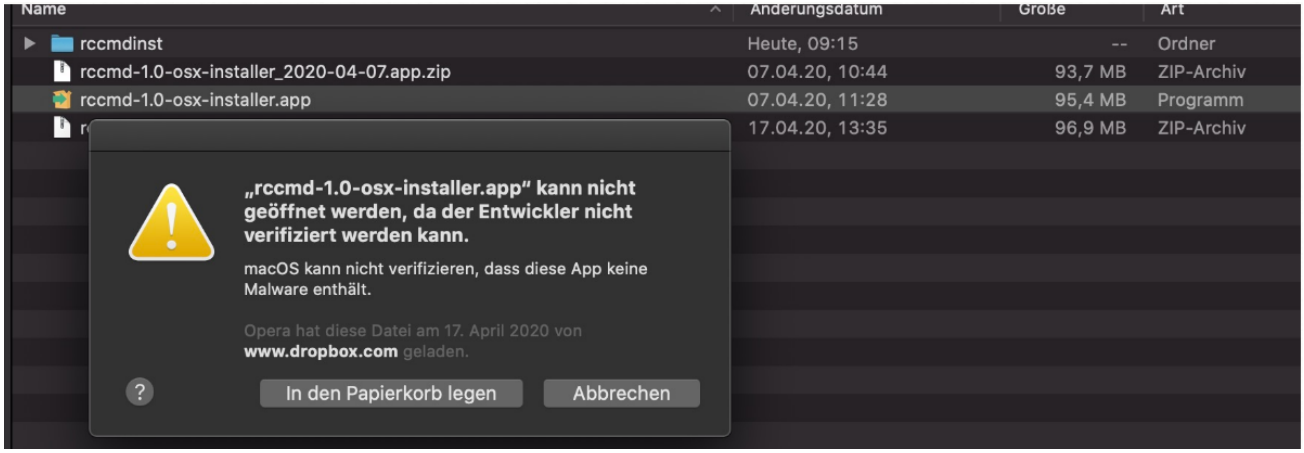
Die Deinstallation ist abgeschlossen, mit Enter beenden Sie diesen Dialog und kehren zur Konsole zurück.

Installation - RCCMD für MAC OS

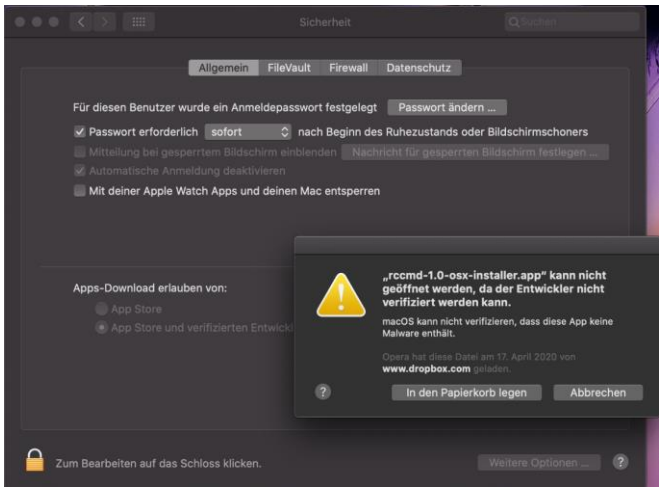
Installation unter MAC OS

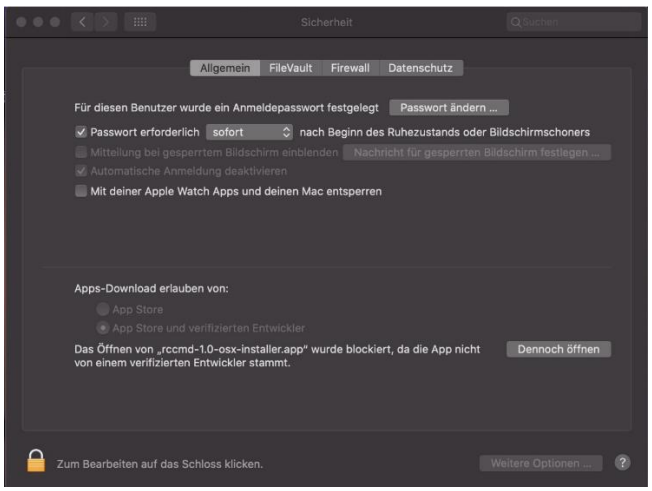
Datei zur Installation freigeben

Apple unterscheidet zwischen installierbarer Software und original zertifizierte Software. Wenn Sie ein Programm für MAC OS herunterladen, welches letztendlich nicht aus dem Apple Store selber kommt, wird das MAC OS dieses beim ersten Installationsversuch eventuell einfach ablehnen und anbieten, in den Papierkorb zu legen:



Damit die Installation fortgesetzt werden kann, muss unter Einstellungen/Sicherheit auf das Schlosssymbol geklickt werden. Nun auf Abbrechen bei der Warnmeldung klicken. Danach gibt es die Option „Dennoch öffnen“:





Nun erscheint erneut eine Warnmeldung mit der Option „Öffnen“:

Die Freigabe für die Installation erteilen

Wenn man jetzt unter Apple etwas installieren möchte, sind mitunter erweiterte Systemrechte notwendig, damit die Installation auch durchgeführt werden kann.

Der Installationsmanager von Apple wird dies bezüglich dann das entsprechende Passwort haben, um die Kontrolle über den gesamten Installationsprozess das entsprechende Programm zu übergeben:

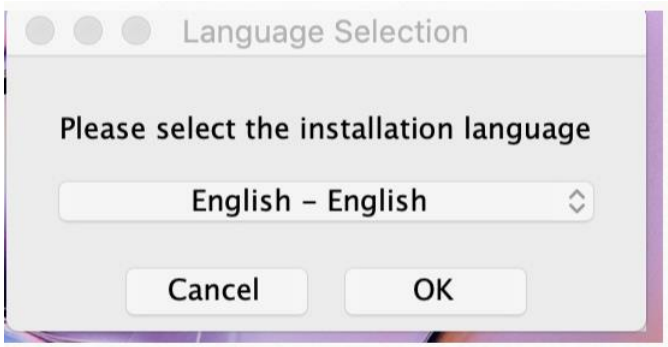
RCCMD Installationsdialog

Der Installer ist multilingual, Sie können entweder die Standardsprache (Englisch) wählen oder eine Sprache, die Ihnen für die Installation sinnvoll erscheint.

Die Sprache des Installers hat hierbei nichts mit der Sprache von RCCMD selber zu tun – Sie können also auch im späteren Verlauf die Sprache noch ändern.

Für die Schnellanleitung wird die englische Spracheinstellung belassen.

➔ Klicken Sie auf OK, wenn Sie Ihre Wahl getroffen haben.



Der RCCMD Begrüßungsscreen

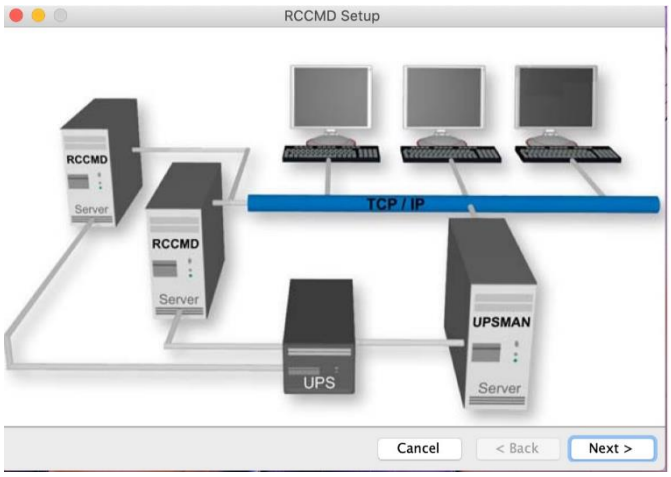
Nach der Auswahl der Sprache können Sie mit der eigentlichen Installation beginnen:

Der Installer fragt vor der eigentlichen Installation zunächst ein paar Rahmendaten ab, die für die grundlegenden Einstellungen notwendig sind.

Bevor Sie fortfahren, achten Sie darauf, dass Sie den gültigen Key griffbereit haben.

Sie können bis zum Beginn der Installation jederzeit mit „Cancel“ die Installation abbrechen, es werden keine Änderungen an Ihrem Betriebssystem durchgeführt.

➔ Klicken Sie auf Next.



Copyrights, Lizenzvereinbahrung, etc.

Wir möchten Sie kurz aufklären, was Sie dürfen, nicht dürfen, wie die Software benutzt wird, etc.

Informationen, die innerhalb von 0.8 Sekunden gelesen werden können, bevor man auf „I accept the agreement“ klickt.

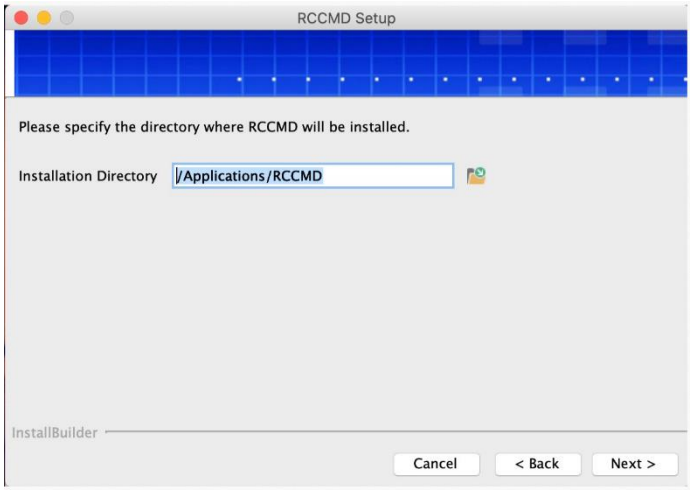
Wenn Sie auf I do not accept the aggreement klicken, wird übrigens die Installation abgebrochen, da Sie nicht zugestimmt haben, bisher gespeicherte Daten werden wieder entfernt und der Installationsdialog beendet.

➔ Nachdem Sie naheliegenderweise „I accept the agreement“ ausgewählt haben, klicken Sie auf Next.

Installationsverzeichnis auswählen

Der Installer wählt einen für Apple typisches Installations-Verzeichnis aus und schlägt diesen für die Installation vor.

Sie können den Ort nach Ihren Wünschen und Vorstellungen anpassen.



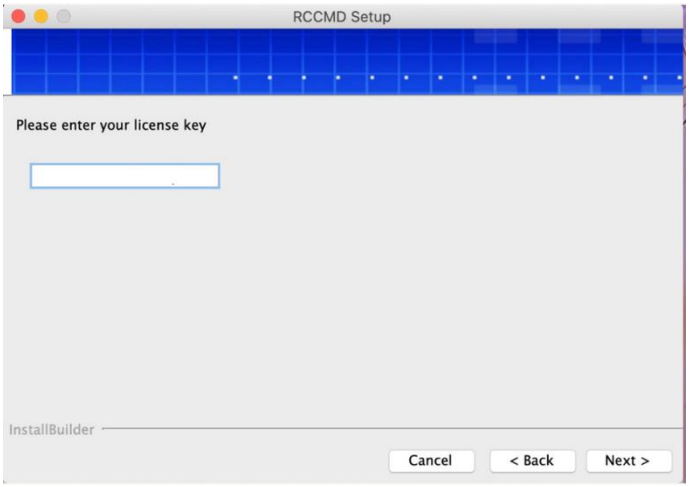
➔ Wenn Sie Ihre Wahl getroffen haben, klicken Sie auf „Next“

Der Lizenzschlüssel:

Geben Sie Ihren Lizenzschlüssel ein – dieser wurde Ihnen mit der USV-Dokumentation von Ihrem Händler übergeben, liegt im der Dokumentation Ihres CS141 / SITEMANAGER oder SITEMONITORS bei oder wurde Ihnen per Mail zugeschickt.

Sollten Sie keinen Lizenzschlüssel zur Hand haben, geben Sie an dieser Stelle einfach „DEMO“ ein, um die Testphase zu starten.

Sie können den Lizenzschlüssel im Anschluss über das Webinterface jederzeit ändern. Mit dem nächsten Neustart von RCCMD wird der neue Schlüssel übernommen und Sie haben eine Vollversion.

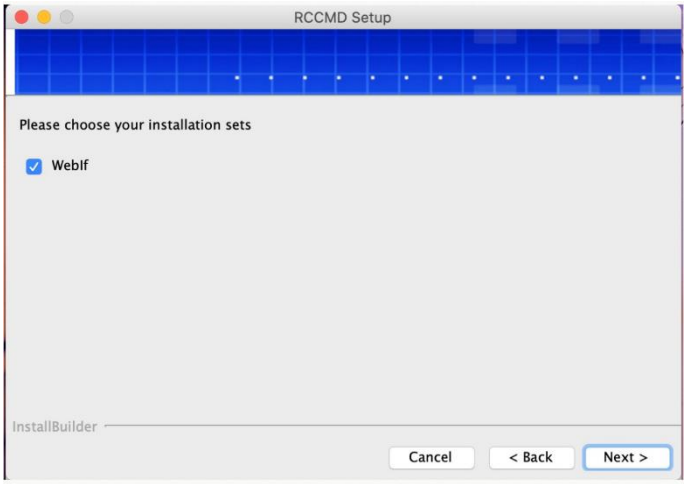


➔ Nachdem Sie den Schlüssel (oder „DEMO“) eingegeben haben, klicken Sie auf „Next“.

Zusätzliche Module auswählen:

Mit dem WebIf wird die Benutzeroberfläche mitinstalliert, die Sie für die komfortable und zwingend notwendige Konfiguration.

Wenn der WebIf nicht angewählt ist, wählen Sie ihn bitte aus, damit er installiert wird.

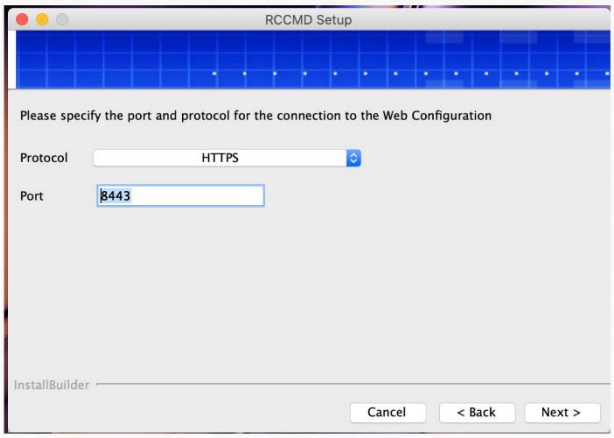


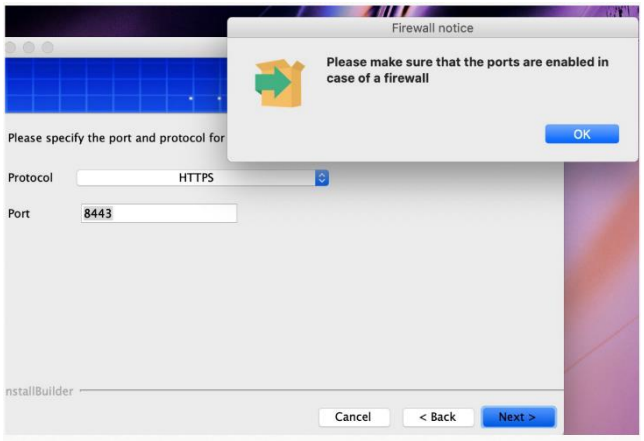
➔ Klicken Sie anschließend auf „Next“

http(s) und Portauswahl

RCCMD wird über eine moderne Weboberfläche konfiguriert.

Um auf die Weboberfläche zugreifen zu können, muss RCCMD wissen, ob Sie http/https verwenden möchten und auf welchem Port intern die Oberfläche erreichbar sein soll. Standardport für RCCMD ist der Port 8443, Sie können aber jeden Port, der zu Ihrem Netzwerk passt und nicht belegt ist, entsprechend auswählen





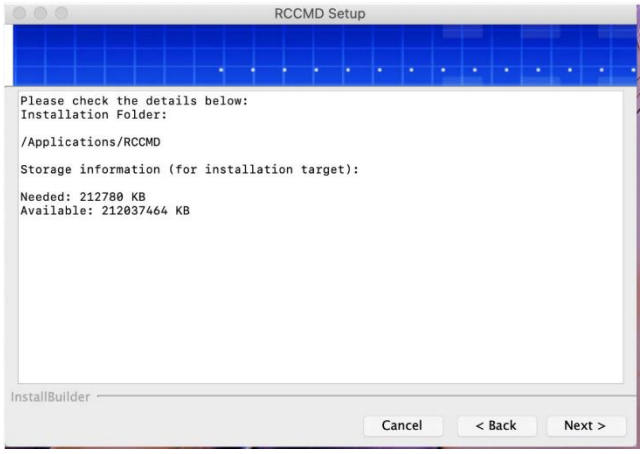
Bitte beachten Sie:

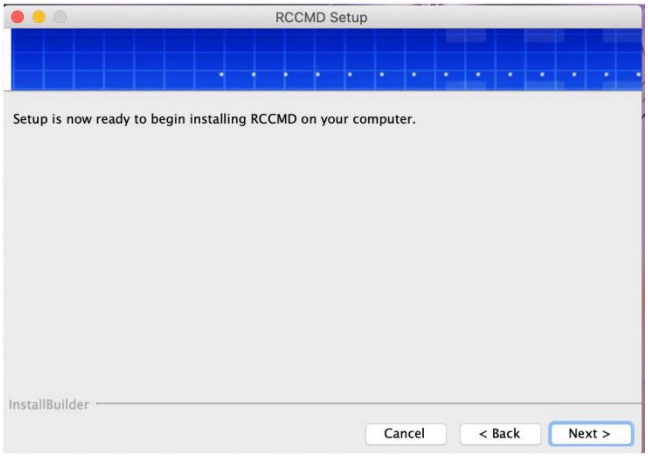
RCCMD bringt zwar ein eigenes Zertifikat mit, dieses wurde jedoch nicht auf dem MAC OS erstellt. Dies wird Ihr Webbrowser natürlich feststellen und bemängeln, dass es zwar ein gültiges Zertifikat gibt, jedoch nicht gewährleistet sein kann, dass die Webseite auch die ist, die sie vorgibt zu sein. Sie können diesen Hinweis dem entsprechend ignorieren.

➔ Klicken sie auf „Next“

Zusammenfassung und Installation starten

Im nächsten Schritt zeigt Ihnen RCCMD Ihre Auswahl, also das Installationsverzeichnis, den verfügbaren Speicherplatz und die den geschätzten Speicherplatz, der für die Installation notwendig ist. Mit „Back“ können Sie zurück zu den einzelnen Konfigurationsschritten gehen und mit „Cancel“ die Installation abbrechen und verwerfen.



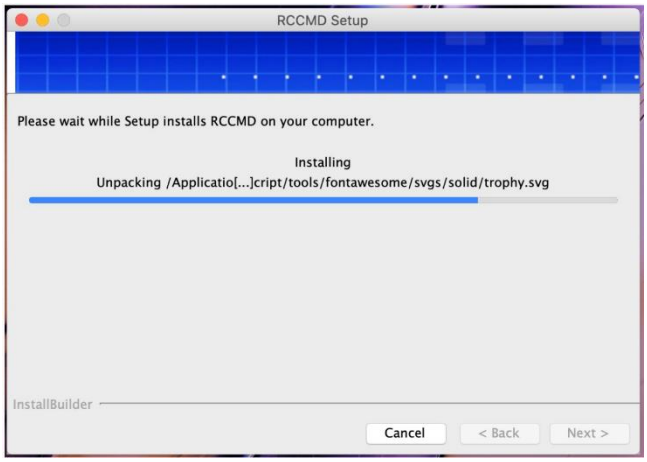


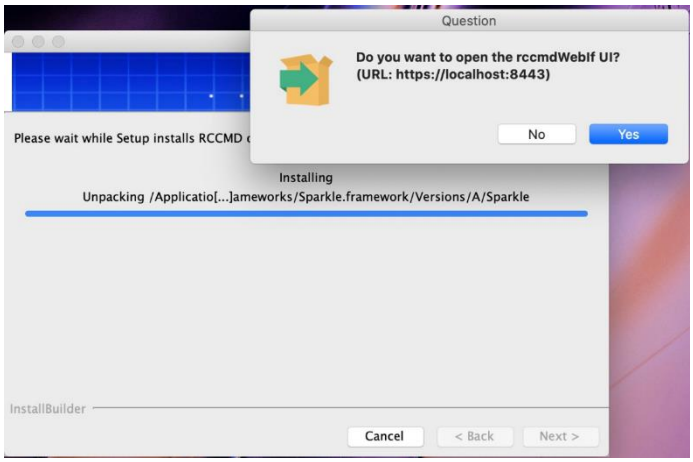
➔ Klicken Sie auf „Next“ und bestätigen Sie, wenn alle Einstellungen korrekt sind.
➔ Klicken Sie auf „Next“ und bestätigen Sie, dass Sie die eigentliche Installation beginnen wollen.

Installationsfortschritt und Firewall

Sie können den Installationsprozess verfolgen.

RCCMD wird Sie fragen, ob die Firewall automatisch konfiguriert werden soll, damit Sie im Anschluss auf das Webinterface zugreifen können. Danach ist die Installation abgeschlossen und RCCMD ist einsatzbereit.



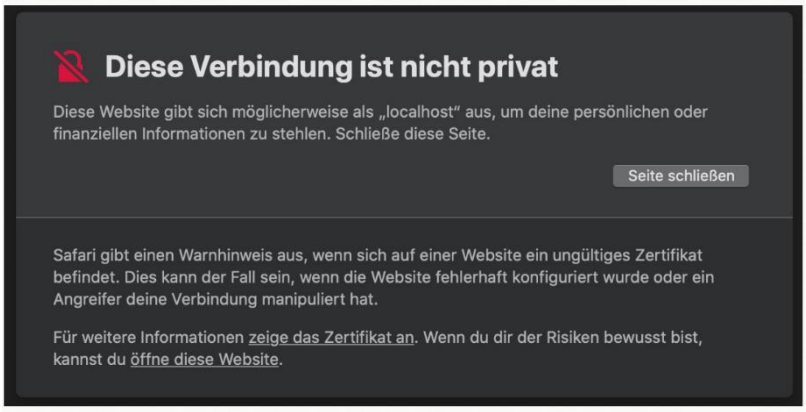


➔ Bestätigen Sie die Frage mit „YES“

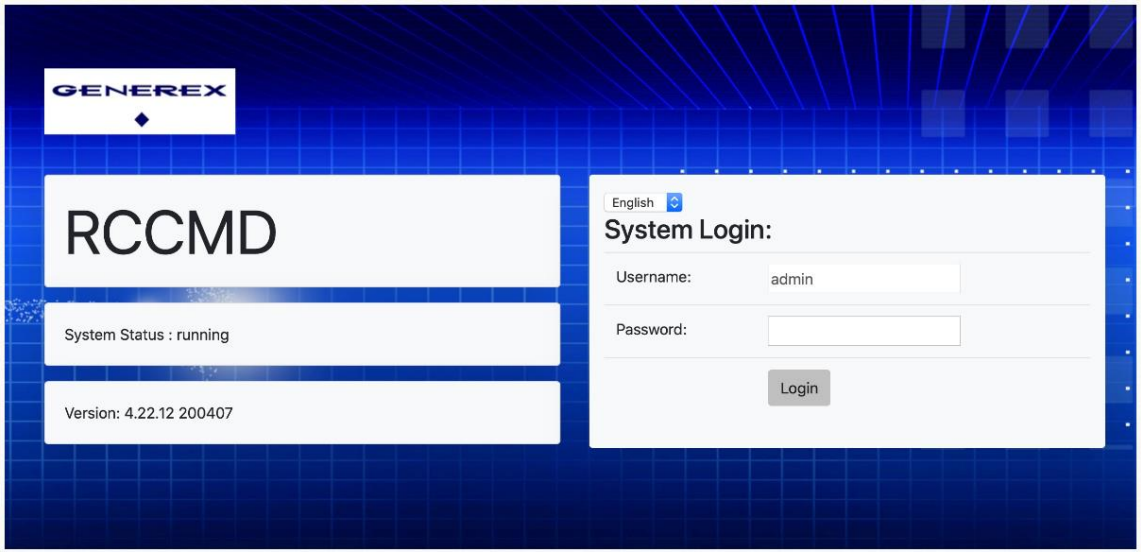
Der erste Start nach der Installation

Der Webbrowser Safari wird zwangsläufig feststellen, dass RCCMD ein vermeintlich nicht gültiges Zertifikat verwendet. Das ist so nicht ganz richtig:

Das Zertifikat ist als solches durchaus gültig, aber es wurde nicht auf diesem Rechner ausgestellt. Damit kann sich der Rechner nicht als glaubwürdig vor sich selber authentifizieren. Da Sie sich jedoch auf Ihrem eigenen Rechner befinden und über das WebIF bzw. über die URL https://localhost:8443 vor dem Gerät sitzen, können Sie diesen Hinweis ignorieren und das Zertifikat dauerhaft bestätigen.



Schnellkonfiguration
Die Installation von RCCMD auf einem MAC OS ist abgeschlossen. Fahren Sie jetzt fort mit der Schnellkonfiguration von RCCMD über das Webinterface.



RCCMD Schnellkonfiguration: Windows, Linux und MAC OS

Schnellkonfiguration - Das Wichtigste in Kürze
Für Windows, Linux und Mac OS

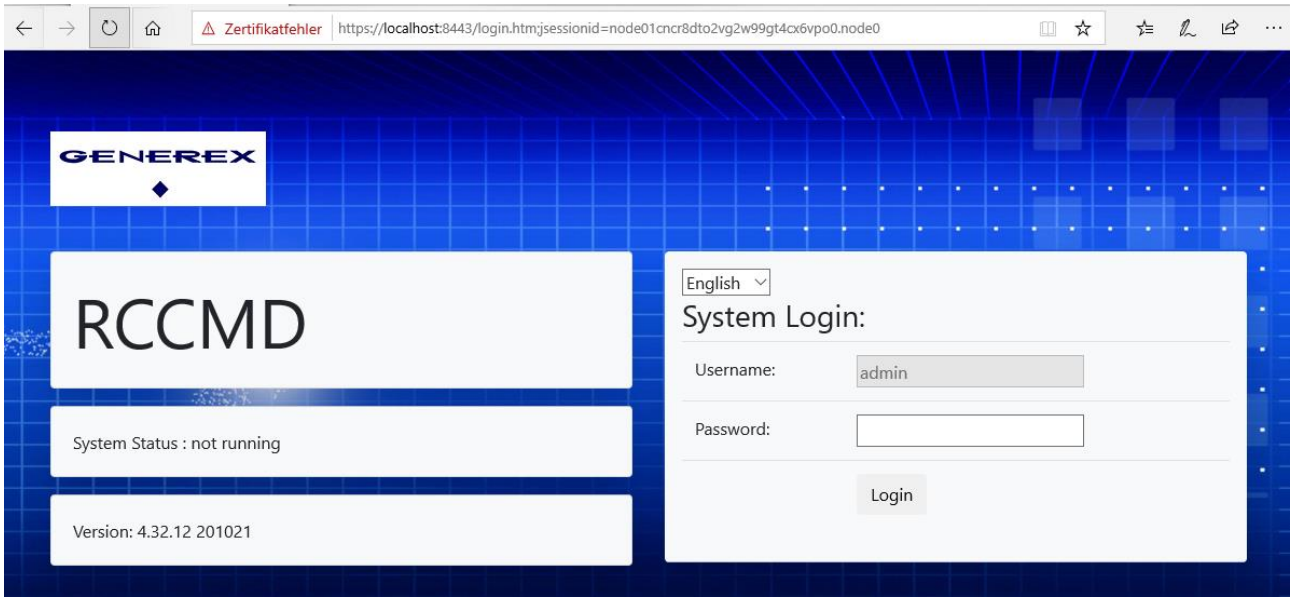
Login und Schnellabsicherung

In diesem Kapitel geht es um den Schnelleinstieg und die Absicherung Ihrer RCCMD – Installation.

Zugang zum Webinterface:

- https://127.0.0.1:8443 ,
- https://[IP-Adresse des Computers]:8443,
- https://localhost:8443

Passwort: RCCMD bzw. das von Ihnen vergebene Passwort.

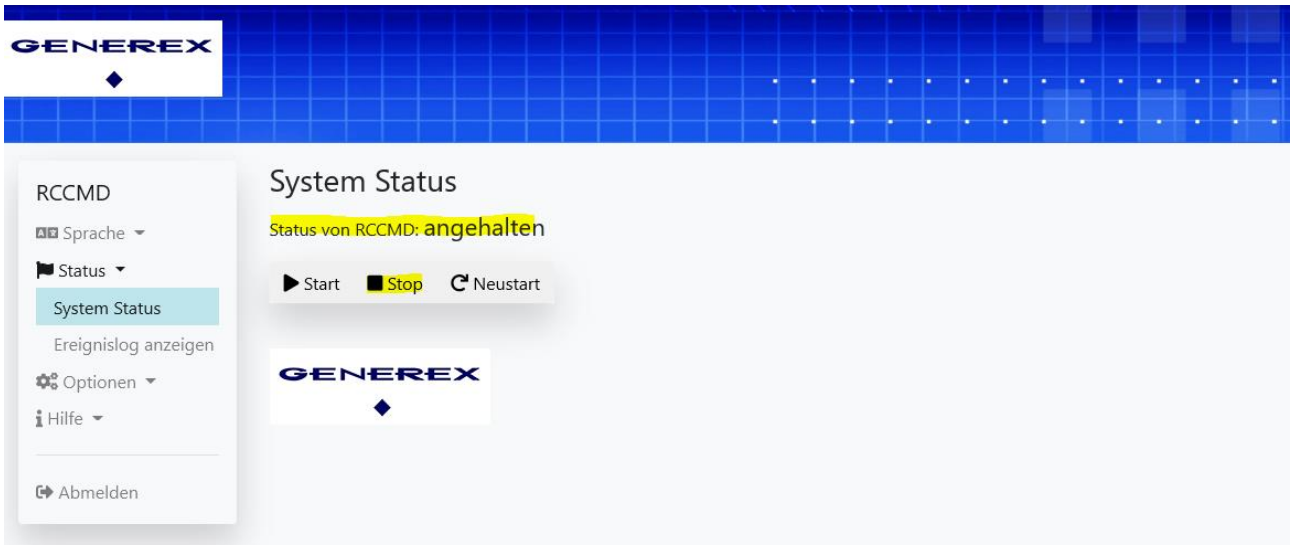


Entweder haben Sie bei der Installation ein Passwort vergeben, dann geben Sie dieses jetzt an. Wenn Sie das Feld leer gelassen haben, verwenden Sie dieses originelle Passwort:

- RCCMD oder das von Ihnen bei der Installation eingegebene Passwort

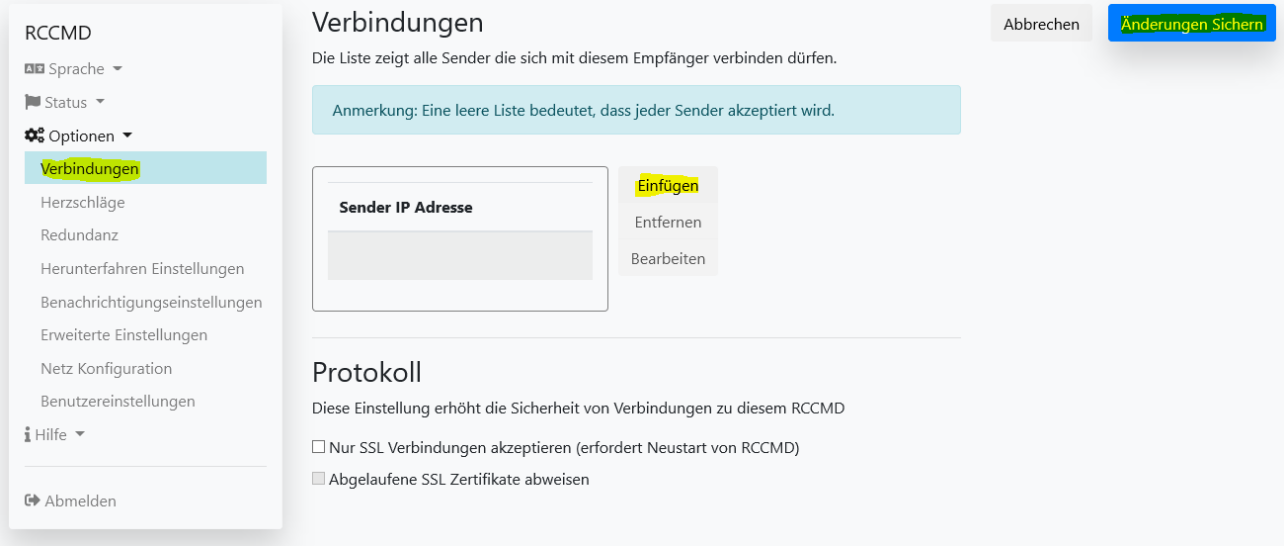
Nach der Anmeldung können Sie auf die Konfigurationsmenüs zugreifen:

Schritt 1: Klicken Sie auf Status > System Status



Vergewissern Sie sich, dass unter System Status RCCMD auf “angehalten” steht. Das stellt sicher, dass nicht versehentlich Ihr Server heruntergefahren werden kann.

Schritt 2: Optionen>Verbindungen

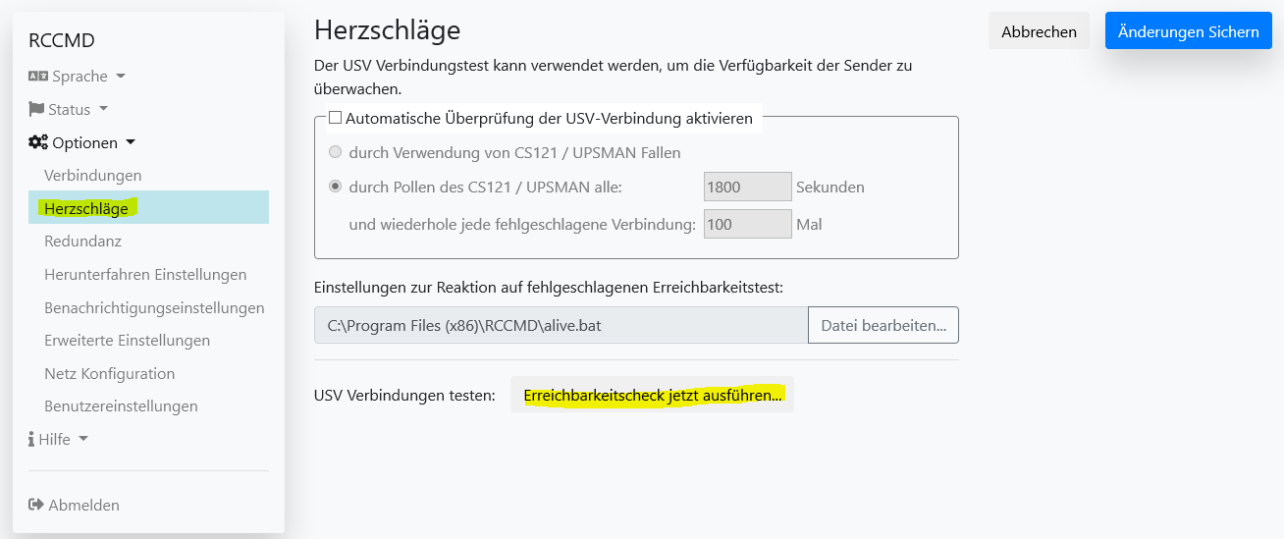


Drücken Sie unter Verbindungen auf “Einfügen” und geben Sie die IP-Adresse des zuständigen CS121/ CS141/UPSmanagers, … - kurz gesagt den gültigen RCCMD Shutdown Sender ein. Achten Sie darauf, dass Sie auch oben rechts auf “Speichern klicken, damit die hinterlegte IP-Adresse Gültigkeit hat.

Was Sie mit diesem Schritt unternehmen:

Sobald hier eine IP-Adresse hinterlegt ist, akzeptiert der RCCMD Client nur noch genau DIESE IP-Adresse als berechtigten Sender. Andere Signale werden zwar höflicherweise dokumentiert, die Ausführung jedoch verweigert.

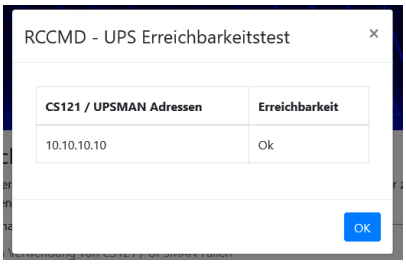
Schritt 3: Heartbeats kontrollieren unter Optionen>Herzschläge



Über diese Funktion können Sie feststellen, ob der RCCMD Client auch seinen CS141 erreicht und die Kommunikation möglich ist.

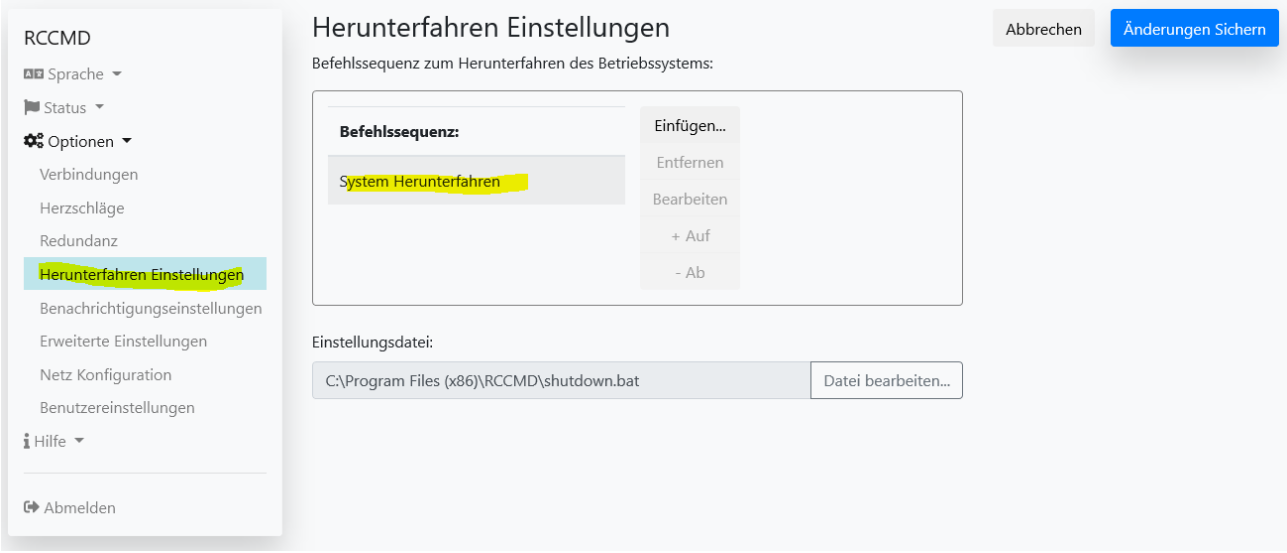
Bitte beachten Sie, dass bei Lizenzprodukten - also Hersteller von SNMP-Karten, die eine RCCMD-Lizensierung durchgeführt haben, diese Funktion nicht unbedingt von der Hardware her unterstützen.

Alle GENEREX-Karten (BACS / CS121/ CS141/ SITEMONITOR / SITEMANAGER) unterstützten diese Funktion und müssen an dieser Stelle ein “OK” geben.



Schritt 4: Herunterfahren Kontrollieren

Gehen Sie auf Optionen > Herunterfahren Einstellungen



Standardmäßig sollte hier als Befehlssequenz “System Herunterfahren” bereits enthalten sein:

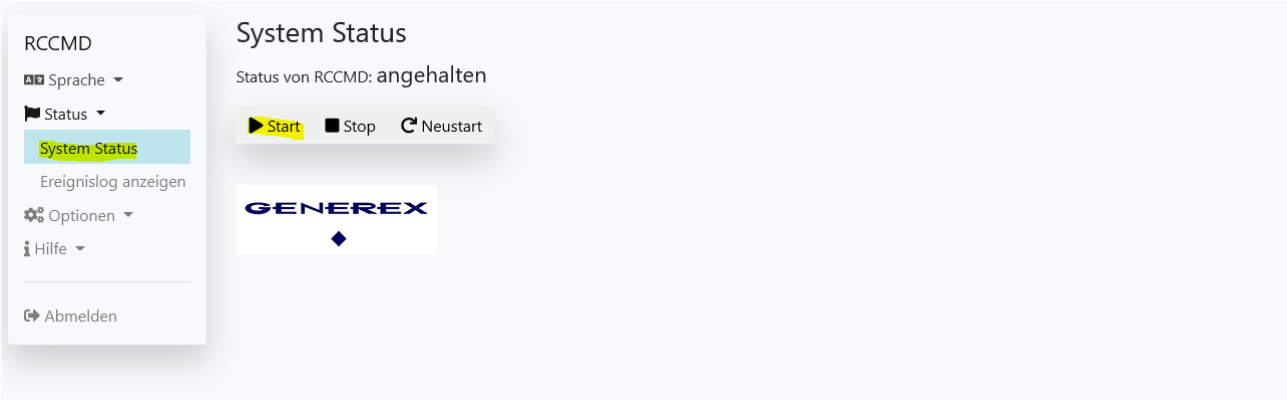
Das Windows Betriebssystem kriegt den Befehl, herunterzufahren und die Hardware auszuschalten. Sollte der Computer hinterher einfach wieder neu starten, ist dieses im BIOS eingestellt, das müssten Sie je nachdem, was Sie erreichen wollen, dann im BIOS des Mainboards nachjustieren.

Wie funktioniert diese Liste:

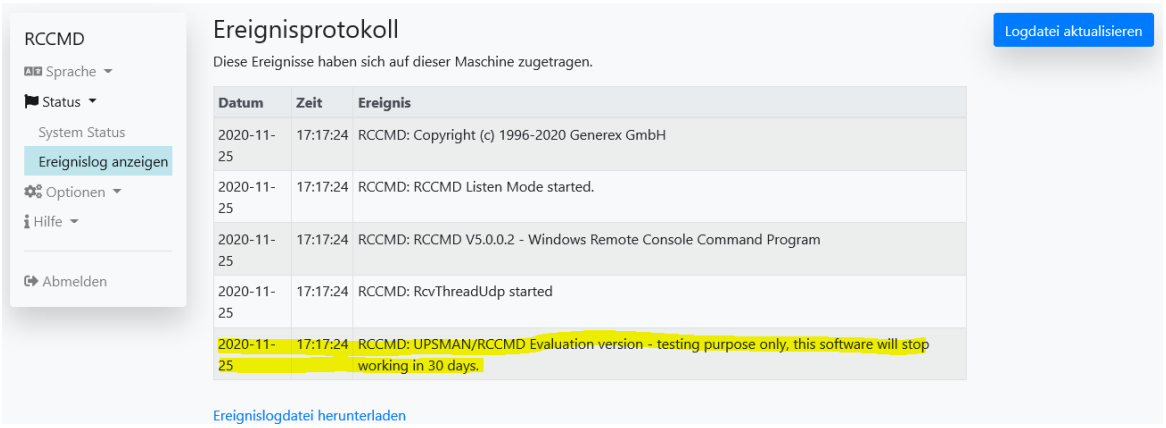
Wird ein RCCMD-Shutdown über einen gültigen Sender ausgelöst, wird diese Liste von Oben nach Unten wie eingetragen ausgeführt. Achten Sie also darauf, dass “System Herunterfahren” immer der letzte Punkt ist, der ausgeführt wird.

Schritt 5: Lizenz kontrollieren und ändern

Drücken Sie unter Status>System Status auf Start.

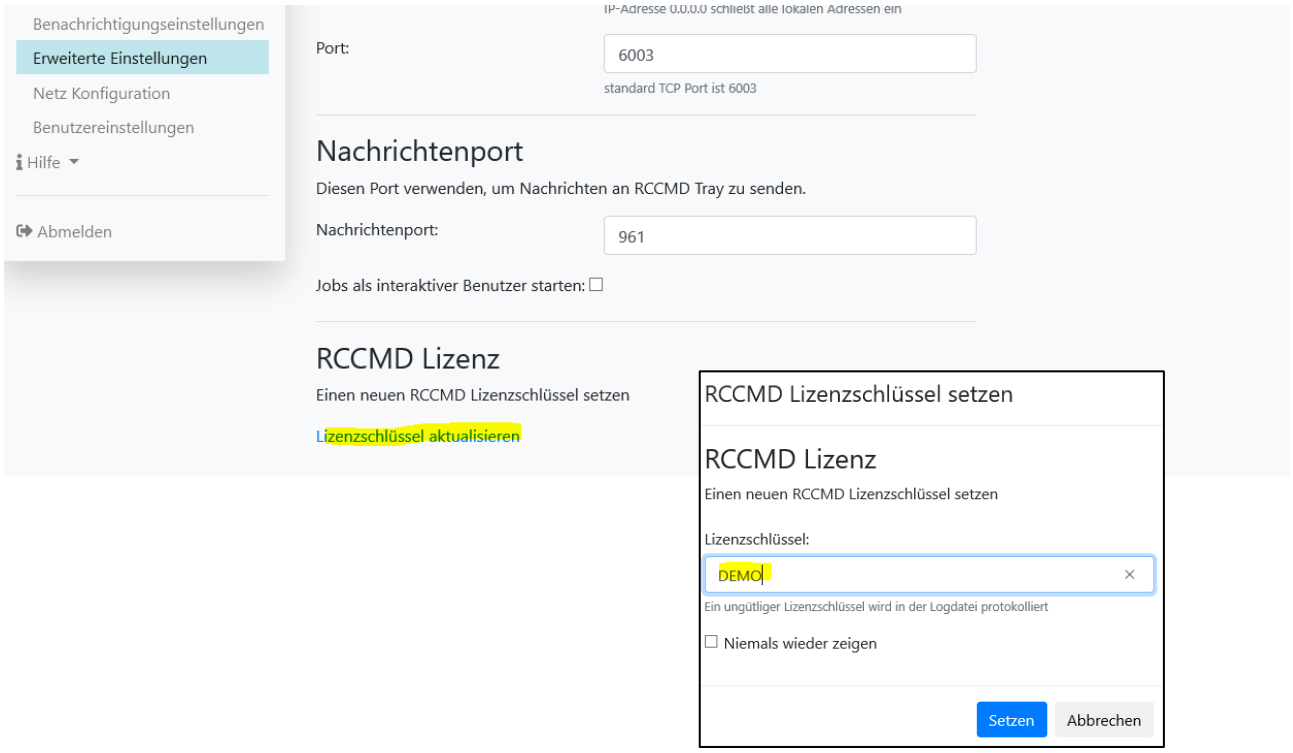


Und gehen Sie anschließend auf “Ereignislog anzeigen”. Wenn Sie diesen Eintrag sehen, ist der Key, den Sie eingegeben haben, fehlerhaft:



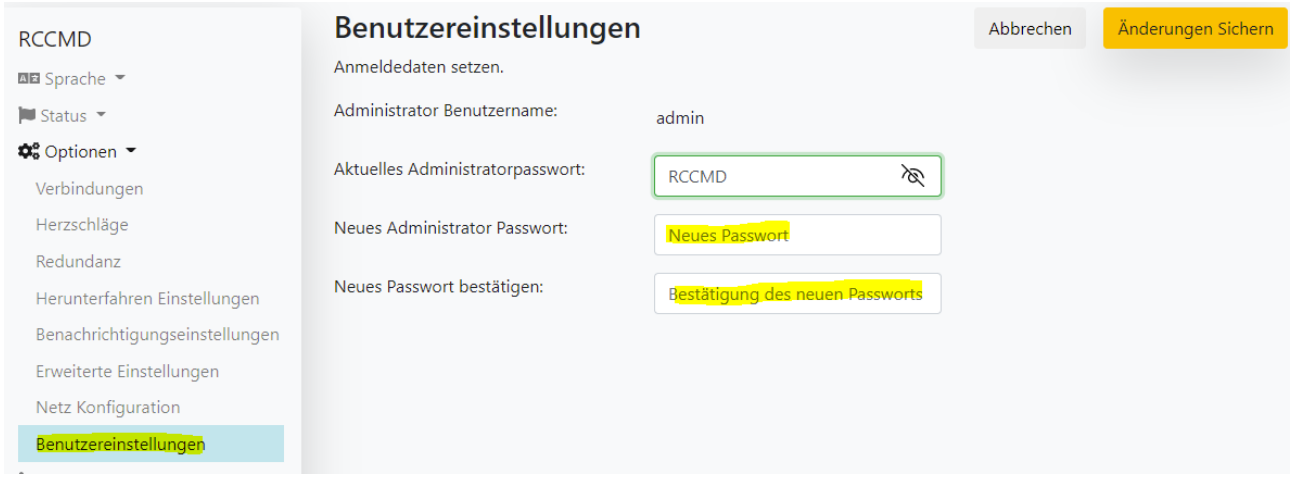
So ändern Sie den Key:
Klicken Sie auf Optionen>Erweiterte Einstellungen

Ganz unten finden Sie den Eintrag “Lizenzschlüssel aktualisieren”:



Geben Sie hier einfach den Key erneut ein und klicken Sie unter “Status” auf Neustarten. Der Testkey-Eintrag erscheint so lange, bis ein gültiger Key eingegeben wurde.

Schritt 6: Änderung des Passworts
Klicken Sie auf Optionen>Benutzereinstellungen



Ändern Sie bitte das Passwort, um zu verhindern, dass unbefugte Zugang zu den Einstellungen erhalten. Weitere Möglichkeiten zur Absicherung finden Sie im Anhang im Security Guide.

Das RCCMD Web Interface

Die Konfigurationsmenüs im Detail erklärt

Alle Optionen für den RCCMD Client
für Windows / Linux / Unix / MAC – basierte Installationen.

Die Anmeldemaske

Nach der Installation können Sie sich über das Webinterface anmelden und mit der Konfiguration von RCCMD beginnen. Der Benutzernahme ist dabei vom System vorgegeben und kann nicht geändert werden:

- Alle konfigurierten Aktionen sind administrative Eingriffe in ein laufendes Betriebssystem

Gültigkeit von Passworten:

Wenn Sie bei der Installation kein Passwort vergeben haben:

Verwenden Sie in diesem Fall das Standardpasswort **RCCMD**

Wenn Sie bei der Installation ein eigenes Passwort vergeben haben:

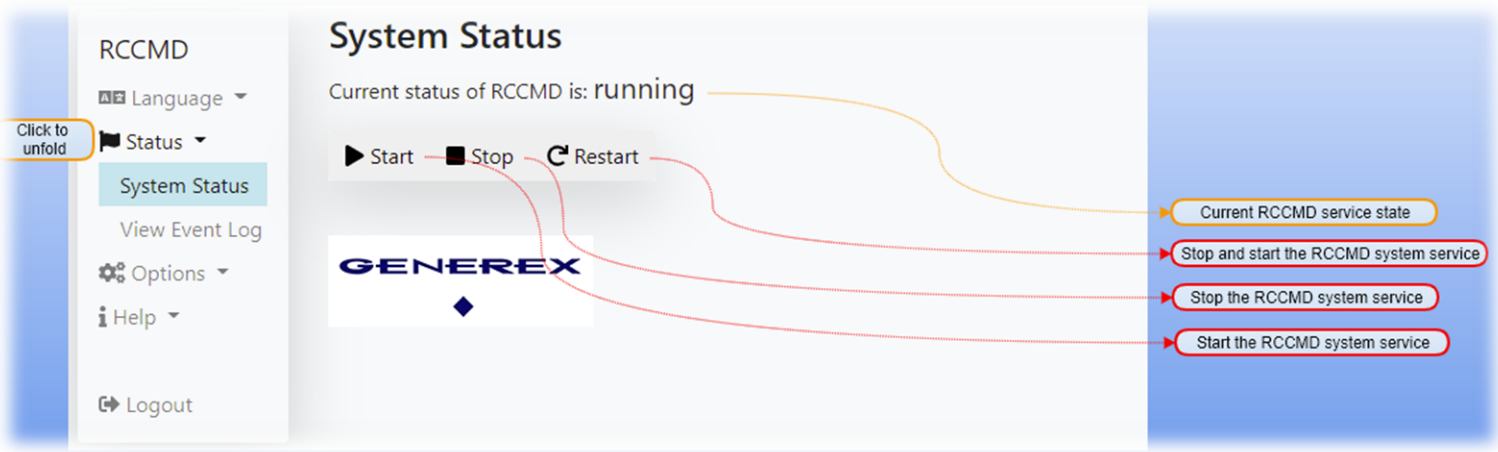
Verwenden Sie das Passwort, dass Sie vergeben haben.

Tipp:

Der aktuelle Systemstatus bei der Erstkonfiguration steht immer auf angehalten:

In diesem Systemzustand wird RCCMD weder gültige Signale empfangen noch umsetzen können. Dies ist ein gewollter Zustand, weil im gegenwärtigen Konfigurationsstand jedes gültige RCCMD Shutdownsignal entsprechend umgesetzt wird.

Systemzustand überprüfen



Nach der Anmeldung werden Sie zum aktuellen Systemstatus weitergeleitet. RCCMD kann von hier aus grundlegend aktiv gesteuert werden:

Start

Startet den RCCMD Dienst und stellt die Konfiguration scharf. Sobald RCCMD aktiv ist, können RCCMD-Signale empfangen und umgesetzt werden.

Stop

Mit dieser Funktion wird der RCCMD Service angehalten. Die eingehenden Signale werden nicht überwacht und RCCMD wird bei gültigen Shutdownroutinen weder protokollieren noch entsprechend auslösen.

Neustart

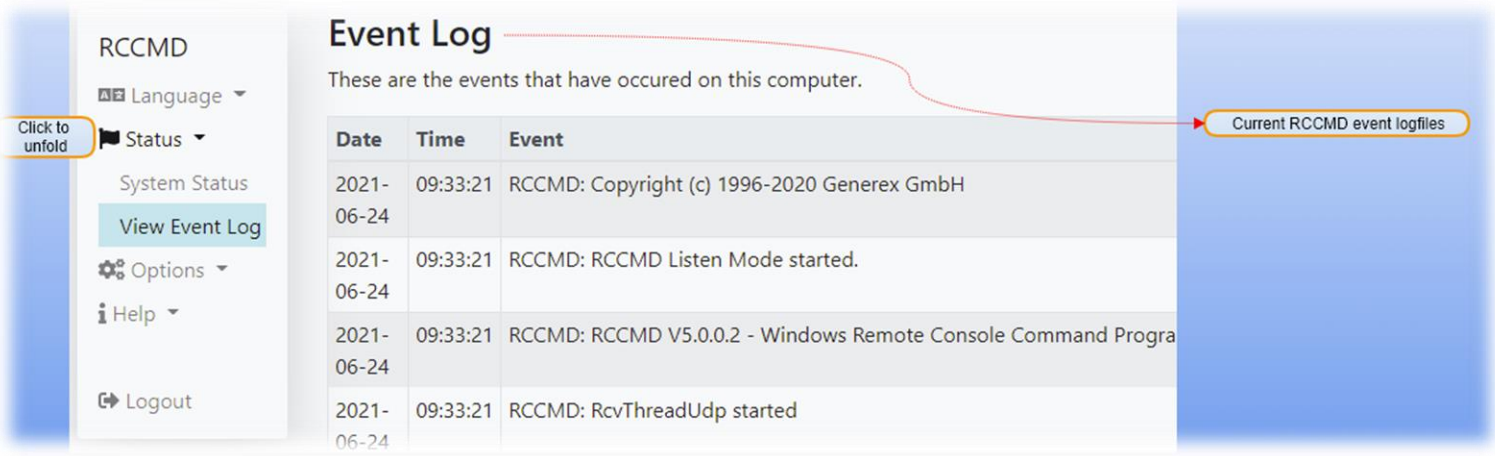
Der Neustart stoppt den RCCMD Dienst und startet ihn anschließend wieder. Diese Funktion fasst die beiden anderen Funktionen zusammen.

Tipp

Wozu ein RCCMD „Neustart“?

In einigen Fällen muss RCCMD bei der Initialisierung Konfigurationsdateien einlesen. Dieses kann jedoch nur bei einem Neustart erfolgen- Dafür muss der Server nicht neu gestartet werden, es langt, wenn RCCMD sich kurz beendet und anschließend selber neu startet. Wenn dieser Schritt bei der Änderung von Konfigurationen notwendig ist, wird Sie RCCMD darüber automatisch via Pop-Up-Fenster informieren.

Logfiles

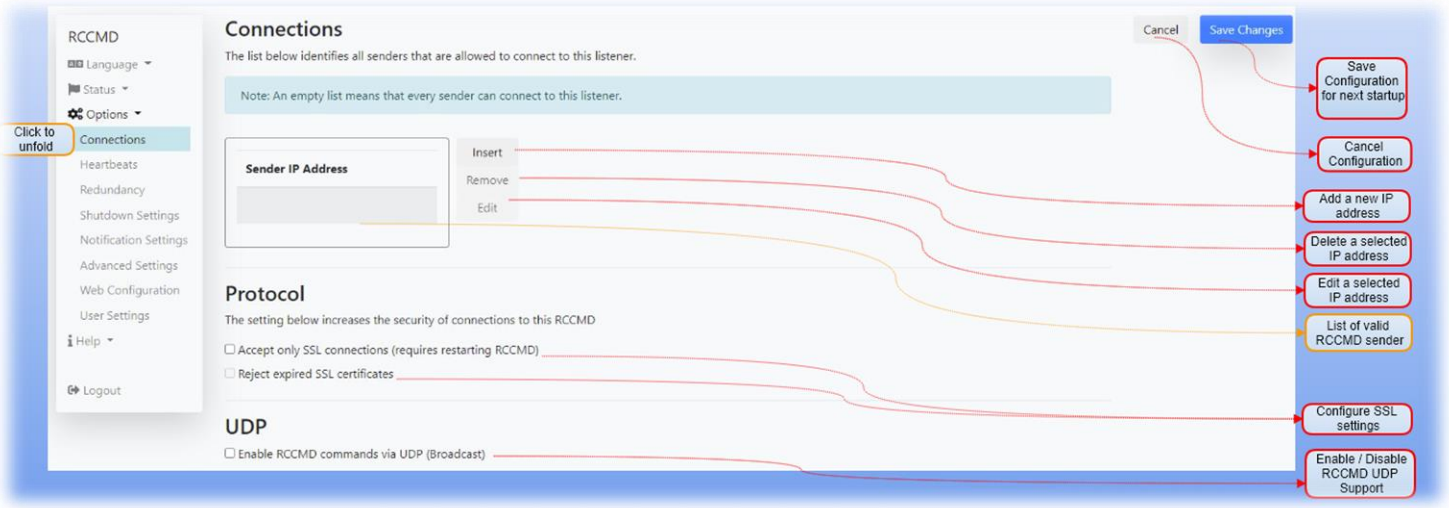


Sobald RCCMD aktiv ist, wird es jeden eingehenden Verkehr sowie die entsprechenden Aktionen protokollieren. Enthalten sind hierbei

- Datum
- Uhrzeit
- Sender
- Geforderte Aktion
- Ausführungsstatus

An Hand dieser Dateien können Sie den Weg eines RCCMD Signals zur Quelle zurückverfolgen und auf diese Weise Probleme beim Senden und Empfangen eingrenzen.

Verbindungen

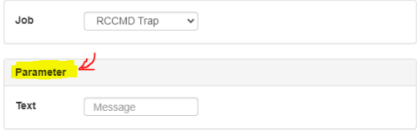


In größeren Installationen kann es vorkommen, dass ein Client nicht unbedingt herunterfahren darf. Ein typisches Beispiel hierfür wäre z.B. eine SQL-Datenbank, die erst heruntergefahren wird, wenn alle Verbindungen richtig geschlossen wurden, oder spezielle Backupserver oder Domänencontroller, welche als letztes herunterfahren und als erstes Starten müssen. Es gibt zudem viele Szenarien, bei denen ein RCCMD-Client nur von bestimmten Quellen ein Signal umsetzen darf, und in jedem anderen Fall die Ausführung ablehnen muss.

Tipp:

Auch innerhalb der RCCMD-Konfiguration ist diese Einstellung notwendig, wenn Sie Redundanzverhalten definieren möchten: Sobald zwei oder mehr USV-Anlagen vorhanden sind, müssen auch die entsprechenden Sender bekannt sein.

RCCMD UDP Broadcast Support



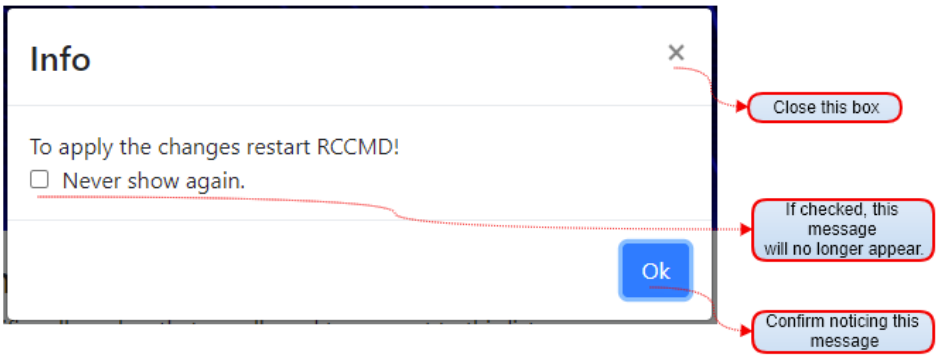
Sobald ein CS141 über einen Job Informationen über das Netzwerk sendet und keine IP-Adresse verwendet wird, geschieht dies unidirektional über UDP. Das erkennen Sie daran, dass im Konfigurationsdialog für den Job im CS141 unter Parameter keine IP-Adresse definiert werden kann, bzw. Sie die Möglichkeit haben, einen „Broadcast“ zu aktivieren.

Ein RCMD Client ignoriert für gewöhnlich Broadcast – Nachrichten bis dieses Feature ausdrücklich aktiviert wurde. Beachten Sie bitte hierzu, dass UDP Datenpakete nicht durch Handshakes wie bei TCP abgesichert sind. Wenn Sie Broadcastnachrichten nicht benötigen, deaktivieren Sie bitte diese Funktion, um eventuelle IP-Spoofing- Angriffen vorzubeugen.

Hinweisfenster unter RCCMD

In einigen Fällen ist es notwendig, RCCMD als Service kurz neu zu starten. Dieses kann unter Systemstatus innerhalb der Konfigurationsoberfläche durchgeführt werden.

Wenn dieser Schritt notwendig ist, wird Sie RCCMD darauf direkt beim Übernehmen der Daten hinweisen:



Niemals wieder anzeigen

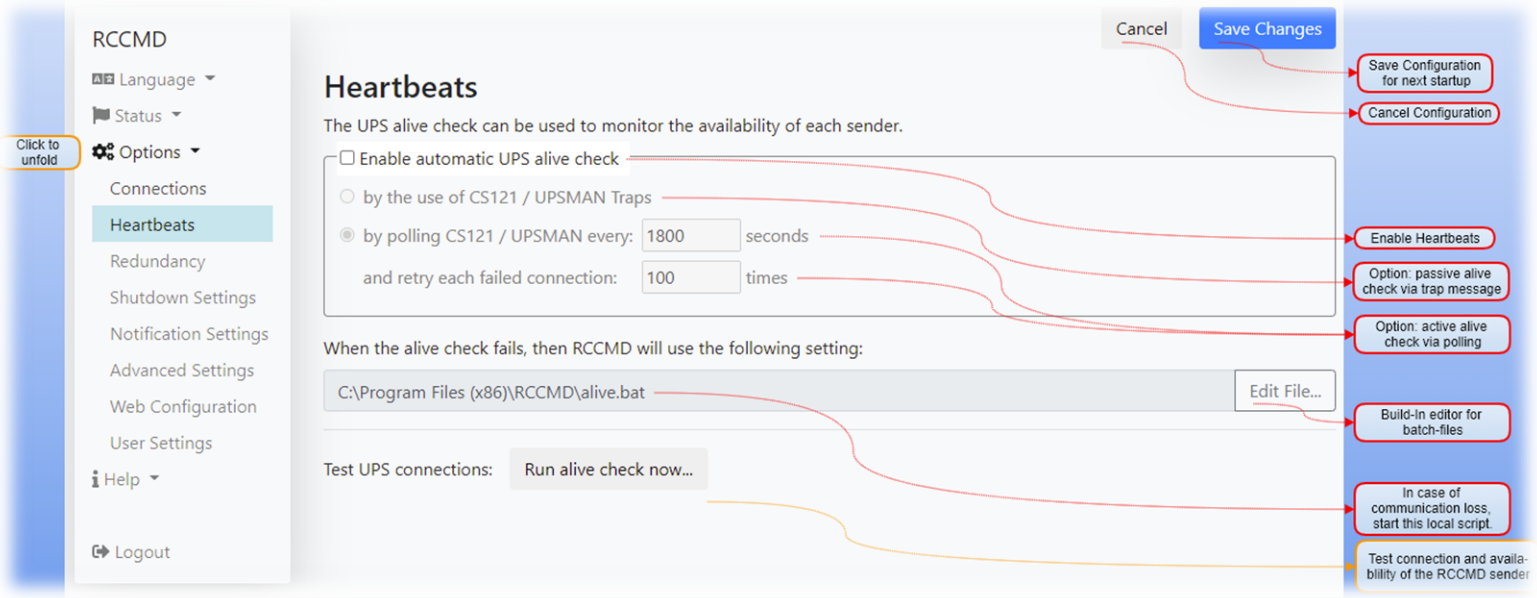
Dieses Fenster wird nicht mehr angezeigt, bis Sie den Webbrowser geschlossen und wieder geöffnet haben. Sie können also ganz entspannt alle Konfigurationen durchführen und anschließend RCCMD neu starten.

OK

Ansonsten wartet der kritische RCCMD Service generell auf Ihre Anweisung. Dieser Button ist die allgemeine Lesebestätigung und aktiviert lediglich vorübergehend die Funktion „Niemals wieder zeigen“

RCCMD wird nur Ausnahmesituationen selber neu starten, wenn es für einen Konfigurationsschritt zwingend notwendig

Herzschläge / Heartbeats



Unter bestimmten Umständen kann die Verbindung zwischen RCCMD und CS141 zusammenbrechen. Das passiert z.B. wenn bei einem Stromausfall ein Switch vergessen wurde, und dieser dann weg bricht. In dem Fall würde der CS141 zwar ein gültiges Shutdown Signal senden, jedoch würde dieses niemals sein Ziel erreichen können.

Ein weiteres Szenario wäre hier ein defekter Switch oder Router:

Da RCCMD ein reines Empfangsprogramm ist, welches auf den Eingang von Signalen reagiert, kann es nicht wissen, ob die Verbindung generell richtig geschaltet ist.

Abhilfe schaffen hier die Heartbeats:

UPSMAN Traps

In dem Fall sendet ein RCCMD Server unaufgefordert eine Trap-Nachricht an den RCCMD-Client. Der Empfang dieser Nachricht wird entsprechend protokolliert.

By Polling

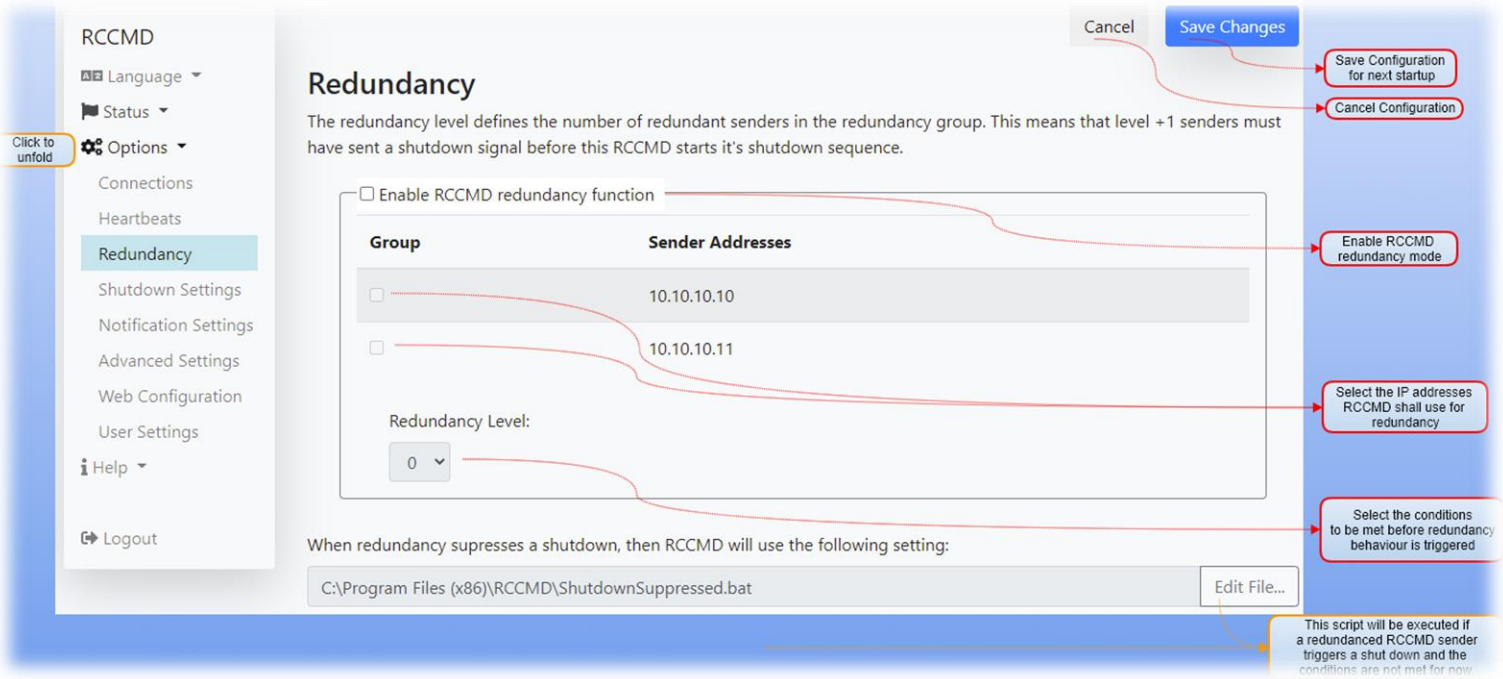
Der RCCMD Client fordert zyklisch vom RCCMD Server eine Nachricht an und protokolliert die Erreichbarkeit der Gegenstelle. Wenn diese Verbindung nicht möglich ist, kann der Vorgang frei definierbar oft wiederholt werden.

Sollte das Erreichbarkeitstest nicht erfolgreich sein, kann ein automatisches Skript gestartet werden.

Dieses Skript ist eine Standard Batch Datei, welche frei editiert werden kann. Dabei mach Ihnen RCCMD keine Vorgaben, was mit diesem Skript erreicht werden soll oder kann.

Tipp: RCCMD muss natürlich irgendwie wissen, welche Geräte letztendlich geprüft werden sollen. Die Liste der zu prüfenden Geräte wird aus der Liste genommen, die Sie unter Verbindungen eintragen: Grund ist, dass diese Geräte für den RCCMD Client von besonderer Relevanz sind.

Redundanzlevel einstellen



Zunächst einmal:

Unterscheiden Sie bitte zwischen CS141 und USV – Die USV kann nichts senden, nur der CS141, der an der USV angeschlossen ist. Das kann ein externes Gerät über RS232 / RS485 oder auch eine interne Slotkarte sein. Technisch betrachtet sind es eigenständige Geräte, aber wenn man den Weg des Signals von der USV ausgehend verfolgt, ist es einfacher zu visualisieren, wenn man den CS141 als Bestandteil und damit die USV als „Sender“ betrachtet...

Wenn in einem, Netzwerk mehr als eine USV vorhanden ist, können Systeme redundant angeschlossen werden. In diesem Fall kann es vorkommen, dass der Ausfall einer von zwei Stromversorgungen nicht unbedingt einen Notfallshutdown auslösen muss.

RCCMD kann so eingestellt werden, diese Netzwerkkonfiguration zu berücksichtigen. Die Konfiguration verläuft nach folgendem Muster:

1. Definieren Sie unter Verbindungen die IP-Adressen gültiger Sender
2. Definieren Sie unter Redundanz, welcher dieser Sender zusammen funktioniert
3. Stellen Sie den Redundanzlevel ein:

   Der Redundanzlevel folgt einem klaren Muster: Sobald einer der ausgewählten gültigen Sender einen Shutdown sendet, wird an Hand des Redundanzlevels festgehalten, wie viele *weitere* Sender einen solchen Shutdown senden müssen:

   0 - Kein weiterer Sender ist notwendig.

1 – Mindestens ein weiterer der ausgewählten Sender muss einen Shutdown senden
2 – Mindestens zwei weitere der ausgewählten Sender müssen einen Shutdown senden
3 – Mindestens drei weitere der ausgewählten Sender müssen einen Shutdown senden

Die Anzahl der verfügbaren Maximal-Redundanz wird automatisch an die Anzahl der unter „Gruppe“ ausgewählten IP-Adressen gültiger Sender angepasst. Sie können also niemals mehr Geräte auswählen als wirklich vorhanden sind.

Überspielen eines Redundanz-Shutdowns durch direkte Befehle

Es kann immer wieder vorkommen, dass ein Shutdown ausgeführt werden muss, obwohl beide USV-Anlagen in Ordnung sind und die Hauptstromversorgung fehlerfrei läuft - ein typisches Szenario wäre hier eine defekte Klimaanlage, welches das Überhitzen von Servern und weiterer Infrastruktur zur Folge hätte.

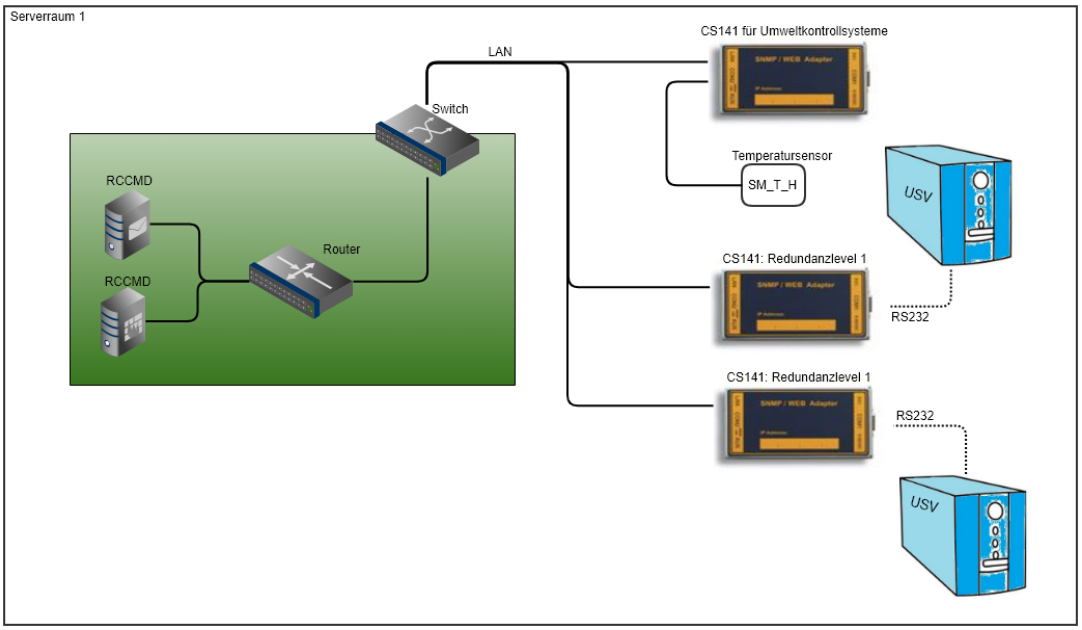
Server sollten auch hier rechtzeitig heruntergefahren werden können. RCCMD bietet Ihnen jetzt mehrere Möglichkeiten an:

Sie erstellen ein eigenes Shutdownskript, welches Sie über ein Custom Command direkt ansteuern.

> Mit diesem Befehl können Sie ein beliebiges Skript starten, welches skriptgesteuert einen Shutdown auslöst. Da es sich hierbei nicht um den Job „RCCMD Shutdown“ handelt, welcher gezielt mit der USV in Verbindung gebracht wurde, würde der RCCMD Client es entsprechend umsetzen, da die IP-Adresse des Senders unter Verbindungen eingetragen ist.

Sie nutzen einen unabhängigen dritten CS141

> Dieser CS141 wurde z.B. rein für Umgebungskontrollsysteme ausgerüstet:
>
> Darunter fallen je nach Ausbaustufe bis zu 8 analoge Sensoren und 4 Digitale Inputs. Darunter fallen u.a. Brand- und Rauchsensoren, Glasbruchsensoren, Zugangskontrollsysteme, Gasmelder, Temperaturfühler, Füllstandsmelder, digitale Alarmdrähte, Batteriemanagementsysteme, Bewegungsmelder, etc.



> In diesem Fall würden Sie alle drei CS141 unter *Verbindungen* eintragen, jedoch bei *Redundanz* nur die beiden Sender auswählen, welche sich direkt mit der USV und dem Notfallshutdown bei Problemen mit der USV befassen. Der dritte CS141, welcher ausschließlich die Umweltkontrollsysteme betreut, könnte in dem Fall unabhängig davon einen RCCMD Shutdown senden, sollte dieses notwendig sein.

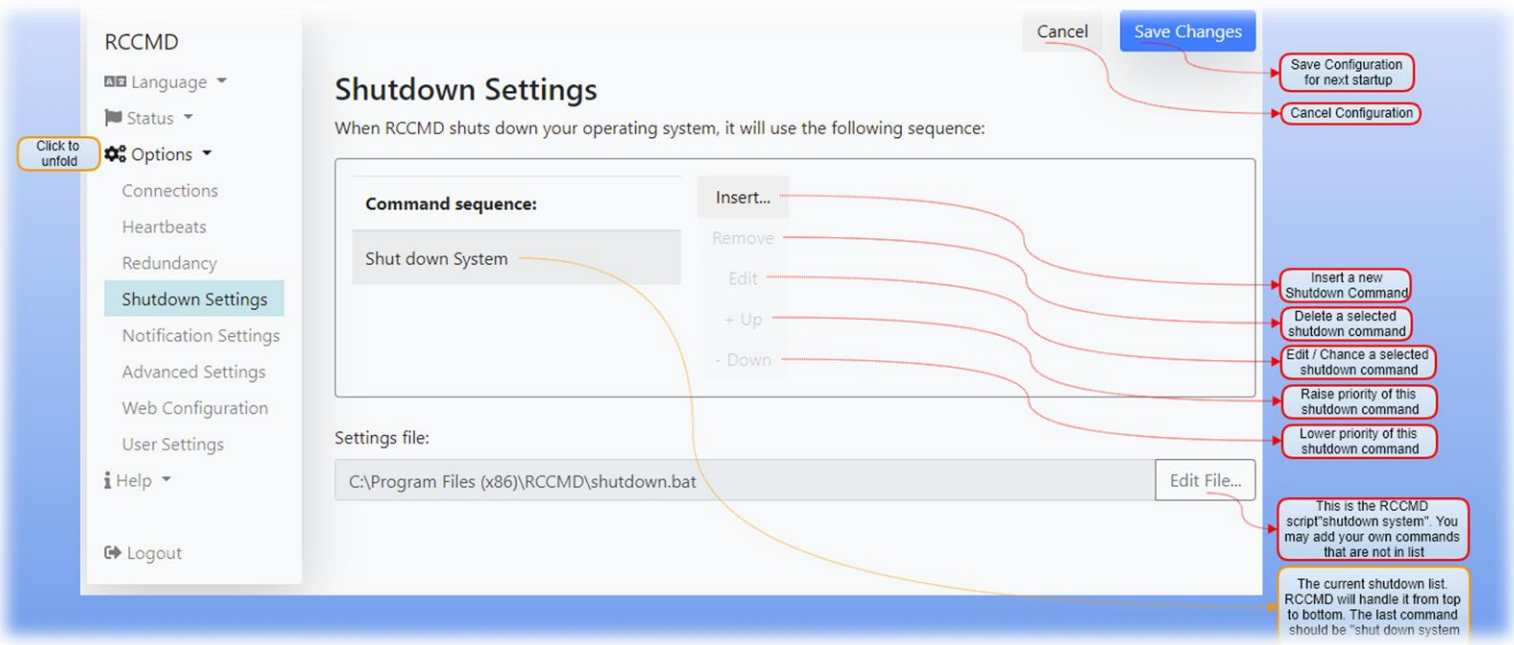
Rücknahme eines Shutdowns:

Ab einer Redundanz von 1 (= zwei Geräte) kann ein Shutdown auch wieder zurückgenommen werden – dies ist z.B. der Fall wenn die Hauptstromversorgung bei einer USV wiederhergestellt wurde. Dies geschieht beim Sender mit dem Custom Command „WAKEUP“ – Dieser signalisiert dem RCCMD Client, dass die Ursache für eine Störung behoben wurde, und der Zähler wird entsprechend korrigiert.

Tipp:

Jeder CS141 darf in diesem Zusammenhang generell nur ein Shutdownsignal senden. Der RCCMD – Client merkt sich, welcher Sender bereits gesendet hat und welcher Sender ein entsprechendes Gegenkommando gesendet hat, also wieder berechtigt wäre. Der Neustart des RCCMD-Clients – normalerweise ein Start nach dem Herunterfahren des Computers – setzt diesen Zähler generell auf 0 zurück. Wenn Sie also nach der Konfiguration die eingehenden Signale testen, starten Sie in jedem Fall den RCCMD Client noch einmal neu, um ein versehentliches Herunterfahren zu verhindern.

Herunterfahren: Einstellungen



RCCMD für Windows bietet Ihnen umfangreiche Möglichkeiten, einen Shutdown durchzuführen. Um die Schnellkonfiguration zu ermöglichen, ist der Befehl „System herunterfahren“ bereits als Grundeinstellung vorkonfiguriert:

Sobald RCCMD ein gültiges Shutdownsignal erhält, wird das Skript shutdown.bat gestartet, welches das Betriebssystem anweist, alle Programme und Prozesse zu beenden, das Betriebssystem herunterzufahren sowie die dazugehörige Maschine auszuschalten.

Tipp:

Dieser Befehl sollte in der Befehlssequenz der letzte Befehl sein, den RCCMD ausführen soll, da sich RCCMD damit selber ausschalten wird. Alle Befehle, die diesem Befehl nachgelagert sind, werden in der Sequenz nicht mehr ausgeführt werden können.

Das Skript, dass diesem Befehl seine Wirksamkeit gibt, ist die Datei *shutdown.bat* Sie finden dieses Skript unterhalb der Einstellung von Befehlssequenzen und können mit „Datei bearbeiten“ die Batchdabei nach Belieben anpassen, erweitern und ändern.

Hinzufügen eines Befehls in eine Befehlssequenz

Klicken Sie auf Einfügen, um einen neuen Befehl der aktuellen Sequenz hinzu zu fügen.

RCCMD präsentiert Ihnen eine Liste von möglichen Befehlen:

Befehl	Betriebssystem	Beschreibung
System herunterfahren	Linux, Windows MAC	Die Programme werden regulär beendet, und das Betriebssystem regulär heruntergefahren.
Vom System abmelden	Windows Linux MAC	Alle Nutzer werden abgemeldet und die Vordergrundprozesse beendet. Das System bleibt aktiv und zeigt die Anmeldemaske.
System ausschalten	Windows, Linux, MAC	Alle aktiven Prozesse werden beendet und das System ausgeschaltet.
System Neustart	Windows, Linux, MAC	Ähnelt dem Herunterfahren, nur dass der Computer nicht ausgeschaltet wird, sondern anschließend neu startet.

Ruhezustand einnehmen (Suspend)	Windows, Linux MAC	Ein Energiesparmodus, bei der alle nicht für den direkten Betrieb notwendigen Komponenten ausgeschaltet werden, um Strom zu sparen. Das Betriebssystem speichert alle für den Betrieb notwendigen Daten im RAM-Speicher, um die Festplatte nicht zu belasten. Der Computer wird in einen Tiefschlafmodus versetzt, aber ist nicht stromlos. *Sollte der Computer ausgeschaltet werden, sind die im RAM gespeicherten Daten verloren.*
System in Standby versetzen (Hibernate)	Windows Linux, MAC	Ein Energiesparmodus, bei der alle nicht für den direkten Betrieb notwendigen Komponenten ausgeschaltet werden, um Strom zu sparen. Das Betriebssystem lagert flüchtige Daten auf die Festplatte aus, leert den RAM-Speicher und versetzt den Computer in einen stromlosen Zustand.
Lotus Notes beenden	Windows only	Lotus Notes reagiert empfindlich, wenn man einfach das Betriebssystem herunterfährt und muss speziell vorher heruntergefahren werden.
Siemens SIMATIC beenden	Windows only	Ein SIMATIC Server ist sehr empfindlich, wenn man sich nicht ganz exakt an eine Shutdownsequenz für SIMATIC hält. Dieser Job beendet sauber den SIMATIC Server, bevor im nächsten Schritt das Betriebssystem heruntergefahren werden kann.
Einige Sekunden warten	Windows, Linux MAC	Speziell dann, wenn Sie eigene Skripte laufen haben, die wiederum Parallelskripte auslösen oder spezielle Speicher- und Kopierbefehle enthalten, kann es passieren, dass die Skripte nicht genug Zeit haben, um sauber bis zum Ende zu laufen und ihre jeweilige Aufgabe zu erfüllen. Mit diesem Eintrag in der Shutdownsequenz können Sie eine Zeitschaltuhr definieren, die RCCMD wartet, bevor zum nächsten Punkt gesprungen wird.
RCCMD Herunterfahren weiterleiten	Windows, Linux, MAC	Auch RCCMD kann Shutdownsignale versenden – daher ist es wichtig, gültige Sender zu definieren, die berechtigt sind, einen Shutdown anzuweisen. Sie können also nicht nur das Redundanzverhalten über USV und CS141 steuern, Sie können einen RCCMD-Shutdown auch über unterschiedliche Server hinwegspringen lassen.
Eine Hyper-V-VM herunterfahren	Windows Only Verfügbar ab Version 4.57.12 240429	Windows PowerShell Befehl, mit dem gezielt eine mit Hyper-V betriebene virtuelle Maschine heruntergefahren werden kann.
Alle Hyper-V-VMs herunterfahren	Windows Only Verfügbar ab Version 4.57.12 240429	Windows PowerShell Befehl, mit dem gezielt alle mit Hyper-V betriebenen virtuellen Maschine heruntergefahren werden kann. Vorsicht bei Hyper-V – Clustern, der Clustermanager werden bei diesem Befehl ALLE virtuellen Maschinen herunterfahren, die sich im Cluster befinden!
Manueller Befehl	Windows, Linux, MAC	Der Manuelle Befehl gibt Ihnen die volle Handlungsfreiheit, lokal auf Ihrem System Skripte in einer Sequenz ausführen zu lassen – Sie können Programme Starten, Prozesse beenden, Befehlszeilen ausführen, etc.

Die Befehlssequenz wird immer von oben nach unten „wie gelesen“ abgefahren und ausgelöst. Je nach Art der Befehle, die dabei ausgelöst werden, kann es innerhalb von komplexen Strukturen zu Widersprüchen oder Problemen mit dem Rechtemanagement kommen, die sich sehr unterschiedlich auswirken können:

Ein typisches Problem wäre zum Beispiel, wenn Sie über den „Manuellen Befehl“ innerhalb der Befehlssequenz ein externes Backup-Programm mit eigenen Shutdown-Szenarien starten und Eintrag in der Befehlssequenz, der das das Betriebssystem herunterfahren soll, nicht entfernt haben:

Sobald das Backup-Programm gestartet wurde, führt RCCMD folgerichtig seinen nächsten Befehl in der Kette aus und zwingt letztendlich das Backup-Programm, sich zu beenden – was zu sehr unterschiedlichen Ergebnissen führen kann:

- Das Betriebssystem fährt herunter, das Backup-Programm meldet einen Fehler
- Das Backup-Programm weigert sich und übernimmt die Shutdownkontrolle
- Das Betriebssystem wird interaktiv, fragt per Dialogbox nach, was geschehen soll und wartet...

Achten Sie also bei komplexeren Strukturen und eigenen Skripten immer auf eventuelle gegenseitige Abhängigkeiten sowie dem Rechtemanagement, welches stark von dem Betriebssystem beeinflusst wird.

Windows ONLY: Der PowerShell / BATCH – Mode Schalter

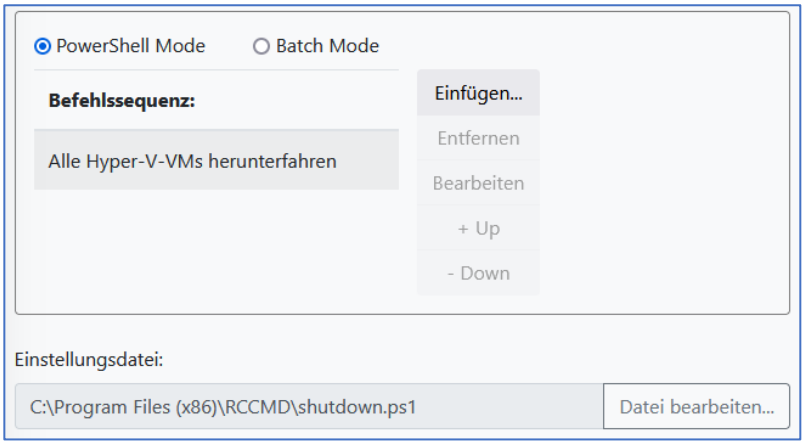
Bitte beachten:

Diese Funktion ist ab RCCMD Version 4.57.12 240429 exklusiv für Windows verfügbar.

Sollte Ihre Windows -Version von RCCMD diese Funktion nicht anzeigen, aktualisieren Sie bitte auf die neuste Version von RCCMD

Mit dem Windows PowerShell Modus können Sie innerhalb von Windows Betriebssystemen zwischen dem bekannten BATCH-Modus und der modernen Windows PowerShell wählen.

In beiden Fällen stehen Ihnen unter „Einfügen“ vorkonfigurierte Befehle zur Verfügung.

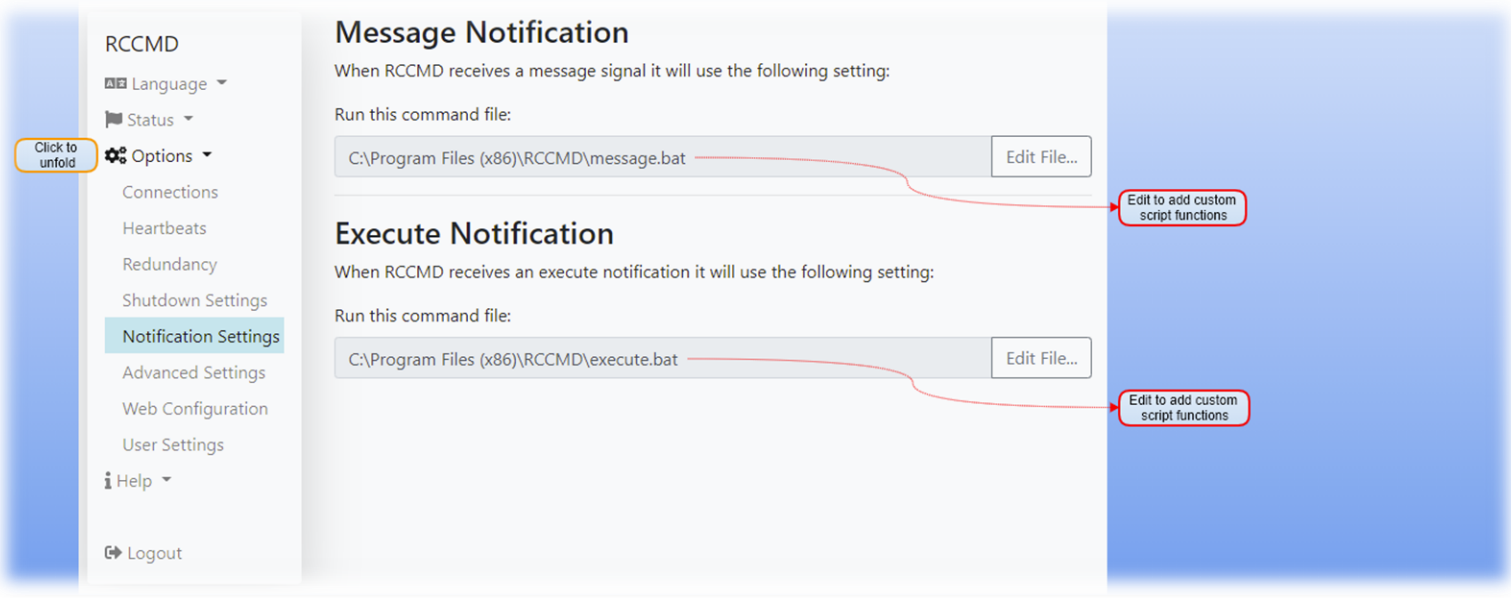


Erfahrene Systemintegratoren können mit dem integrierten Datemanager (Datei Bearbeiten) direkt das enthaltene PowerShell-Script an ihre Anforderungen für einen strukturierten Systemshutdown anpassen, und so selbst komplexe Hyper-V – Cluster - Strukturen mit einer RCCMD – automatisiert und struktruiert herunterfahren.

Tipp: Einführung und Kurz-Tutorial in die Windows Power Shell

Eine Einführung in die Windows PowerShell finden Sie in Kapitel 8, Einstieg in RCCMD mit Windows PowerShell und Hyper-V
Um direkt zum entsprechenden Kapitel zu gelangen, -> **HIER KLICKEN** <-

Benachrichtigungseinstellungen



Diese Batch-Dateien regeln die interne Konfiguration Ihrer RCCMD-Installation und bestimmen, welche Jobs ausgelöst werden können. Sie können diese Dateien ändern und erweitern, um zusätzliche Funktionen zu implementieren oder automatische Skriptabläufe zu starten.

Bitte beachten Sie folgende Sicherheitshinweise:

1. Die Änderung der voreingestellten Batchdateien geschieht auf eigenes Risiko.
   Wenn Sie diese Dateien anpassen und erweitern, ändern Sie das grundsätzliche Verhalten des RCCMD Clients.
2. Fertigen Sie vor dem Ändern eine Kopie der jeweiligen Originaldatei an
3. Bennen Sie die Dateien nicht um – RCCMD wird diese sonst nicht mehr finden können.

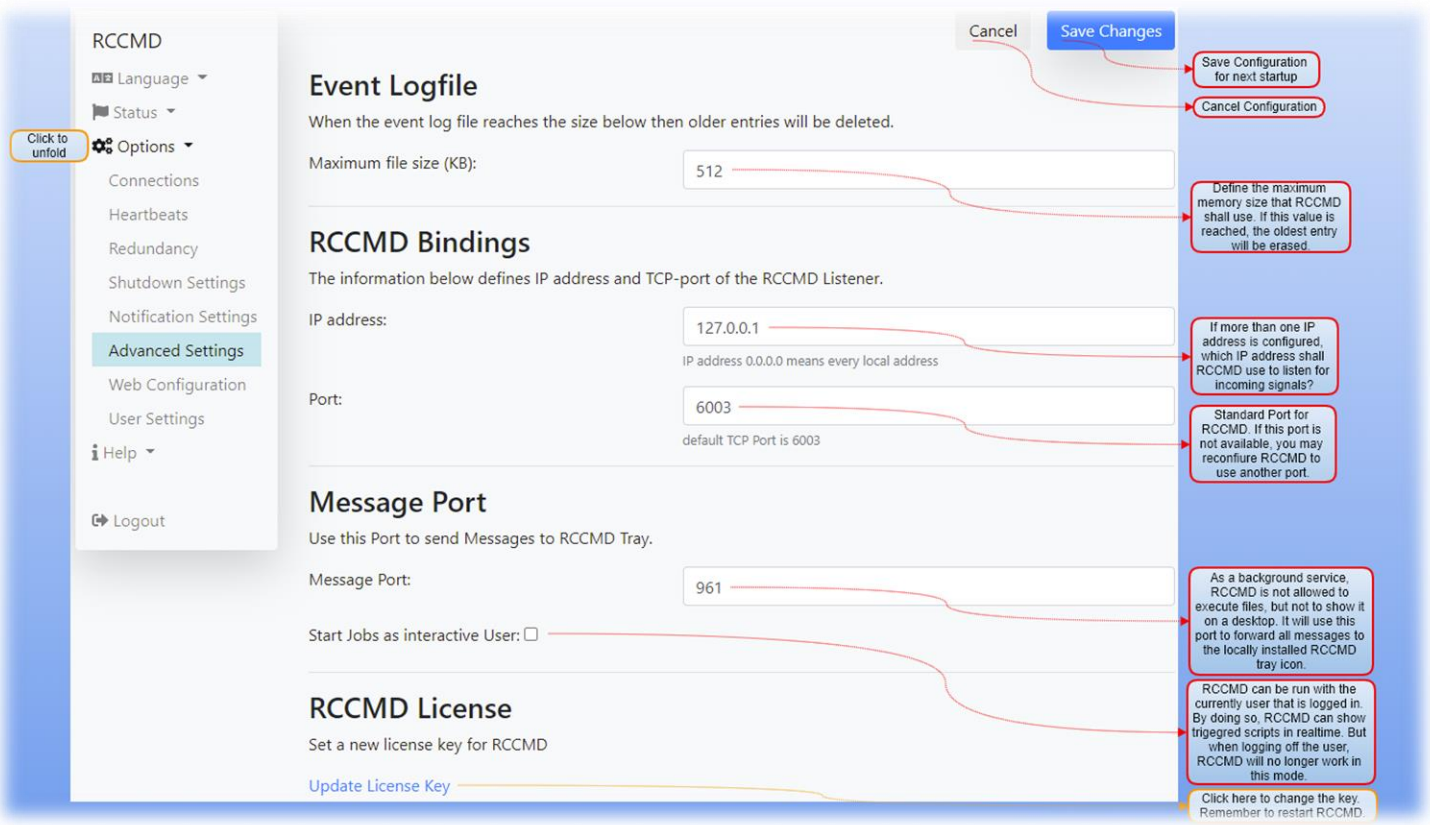
RCCMD verwendet an dieser Stelle drei unterschiedliche Gruppen von Kommandos, die eingehen können. Je nachdem welches Kommando Sie von einem gültigen RCCMD Sender zu diesem Client schicken, wird eins dieser drei Skripte zunächst gestartet.

Nachrichten Anzeige	Das ist das Skript, welches die RCCMD Alarm Box steuert, die Ihnen dieses wunderschöne Fenster mit Hinweisen auf den Bildschirm zaubert. Sobald Sie Nachrichten von einem CS141 bekommen, wird diese Batchdatei aufgerufen.
Ausführanmerkung	Dieses Skript nimmt RCCMD Kommandos entgegen, wenn Kommandos ausgeführt werden sollen, welche Programme oder Skripte starten.

Tipp

Diese Skripte werden immer als erstes aufgerufen! Sobald Sie also ein „Custom Command“ absenden, um z.B. die Batch-Datei HalloWellt.bat zu starten, wird zuerst die Ausführanmerkung gestartet, welches dann den Start der Bach-Datei „HalloWelt.bat“ organisiert - Was immer in diesen Dateien von Ihnen hinzugefügt wird, es wird bei jedem Aufruf immer als erstes ausgeführt und kann nicht auf bestimmte „Jobs“ eingegrenzt werden.

Erweiterte Einstellungen



Ereignisprotokolldatei

Geben Sie an, wie groß die Protokolldatei in KB werden darf, bevor RCCMD anfängt, die jeweils ältesten Einträge zu überschreiben. Dabei wird noch folgendem Schema vogegangen:

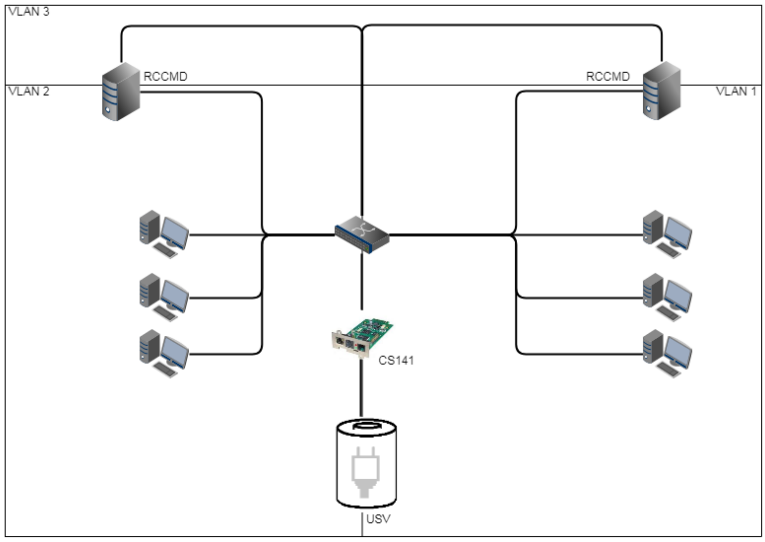
Eintrag 1 -> Dieser Eintrag wird entfernt.
Eintrag 2
Eintrag 3
Eintrag 4 -> Dieser Eintragg kommt neu hinzu.

Der erste Eintrag ist generell der älteste Verfügbare Eintrag und der jüngste Eintrag ganz unten in der Eventliste.

RCCMD Bindings

RCCMD Bindings ist ein filigranes Hilfsmittel, mit dem Sie den Datenverkehr eingrenzen können. Da diese Einstellung tief in Ihre Netzwerkeinstellung eingreift, sollte sie mit entsprechender Vorsicht verwendet werden.

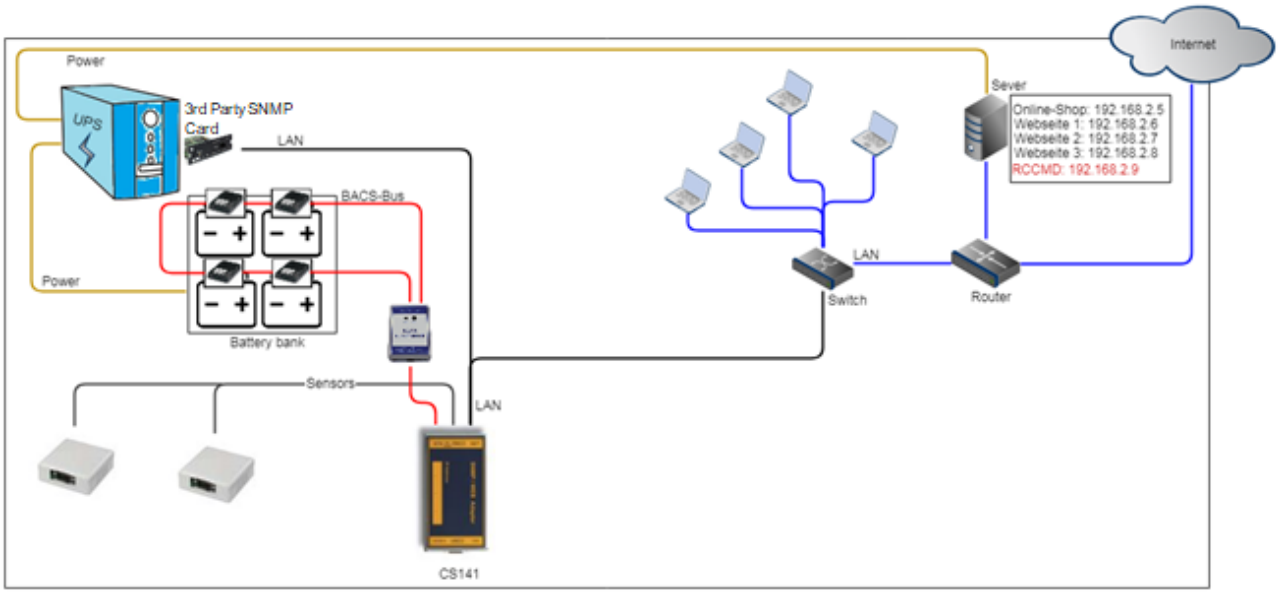
Die Bindings erlauben, den Listener von RCCMD auf eine bestimmte Netzwerkkarte oder beim Multihoming auf eine spezielle IP-Adresse innerhalb eines Netzwerkadapters fest zu definieren. Dieser Fall tritt ein, wenn Sie zum Beispiel über ein VLAN das Netzwerk logisch in ein Produktionsnetzwerk und ein Infrastrukturnetzwerk unterteilen:



In diesem Anwendungsfall können zwei oder mehr Netzwerkadapter in einem Server installiert sein.

Mit dieser Separation können Sie verhindern, dass die Nutzer innerhalb des Netzwerkes auf die RCCMD-Installation zugreifen und versehentlich einen Server herunterfahren – dieses ist ausschließlich über Geräte möglich, die sich in VLAN 3 befinden bzw. über einen Router entsprechend freigeschaltet wurden.

Ein weiterer Anwendungsfall wäre das sog. Multihoming:



Es ist bei modernen Netzwerkgeräten nicht unbedingt notwendig, dass eine IP-Adresse mit einer Netzwerkschnittstelle fest verknüpft ist. Tatsächlich können über eine Netzwerkschnittstelle mehrere IP-Adressen verbunden werden – diese teilen sich dann Hardware, bilden aber sonst in sich geschlossene Instanzen. Ein solcher Anwendungsfall ist zum Beispiel ein Webserver, welcher unterschiedliche Webseiten mit einer jeweils eindeutigen IP-Adresse verwaltet:

In diesem Beispiel ist der Server an einem Router angeschlossen, der festlegt, welche Signale aus dem Internet stammen und welche ihren Ursprung im lokalen Netzwerk haben. RCCMD kann auf diese Weise angewiesen werden, lediglich auf einer bestimmten IP-Adresse auf RCCMD-Signale zu lauschen.

Tipp

Diese Konfigurationen sind Spezialfälle. Der Regelfall sieht vor, dass Sie die Einstellung 127.0.0.1 / local host auf Port 6003 stehen lassen können. In dem Fall wird RCCMD auf allen verfügbaren IP-Adressen lauschen, ob ein gültiges Signal eingeht. Da Sie unter dem Menü Connections die gültige Senderadresse definiert haben, wird RCCMD das Signal zwar bemerkten, jedoch die Ausführung verweigern und diese Tatsache als ungültiger RCCMD- Befehl im Log vermerken.

Nachrichten Port

Normalerweise ist RCCMD ein Hintergrunddienst, dem es nicht gestattet ist, Nachrichten auf dem Display anzeigen zu lassen. Hierfür übergibt der RCCMD – Dienst die Informationen an den Web-If, welcher als Vordergrundprozess zur Interaktion mit einem Benutzer berechtigt ist und Vordergrundprozesse auslösen und anstoßen kann.

Sonderfunktion: Jobs als interaktiver Benutzer starten

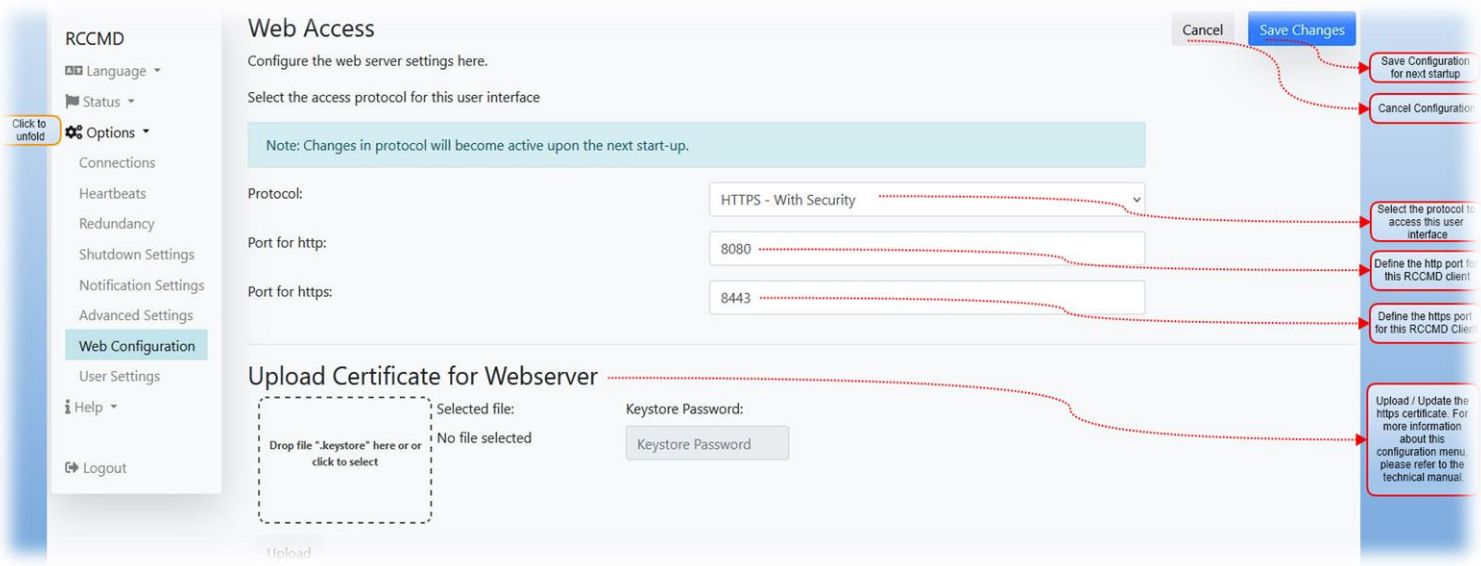
Diese Funktion erlaubt es RCCMD, mit den Rechten des aktuell angemeldeten Benutzers als Vordergrundprozess mit dem System zu interagieren. Bedingung ist hierbei, dass irgend ein Nutzer angemeldet sein muss, da ansonsten übergebene Befehle nicht ausgeführt werden können.

RCCMD Lizenz

Jede RCCMD-Installation benötigt eine entsprechende Lizenz. Sollten Sie beim Start keine Lizenz zur Hand haben, startet automatisch eine 30-tägige Demonstrationslizenz. Danach wird RCCMD sich beenden bis Sie eine gültige Lizenz eingetragen haben.

Bitte beachten Sie, dass RCCMD-Clients im Netzwerk einander abstimmen: Sollten Sie eine doppelte Lizenz vergeben haben, wird nur die erste Installation, welche die Lizenz für sich beansprucht, laufen. Die anderen Lizenzen werden sich entsprechend mit einer Fehlermeldung beenden.

Netzkonfiguration



Über den Netzzugriff stellen Sie die Kontaktmöglichkeiten über das Webinterface ein.

Vorgegeben für den Webzugriff auf RCCMD sind folgende Einstellungen:

Protokollmöglichkeiten:	HTTP / HTTPS
Port für http:	8080
Port für https:	8443

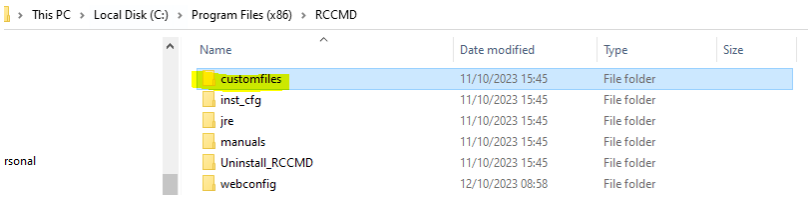
Save / Restore Configuration

Für diese Funktion benötigen Sie die RCCMD Software v 4.49.12 231011 *oder höher*

Wichtig: Mit der Version 4.49 werden einige Änderungen für ein Backup/ Restore eingeführt

Neuer Ordner in RCCMD: Die customfiles

RCCMD unterstützte schon immer die Möglichkeit, dass Nutzer innerhalb der RCCMD Anwendung eigene Skripte starten konnten. Mit der Einführung der BACKUP / RESTORE – Lösung wurde ein neuer Ordner für die eigenen Skripte eingeführt:



Das Backup umfasst nicht nur die von RCCMD selbst verwendeten Konfigurationen, sondern wird mit der Version 4.49 alles, was Sie unter customfiles ablegen*, sichern und wiederherstellen, wenn Sie das Backup einspielen. Das ermöglicht eine schnelle und komfortable Wiederherstellung von Konfigurationen.

Wie starte ich meine custom files aus dem Ordner customfiles

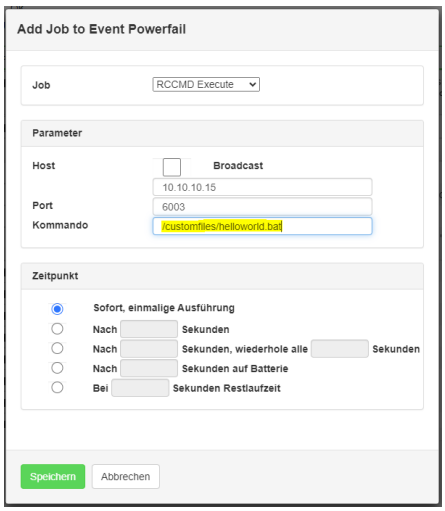
Da der Ordner „customfiles“ ein Unterordner der RCCMD-Installation ist, benötigt der CS141 zum Ausführen im Job „RCCMD Execute“ künftig einen relativen Pfadnamen. Für das Windows-Skript helloworld.bat z.B. würde dieser Start so aussehen:

/customfiles/helloworld.bat

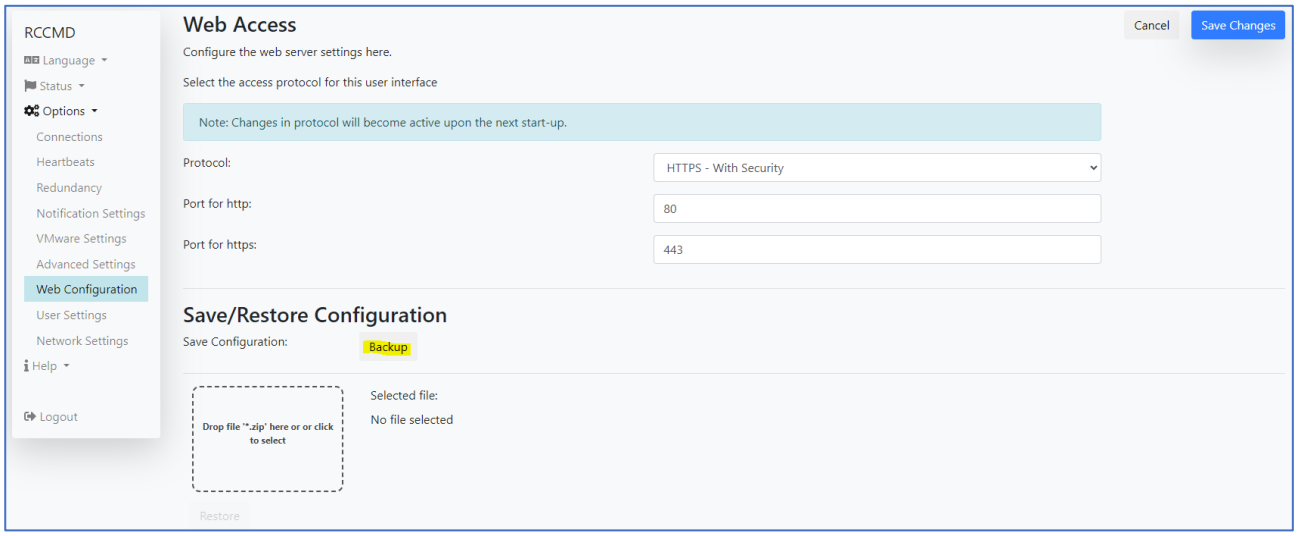
RCCMD wird daraufhin im Unterordner „customfiles“ nach der angegebenen Batch-Datei suchen, und diese mit lokalen Adminrechten ausführen. Wenn Sie das Startskript hingegen im Installationsverzeichnis von RCCMD ablegen, dann bleibt es bei der alten Schreibweise:

helloworld.bat

Sofern sich die Batch-Datei im Installationsverzeichnis von RCCMD befindet, wird RCCMD diese dann auch direkt starten.



Wie erstelle ich ein Backupfile bzw. spiele das Backup wieder ein



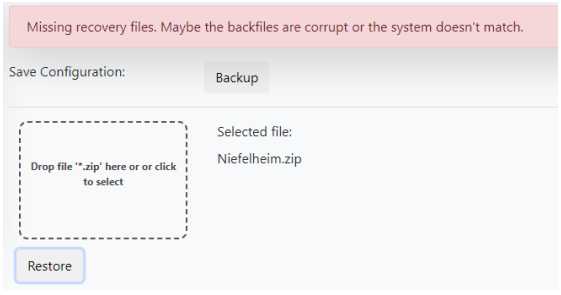
1. *Klicken Sie auf „Backup“*

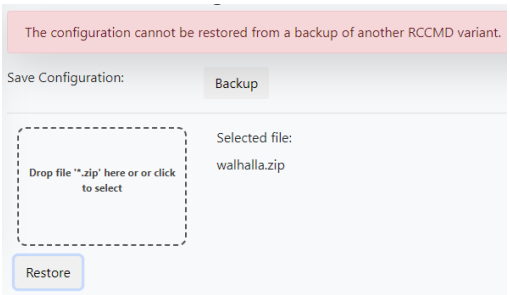
   RCCMD wird daraufhin einen eindeutig gekennzeichneten zip-File zum Download für ein späteres Recovery bereitstellen.

> ***Tipp: Begrenzter Speicherplatz im Ordner „customfiles“: 20 MB***
>
> Das Backup unterscheidet nicht zwischen Dateitypen, Sie können also beliebige Informationen dort ablegen – also auch spezielle Wartungshinweise, Netzwerkpläne, Kurzdokumentationen, etc. – Wenn Sie also RCCMD wieder aufspielen, haben Sie alle Informationen gebündelt an einem Ort zur Verfügung. Zu beachten gibt es lediglich, dass der Ordner nicht größer als 20 MB werden darf. Sollte dies der Fall sein, gibt es beim Erstellen des Backups eine entsprechende Fehlermeldung.

2. *Schieben Sie den Zip-File wie gesichert in die vorgegebene Box, und klicken Sie „Restore“*

   Das integrierte Backupprogramm wird die zip-Datei entpacken und sämtliche Konfigurationen wiederherstellen, inklusive ggfs. selbst erstellter Zertifikate. Zu beachten ist hierbei, dass RCCMD Backups erkennt und bei einer falschen Backup-Datei:

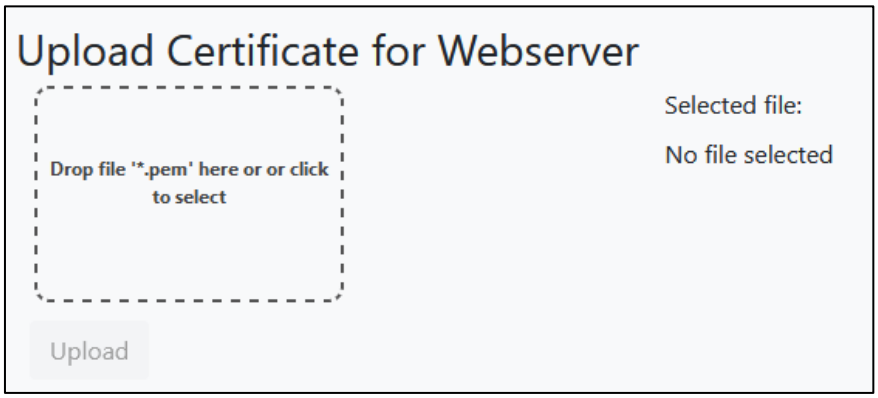




   Je nachdem, ob Sie versuchen, ein Backup Linux <-> VMware bzw. Linux / Vmware <-> Windows einzuspielen, gibt es eine von beiden Fehlermeldungen.

Update Web server certificate

The integrated web server can be configured to follow up company SSL / TLS certificates. For the required pem-file, refer to the local IT department. This function will be used to encrypt the communication between the web interface of the RCCMD installation and the web browser.

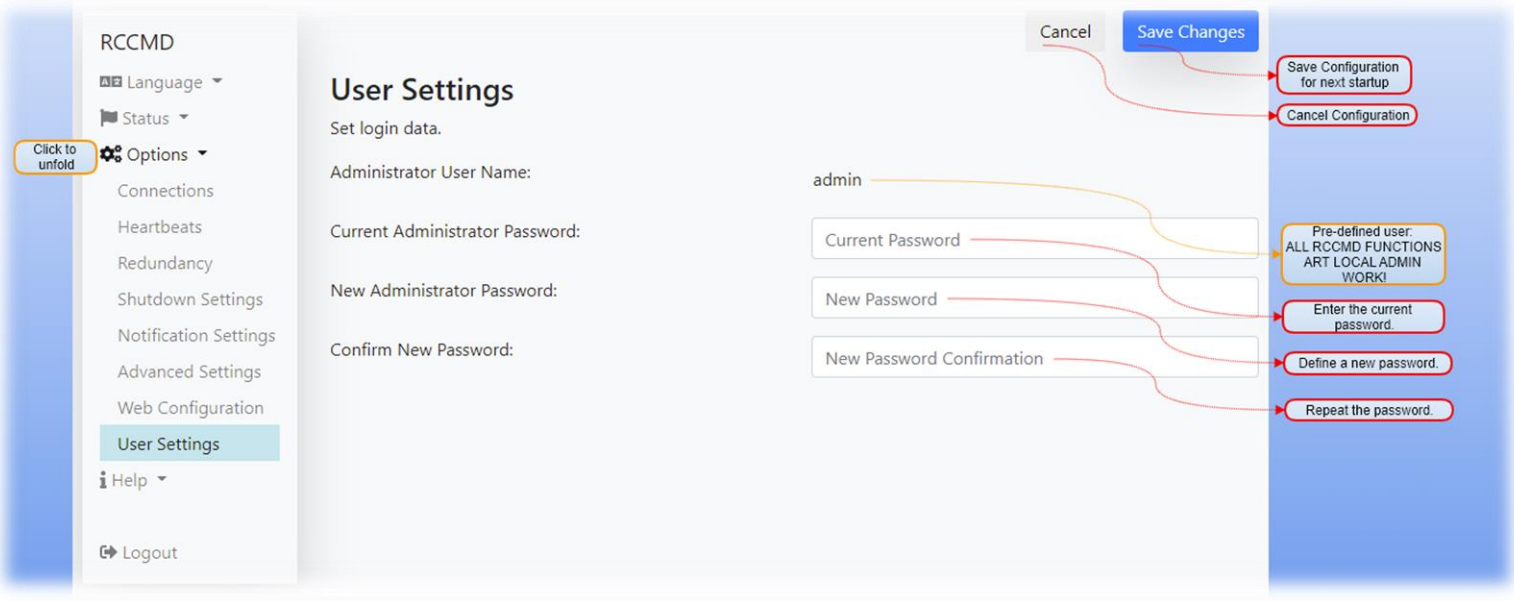


TLS certificate update function:

1. Create a backup file before using this function
2. Place the *.pem file in the according upload box
3. Click upload
4. Restart RCCMD at System status.

The Web browser should now show your own certificate. If your web browser can not access the web interface, re-install RCCMD and check the certificate.

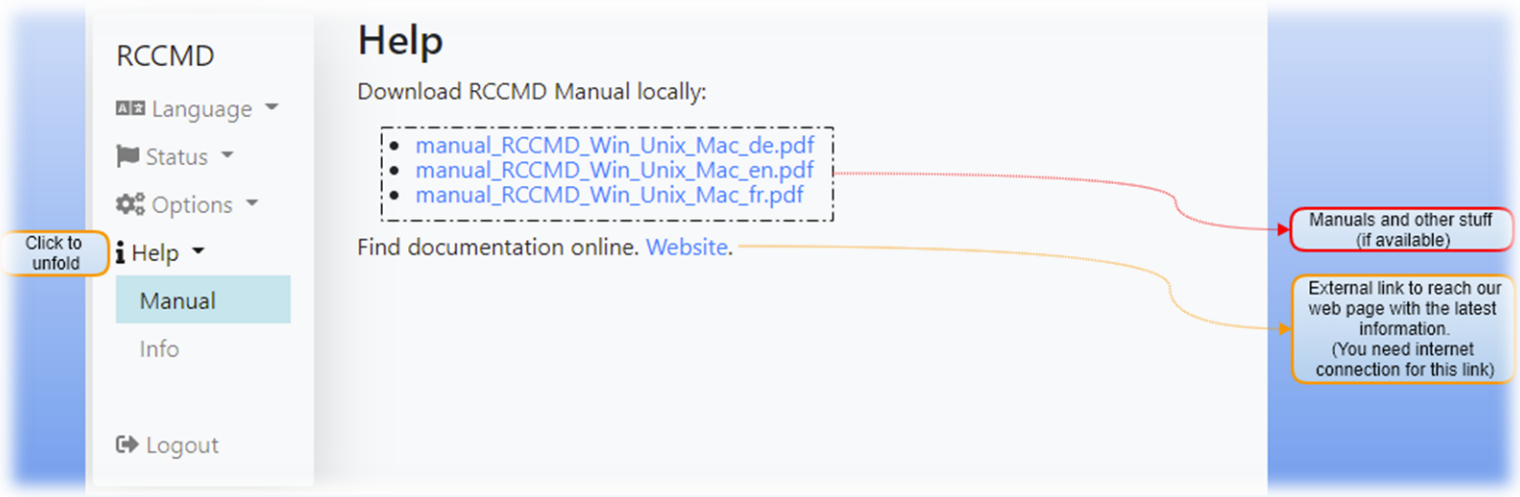
Benutzereinstellungen:



Anders als der CS141 hat RCCMD hier lediglich einen vorgegebenen Benutzer über den der RCCMD Client konfiguriert werden kann.

Um das Passwort zu ändern, benötigen Sie folgende Informationen:

Aktuelles Administratorpasswort:	*Dies ist das Passwort, mit dem Sie sich derzeitig angemeldet haben*
Neues Adminsitratorpasswort	*Ändern Sie das Passwort*
Neues Passwort bestätigen	*Aus Sicherheitsgründen müssen Sie das neue Passwort ein weiteres Mal eingeben, um Flüchtigkeitsfehler oder Zahlen/Buchstabendreher zu vermeiden*



Die Hilfesektion bietet Ihnen zwei Unterpunkte, die Ihnen weiterführende Informationen liefert:

1. Dokumentation und Bedienungsanleitung

   Anleitung

   Die zu dem Zeitpunkt als Ihre RCCMD – Version veröffentlicht wurde aktuelle Bedienungsanleitung ist lokal bei Ihrem RCCMD -Client hinterlegt. Das erlaubt einen direkten Zugriff auf die Bedienungsanleitung, sollte sich Ihre Installation in einem speziell geschützten Bereich befinden, bei der keine Internetverbindung vorhanden ist.

   Dokumentation Online

   Hinter diesem Weblink verbirgt sich das Downloadportal von Generex, dem Hersteller dieser Software. Hier finden Sie online die aktuellste verfügbare Systemdokumentation sowie zahlreiche weiterführende Informationen.

2. Info-Kasten

   Jede RCCMD-Lizenz ist mit einer zweijährigen Updateberechtigung versehen. Die Lizenzen verlieren danach nicht ihre allgemeine Gültigkeit, sie werden bei einer neueren Softwareversion von RCCMD lediglich feststellen, dass der Lizenzkey nicht mehr eintragbar ist.

   Sie können über die Info-Box leicht herausfinden, ob Ihre Lizenz noch Updateberechtigt ist:

   Dabei schlüsseln sich die Zahlen wie folgt auf:

1.18	Die Programmversion
.12	Die OEM-Version mit der Sie diese RCCMD-Lizenz erworben haben
190214	Rückwärts betrachtet das Build-Datum: 14.02.2019

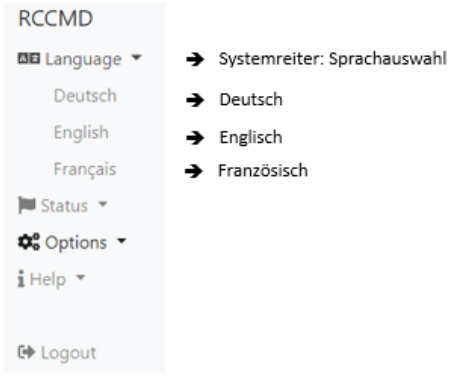
   Die gemäß diesem Screenshot vorliegende Version hat demnach folgende Daten:

   Es ist die Programmversion 4.18 von der OEM 12 – GENEREX mit dem Build-Datum 14.02.2019, updateberechtigt bis 14.02.2021

Die RCCMD –Appliance –
Alle Optionen der Weboberfläche im Detail erklärt

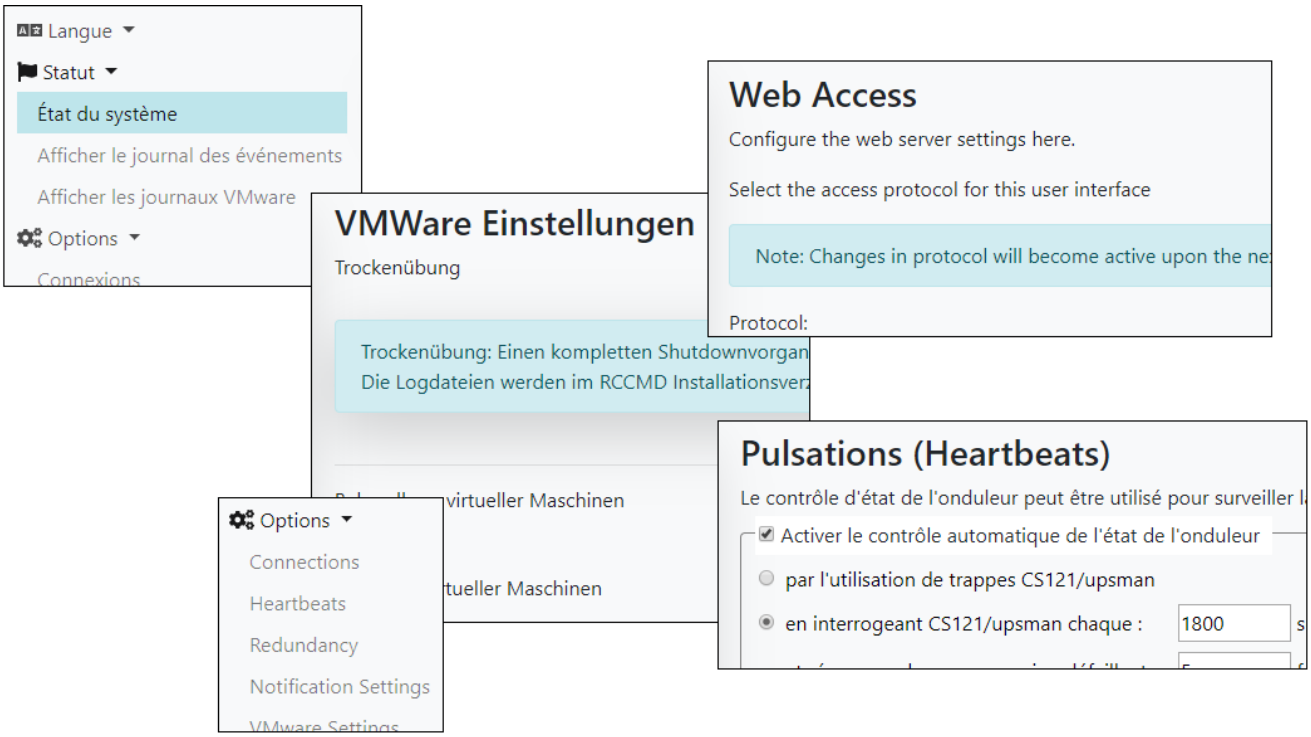
Auswahl der Systemsprache

Für diese Funktion öffnen Sie den Systemreiter Sprache



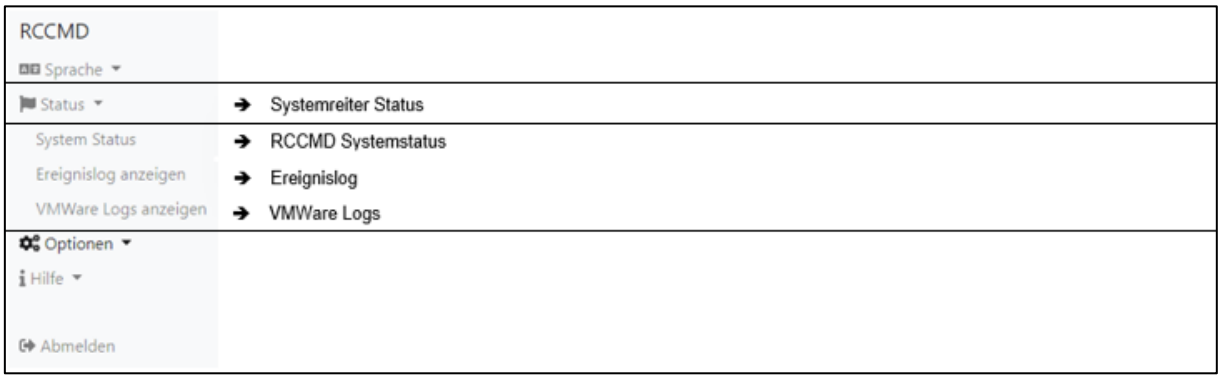
Die Grundeinstellung nach Installation ist generell Englisch.

RCCMD unterstützt die Sprachen Deutsch, Englisch und Französisch. Zum Umschalten auf das entsprechende Sprachpacket wählen Sie die entsprechende Sprache aus:

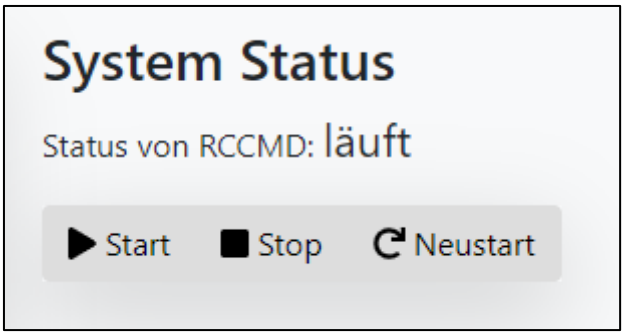


Menü-Abschnitt: Status

In diesem System-Menü finden Sie allgemeine Informationen über den Zustand von RCCMD, umgesetzte und fehlgeschlagene Kommunikationsversuche sowie Logdateien mit eindeutigem Zeitstempel



Der Systemstatus



Der Systemstatus ist ein kleines Aktionsmenü, welches Ihnen sofortigen Aufschluss über den aktuellen Betriebszustand von RCCMD liefert:

Generell hat der RCCMD Service – nicht zu verwechseln mit dem Web Frontend – nur zwei Systemzustände:

läuft -> Die aktuelle Konfiguration ist gültig und wird auf Anweisung ausgeführt werden

Angehalten -> Der RCCMD Service ist angehalten, beim nächsten Start wird die Konfiguration neu eingelesen und aktiviert.

Die Besonderheit dieser Funktion liegt im Detail

Alle aktuellen Konfigurationen werden temporär zwischengespeichert, RCCMD wird mit der zuletzt gestarteten Konfiguration im Hintergrund weiterarbeiten.

Um die neue Konfiguration gültig zu machen, müssen Sie aktiv eingreifen und den RCCMD Service stoppen und neu anstoßen.

Ereignislog anzeigen

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 protokolliert alle Ereignisse, die den RCCMD-Dienst betreffen mit:

- Benachrichtigungen
- Systemereignisse
- Aktionen
- Ausgeführte Skripte

Dabei werden folgende Informationen mitgeliefert:

- Datum des Ereignisses
- Uhrzeit, wann das Ereignis eingegangen ist
- IP-Adresse, von wem das Signal eingegangen ist, das ein Ereignis auslöst
- Erfolg/Misserfolg des ausgeführten Jobs zu diesem Ereignis.

Über diesen Ereignisbericht lassen sich komplexe Ereignisketten in Einzelschritte aufgeschlüsselt zurückverfolgen und in verbindung mit den Ereignislogs des dazugehörigen CS141 exakt auswerten.

So können Sie genau nachverfolgen:

- Wann ein Server heruntergefahren wurde
- Warum ein Server heruntergefahren wurde
- Wie schnell ein System auf einen Störfall reagiert hat.

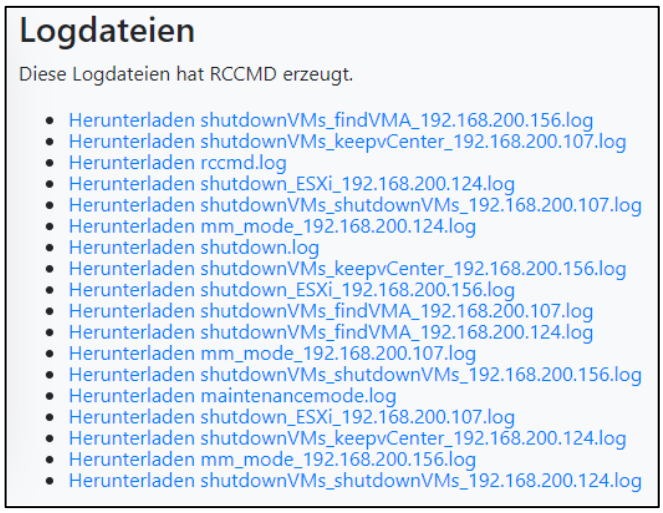
Ereignisberichte helfen, komplizierte Problemlagen aufzuschlüsseln und geben Hinweise auf zukünftige Probleme.

Ereignisproktokolle herunterladen

In größeren Unternehmen sind regelmäßige Statusberichte zur IT-Sicherheit notwendig. RCCMD erlaubt daher das Herunterladen und den Export der Logdateien in eine CSV-Datei, welche Sie beliebig in externe Überwachungssysteme und Datenbanken einbinden können.

Unter dem letzten Log-Eintrag ist dieser Link abgelegt:

VMware Logs



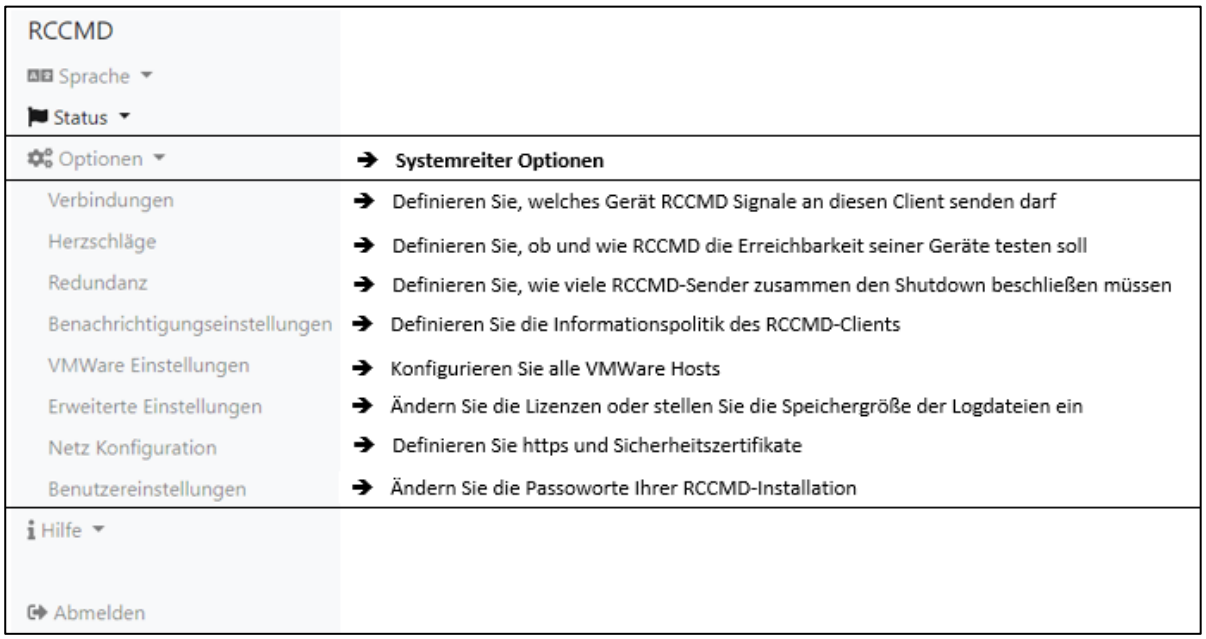
Die RCCMD Appliance bietet umfangreiche Logdateien, um Sie bei der Aufarbeitung eines Störfalls zu unterstützen. Dabei protokolliert RCCMD folgende Informationen:

- **Datum**
- **Uhrzeit**
- **Eingegangene Signale**
- **Eigene Kommunikationsversuche**
- **Ausgeführtte Skripte**
- **Dry-Run Ergebnisse**

Je nach Detailtiefe der Auswertungen können Sie über diese Logfiles den Weg eines Shutdowns selbst über komplexe Netzwerkknoten hinweg zurückverfolgen und mit anderen Logfiles abgleichen

Menü-Abschnitt: Optionen

Unter Optionen werden alle Einstellungen vorgenommen, welche von RCCMD benötigt werden, um Ihr Netzwerk erfolgreich zu betreuen:



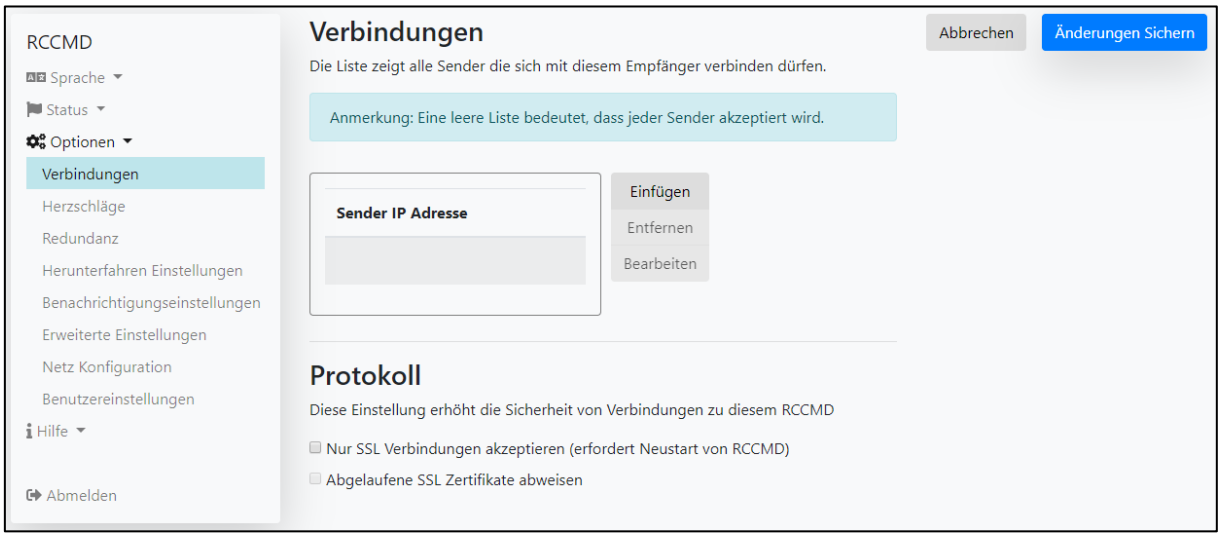
Verbindungen

Die Verbindungen definieren zwei unterschiedliche Konfigurationen:

Definieren Sie die erlaubten eingehenden Verbindungen

Wenn Sie dieses Feld leer lassen, dürfen alle eingehenden RCCMD Shutdown Signale einen Shutdown auslösen. Überraschenderweise ist das ein ungünstiger Zustand. Mit der Eingabe einer Sender-IP grenzen Sie ein, welche Geräte grundsätzlich berechtigt sind, *diesem* RCCMD Client ein Kommando zu schicken.

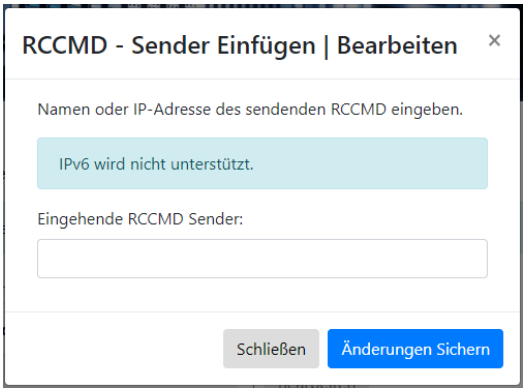
RCCMD Kommandos von nicht ausdrücklich berechtigten Geräten werden protokolliert, der RCCMD Client verweigert jedoch die Ausführung.



RCCMD bietet Ihnen folgende Konfigurationsmöglichkeiten:

Einfügen und Bearbeiten

Fügen Sie eine neue IP-Adresse hinzu.
Mit *Änderungen Sichern* wird zu der Adresse zulässiger IP-Adressen hinzugefügt. *Schließen* bricht den Vorgang ab und beendet den Konfigurationsdialog.



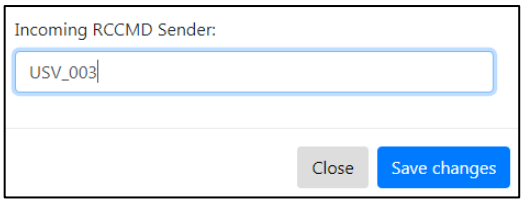
Wiederholen Sie den Vorgang so lange, bis alle RCCMD-Berechtigten Sender aufgenommen wurden.

Sollten sich die Einstellungen im Lauf der Zeit ändern, können diese über die Editierfunktion an den laufenden Betrieb angepasst werden:

Wählen Sie eine IP-Adresse aus und betätigen Sie Edit. Die ausgewählte IP-Adresse wird Ihnen im Konfigurationsdialog angeboten und kann von Ihnen gemäß Ihren Vorstellungen geändert werden. Mit Save Changes schließen Sie den Vorgang ab.
Close bricht den Vorgang ab und beendet den Konfigurationsdialog

Gültig ist hierbei sowohl die IP-Adresse des Senders als auch ein gültiger Hostname:

Wenn Sie ausschließlich mit Hostnamen arbeiten, benötigen Sie zusätzlich einen DNS-Server, welcher die aktuellen IP-Adressen und die den IP-Adressen zugehörigen Hostnamen kennt und diese auch publizieren kann.



Als Sender konfigurieren Sie den entsprechenden Server innerhalb der Eventkonfiguration des CS141:

Im kritischen Ressourcenmanagement empfiehlt es sich, möglichst viele eventuelle Störquellen zu beseitigen. Wenn Sie z.B. einen Server brauchen, welcher die Hostnamen in IP-Adressen auflösen kann, wird die Kommunikation nicht mehr funktionieren, sobald der Server nicht verfügbar ist.

Deshalb gilt die generelle Empfehlung, in bestimmten Bereichen manuelle IP-Adressen zu verwenden, da im Notfall alle Geräte autark starten und miteinander direkt kommunizieren können.

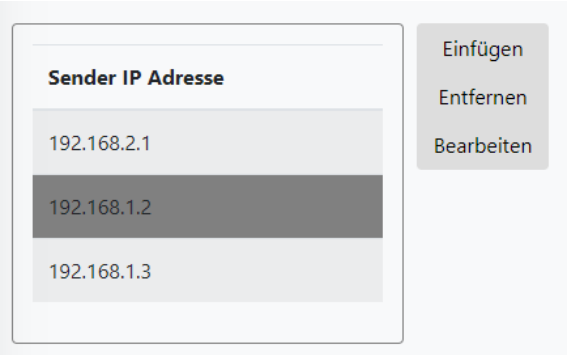
Tipp

Sollten Sie den CS141 konfigurieren und sehen wollen, ob die von Ihnen konfigurierten Jobs richtig bei RCCMD eingehen, können Sie über Connections indirekt eine Eingangsprotokollierung realisieren. Solange der Sender nicht explizit unter Connections eingetragen ist, wird RCCMD die Ausführung protokollieren, jedoch die Ausführung verweigern.

Es muss jedoch mindestens eine IP-Adresse eingetragen werden, um diese Filterfunktion zu aktivieren.

Löschen von Einträgen

Wählen Sie eine bestehende IP-Adresse aus.
Mit *Entfernen* können Sie diese IP-Adresse aus der aktuellen Liste entfernen.



Redundanzverhalten vorbereiten

Einige Einstellungen bauen aufeinander auf. Wenn Sie mehrere USV-Anlagen im Betrieb haben, welche zusammen eine Umgebung absichern, kann es notwendig sein, nicht nur die Geräte anzugeben, die grundsätzlich berechtigt wären, einen Shutdown auszulösen:

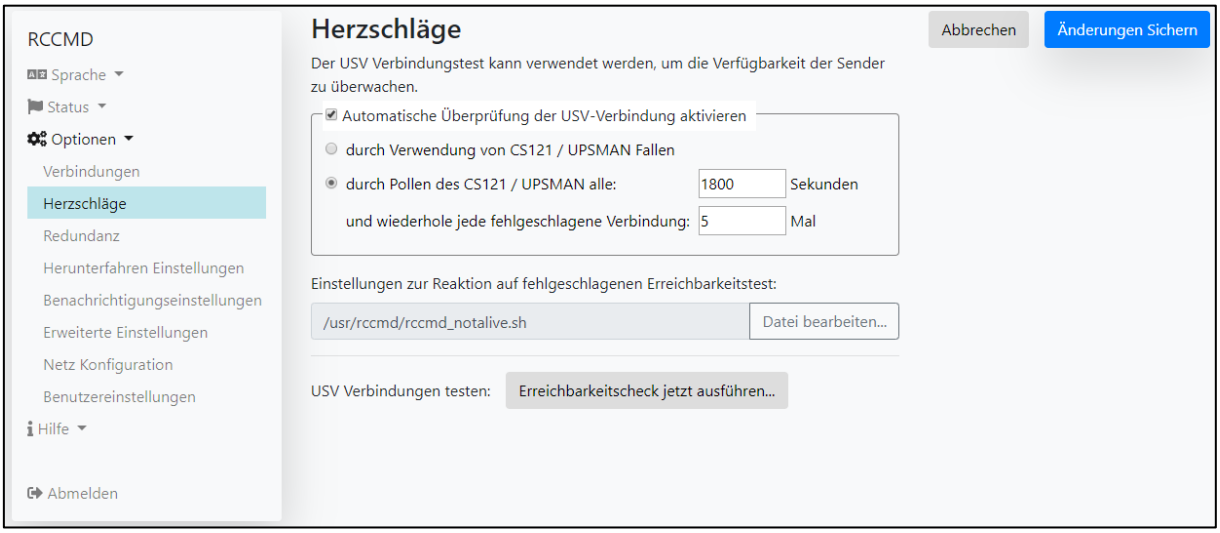
Wenn Sie zwei oder mehr IP-Adressen eingeben, wird automatisch das Menü „Redundanz“ freigeschaltet und kann verwendet werden. In dem Menü können Sie genauer definieren:

- Welche Sender zusammen einen Shutdown auslösen
- Welche Sender einzeln einen Shutdown auslösen

RCCMD wird an dieser Stelle dann differenzierter das Shutdownverhalten betrachten. Näheres erfahren Sie im Menüpunkt „Redundanz“.

Herzschläge

Die Heartbeats bieten ein Sicherheitsnetz, mit dem die Kommunikation zwischen RCCMD Client und dem zugehörigen Server überwacht und protokolliert werden kann:



Dabei werden im Prinzip zwei grundlegende Störquellen überprüft:

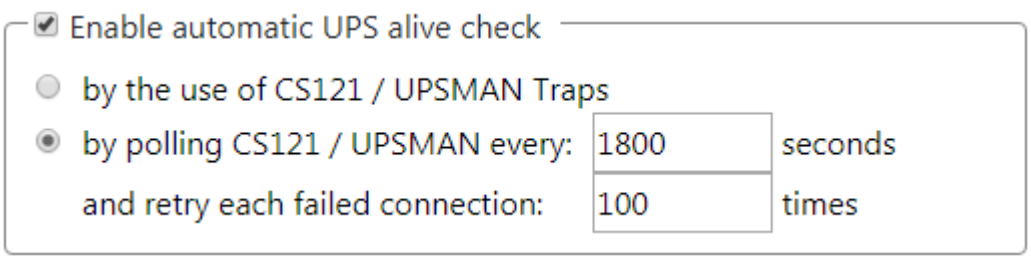
1. Das Netzwerk und die allgemeine Erreichbarkeit
2. Der UPSMan-Service auf dem CS141bzw. dem gültigen Sender

Die Heartbeats Funktion ist kein Netzwerkdiagnosetool zum Aufspüren von Störungen.

RCCMD kann mit diesem Test lediglich herausfinden, ob der Sender grundsätzlich erreichbar ist und wenn, ob er auch ordnungsgemäß funktioniert.

Dazu bietet der RCCMD Client zwei grundlegende Möglichkeiten an:

1 Automatisch



Sie können zwischen zwei unterschiedlichen Optionen auswählen:

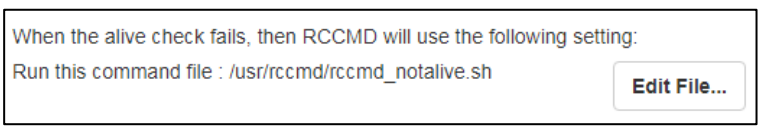
UPSMAN Traps

In dem Fall sendet ein RCCMD Server unaufgefordert eine Trap-Nachricht an den RCCMD-Client. Der Empfang dieser Nachricht wird entsprechend protokolliert.

By Polling

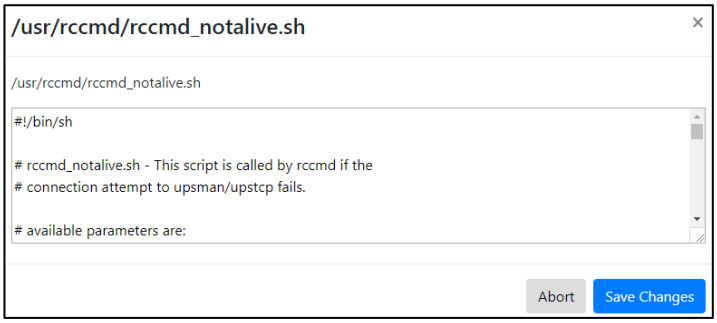
Der RCCMD Client fordert zyklisch vom RCCMD Server eine Nachricht an und protokolliert die Erreichbarkeit der Gegenstelle. Wenn diese Verbindung nicht möglich ist, kann der Vorgang frei definierbar oft wiederholt werden.

Sollte das automatische Polling nicht erfolgreich sein, kann ein automatisches gestartet werden.



Skript

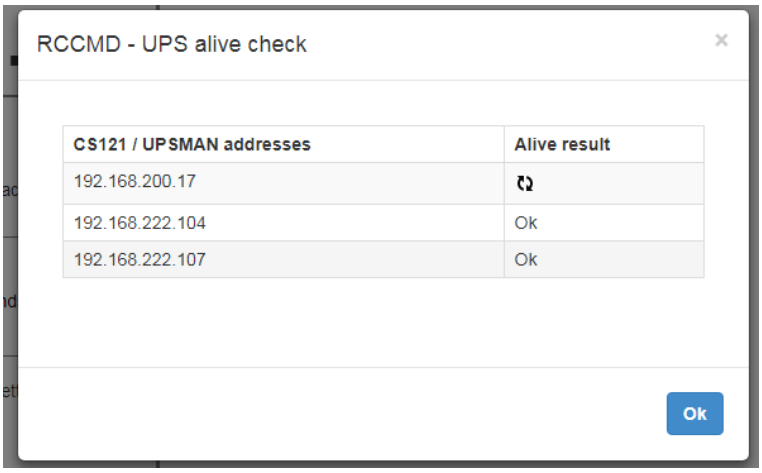
Dieses Skript ist frei konfigurierbar und kann individuell an Ihre Anforderungen angepasst werden. Sie können mit Edit File… die Datei im Webbrowser direkt editieren und anpassen. Bei diesem Skript handelt es sich um eine klassische Batchdatei, welche Sie Ihren Vorstellungen anpassen können.



Manuell

Mit Test UPS connections stellt Ihnen RCCMD ein Werkzeug bereit, welches eine schnelle Erreichbarkeitsdiagnose ermöglicht.

Run alive check now… öffnet ein zusätzliches Fenster, bei dem alle unter Connections eingetragenen RCCMD – Geräte abgefragt werden. Fehlende Kommunikationsbereitschaft und Nichterreichbarkeit wird entsprechend angezeigt:



Folgende Symbole werden verwendet:

🗘 … die Verbindung wird gerade geprüft

Ok … die Verbindung hat funktioniert, das Gerät ist erreichbar

Not Ok … die Verbindung ist gestört, das Gerät ist nicht erreichbar

Anders als im automatischen Modus wird in diesem Zusammenhang kein Skript automatisch gestartet- Das Ergebnis dient zur Information und Fehlerbeseitigung.

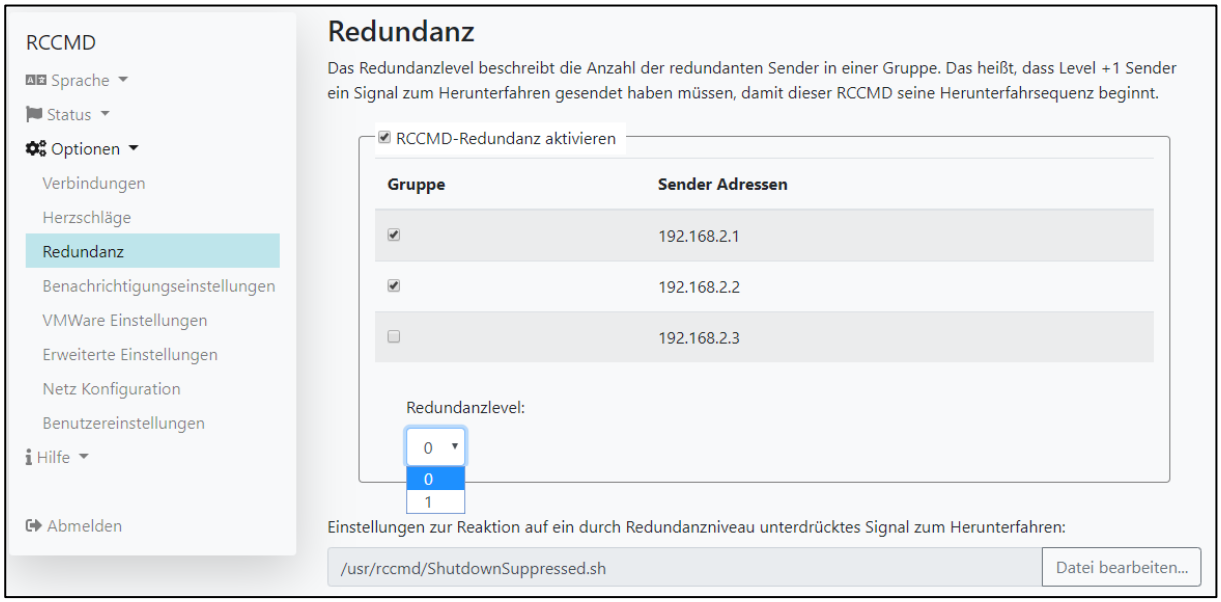
Unter folgenden Bedingungen kann ein Alive Check fehlschlagen:

- Netzwerkstörung oder defekte Infrastruktur
- Zielgerät ist ausgeschaltet
- Gesperrte oder falsch konfigurierte Ports
- Fehlerhaftes Routing
- UPSMan Service antwortet nicht

Anders als bei der automatischen Überprüfung mittel *by polling* wird in diesem Fall kein automatisches Skript bei einem Fehlschlag ausgeführt, da RCCMD davon ausgeht, dass Sie als berechtigter Administrator diesen manuellen Vorgang direkt überwachen.

Bitte beachten Sie, dass die Konfiguration erst wirksam wird, nachdem Sie auf das grüne Save Changes gedrückt haben, da für diese Funktion der RCCMD Client neu starten muss.

Redundanz



Das Redundanzverhalten greift die Einstellungen unter Verbindungen und Herzschläge wieder auf:

Damit das Redundanzverhalten ordnungsgemäß funktioniert, müssen zwei Vorbedingungen erfüllt sein:

1. Es müssen zwei gültige IP-Adressen unter Verbindungen angegeben werden.

Es müssen mindestens zwei IP-Adressen hinterlegt sein, welche RCCMD Kommandos senden dürfen - RCCMD soll schließlich erst einen Shutdown ausführen, wenn zwei Sender gleichzeitig dies angewiesen haben.

2. Die Herzschläge stehen auf „Automatic UPS alive check by polling“

RCCMD wird über die Herzschläge angewiesen, automatisch die Verfügbarkeit eingetragener IP-Adressen zu prüfen:

Sollte die eine USV nicht mehr erreichbar sein und das Redundanzsystem einen Shutdown senden, wird RCCMD davon ausgehen, dass ein schwerwiegendes Problem vorliegt und das System herunterfahren.

Tipp:

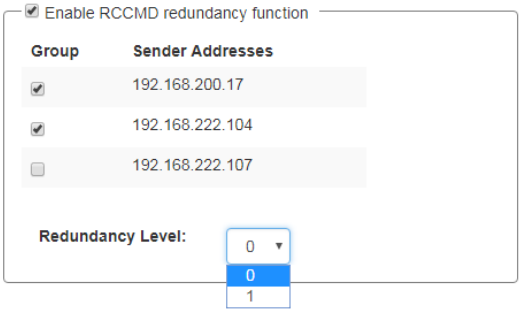
Bedenken Sie, dass die Intervalle zwischen den Prüfungen ausschlaggebend für ein Herunterfahren sind.

Das Redundanzverhalten bezieht sich ausschließlich auf das RCCMD Kommando Shutdown.

Alle anderen Kommandos werden individuell behandelt und im Log entsprechend vermerkt. Mit der Möglichkeit, eigene Skripte auszuführen, bietet RCCMD Ihnen die Möglichkeit, die Standardprozedur im Notfall zu überbrücken.

Redundanzverhalten definieren

Aktivieren Sie zunächst die
RCCMD redundancy function. Im Anschluss wählen Sie die IP-Adressen aus, welche ein Shutdown senden dürfen. Der Redundancy Level bezieht sich hier auf einen Wert, der in Abhängigkeit der vorhandenen Anlagen funktioniert:



Anzahl ausgewählter Anlagen X -1

Wenn Sie zwei Anlagen ausgewählt haben, bedeutet das, dass eine Anlage einen Shutdown anweist. Da nur zwei Anlagen ausgewählt wurden Es kann nur noch maximal eine weitere Anlage diesen Befehl senden.

Bei 3 ausgewählten anlagen ist damit der maximale Wert 2:

Wenn 1 Anlage + 2 weitere Anlagen den Shutdown anweisen, wird es ausgeführt. Welche der drei Anlagen in dem Fall den ersten Shutdown sendet, ist in diesem Zusammenhang nicht entscheidend.
Alternativ können Sie hier auch den Wert auf 1 ändern: In der Konsequenz würden zwei von drei Anlagen zusammen einen Shutdown beschließen dürfen, wobei sich die Kombination dynamisch ändern kann.

Tipp

Bedenken Sie bitte, dass eine Shutdown-Anweisung so lange aktiv bleibt, bis die Anlage, die den Shutdown angewiesen hat, diesen auch explizit zurücknimmt. Dieses wird über den RCCMD Custom Command *wakeup* gesteuert.

Shutdownverhalten bei zwei USV-Anlagen

Das Redundanzverhalten sieht vor, dass im Fall eines Shutdownsignals unmittelbar die Konnektivität und die Verfügbarkeit der zweiten USV-Anlage überprüft wird. Wenn diese direkt antwortet, wird der Shutdown unter Vorbehalt bis auf weiteres unterdrückt:

Sobald die zweite Anlage ebenfalls einen Shutdown anweist, wird dieses Kommando ausgeführt und das System heruntergefahren.

Wird hingegen von der ersten Anlage ein Shutdownsignal gesendet und die zweite Anlage ist nicht erreichbar, fährt RCCMD das System herunter – Grund ist, dass RCCMD in diesem Fall davon ausgeht, dass die zweite Anlage nicht verfügbar ist.

Shutdownverhalten bei drei gültigen Sendern

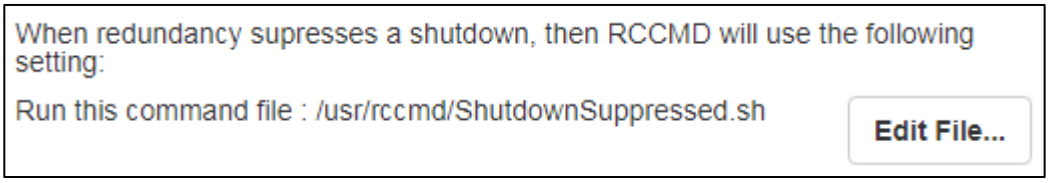
Ab drei Anlagen oder Sendern lässt sich das Verhalten über den Redundancy Level individuell an die notwendigen Bedingungen anpassen:

1. Wenn eine von drei Anlagen einen Shutdown sendet
2. Wenn zwei von drei Anlagen einen Shutdown senden
3. Alle drei Anlagen müssen gemeinsam den Shutdown beschließen.

Dabei kann jede Anlage individuell seinen Shutdown anweisen und über das RCCMD Custom command *wakeup* wieder zurücknehmen. RCCMD wird den Shutdown generell erst dann ausführen, wenn die exakte Shutdownbedingung erfüllt ist.

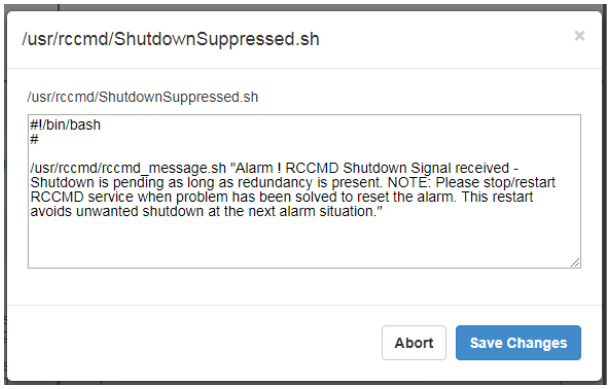
Redundanzbezogenes Skripting

Wenn Sie Redundanzverhalten nutzen, wartet der RCCMD Client mit der Ausführung des Shutdowns bis die entsprechende Anzahl von Anlagen den Shutdown ebenfalls anweisen.

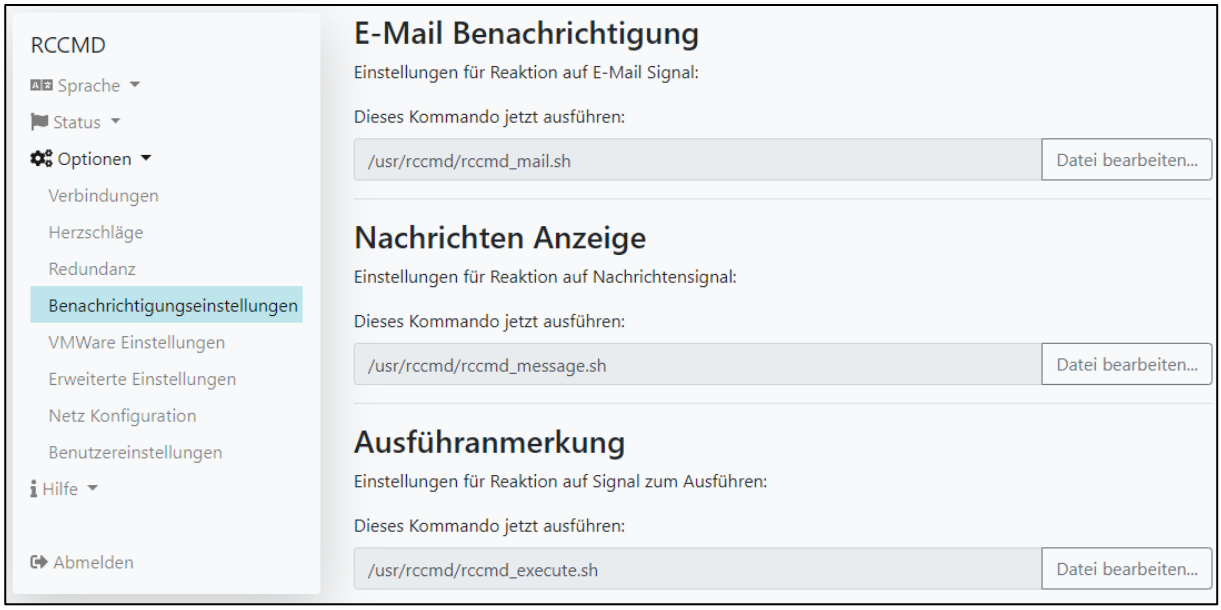


Da dieser Vorgang sich direkt auf den Betrieb der zu überwachenden Server auswirkt, wird ein automatisches Skript gestartet, dass auf diesen Vorfall hinweist.
Mit *Edit File…* können Sie dieses Skript ihren individuellen Anforderungen anpassen.

Per Default ist ein Hinweistext definiert, welcher Sie auf ein redundanzbasiertes Shutdownverhalten hinweist.



Benachrichtigungseinstellungen



Je nachdem, welches Kommande von einem RCCMD Sender eingeht, werden drei grundlegende Skripte automatisch ausgeführt, welche dann alle weiteren Funktionen von RCCMD starten oder steuern:

Die RCCMD -Routinen sind vorkonfiguriert und werden im Normalfall nicht angefasst werden müssen.

Sollten Sie jedoch eigene Skripte noch zusätzlich ausführen wollen, die RCCMD ausführen soll, können Sie diese Skripte entweder direkt in die entsprechende sh-Datei schreiben oder aber innerhalb der sh-Datei neue Skripte und komplett eigene Routinen starten lassen.

Warnung:

Wenn Sie diese Skripte ändern, anpassen oder erweitern, ändern Sie das gesamte Verhalten von RCCMD innerhalb Ihres Systems. Fertigen Sie unbedingt vor dem Editieren eine Sicherheitskopie an, um auf den Originalzustand zurück zu kommen. Änderungen an der Originalkonfiguration können zu einem unverhersehbaren Verhalten von RCCMD führen.

Wann werden die Skripte ausgeführt

RCCMD unteschеidet zwischen drei unterschiedlichen Nachrichtensignalen:

Email-Signale

Wenn der CS141 wird im Normalfall auf seinen eigenen Mail-Client zurückgreifen – Dies ist auch der empfohlene Weg. In einigen Hochsicherheitsnetzen kann es jedoch nicht gewünscht sein, dass der Webmanager eigene Mails versenden kann. Der RCCMD Client kann hier als Schnittstelle verwendet werden, um kurze Mailbotschaften weiterzuleiten.

Sie können auch RCCMD über beliebige Skripte triggern.

Basis für diese Funktion ist das freeware Linux-Tool send mail, über das RCCMD eMails versenden kann. Sie können das Tool jederzeit konfigurieren, indem Sie sich über eine Konsole auf der Linuxoberfläche des RCCMD Clients einloggen.

Um eine Email von einem CS141 weiterleiten zu lassen, verwenden Sie die Custom Commands und geben unter Eingabe der Ip-Adresse folgenden Befehl ein:

Mail zieladresse@zielserver.de <Textkörper>

Sie würden also beim CS141 eingeben:

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

Der RCCMD wird in diesem Fall eine Email auf den Weg bringen, in dessen Betreff „Jean-Luc Picard was here“.

Muss dieses Skript eine Mail auslösen?

Nein, dieses Skript mail.sh wird lediglich bei diesem Befehl direkt getriggert. Selbstverständlich können Sie auch die Inhalte nach Ihren Vorstellungen anpassen, entfernen und sogar das ganze nach Ihren Wünschen neu aufbauen.

➔ Wenn Sie dis tun, wird jedoch die ursprüngliche Funktion nicht mehr gewährleistet sein, Sie editieren dieses Skript auf eigenes Risiko!

Nachrichtenanzeige

RCCMD kann im Prinzip auf jeder kompatiblen Hardware- und Softwareplatform installiert werden. Dabei ergeben sich in manchen Fällen gewisse Skriptdiskrepanzen:

Dieses Skript steuert den Eingang von Nachrichten und ist dafür zuständig, dass diese auf dem Monitor angezeigt werden. Da die RCCMD Appliance ein Serverprogramm ohne grafische Oberfläche ist, das ohne eine dauerhafte Monitorüberwachung betrieben wird, sollten Sie dieses Skript einfach belassen, wie es ist:

Da es bei jedem Benachrichtigungsereignis zunächst getriggert wird, würde auch der Inhalt jedes Mal ausgeführt werden und Sie sollten bestenfalls Routineskripte, die immer automatisch durchlaufen sollen, hinzufügen.

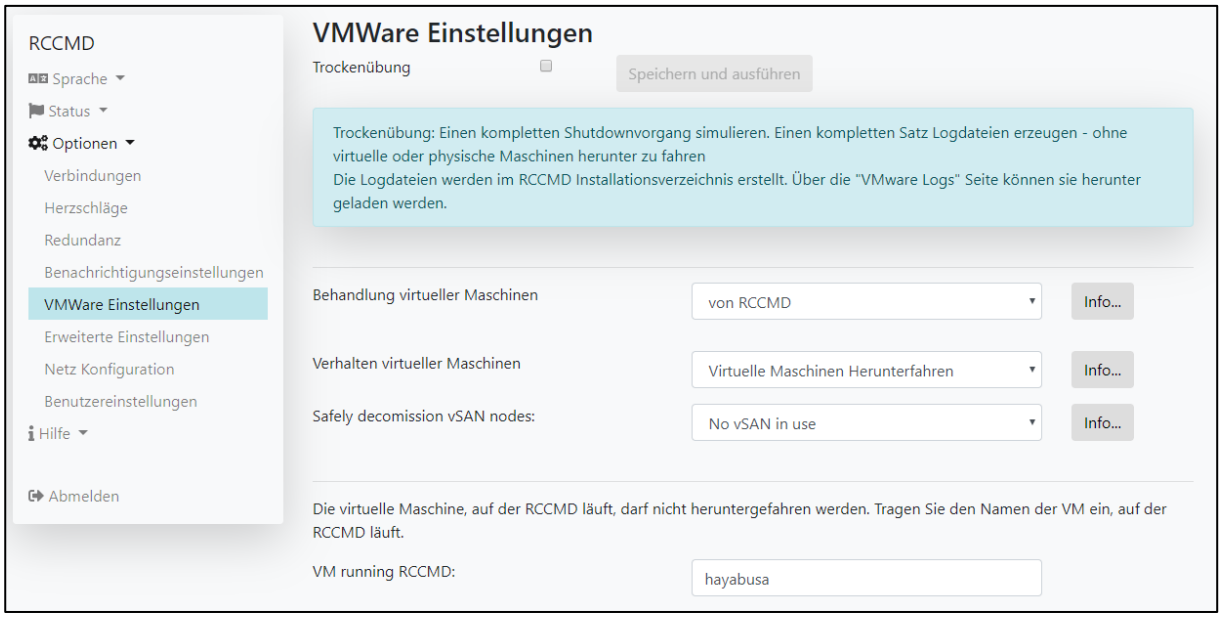
Ausführanmerkung

Jetzt wird es interessant:
Dieses Skript führt die vom CS141 eingehenden Steuerbefehle aus. Sobald Sie einen Shutdown gesendet haben, wird dieses Skript gestartet und beginnt mit der strukturierten Shutdownroutine.

Dieses Skript kann zudem mit Ihren Ideen zusätzlich erweitert werden, so dass Sie umfangreiche Möglichkeiten in der Hand haben, den Shutdown speziell auf Ihr Netzwerk zuzuschneiden.

➔ Dieses Skript ist gefährlich, da Änderungen direkt in die Basisfunktionen des RCCMD-Clients eingreifen. Von Ihnen getätigte Änderungen und Erweiterungen werden sich direkt auf das Shutdownverhalten auswirken. Solide Fachkenntnisse im Scripting unter Linux sind für Änderungen an dieser Voraussetzung.

VMWare – Einstellungen



Die VMware – Einstellungen regeln das gesamte Shutdownverhalten der Server und Hosts innerhalb der VMware. Je nach Ausbaustufe und Konfigurationsart sind unterschiedliche Anhaben über das Zielsystem notwendig. Zu diesen Angaben gehören neben den Basisdaten wie IP-Adressen, Zugangsdaten mit den notwendigen Berechtigungen unter anderem auch spezielleres Wissen über das Shutdownverhalten Ihrer IT-Landschaft wie benötigte Zeitfenster. Ein weiterer Punkt ist, dass diese Daten sich im Lauf der Zeit ändern können und durch regelmäßige Kontrollen ggfs. an die geänderten Anforderungen angepasst werden müssen.

➔ RCCMD wird bewertet Shutdownzeiten nach der eingegebenen Datenlage

Teil 1: Die Grundeinstellungen

Die Grundeinstellungen gehen davon aus, dass Sie **Hosts ohne vCenter betreiben**. Sie können mit einer RCCMD-Installation beliebig viele Hosts direkt herunterfahren. Folgende Informationen sind notwendig:

Behandlung virtueller Maschinen

Dieser Punkt definiert, ob Sie die Hosts und virtuellen Maschinen von RCCMD oder von einem vCenter betreuen lassen möchten. Wenn Sie die Hosts im Lock-Down Modus betreiben, werden z.B. die Steuerbefehle exklusiv von einem vCenter zugelassen. Selbst wenn Sie die Zugangsdaten richtig eingeben, wir der Host die Ausführung verweigern. In der Grundeinstellung ist „von RCCMD“ voreingestellt.

Verhalten virtueller Maschinen

Definieren Sie mit dieser Einstellung, ob Sie vMotion verwenden wollen oder die Maschinen heruntergefahren werden sollen. Wenn Sie die virtuellen Maschinen herunterfahren lassen, wird dies unmittelbar über den Host gesteuert: Die virtuellen Maschinen werden regulär heruntergefahren und im Anschluss der Host ausgeschaltet. Wenn Sie vMotion aktivieren, ist das lokale Herunterfahren von virtuellen Maschinen das Sekundärprotokoll – In der Grundeinstellung ist „Virtuelle Maschinen herunterfahren“ voreingestellt.

Folgende Einstellungen sind hier möglich:

Virtuelle Maschinen herunterfahren

Die virtuellen Maschinen werden heruntergefahren und entsprechend ausgeschaltet. Dabei wird das Server-Journal geschrieben, um ein sauberes Hochfahren nach dem Shutdown zu gewährleisten. Dabei werden alle Programme beendet, bevor das Betriebssystem ausgeschaltet wird.

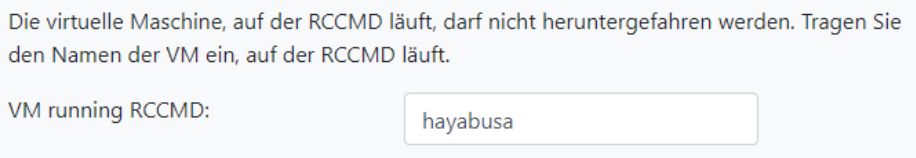
Virtuelle Maschinen in Standby versetzen

Bei dieser Technik wird ein Speicherabbild auf der virtuellen Festplatte der VM abgelegt und das Betriebssystem auf diese Weise in den Tiefschlafmodus versetzt. Dabei werden im Idealfall die Programme nicht geschlossen und können nach dem Start der virtuellen Maschine weiterlaufen. Da der Host bei dieser Methode kein Server-Journal schreibt, besteht die Gefahr, dass nicht gesicherte Daten in dem Fall verloren gehen können, wenn z.B. ein Programm den Tiefschlafmodus nicht unterstützt und

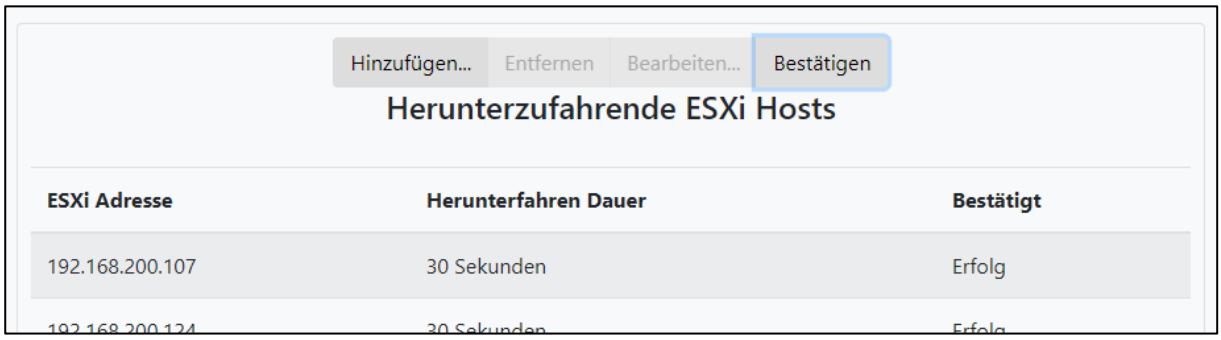
Für die Verwendung des Maintenance Mode sind zusätzliche Angaben notwendig, Zugangsdaten für das vCenter sowie das Zeitfenster, dass zur Verfügung stehen soll, innerhalb dem das vCenter die einzelnen virtuellen Maschinen migriert.

Safely decomission vSAN nodes auf no vSAN in use

Diese Einstellung definiert das Shutdownverhalten im Falle eines vSAN’s – Dabei hat das vCenter drei unterschiedliche Grundeinstellungen bereit, welche Sie hier auswählen können. Wenn Sie ein vSAN betreiben, beachten Sie bitte die Grundvoraussetzungen, die für den Betrieb von RCCMD in Verbindung mit einem vSANs vorliegen müssen. In der Grundeinstellung ist ***„No vSAN in use“*** eingestellt.



Herunterzufahrende ESXi Hosts



In diesem Menü definieren Sie die ESXi-Hosts, die Sie herunterfahren möchten. Dabei können Sie über die Menüleiste folgende Funktionen ausführen:

- Hinzufügen: Fügen Sie einen weiteren Host hinzu. Um einen Host zu entfernen
- Entfernen: Wählen Sie einen Host aus und klicken Sie auf Entfernen, um ihn aus der aktuellen Liste zu entfernen
- Bearbeiten: Wählen Sie einen Host aus. Mit Bearbeiten können Sie die Zugangsdaten Editieren
- Bestätigen: Wenn Sie diesen Button drücken, wird die aktuelle Konfiguration gespeichert und die Zugangsdaten validiert. Unter *Bestätigt* sehen Sie dann, ob der Host erfolgreich angesprochen werden konnte.

Tipp: Die virtuellen Maschinen gehen aus, aber der Host schaltet nicht ab

In diesem Fall hat der Nutzer, den Sie für den Shutdown eingetragen haben, keine Root-Rechte und damit wird der Befehl zwar angenommen, aber der Host fährt selber fährt nicht runter und schaltet aus. Der verwendete Shutdown-Nutzer muss auf jeden Fall Root-Rechte besitzen

Teil 2: Die erweiterten Einstellungen

Verhalten virtueller Maschinen steht auf Maintenance Mode (vMotion)

RCCMD blendet Ihnen zwei neue Menüabschnitte ein:

- Maintenance Mode Timout in Sekunden

Dieser Wert definiert das Zeitfenster, dass vCenter zur Verfügung gestellt bekommt, eine Maschine auf einen anderen Host zu migrieren. Maschinen, die innerhalb dieses Zeitfensters nicht migriert wurden und noch auf dem Host zurückbleiben, werden im Folgeschritt von dem Host heruntergefahren und entsprechend ausgeschaltet.

- vCenter Login Daten

Für diese Funktion benötigt RCCMD zusätzlich gültige Zugangsdaten zum vCenter, welches die Migration durchführen soll.

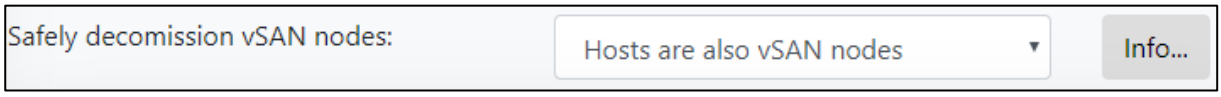
Beachten Sie, dass ein RCMD-Client zwar viele Hosts herunterfahren jedoch immer nur ein vCenter zurzeit betreuen kann.

Wenn Sie mehrere Unterschiedliche Konfigurationsartein konfigurieren müssen, kann es daher notwendig werdne, 2 RCCMD Appliances zuammen zu verwenden.

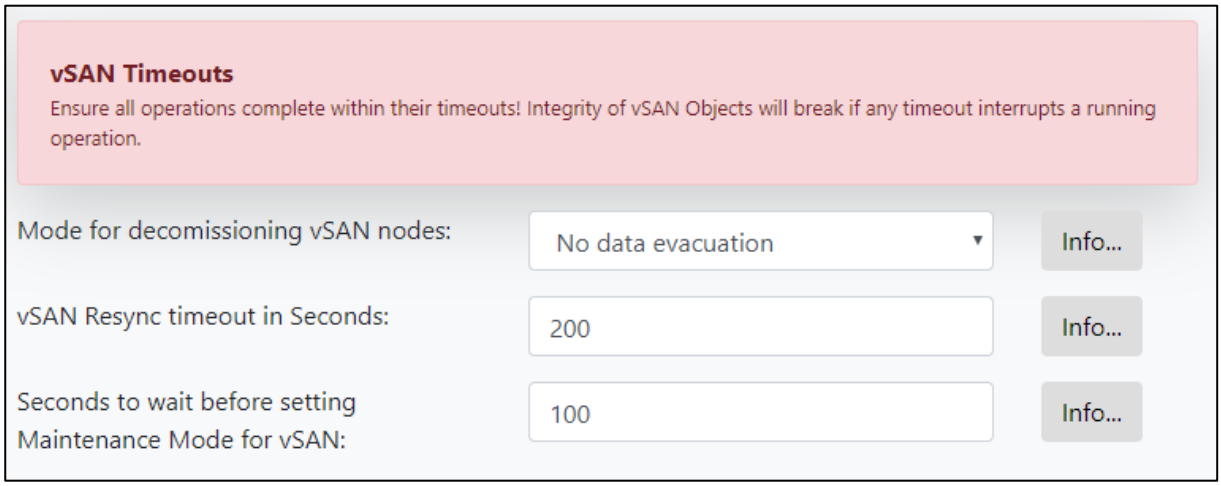
Werte testen

Überprüfen Sie die Zugangsdaten Ihres vCenters. Sollten die Zugangsdaten falsch sein, können Sie die Daten Anpassen.

Teil 3.: Safely decomission vSAN nodes steht auf vSAN in Use



Dieses Menü blendet weitere Submenüs sowie *eine Warnung* ein:



Diese Warnung sollten Sie ernst nehmen:

Ein vSAN reagiert unberechenbar, wenn laufende Prozesse einer Shutdownroutine falsch beendet wurden. Dies kann im schlimmsten Fall zu einer Beschädigung der Daten oder sogar zu einem totalen Datenverlust führen.

Shutdownmöglichkeiten

No data evacuation

Dies ist der schnellsten Weg, um den Systemshutdown zu gewährleisten. Dabei werden die virtuellen Maschinen heruntergefahren und anschließend synchronisiert das vCenter alle Hosts, die sich innerhalb des vSAN's befinden. Dabei werden keine Daten migriert und zu anderen Hosts verschoben.

Evacuate all data to other hosts

Im Prinzip ist es die selbe Funktion, die auch das vMotion auslöst. Ein vSAN kann auch über unterschiedliche Standorte aufgespannt werden, so dass Sie virtuelle Maschinen auch auf externe Hosts auslagern können, die nicht in dem vSAN Cluster liegen, welches Sie gerade herunterfahren möchten.

Ensure data accessibility

Bei dieser Funktion werden Daten verschoben, sofern das vSAN-Cluster selber nicht genug Redundanzmöglichkeiten aufweisen kann.

Tipp

RCCMD stellt eine Shutdownlösung vor, bei der Sie Ihr komplettes vSAN im Notfall schnellstmöglich strukturiert herunterfahren können – virtuelle Maschinen, die im Vorfeld bereits an einen anderen Ort migriert wurden, sind hiervon nicht betroffen. Da Sie das vSAN anhalten und herunterfahren wollen, ist No data evacuation naheliegend, da ansonsten die virtuellen Maschinen verschoben und nicht heruntergefahren werden.

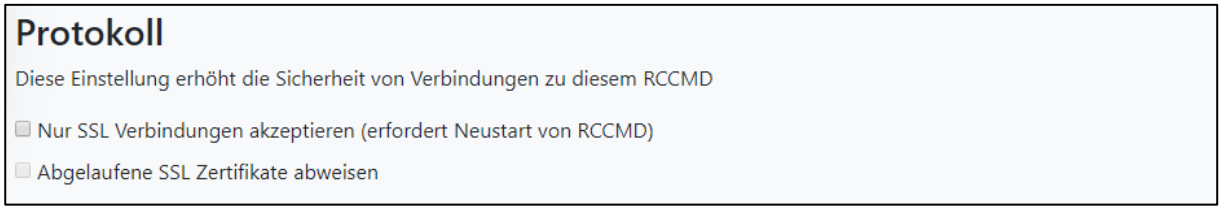
vSAN Resync timeout in Seconds

Bei dieser Einstellung handelt es sich um das grundlegende Zeitfenster, das ein vCenter zur Verfügung hat, die Datenbestände zwischen den Hosts zu synchronisieren, bevor der nächste Punkt in der Shutdownsequenz gestartet wird. Dieses Zeitfenster ist sehr schwierig zu definieren, da der Resync ein sehr relativer Wert ist – im Prinzip kann man sagen, es dauert so lange, wie es eben dauert...

Seconds to wait before setting Maintenance Mode for vSAN

Sobald der Resync abgeschlossen wurde, ist in der Regel das vCenter als letzte noch existierende virtuelle Maschine einen Shutdown. Mit dieser Einstellung definieren Sie, wie lange das vCenter Zeit hat, sich selber herunterzufahren, bevor der nächste Programmpunkt in der Shutdownsequenz gestartet wird.

Verbindungssicherheit erhöhen



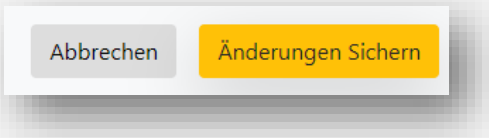
Diese Funktion erhöht die Sicherheit in Ihrem Netzwerk, bedeutet im Umkehrschluss jedoch auch einen erhöhten Administrationsaufwand:

Sie können den RCCMD anweisen, ausdrücklich SSL-Verschlüsselte Kommunikation mit einem gültigen Zertifikat zu akzeptieren. Hat ein Sender kein SSL-Zertifikat, um sich auszuweisen, wird die Verbindung abgebrochen.

Zusätzlich zu dieser Funktion können Sie RCCMD anweisen, SSL- Zertifikate auf Ihre Aktualität zu überprüfen. Ist das Zertifikat verglichen mit der aktuellen Serverzeit abgelaufen, wird es als ungültig eingestuft und die Verbindung entsprechend abgebrochen.

Tipp

Sicherlich ist Ihnen schon aufgefallen, wie oft wir darauf hinweisen, dass die Speichern-Funktion die Farbe verändert. Wenn Sie Daten innerhalb einer Maske Eingeben oder ändern, werden die Daten nur temporär vorgehalten, ohne dass es eine Auswirkung auf die Konfiguration hat.Das hat einen Grund:



RCCMD läuft im Hintergrund persistent und schreibt sofern möglich nur auf ausdrückliche Anweisung die Konfigurationsdatei neu. Als Hinweis ändert das Änderungen Sichern seine Farbe: Wenn Sie vergessen, diesen Button vor dem Verlassen der Menüseite zu speichern, werden die Daten wieder verworfen.

VMware Dry Run

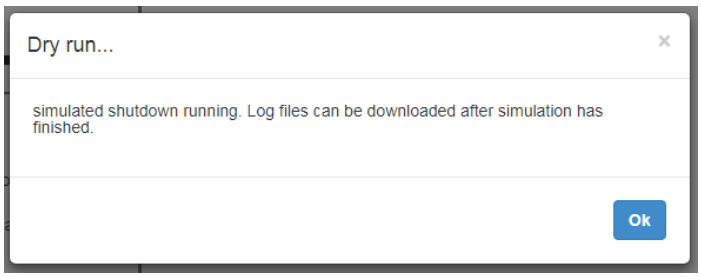
Mit dem Dry Run bietet RCCMD innerhalb der VMware-Settings eine ganz besondere Funktion an:

Der Dry Run ist ein Simulationsmodus, bei dem Ihre RCCMD-Installationen das Shutdownverhalten simuliert, jedoch nicht physikalisch ausführt.

Diese Funktion ist dann interessant, wenn Sie eine RCCMD -Installation auf einem Produktionsserver installieren:

Versehentliches Herunterfahren wird auf diese Weise unterbunden.

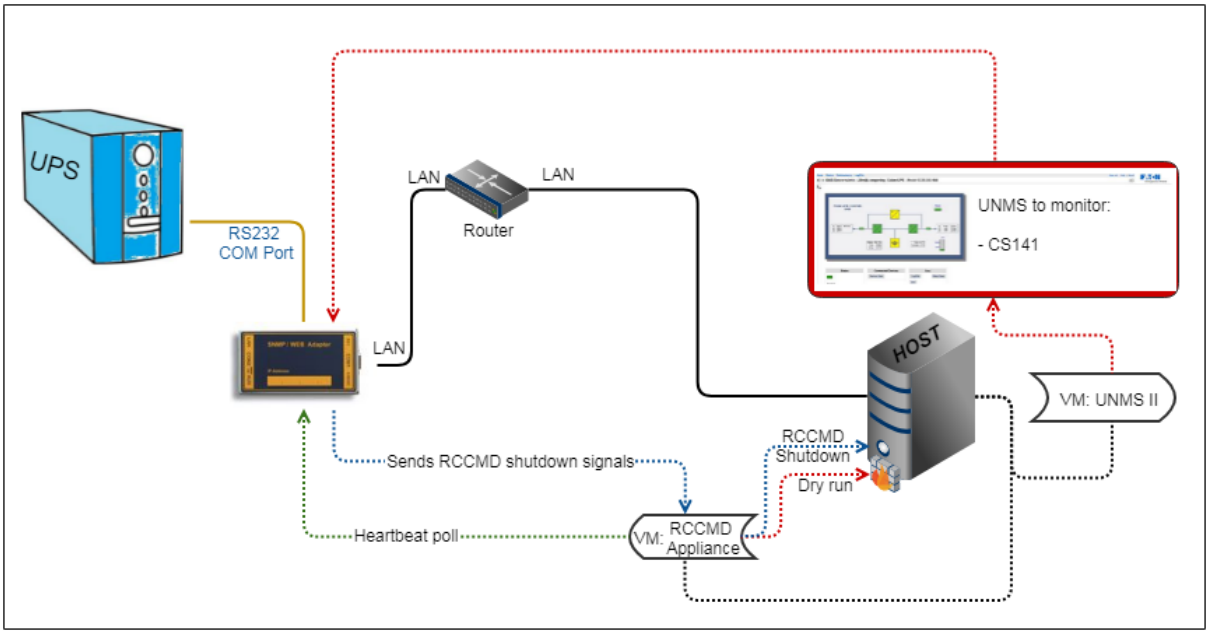
Mit Save and Execute wird diese Funktion aktiviert und schützt so Ihre weiteren Konfigurationsarbeiten vor einem versehentlichen Shutdown.



Tipp

Wichtig in diesem Zusammenhang ist, dass einige Konfigurationsmenüs bei der Testphase gesperrt sind und nicht „zwischendurch“ angepasst werden können.

Was passiert beim sog. „Dry run …“?



Im Normalfall werden von einem CS141 oder einem gültigen RCCMD Server Client gesendet – der RCCMD Software. Welcher Befehl letztendlich gesendet wird und was er auslöst, ist von dem Betriebsszenario abhängig. Da Sie über das Eventhandlig vom CS141 auch individuelle Befehle absetzen können, um sehr filigrane und komplexe Skripte zu starten, besteht die Möglichkeit, einen Server über Skripte weitgehend zu automatisieren: Sie müssen nicht zwangsläufig einen Server mit RCCMD herunterfahren.

Unter VMware ist das Verhalten des Clients im Normalbetrieb anders als bei einem Einzelserver:

Die RCCMD Appliance hat das Ziel, das innerhalb einer VMware – Umgebung strukturiert alle Hosts heruntergefahren werden sollen. Dabei geben Sie innerhalb von RCCMD die Zugangsdaten der Hosts an, die Sie speziell steuern möchten. Als Konsequenz wird RCCMD nun diese Hosts mit all seinen virtuellen Maschinen herunterfahren, und seine eigene virtuelle Maschine herunterfahren, nachdem alle Steuerbefehle abgesetzt wurden.

Wenn Sie den „Dry run“ aktivieren, wird RCCMD in einen selbstlaufenden Simulationsmodus versetzt:

2. Alle eingetragenen Hosts werden kontaktiert
3. Alle Zugangsdaten werden überprüft
4. Es wird eine Protokolldatei geschrieben, in der Erfolg und Misserfolg festgehalten werden
5. Der Standard RCCMD Shutdown wird unterdrückt

In dem Moment, wo der Dry Run aktiv ist, können Sie über den CS141 zwar die RCCMD Installation erreichen, jedoch keine Hosts herunterfahren

Tipp:

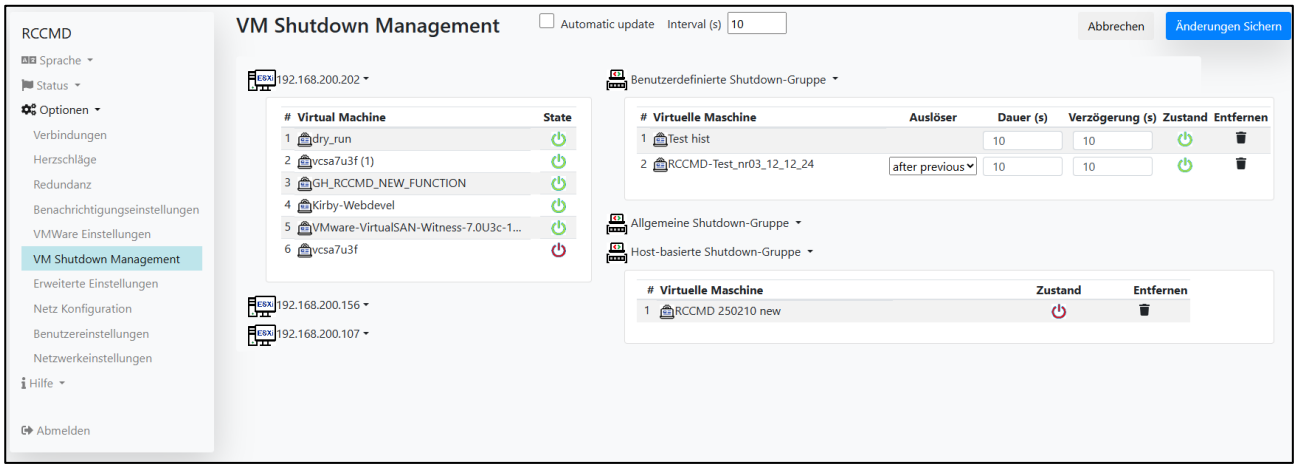
Sollten Sie diese Skripte ändern, anpassen oder entsprechend neue Unterskripte hinzufügen, werden diese in der Konsequenz ausgeführt. Der Dry Run kennt nur seine eigenen Standardskripte – er überprüft nicht die Änderungen, die Sie manuell hinzugefügt haben.

Das hat Vor- und Nachteile

1. Ihre „scharfen“ Skripte werden gnadenlos ausgeführt, der Dry Run sollte vorher stattfinden!

2. Sie können mit dem Hinzufügen von eigenen Skripten, welche harmlose Aktionen auslösen, überprüfen, ob Ihre „scharfen“ Skripte funktionieren würden, also alle administrativen Freigaben auf dem Zielsystem erfüllt sind.

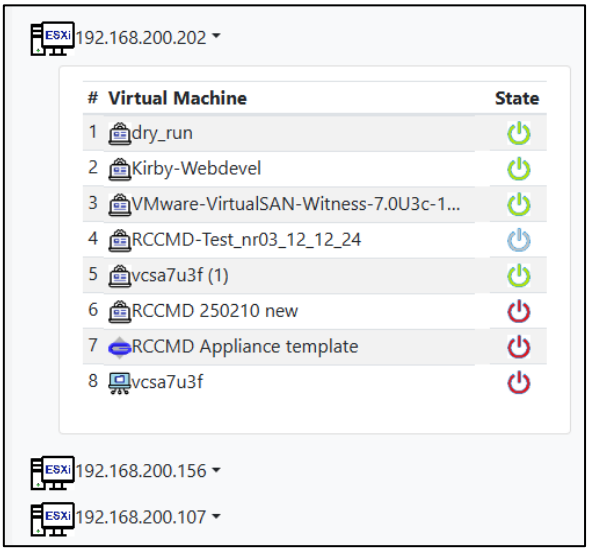
VMware Shutdown Management



Das VMware Shutdown Management bietet die Möglichkeit, virtuelle Maschinen in einem direkten Bezug zueinander herunterzufahren. Entscheidend hierfür ist, dass die jeweiligen Hosts in den VMware-Einstellungen konfiguriert und verifiziert wurden.

Während die VMware-Einstellungen einen globalen Shutdown auslösen, bei der alle virtuellen Maschinen gleichzeitig herunterfahren, wird über das VMware Shutdown Management im Vorfeld eine gegenseitige Abhängigkeit zwischen einzelnen virtuellen Maschinen sowie eine klare Reihenfolge für den Shutdown definiert und der jeweilige Betriebszustand angezeigt:

	Die virtuelle Maschine ist derzeitig ausgeschaltet. Alle Daten sind gesichert.
	Die virtuelle Maschine pausiert gerade bzw. befindet sich im Tiefschlaf Modus.
	Die virtuelle Maschine läuft und ist bei einem Stromausfall betroffen.
	Die in einer statischen Gruppe abgelegte virtuelle Maschine wurde nicht gefunden. RCCMD wird gem. den Einstellungen zum nächsten Eintrag springen.
	Gastsystem: Eine virtuelle Maschine mit diesem Ikon ist eine VM mit einer beliebigen Funktion.
	vCenter: Eine virtuelle Maschine mit diesem Ikon ist das vCenter für den jeweiligen Cluster.
	Die RCCMD Appliance: Dies ist der Name der virtuellen Maschine, der für die Appliance vergeben wurde.

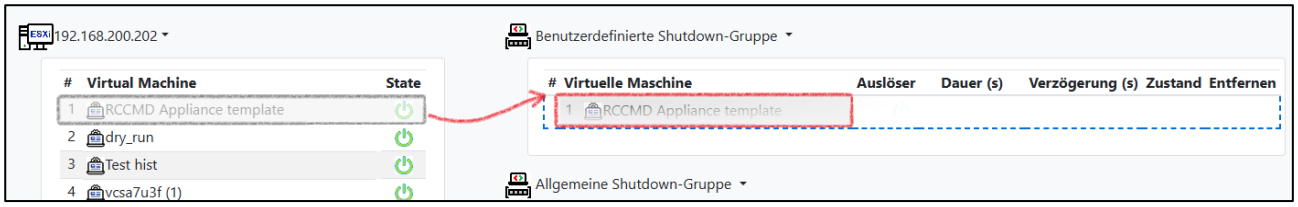


Alle derzeitig ausgerollten virtuellen Maschinen werden unter dem ESXi-Host inklusive des jeweiligen Betriebszustands abgebildet. Diese Liste wird bei einem Shutdown in Echtzeit aktualisiert, sollte also später eine virtuelle Maschine hinzugefügt werden

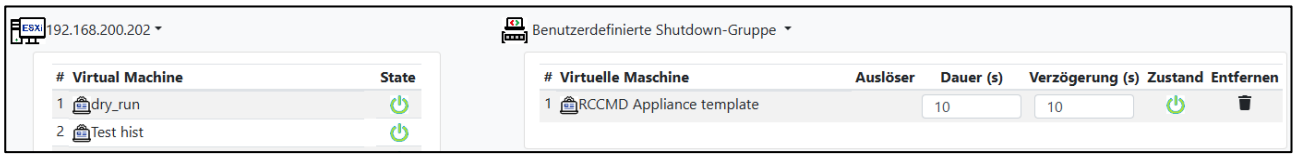
Hinzufügen und Entfernen von einzelnen virtuellen Maschinen

Hinzufügen:

Um eine virtuelle Maschine einer Shutdowngruppe hinzuzufügen, schieben Sie diese via Drag and Drop in die gewünschte Shutdowngruppe:



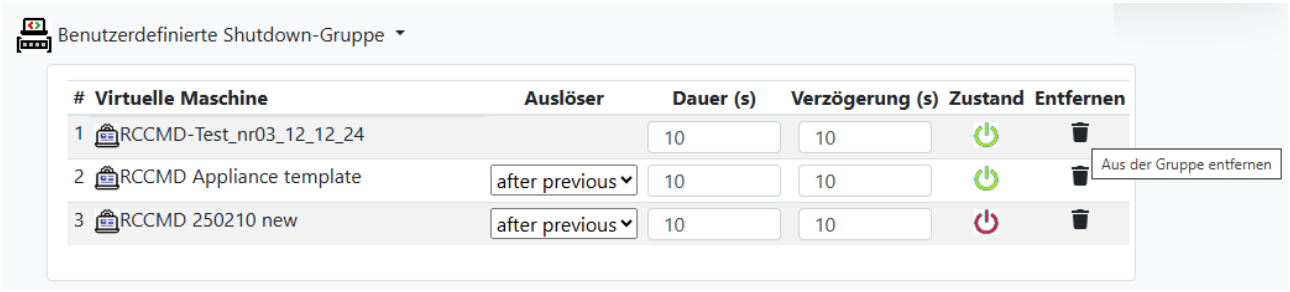
Die virtuelle Maschine wird künftig nicht mehr in RCCMD unter dem Host angezeigt, sondern wird entsprechend über die Gruppe heruntergefahren.



Bitte beachten Sie, dass diese Einstellung unabhängig von den Einstellungen des ESXi Hosts bzw. vCenters ist. RCCMD wird künftig auf alle unter *VMware Einstellungen* bekannt gegebenen bekannten Hosts nach dieser virtuellen Maschine suchen, um sie herunterzufahren.

Entfernen

Zum Entfernen einer virtuellen Maschine aus einer festen Shutdowngruppe schieben Sie die Datei einfach wieder zurück auf den jeweiligen Host.

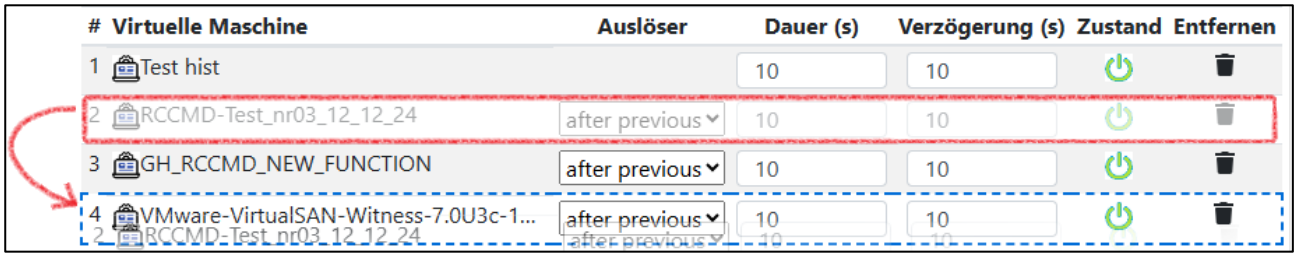


Sollten Sie sich nicht sicher sein, wo sich die virtuelle Maschine gerade befindet, drücken Sie auf den kleinen Papierkorb unter „Entfernen“. Der Eintrag wird daraufhin aus der Liste entfernt, und entsprechend dem ESXi Host, auf der sie gerade beheimatet ist, hinzugefügt.

Tipp: RCCMD löscht keine virtuellen Maschinen

Das Shutdown Management ermöglicht Ihnen, die virtuellen Maschinen automatisiert in Abhängigkeit zueinander herunterzufahren. RCCMD wird zu keinem Zeitpunkt eine virtuelle Maschine von Ihrem Server löschen.

Shutdownreihenfolge ändern und virtuelle Maschinen Verschieben



Sie können die virtuellen Maschinen innerhalb der Nutzerspezifischen Gruppen frei bewegen. Schieben Sie diese hierzu einfach an die Stelle, wo sie in der Shutdownlogik heruntergefahren werden soll.

- Innerhalb einer Shutdowngruppe
- Zwischen unterschiedlichen Shutdowngruppen

Shutdowngruppe 1 - Das Zeitmanagement der benutzerdefinierten Shutdown Gruppe

Der Auslöser in der benutzerdefinierten Shutdown-Gruppe bietet zusammen mit der Dauer (s) und der Verzögerung (s) zahlreiche Möglichkeiten, eine Shutdownsequenz zu optieren:

Die Timing Funktionen und der Auslöser bieten die Möglichkeit, einen individuellen Zeitrahmen innerhalb der Shutdownsequenz zu definieren - auf dieser zeitgesteuerten Basis werden dann alle virtuellen Maschinen geordnet heruntergefahren. Beachten Sie bei der Planung der Zeiten, dass die hier eingetragenen Werte keinen Einfluss die reale Shutdownzeit der virtuellen Maschine hat, sondern ausschließlich von RCCMD für das interne Shutdowntiming von RCCMD herangezogen wird.

Auslöser und Zeitmanagement der benutzerdefinierten Shutdown Gruppe

Die erste virtuelle Maschine bietet zwei verschiedene Zeitfenster an, welche sich auf das Shutdownmanagement auswirken:

Dauer (s)	Verzögerung (s)
90	10

Dauer definiert, wie lange eine virtuelle Maschine benötigt, um heruntergefahren zu werden. Verzögerung gibt an wie lange ein Shutdownsignal und der Start der Shutdowndauer restriktiv verzögert wird.

Ab der zweiten virtuellen Maschine in der Liste gibt es zusätzlich einen Auslöser, der definiert, wann die jeweiligen Zähler gestartet werden sollen. Mit dem Auslöser wird der Shutdown restriktiv an den Shutdown der vorigen virtuellen Maschine gebunden:

Auslöser	Dauer (s)	Verzögerung (s)
	90	10
after previous	130	20

„after previous“ definiert, dass die individuelle Verzögerung erst startet, wenn der Shutdown-Timer (Dauer (s)) der vorangegangenen virtuellen Maschine ausgelaufen ist. In diesem Beispiel wird also die zweite virtuelle Maschine mit einer Shutdownzeit von 130 Sekunden erst starten, wenn die 90 Sekunden abgelaufen sind +20 Sekunden Zeitverzögerung.

Auslöser	Dauer (s)	Verzögerung (s)
	90	10
with previous	130	20

„with previous“ definiert, dass die Verzögerung der nachfolgenden virtuellen Maschine zeitgleich mit dem Shutdown-Timer (Dauer (s)) der vorangegangenen Maschine startet: In diesem Beispiel wird die zweite virtuelle Maschine 20 Sekunden nach der ersten virtuellen Maschine ein Shutdown-Signal bekommen und RCCMD den dazugehörigen Shutdown-Timer (Dauer) starten.

Mit steigender Anzahl von virtuellen Maschinen ergibt sich folgende Shutdown-Logik:

Maschine 1 wird nach 10 Sekunden herunterfahren.
Maschine 2 wird 90+20 Sekunden warten, und dann herunterfahren.
Maschine 3 wird 10 Sekunden nach Maschine 2 den Shutdown einleiten.
Maschine 4 wird 10 Sekunden nach Maschine 3 den Shutdown einleiten.
Maschine 5 wird 80 +10 Sekunden nach Maschine 4 den Shutdown einleiten

#	Virtuelle Maschine	Auslöser	Dauer (s)	Verzögerung (s)
1	GH_RCCMD_NEW_FUNCTION		90	10
2	RCCMD-Test_nr03_12_12_24	after previous	130	20
3	vcsa7u3f	with previous	80	10
4	vcsa7u3f (1)	with previous	80	10
5	Test hist	after previous	90	10

Sollte eine virtuelle Maschine, die hier aufgeführt ist, nicht mehr existieren bzw. gefunden werden, wird RCCMD die eingetragenen Shutdownzeiten akribisch befolgen, und lediglich die nicht Auffindbarkeit der virtuellen Maschine anzeigen. Sollten virtuelle Maschinen also im Vorfeld auf andere Rechenzentren migrieren, hat dies keinen Einfluss auf die Shutdownprozedur.

Wenn Dauer (s) der letzten Maschine ausgelaufen ist, wird zur nächsten Shutdown-Gruppe übergegangen: Die allgemeine Shutdowngruppe.

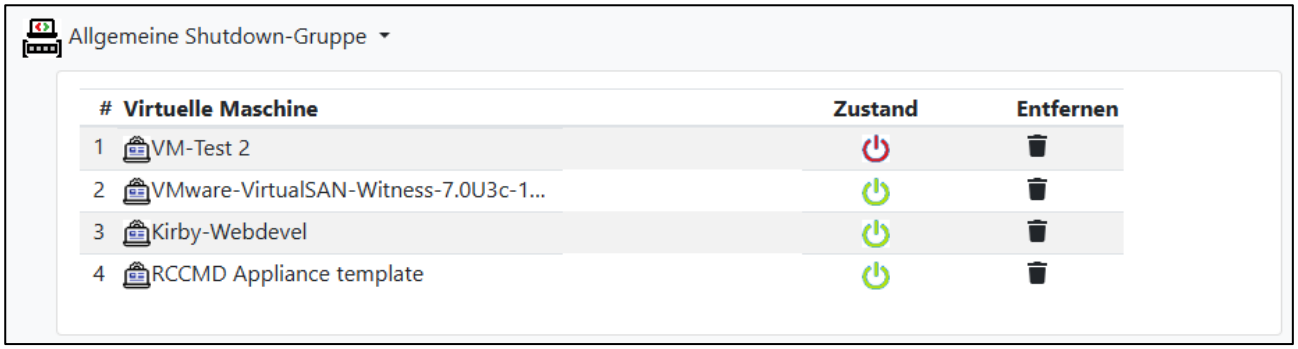
Shutdown-Gruppe 2: Die allgemeine Shutdown-Gruppe

Diese Gruppe ist für alle virtuellen Maschinen gedacht, welche ohne besondere Shutdown-Anforderungen heruntergefahren werden können. Dabei werden globale Richtlinien angewendet:

- Shutdown Duration (Dauer (s)): 90 Sekunden
- Delay (Verzögerung (s)): 0 Sekunden

Die Liste wird direkt von oben nach unten abgearbeitet, ermöglicht jedoch eine grobe Shutdown-Reihenfolge festzulegen: Virtuelle Maschinen, welche länger für einen Shutdown benötigen als die veranschlagten 90 Sekunden, sollten höher platziert werden als solche, die schneller herunterfahren.

In dieser Liste werden bekannte statische virtuelle Maschinen abgelegt, welche bei einem Stromausfall heruntergefahren werden sollen:



Nach dem die Shutdown Duration (Dauer (s)) abgelaufen ist, wird zur Shutdowngruppe 3: Die dynamische Shutdowngruppe

Shutdowngruppe 3: Die dynamische Gruppe

Die dynamische Shutdowngruppe ist eine vollautomatische Systemgruppe, welche alle virtuellen Maschinen erfasst, die nicht explizit einer anderen Gruppe zugewiesen wurden:

Wenn Sie das VM Shutdown Management aufrufen, werden alle bekannten ESXi – Hosts in Echtzeit abgefragt und die verfügbaren virtuellen Maschinen aufgelistet.

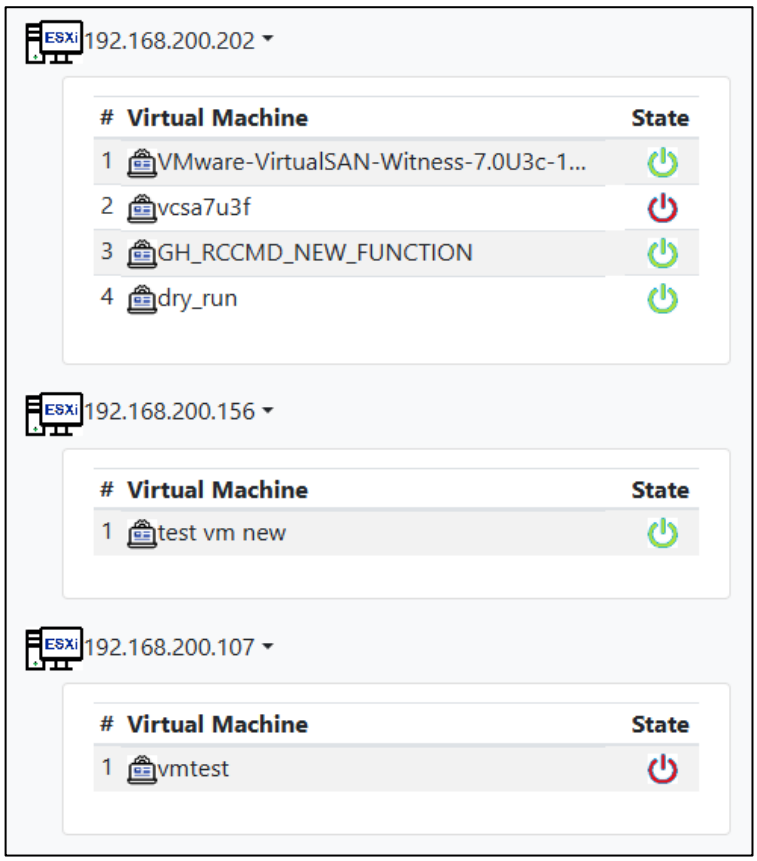
Die Besonderheit dieser Gruppe liegt im Detail:

Sollte eine virtuelle Maschine nach der Konfiguration auf einen der bekannte ESXi-Host migrieren oder erstellt werden, wird RCCMD diese bei einem scharfen Shutdownsignal in Echtzeit erfassen und automatisch dieser Gruppe zuweise.

Virtuellen Maschinen, welche im Vorfeld durch vMotion oder manuelle Eingriffe migriert sind, werden dynamisch aus dieser Liste entfernt.

Damit sind alle virtuellen Maschinen, die auf den Hosts laufen, geschützt und werden bei Bedarf heruntergefahren.

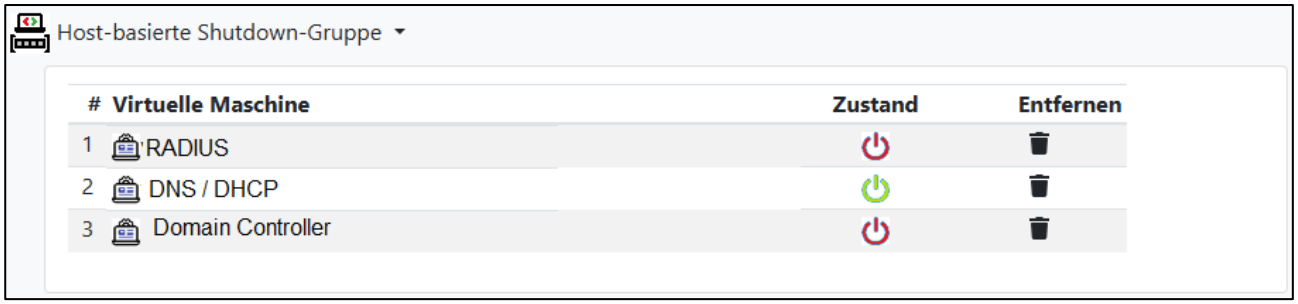
Nach Ablauf von 90 Sekunden wird zur Gruppe Shutdowngruppe 4 weitergeleitet:



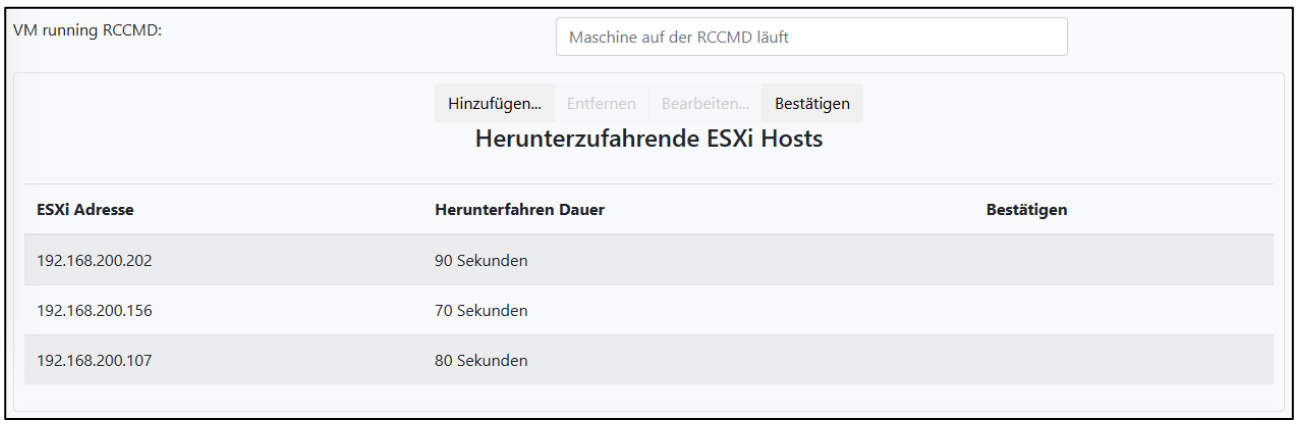
Shutdowngruppe 4: Die Host-basierte Shutdown Gruppe

Die Host-basierte Shutdowngruppe umfasst alle Infrastrukturnahen Server:

- DNS
- DHCP
- Gateway
- RADIUS
- VMware Appliance
- vCenter
- […]



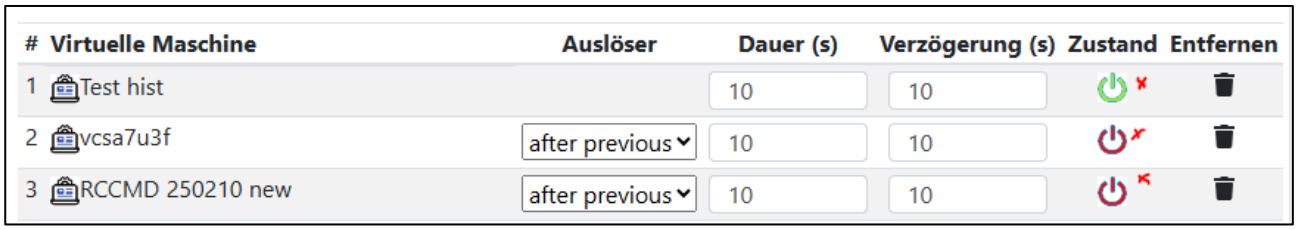
Server, die in dieser Gruppe abgelegt wurden, werden über die VMware Einstellungen heruntergefahren, und anschließend die den ESXi – Hosts.



Virtuelle Maschinen, welche an diesem Punkt noch nicht ausgeschaltet sind, werden kalt ausgeschaltet, wenn die Hosts heruntergefahren werden.

Echtzeitüberwachung bei einem Shutdown

RCCMD bietet einen passiveren Überwachungsmodus, mit dem Sie den Betriebszustand virtueller Maschinen während eines Herunterfahrens in Echtzeit überwachen können:



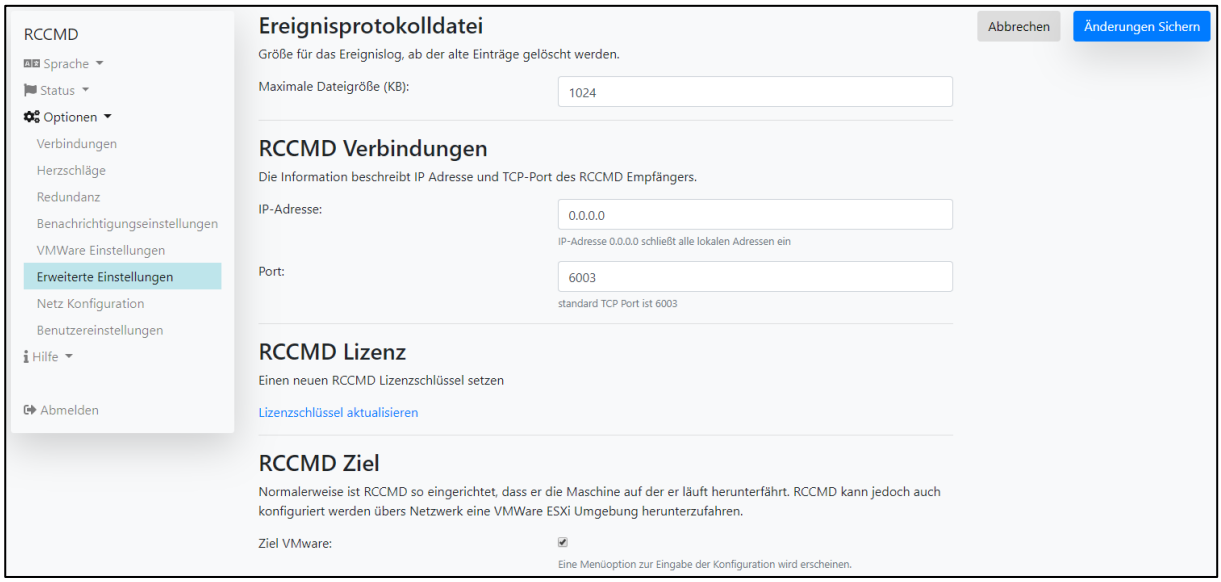
Sobald diese Funktion aktiviert ist, wird die Statusabfrage der virtuellen Maschinen alle xxx Sekunden aktualisiert, bis das Kontrollkästchen deaktiviert wird. Diese Anzeige bleibt bestehen, bis die RCCMD-Appliance endgültig mit dem ESXi-Host heruntergefahren wird und nicht mehr erreichbar ist.
Echtzeit-Überwachungsoptionen:

- Status virtueller Maschinen
- Status von Maschinen, die nicht mehr auf den Servern vorhanden sind
- Status neu hinzugefügter Maschinen (migriert und neu bereitgestellt)
- Status der Verfügbarkeit eines ESXi-Hosts

Hinweis: Eingeschränkte Konfigurationsmöglichkeiten, falls aktiviert.

Zu speichernde Änderungen werden erst nach einem Neustart der RCCMD-Appliance wirksam. Die aktuelle Herunterfahrroutine wird in Echtzeit nicht geändert. Bei einem tatsächlichen Herunterfahren

Erweiterte Einstellungen

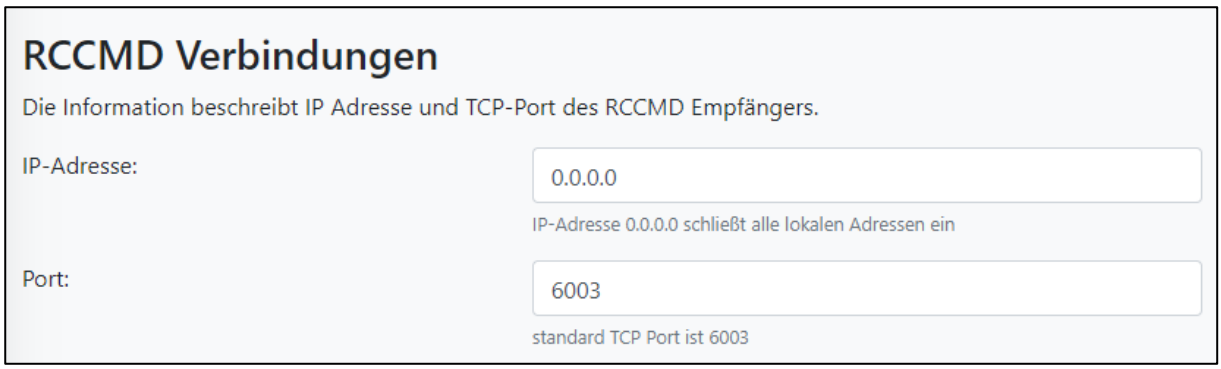


Die Advanced Settings erlauben zusätzliche Einstellungsmöglichkeiten im RCCMD Verhalten. Das Menü ist hierbei in drei Teile unterteilt:

Ereignisprotokolldatei

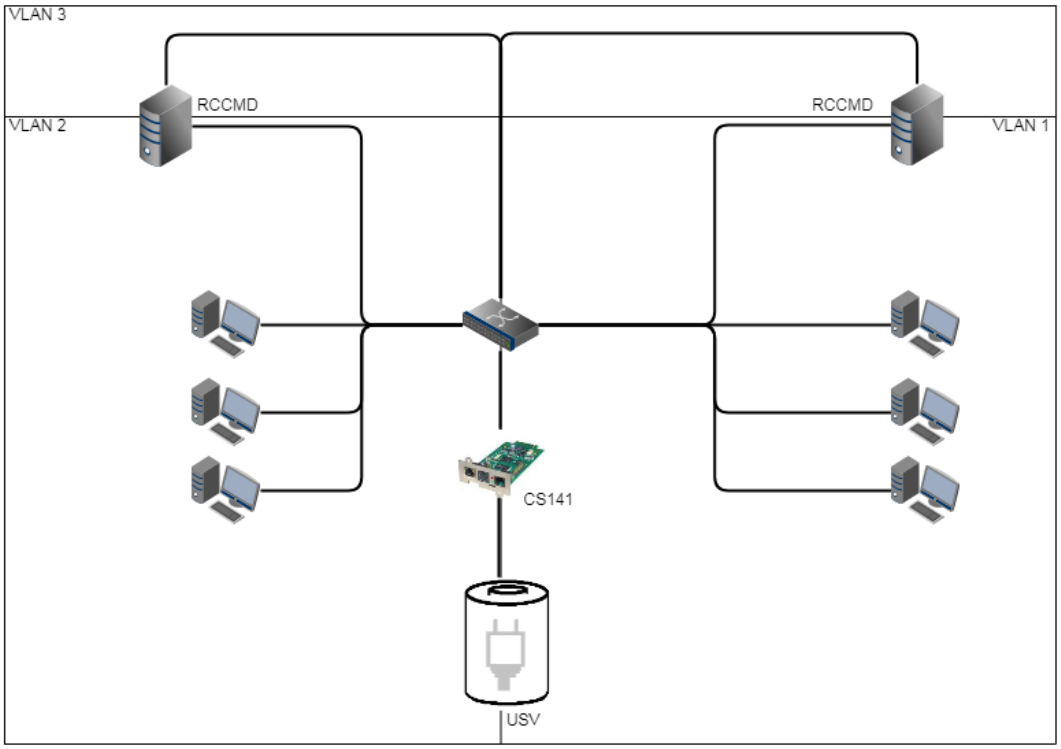
RCCMD protokolliert alle Verbindungen mit, die an eine Installation gerichtet wurden. Da Serversysteme unter Umständen nur begrenzen Speicher zur Verfügung stellen, kann es unter notwendig sein, die Größe der Protokolldatei auf einen maximalen Wert einzugrenzen, den sie an Platz verbrauchen darf. Wird der Wert erreicht, wird der älteste Eintrag im Log überschrieben.

RCCMD Verbindungen



RCCMD Bindings ist ein filigranes Hilfsmittel, mit dem Sie den Datenverkehr eingrenzen können. Da diese Einstellung tief in Ihre Netzwerkeinstellung eingreift, sollte sie mit entsprechender Vorsicht verwendet werden.

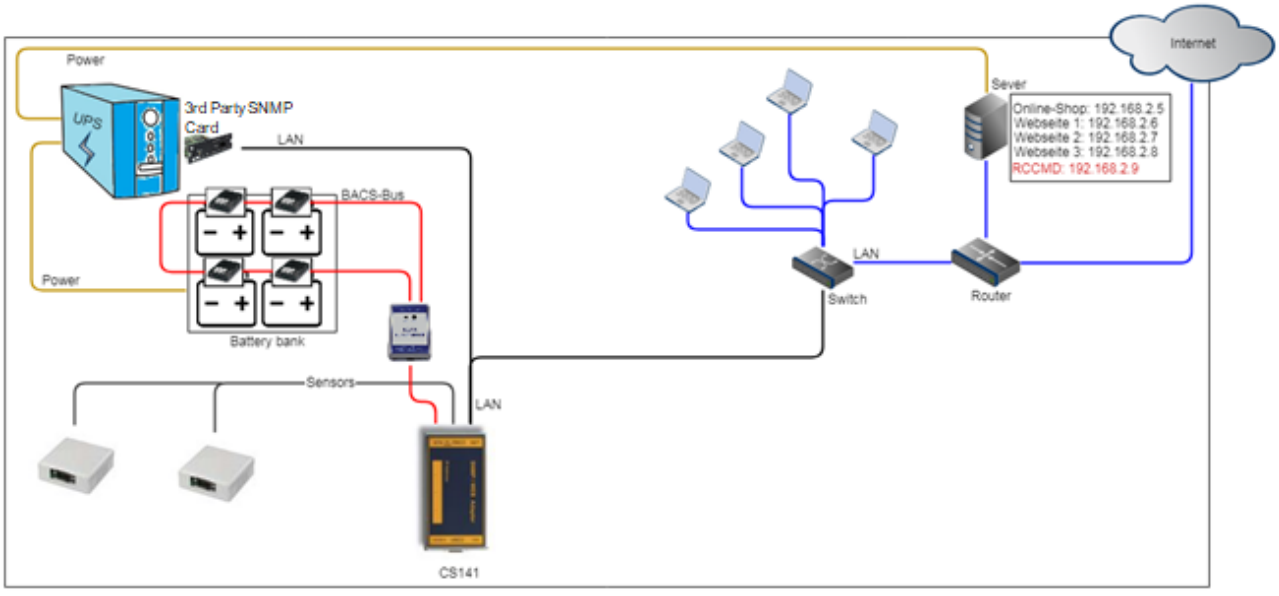
Die Bindings erlauben, den Listener von RCCMD auf eine bestimmte Netzwerkkarte oder beim Multihoming auf eine spezielle IP-Adresse innerhalb einer Netzwerkkarte fest zu definieren. Dieser Fall tritt ein, wenn Sie zum Beispiel über ein VLAN das Netzwerk logisch in ein Produktionsnetzwerk und ein Infrastrukturnetzwerk unterteilen:



In diesem Anwendungsfall können zwei oder mehr Netzwerkadapter in einem Server installiert sein.

Mit dieser Separation können Sie verhindern, dass die Nutzer innerhalb des Netzwerkes auf die RCCMD-Installation zugreifen und versehentlich einen Server herunterfahren – dieses ist ausschließlich über Geräte möglich, die sich in VLAN 3 befinden bzw. über einen Router entsprechend freigeschaltet wurden.

Ein weiterer Anwendungsfall wäre das sog. Multihoming:



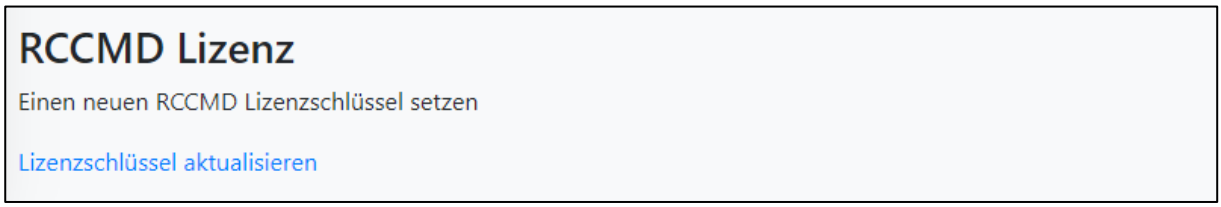
Es ist bei modernen Netzwerkgeräten nicht unbedingt notwendig, dass eine IP-Adresse mit einer Netzwerkschnittstelle fest verknüpft ist. Tatsächlich können über eine Netzwerkschnittstelle mehrere IP-Adressen verbunden werden – diese teilen sich dann Hardware, bilden aber sonst in sich geschlossene Instanzen. Ein solcher Anwendungsfall ist zum Beispiel ein Webserver, welcher unterschiedliche Webseiten mit einer jeweils eindeutigen IP-Adresse verwaltet:

In diesem Beispiel ist der Server an einem Router angeschlossen, der festlegt, welche Signale aus dem Internet stammen und welche ihren Ursprung im lokalen Netzwerk haben. RCCMD kann auf diese Weise angewiesen werden, lediglich auf einer bestimmten IP-Adresse auf RCCMD-Signale zu lauschen.

Tipp

Diese Konfigurationen sind Spezialfälle. Der Regelfall sieht vor, dass Sie die Einstellung 127.0.0.1 / local host auf Port 6003 stehen lassen können. In dem Fall wird RCCMD auf allen verfügbaren IP-Adressen lauschen, ob ein gültiges Signal eingeht. Da Sie unter dem Menü Connections die gültige Senderadresse definiert haben, wird RCCMD das Signal zwar bemerkten, jedoch die Ausführung verweigern und diese Tatsache als ungültiger RCCMD- Befehl im Log vermerken.

Lizenzdaten ändern und aktualisieren

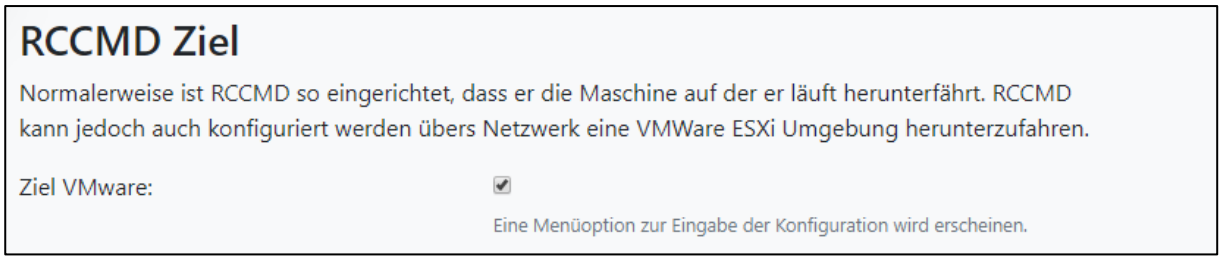


Unter bestimmten Bedingungen kann es notwendig sein, dass Sie einen RCCMD Lizenzschlüssel anpassen oder ändern müssen – z.B. wenn Sie auf einen Corporate Key wechseln oder einen Lizenzschlüssel doppelt vergeben haben.

In dem Fall klicken Sie auf Lizenzschlüssel aktualisieren und geben direkt den neuen Schlüssel ein.

Im Anschluss müssen Sie nur noch unter Status RCCMD einmal stoppen und wieder Starten. Der neue Lizenzschlüssel wird übernommen und ist augenblicklich aktiv.

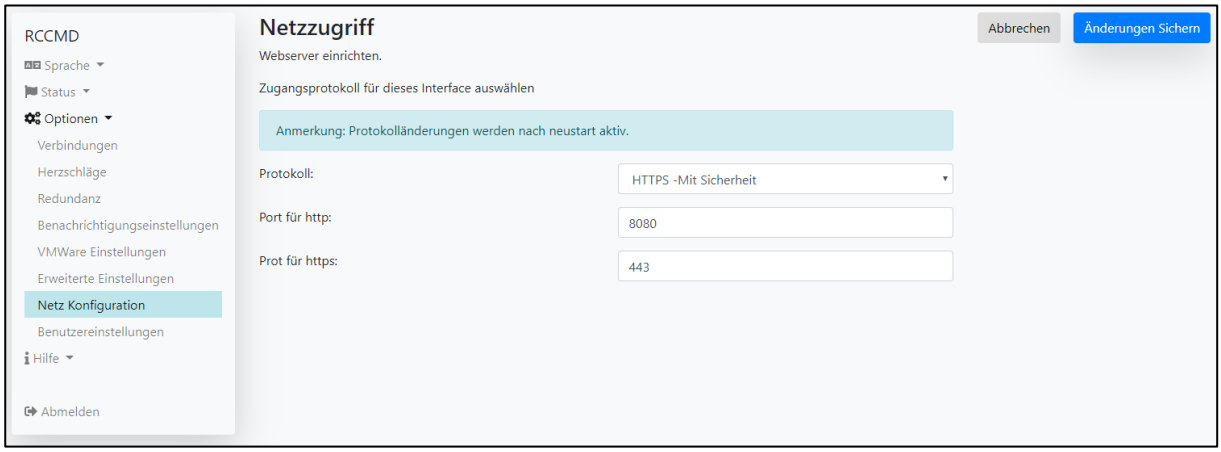
RCCMD Shutdownverhalten anpassen.



Standardmäßig ist diese Funktion aktiviert – Sie aktiviert die grundlegenden Dienste und blendet die Konfigurationsmenüs ein, die Sie für den Betrieb in einer VMware – Umgebung benötigen. Unter bestimmten Umständen kann es jedoch auch einmal notwendig sein, RCCMD auf die eigene VM umzulenken:

Wenn Sie diesen Haken entfernen, wird RCCMD nur noch die eigene VM herunterfahren und ausschalten und die VMware – Umgebung ignorieren. Stattdessen wird das Menü für lokale Shutdowns geladen und entsprechend präsentiert.

Web Access / Netz Konfiguration



Stellen Sie die Verfügbarkeit der RCCMD Webkonsole ein.

Der Default für den Webzugriff lautet:

http: Port 8080

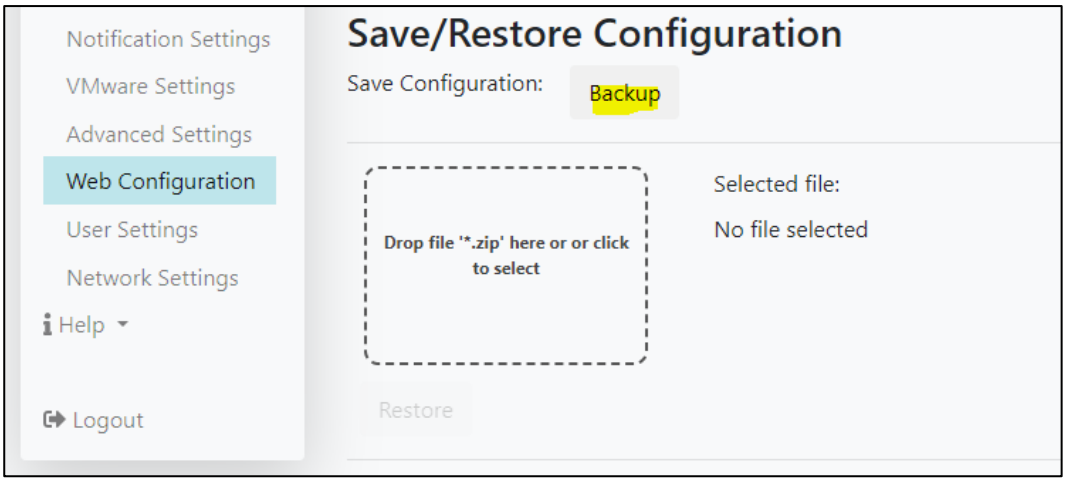
https: Port 8443

Beachten Sie, dass bei Änderung der Standardwerte die Webkonsole von RCCMD nur noch über die von Ihnen eingestellten Ports erreichbar ist.

Backup / Restore

Wichtig: Diese Funktion ist ab Programmversion 4.54.X.231129 verfügbar. Backups aus älteren Programmversionen sind mit dieser Programmversion nicht kompatibel, da sich das Programm geändert hat. Mehr Information hierzu erhalten Sie im Kapitel Desaster Recovery.

Um das Upate zu erleichtern, bietet die RCCMD Appliance eine komfortable Backup & Restore-Funktion an:



Um die Appliance zu aktualisieren, gehen Sie wie folgt vor:

1. Klicken Sie bei der aktuell laufenden Appliance auf “Backup” und laden Sie den zip-File herunter.

2. Fahren Sie jetzt die Appliance herunter und schalten Sie diese aus.

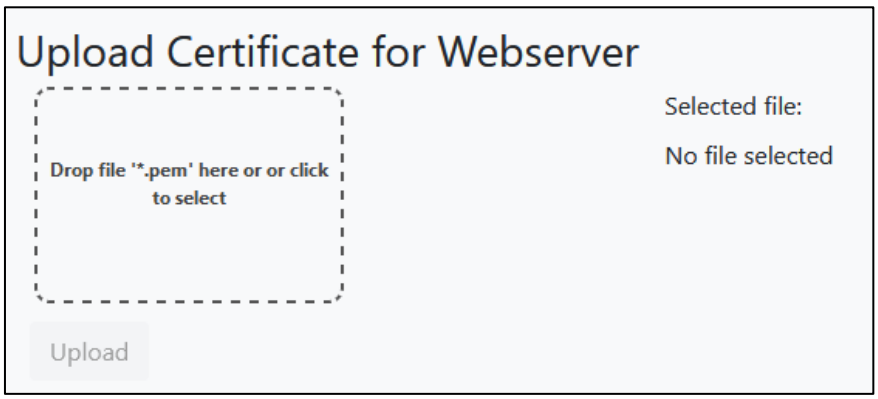
3. Rollen Sie die neue Appliance aus.

4. Platzieren Sie das Backup wie heruntergalden in der vorgesehenen Box und klicken Sie auf Restore

5. Überprüfen Sie alle Einstellungen und Funktionen.

Wenn die neue Appliance wie gewünscht funktioniert, können Sie die alte Appliance von Ihren Server löschen.

Der integrierte Webserver kann mit firmeneigenen SSL-/TLS-Zertifikaten ausgerüstet werden, um die Kommunikation zwischen Webbrowser und Webinterface von RCCMD zu verschlüsseln. Das Zertifikat muss als PEM-Datei vorliegen, setzen Sie sich hierzu mit dem zuständigen Systemadministrator in Verbindung.

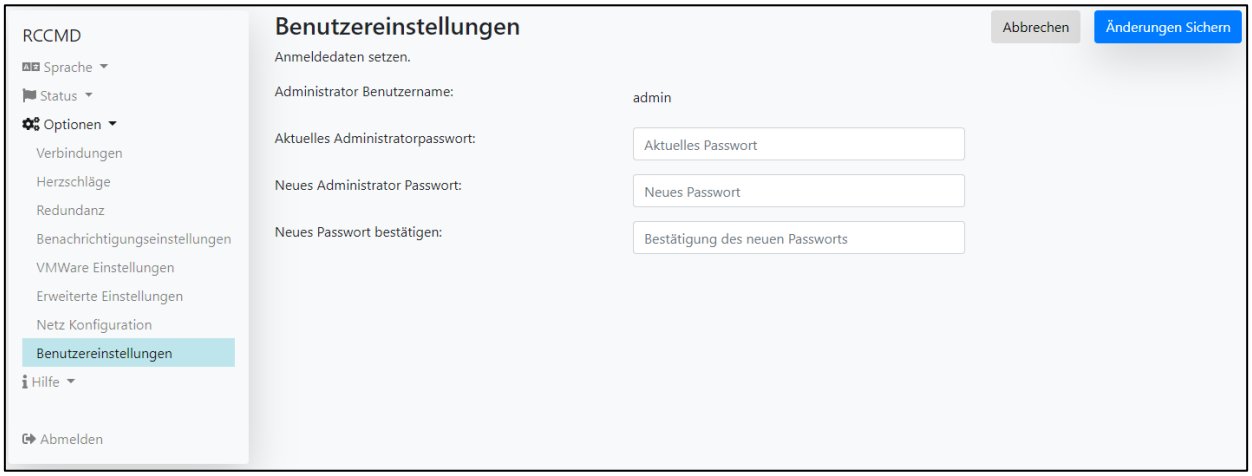


Das Zertikat einspielen::

1. Erstellen Sie mit der Backup-Funktion ein aktuelles Backup
2. Platzieren Sie ihre *.pem – Datei in der vorgesehenen Box
3. Klicken Sie auf Upload, um den Importvorgang zu starten.
4. Starten Sie anschließend RCCMD unter “Status” einmal neu.

Der Webbrowser sollte nach Aktualisierung das von Ihnen hochgeladene Zertifikat anzeigen. Sollte die PEM-Datei beschädigt sein, können Sie jederzeit mit dem Backupfile und einer schnellen Neuinstallation den letztem Zustand wiederherstellen.

User Settings



Passen Sie das Administratorpasswort Ihren Vorstellungen und Firmenrichtlinien an. Bitte beachten Sie, dass dieses Passwort auch für den Nutzer admin auf der Konsole gilt. Im Anhang finden Sie eine Anleitung, wie Sie einen Notfallnutzer einrichten können.

Administrator User Name: *admin*
Dieser Nutzername ist im Programmcode von RCCMD verankert und kann nicht geändert werden.

Current Administrator Password:
Dies ist das aktuell vergebene Passwort.

New Administrator Password
Vergeben Sie das neue Administrator Passwort.

Confirm New Password
Wiederholen Sie das von Ihnen vergebene Passwort. Bitte beachten Sie hierbei, dass Copy and Paste eventuelle Tippfehler 1:1 übernimmt.

Tipp
Je nach Programmversion gibt zwei Default-Passwörter, die vergeben werden können.

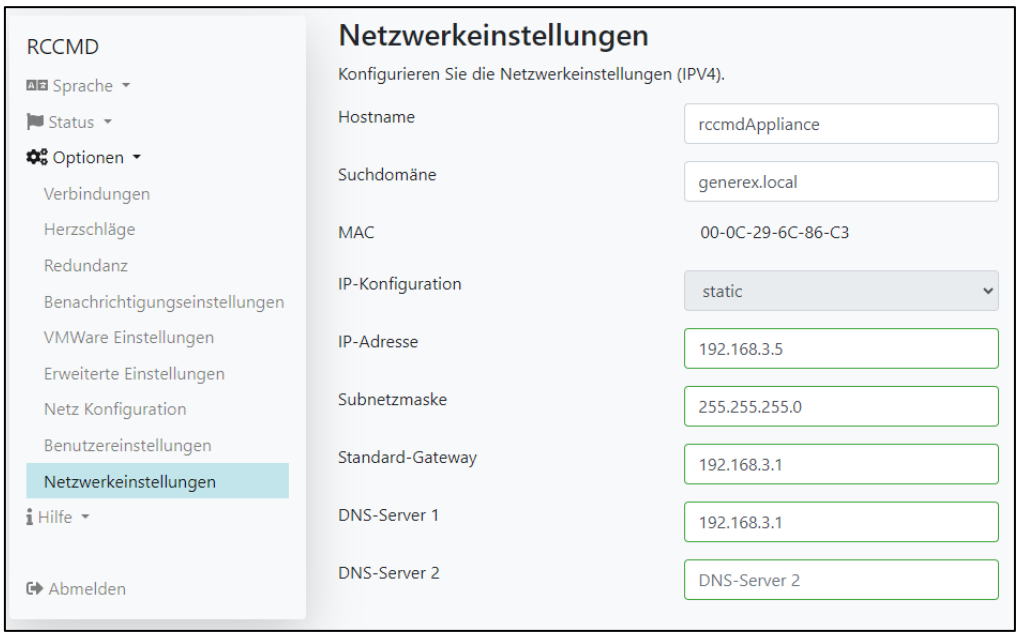
Programmversionen bis 5/2018: cs121-snmp
Programmversionen ab 5/2018: RCCMD

Da Sie unterschiedliche Programmversionen mischen können, ist bei einer Neuinstallation auf das Ausgabedatum zu achten. Mit der Appliance wurde das Default-Passwort geändert.

Die Netzwerkeinstellungen

(Für dieses Konfigurationsmenü benötigen Sie die Version 4.49 oder höher.)

Die Appliance für VMware bietet Ihnen die Möglichkeit, über das Webinterface die IP-Adresse direct einzustellen.



Hostname / Search Domain:	Wenn Sie mit RCCMD über DNS-Namen kommunizieren möchten, Tragen Sie hier die notwendigen DNS-Namen ein. Beachten Sie bitte, dass hier kein Automatismus vorliegt. Der DNS-Name muss ggfs. beim zuständigen DNS-Server manuell nachgepflegt werden.
MAC:	Die Media Access Control (MAC) definiert die Adresse der Netzwerkhardware. Diese wird von VMware beim Ausrollprozess generiert, und kann nicht über dieses Interface geändert werden.
IP-Configuration:	Bestimmen Sie, ob die IP-Adresse über einen DHCP-Server oder statisch zugewiesen werden soll. Beachten Sie bitte, dass ein DHCP-Server bei entsprechender Konfiguration die IP-Adresse ändern kann, wodurch ein Shutdownsignal ggfs. ins Leere laufen kann, weil sich die Ziel-IP geändert hat.
IP-Adressdaten (wenn statisch)	
IP-Adresse / Subnet Mask	Definieren Sie die IP-Adresse und die zugehörige Subnetzmaske. Die Daten erhalten Sie vom zuständigen Administrator
Default Gateway	Sollte RCCMD über Netzwerke hinweg kommunizieren müssen, definieren Sie bitte ein entsprechendes Gateway.
DNS 1/ 2	Der DNS-Server dient zur Namensauflösung, wenn Sie z.B. bei der Appliance keine IP-Adressen, sondern die DNS-Namen von ESXi-Hosts verwenden möchten. Beachten Sie bitte, dass z.B. die ESXi-Host-1.example.local nur dann erreicht werden kann, wenn ein DNS-Server verfügbar ist.

***Tipp**:*

Beim Ausrollen werden Sie in einem Interaktiven Systemfenster von VMware gefragt, ob Sie eine IP-Adresse eingeben möchten. Wenn Sie diese Eingabefelder nicht ausfüllen, geht die RCCMD-Appliance beim ersten Start davon aus, dass ein DHCP-Server im Netz verfügbar ist, und eine IP-Adresse zuteilt. Über die Netzwerkeinstellungen können Sie die IP-Adressdaten von RCCMD sowie das Startverhalten anpassen, und zwischen DHCP und manueller IP-Adresse wählen.

Hilfe

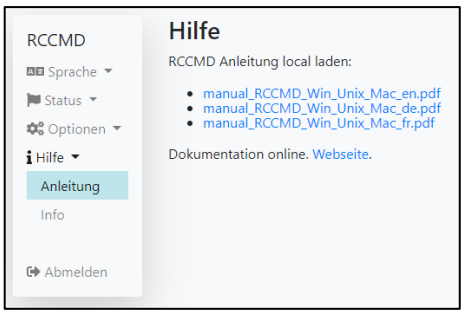
RCCMD Sprache Status Optionen	
Hilfe	➔ Systemreiter: Hilfe
Anleitung Info	➔ Aktuelle Bedienungsanleitung ➔ Allgemeine Systeminformationen, Versionsnummern, Links
Abmelden	

Anleitung

RCCMD ist mitunter in sicherheitskritischen Bereichen installiert, welche keinen Zugriff auf das Internet anbieten oder wo aus sicherheitspolitischen Gründen keine externe Dokumentation mitgebracht werden darf.

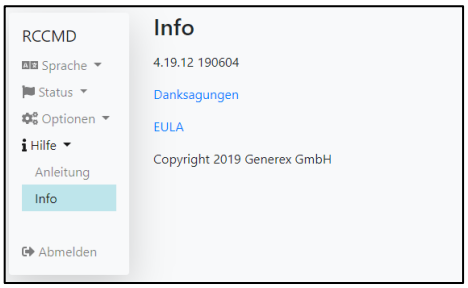
Aus diesem Grund finden Sie unter „Anleitung“ eine Kopie der aktuellen RCCMD lokal innerhalb von RCCMD hinterlegt. Für diese PDF benötigen Sie lediglich einen Webbrowser, der diesen Datei-Typ öffnen kann:

Dadurch haben Sie bei jeder RCCMD Appliance das zu dieser Appliance.



Systeminformationen

EULA-Verträge, Danksagungen und natürlich auch die aktuell laufende Programmversion der RCCMD Appliance finden Sie unter dem Link Info.



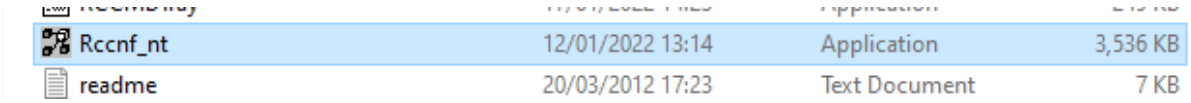
Anhang

Alles, was Sie sonst noch so über RCCMD wissen möchten...

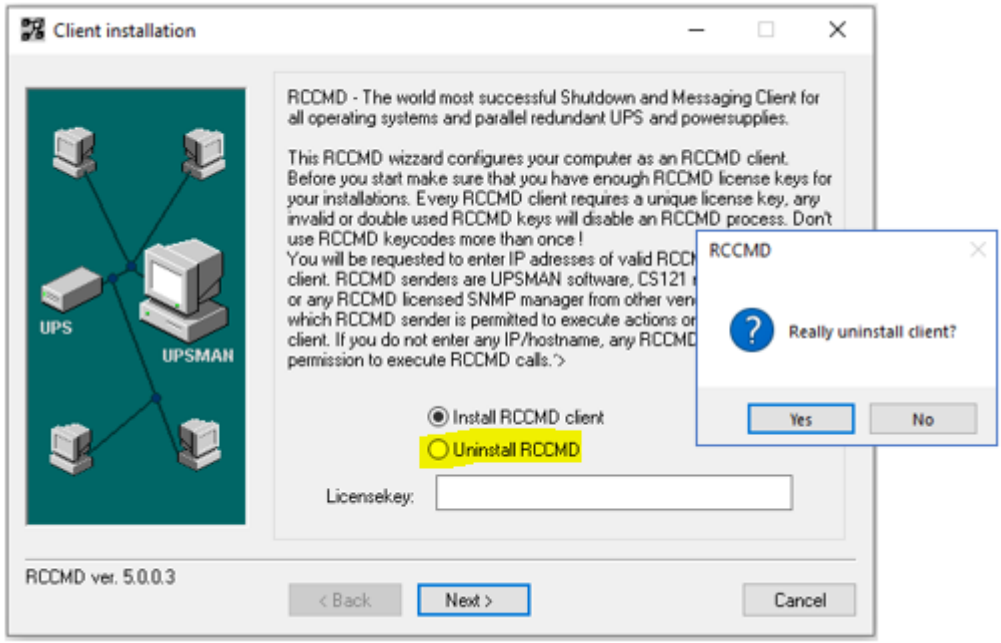
Das Microsoft Windows „Das RCCM_NC“ Configuration Tool

Im Installationsverzeichnichnis von RCCMD finden Sie das „Tool RCCM_NC“, mit dem Sie viele Funktionen der Windows-Version von RCCMD ohne installierten Webbrowser direkt konfigurieren können. Das wird dann interessant, sobald RCCMD ohne Webbrowser konfiguriert werden muss.

Klicken Sie das Tool mit der rechten Maustause an und wählen Sie „Als Administrator ausführen“! aus:



Nach dem Start stehen folgende Konfigurationsmöglichkeiten zur Verfügung:



Install RCCMD client

Mit dieser Funktion wird der Konfigurations/ Installationsdialog ausgeführt.

Uninstall RCCMD

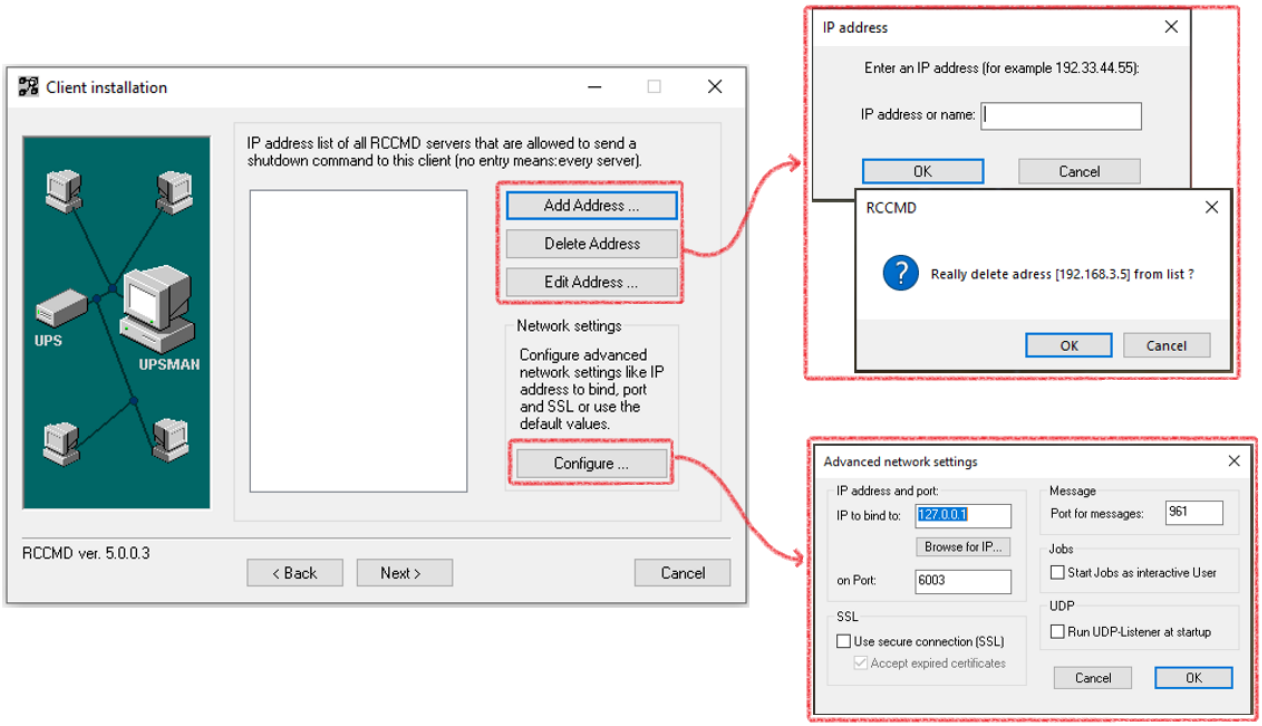
Wählen Sie diese Funktino aus, um die aktuelle RCCMD- Programmversion zu deinstallation

Licensekey

Lizenzschlüssel eingeben / ändern

Grundlegende Navigation:

< Back Next >	Navigieren Sie durch alle Setup-Bildschirme vorwärts/rückwärts. Sie können jede Seite erneut besuchen und Ihre Änderungen übernehmen. Eventuelle Optionen und Funktionen werden dem entsprechend in Echtzeit auf den Folgeseiten dann hinzugefügt oder entfernt.
Cancel	Abbruch der Konfiguration. Die bereits getätigten Eingaben werden verworfen und der Konfigurationsdialog ohne Änderungen an RCCMD geschlossen.
Install	Erscheint dynmasich, meistens auf der letzten Konfigurationsseite. Mit Install wird die aktive Konfiguratiosndatei geschrieben und der RCCMD Service neu gestartet.



Add / Delete / Edit

Definieren Sie,

a. welche Sender-IP diesem RCCMD Client überhaupt ein Signal senden dürfen. Sobald Sie hier eine IP-Adresse eintragen wird die Ausführung von Geräten mit abweichender IP-Adresse verweigert.Mit Add/Edit werden IP-Adressen eingetragen oder geändert, Delete entfernt einen Eintrag aus der Liste.

b. ob Redundanz-Verhalten gewünscht ist: Wenn Sie 2 oder mehr IP-Adressen hinterlegt haben, können Sie im späteren Verlauf dieses Dialogs auswählen, welche IP-Adresse zu einer Redundanzgruppe zusammengefasst werden soll.

Configure / Advanced network settings

IP address and port

Wenn Sie wünschen, dass RCCMD nur auf einer speziellen Netzwerkkarte oder einem abweichenden Port lauschen soll, geben Sie hier die IP-Adresse an, auf die der Listener gelegt werden soll.

SSL

Definieren Sie, ob RCCMD eine SSL – Verschlüsselung für die Kommunikation verwenden soll, und wenn, ob abgelaufene Zertifikate dennoch aktzeptiert werden soll.

Message

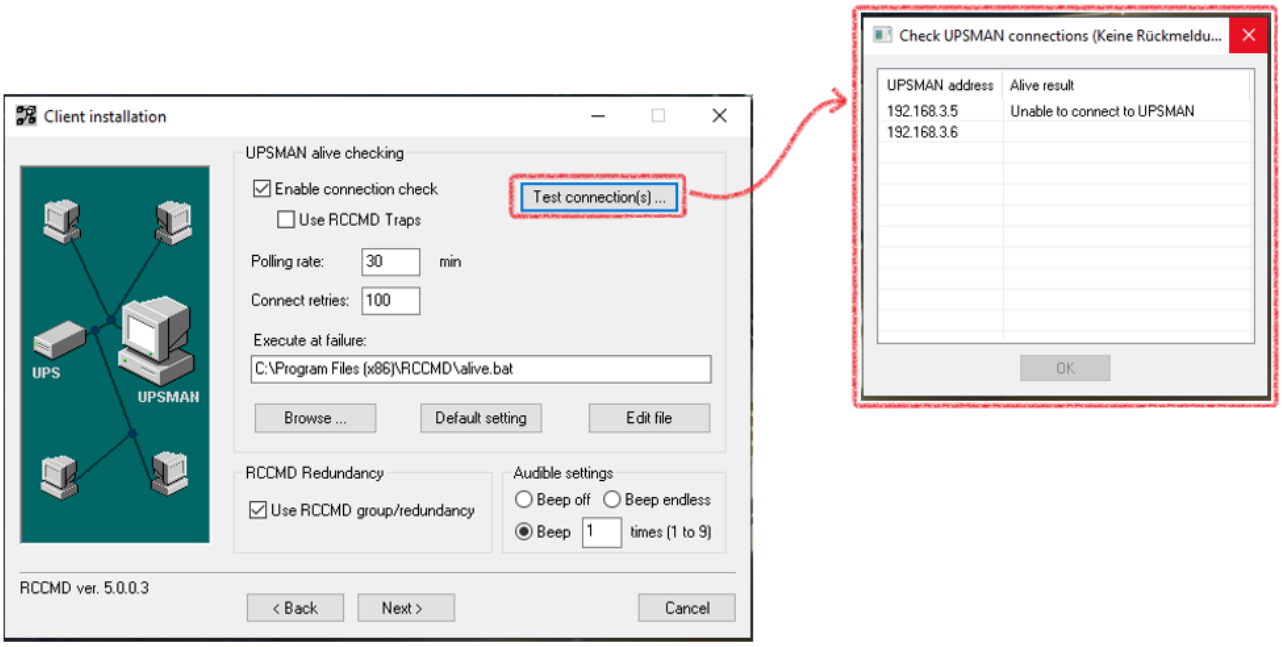
Jobs as interactive User

Normalerweise ist RCCMD ein Hintergrunddienst. Dem entsprechend starten auch alle Skripte im Hintergrund. Mit diesem Haken werden die Skripte als Vordergrundprozess ausgeführt.

Run UDP Listener at startup

Broadcastseignale sind meistens Unifyed Data Packages (UDP), bei denen der Sender nicht erkennt, ob und wie ein Datenpacket sein Ziel erreicht hat. Da UDP-Packete relativ einfach zu fälschen sind (man benötigt letztendlich nur die gültige Sender-IP), ist diese Funktion aus Sicherheitsgründen üblicherweise deaktiviert und muss durch den Anwender manuell aktiviert werden.

Heartbeats / UPSMan alive checking



Enable connection check

RCCMD kann auf Wunsch regelmäßig die eingetragenen gültigen Sender abfragen, ob das entsprechende Gerät noch verfügbar ist. Die *„polling rate“* definiert dabei, in welchen Abständen dies geschehen soll und *„Connect retries“*, wie oft dieser Verbindungstest nacheinander fehlschlagen darf, bevor RCCMD von einem Problem ausgeht.

Test connections

Fragen Sie testweise alle eingetragenen IP-Adressen ab, ob die entsprechenden Geräte auch von RCCMD erreicht werden können.

Execute at failure

Dieses Skript wird ausgeführt, wenn die unter „Connect retries“ angegebene Anzahl an Verbindungsversuchen erreicht wurde. Sie können dabei „Browse“ ein eigenes Skript auswählen oder mit Edit file das aktuell ausgewählte Skript direkt editieren. Default settings löscht alle Einstellungen und stellt den Original-Zustand der Startkonfiguration wieder her.

Use RCCMD Traps

An Stelle von polling wird von den Sendern eine RCCMD Trap-Nachricht gesendet, die als Lebenszeichen interpretiert wird.

Audible Stettings

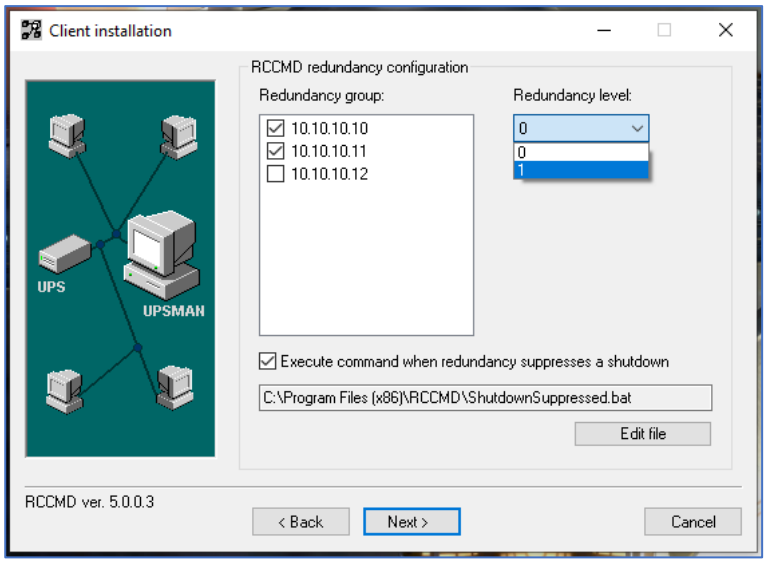
RCCMD blendet bei Bedarf ein Alarmfenster ein und zeigt dies mit einem gelben Warndreick in der Taskleiste an. Diese Funktion steuert das formidable akkustische „BEEP“, es kann auf Wunsch abgestellt werden, endlos Beepen oder eine bestimmte Anzahl von Warn-Beeps von sich geben.

RCCMD Redundancy

Diese Funktion wirkt sich auf den „Next“ -Button auf. Wenn Sie Redundancy aktivieren, wird automatisch ein weiterführender Konfiguratiosnscreen aktiviert, der auf der Folgeseite eingestellt werden kann.

RCCMD redundancy configuration

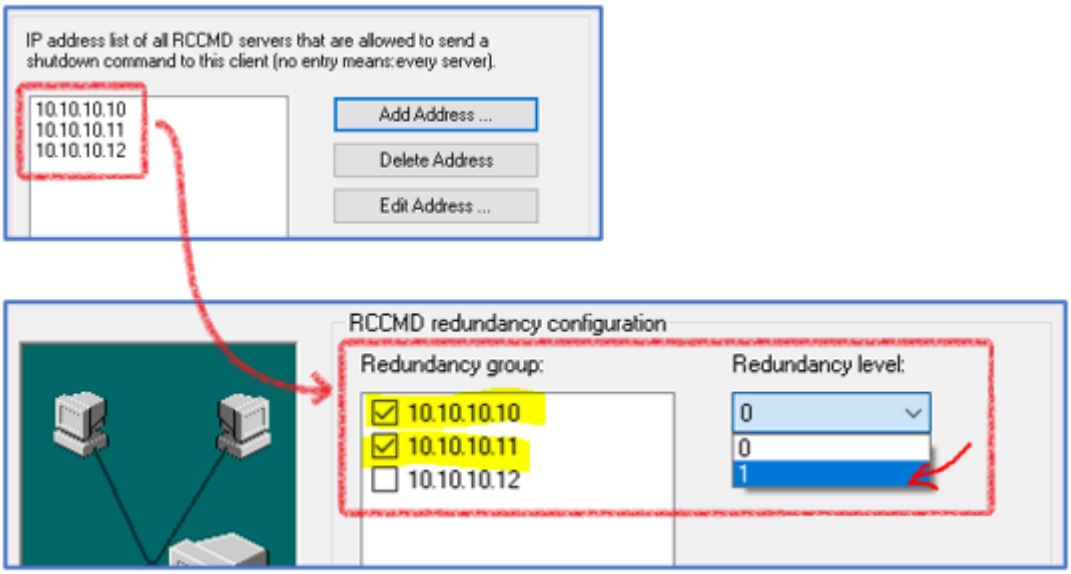
Dieser Screen erscheint nur, wenn Sie im Dialog „UPSMAN alive checking“ den Haken bei RCCMD Redundancy gesetzt haben.



In diesem Dialog möchte RCCMD,.welche unter Connections hinzugefügten IP-Adressen in einer Redundanzgruppe zusammengeführt werden sollen.

Zur Erklärung:

Unter Connections haben Sie gültige Sender hinzugefügt und damit definiert, welche IP-Adresse generell RCCMD-Kommandos an diesen RCCMD-Client senden darf. Aus diesen vorher eingegebenen IP-Adressen können Sie definieren, welche dieser gültigen RCCMD - Sender nur gemeinsam einen Shutdown auslösen können.



In diesem Beispiel dürfen generell 3 gültige RCCMD Sender ein Shutdown senden. Unter Redundancy wurde jedoch definiert, dass die 10.10.10.10 und die 10.10.10.11 nur gemeinsam den Shutdown auslösen können. Ein typisches Scenario wäre, dass zwei CS141 in USV-Anlagen stecken, wärend ein dritter CS141 mit einem SENSORMONITOR die Umgebungstemperaturen der abgesicherten Server überwacht.

Redundancy Level

Der Redundanzlevel bestimmt, wie viele Sender den Shutdown anweisen müssen:

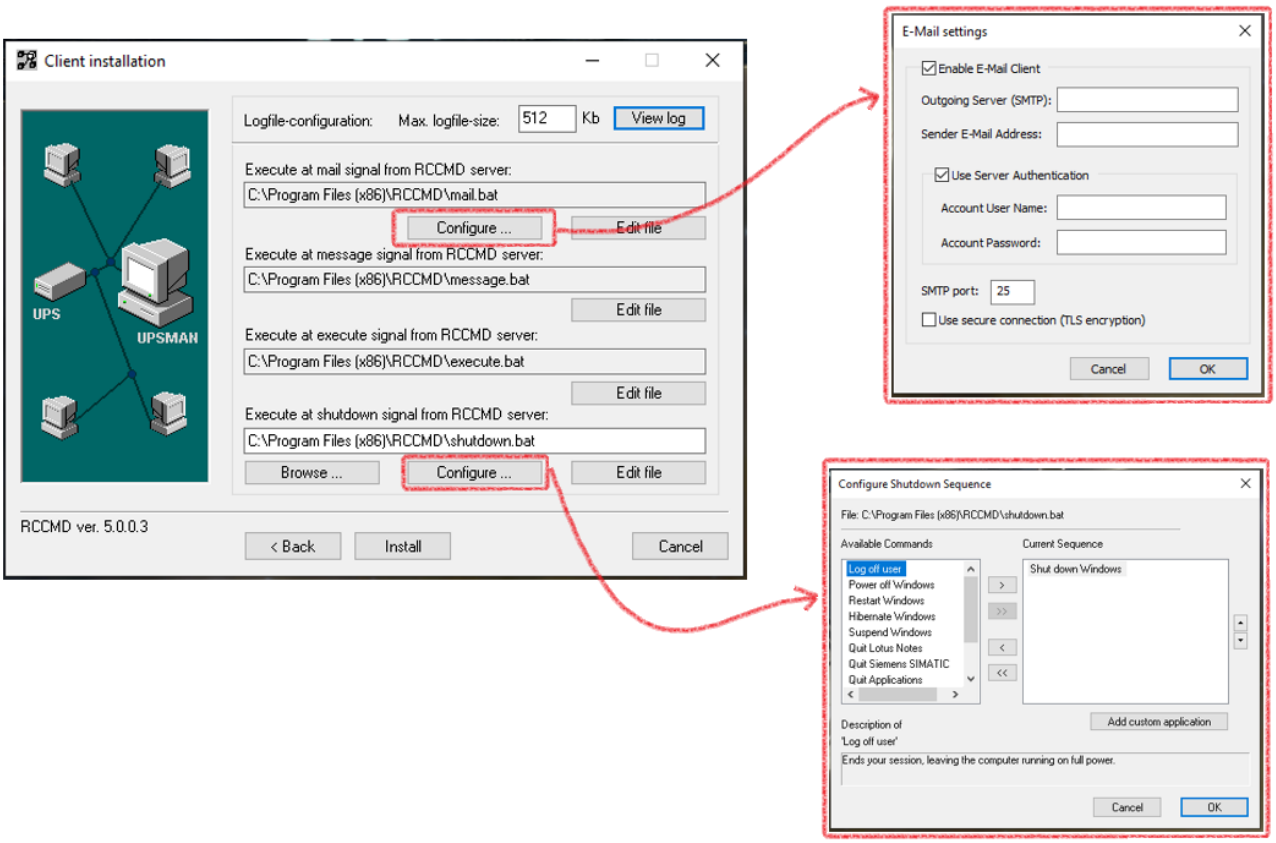
0 definiert hierbei den ersten Sender, der ein RCCMD Shutdown ausgesprochen hat.
1 jede weitere Zahl definiert einen weiteren Sender, der ebenfalls diesen RCCMD Shutdown aussprechen muss.

Bei zwei Geräten ist der maximale Redundanzlevel „1“, weil es nur ein weiteres Gerät gib. Bei drei gültigen Sendern wäre demnach die maximale Redundanzstufe 2, da eins der Geräte das Initialkommando gibt und die weiteren Geräte so betrachten zustimmen.

Execute command when redundancy suprpesses a shutdown

Dieses Skript wird automatisch ausgeführt, wenn der Redundanzlevel den Shutdown unterdrückt hat. Mit edit file können Sie beliebige Aktionen dem Batch File hinzufügen.

RCCMD Shutdown behaviour and logging



Logfile-Configuration

Definieren Sie die Größe des Logfiles, den RCCMD anlegen soll. Wenn die Datei diese Größe erreicht hat, wird jeweils der älteste Eintrag aus der Ereingisliste gelöscht, und durch ein neues Ereignis ersetzt.

Execute at mail signal from RCCMD server

RCCMD kann auch als Mail-Relay arbeiten, etwa, wenn ein CS141 / BACS aus einem geschützten Bereich ohne direkte Anbindung Informationen via Mail teilen soll. Unter Configure aktivieren Sei den integrierten Mail-Client und geben die notwendigen Zugangsdaten an, damit RCCMD entsprechen eine Mail senden kann.

Execute at message signal from RCCMD server

Dieses Skript nimmt den Job „RCCMD Message“ an und zaubert die Message Box auf den Desktop eines Betriebsystem. Normalerweise muss hier nichts geändert werden Beachten Sie bitte, dass dieses Skript bei jeder Message ausgeführt wird, unabhängig von dem Inhalt des Jobs RCCMD Message!

Execute at execute signal from RCCMD server

Ähnlich wie message signal, nur dass der RCCMD Job „Execute“ angenommen wird, wodurch ein CS141 direkt auf dem RCCMD Client mit lokalen adminrechten ein Skriptfile starten kann. Auch hier muss normalerweise nichts angepasst werden, das Skript läuft genau so wie es eingestellt ist Out-Of-The-Box

Execute at shutdown signal from RCCMD server

Klicken Sie auf Configure, um die Shutdown-Routine an Ihre Vorstellungen anzupassen. Jede Aktion wird generell von oben nach unten wie in der Liste abgelegt ausgeführt, wobei das letzte Kommando Shut down Windows oder ähnliches ist. Nach diesem Kommandos werden keine weiteren Befehle mehr ausgeführt, da das Betriebssystem entsprechend RCCMD beendet.

Mitd en intuitiven Schaltflächen fügen Sie hier neue Jobs hinzu, ändern die Reihenfolge der auszuführenden Jobs oder entfernen diese wieder. Mit Add custom application fügen Sie ihre eigenen Skripte hinzu, die innerhalb dieser Shutdownsequence mit ausgeführt werden sollen.

WARNUNG: EDIT FILE ERLAUBT, DEN CHARAKTER JEDER BATCH-DATEI ZU INDIVIDUALISIEREN! DA DIE DIREKTE MANIPULATION DER SKRIPTE DIREKT IN DEN FUNKTIONSABLAUF EINGREIFT, GESCHIEHT DIESES AUF EIGENES RISIKO!

Install

Schließt den Konfigurationsvorgang ab, schreibt den Konfiguraionsfile und startet RCCMD neu. Sie können den Konfigurationsvorgang beliebig oft wiederholen, die vorher eingegeben Daten werden dem entsprechend angezeigt.

RCCMD ist ein sehr mächtiges Systemverwaltungstool – richtig angewendet kann mit RCCMD tansparent zu bestehenden Shutdown- und Gebäudeleitsystemen die komplette Softwareseite eines Notfallkonzeptes übernehmen:

- Migrationen anstoßen
- Shutdowns vorbereiten und eigenverantwortlich duchführen
- Backupsysteme starten
- Systemverzeichnisse sichern und kopieren
- Informieren
- Shutdownsequenzen von einem RCCMD-Client an einen anderen übergeben
- Etc.

Die Weboberfläche bietet hier einen komfortablen Einstieg, zeigt aber letztendlich nur einen geringen Teil dessen, was RCCMD tatsächlich innerhalb eines Netzwerks leisten kann.

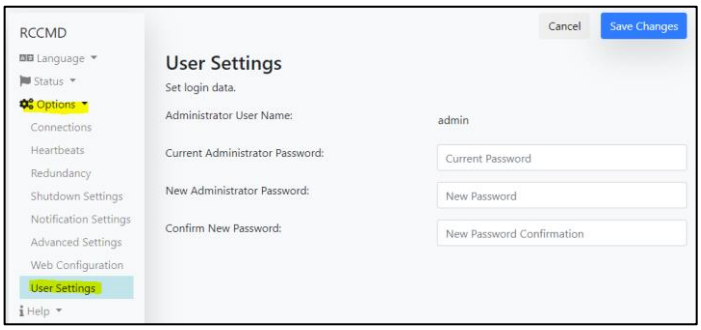
Tipp

RCCMD ist für den sicheren Betrieb in einem Netzwerk ausgelegt. Das schließt ein, dass es sich bestmöglich unauffällig im Hintergrund arbeitet, um eventuellen Hackern das Aufspüren bestmöglich zu erschweren.

1. *Passwortsicherheit (RCCMD für Linux, Windows und VMware*

   Das Startpasswort ist „RCCMD“! Sie sollten es schnellstmöglich ändern.

   Ein Blick in das Handbuch reicht aus, und Hacker haben Zugriff auf die komfortable Konfigurationsoberfläche.



   Was ist ein „sicheres Passwort“?

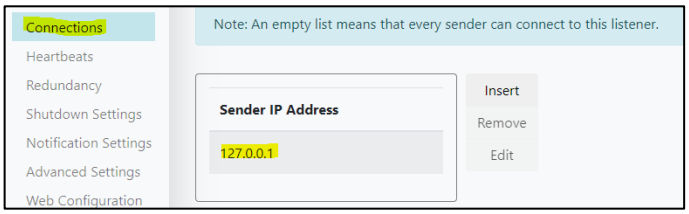
   Erst einmal: Kein Passwort ist unhackbar, und wenn es jemand wirklich drauf anlegt, gibt es viele Möglichketen, ein Passwort heruaszufinden – Der Trick bei einem guten Passwort ist, dass ein potentieller Angreifer das Interesse verliert oder aufgibt, weil er befürchten muss, entdeckt zu werden, bevor er sein Ziel erreicht.

   Ein sicheres Passwort erfüllt folgende Kriterien:

   - 8 – 12 Zeichen lang
   - Groß- und Kleinschriebung
   - Zahlen
   - Mindestens ein Sonderzeichen
   - Kein Bezug zur Person und dessen dem Alltag

2. *Berechtigte Sender für den Shutdown: Einstellung notwendig*

   RCCMD war schon immer auf bestmögliches Handling auch durch ungeübte Nutzer ausgelegt. Im einfachsten Fall konnte man RCCMD einfach installieren und einschalten – schon war die EDV auf der Serverseite gegen einen Stromausfall geschützt.



   Das wurde jetzt geändert:

   Neu ist, dass jetzt die IP-Adresse 127.0.0.1 voreingestellt ist. Das bedeutet, dass RCCMD eigentlich nur von einem Sender ein Shutdown-Signal entgegennimmt: Von sich selber (127.0.0.1 ist der sog. „Local Host“). Bevor Sie nicht manuell einen gültigen Sender hinzugefügt haben, wird RCCMD jedes eingehende RCCMD – Signal im Logfile als abgehlent dokumentieren.

   Sicherheitsempfehlung:

   Minimieren Sie die Anzahl der berechtigten Sender! Je weniger Geräte diesem RCCMD ein Shutdownsignal oder Steuerbefehle (RCCMD Execute’s) senden drüfen, desto sicherer wird Ihre RCCMD Installation.

3. *UDP Broadcast – Signale*

Unter Connections finden Sie die Funktion „Enable UDP Broadcast“:

Diese Funktion wird benötigt, wenn Sie vom CS141 aus einen der folgenden Jobs als Broadcast ausgeben möchten:

- RCCMD Shutdown
- RCCMD Message
- RCCMD Execute

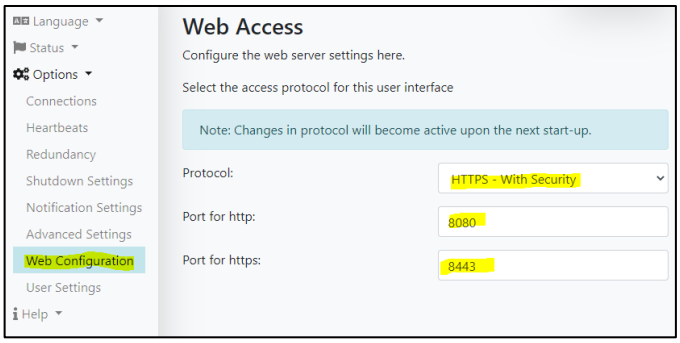
UDP bietet den Vorteil, dass mit extrem niedriger Latenz gearbeitet werden kann, um Nachrichten oder Steuerkommandos vom Sender zu beliebig vielen Empfängern zu übertragen, allerdings dafür auch den Nachteil, dass letztendlich Sender und Empfänger sich nicht kennen. Ein Hacker kann abgefangene UDP-Packete auswerten und ggfs. fälschen-

Sicherheitsempfehlung:

UDP sollte wenn möglich nur eingesetzt werden, wenn sich Sender und Empfänger in einem speziell gesicherten Infrastrukturnetzwerk aufhalten. Ist dies nicht der Fall, empfehlen wir, UDP zu deaktivieren.

4. *Ports*

Hier gehen die Meinungen ein wenig auseinander:



Bei RCCMD (und im CS141) können die Ports angepasst werden, so dass sie den Standard verlassen. Eigentlich ist diese Funktion für den Fall da, dass die Standardports von anderen Anwendungen bereits verwendet und blockiert werden.

Man muss allerdings erwähnen, dass natürlich die Betriebssicherheit steigt, wenn das RCCMD Webinterface – unabhängig von http oder https – zunächst eimal nicht auf 8080 (http) oder 8443 (https) antwortet, sondern zum Beispiel auf Port „1956 (http)“ bzw. „2578 (https)“ – Selbst wenn ein potentieller Angreifer weiß, dass RCCMD in Benutzung ist, müsste er erst einmal die notwendigen Ports ausfindig machen, auf denen eine Web-Anfrage an RCCMD überhaupt beantwortet wird.

Sicherheitsempfehlung für das Webinterface:

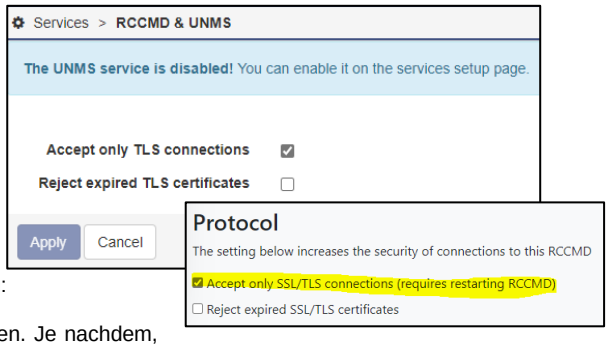
Kann man als flankierende Maßnahme zu ein einem starken Zugangspasswort machen – dann ist nicht nur das Passwort eine Hürde, sondern man muss auch wissen, auf welchem Port das Webinterface überhaupt erreichbar ist. Beachten Sie aber bitte, dass diese Änderungen auch eventuell eine Anpassung von Routern, Firewalls, etc. mit sich führen könnte.

Sicherheitsempfehlung für die Kommunikationsports (6003, 961)

Auf Port 6003 befindet sich standardmäßig der RCCMD Listener, und über Port 961 kommuniziert der RCCMD Service mitd em Service-Tray. Die Anpassung ist nicht erforderlich, sofern keine Sicherheitsbedenken gegenüber Standardports, oder aber der Port bereits anderweitig verwendet wird. Es gilt die gleiche Überlegung wie bei der Frage ob https / http – Ports angepasst werden sollten, und welchem Aufwand in der Netzwerkkonfiguration dem gegenüberstehen würde.

Warum funktionieren die Heartbeats mit TLS nicht?

Wir haben einige Einstellungen geändert, um den modernen IT-Richtlinien zu entsprechen: Eine der wichtigsten Änderungen ist, dass alle Dienste mit Ausnahme des Webservers am CS141 & BACS System nun standardmäßig ausgeschaltet sind.



Unter "Devices > Setup" müssen Sie den UNMS & RCCMD Trap Service aktivieren - dadurch wird die RCCMD Heartbeat Funktion aktiviert. Öffnen Sie in RCCMD Verbindungen und schauen Sie sich "Protocol" an: Accept only SSL/TLS connections" ist standardmäßig aktiviert.

Wenn Sie die "Heartbeats" verwenden möchten, müssen die Konfiguration sowohl bei RCCMD als auch beim CS141/BACS identisch sein:

Beide Endpunkte müssen bei "SSL/TLS" entweder auf ON oder OFF stehen. Je nachdem, welches Zertifikat Sie verwenden, können Sie auch "Abgelaufene SSL/TLS Zertifikate ablehnen" wählen.

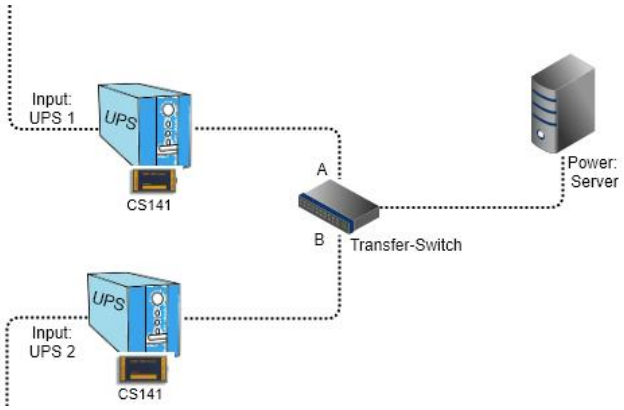
Bitte beachten Sie dies:

Technisch betrachtet ist es normal, dass Standard- (oder Beispiel-) Zertifikate abgelehnt werden, sobald Sie auf einer Seite “Reject expired TLS certifactes” aktivieren. Wenn diese Funktion gewünscht wird, werden gültige Zertifikate benötigt - wenden Sie sich bitte an den lokalen Systemadministrator.

Was wird für „Redundanz“ benöitigt?

Um es auf den Punkt zu bringen, für eine Sinnvolle Redundanz-Schaltung benötigen Sie 2 CS141, die zusammenarbeiten:

Um die Sache einfacher zu gestalten, gehen wir in diesem Tutorial von einem Standardfall aus, der besagt, dass 2 USV-Systeme im Einsatz sind, die jeweils unterschiedliche Stromkreise angeschlossen sind, und gemeinsam dann über ihre Ausgänge z.B. mit einem Transferswitch die Stromversorgung sicherstellen



Der Transferswitch wird das Problem erst bemerken, wenn eine der beiden USV-Anlagen sich herunterfährt, oder zur Wartung komplett abgeschaltet wurde, und ggfs. automatisch umschalten, aber hat logischwerweise keine Information darüber, in welchem Betriebszustand sich die jeweilige USV befindet, oder wie viel Restlaufzeit noch verfügbar ist:

➔ Wenn wir davon ausgehen, dass Input A aktiv ist, und Input UPS 1 ausfällt, würde der Transferswitch also auf Input B umschalten, sobald UPS1 sich selber herunterfährt.
➔ Dasselbe würde der Transferswitch machen, wenn UPS Input 1 und 2 gleichzeitig ausfallen, und je nach Auslastung wird UPS 2 dann die Last übernehmen, die durch den Server entsteht, bis die Batterien erschöpft sind.

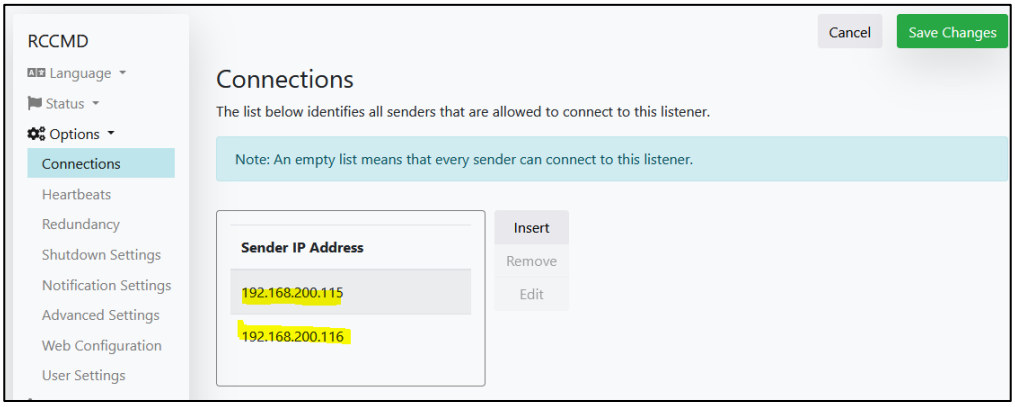
Der Server muss der Logik folgend also rechtzeitig herunterfahren, bevor beide USV-Anlagen nicht mehr genug Notstrom bereitsstellen können.

Wo wird die Redundanz konfiguriert?

Das Redundanzverhalten wird im jeweiligen RCCMD Client konfiguriert. Hiezu sind mehrere Informationen notwendig:

1. Wer darf dem RCCMD Client Shutdownbefehle senden?

Das entscheidet sich unter „Connections“:



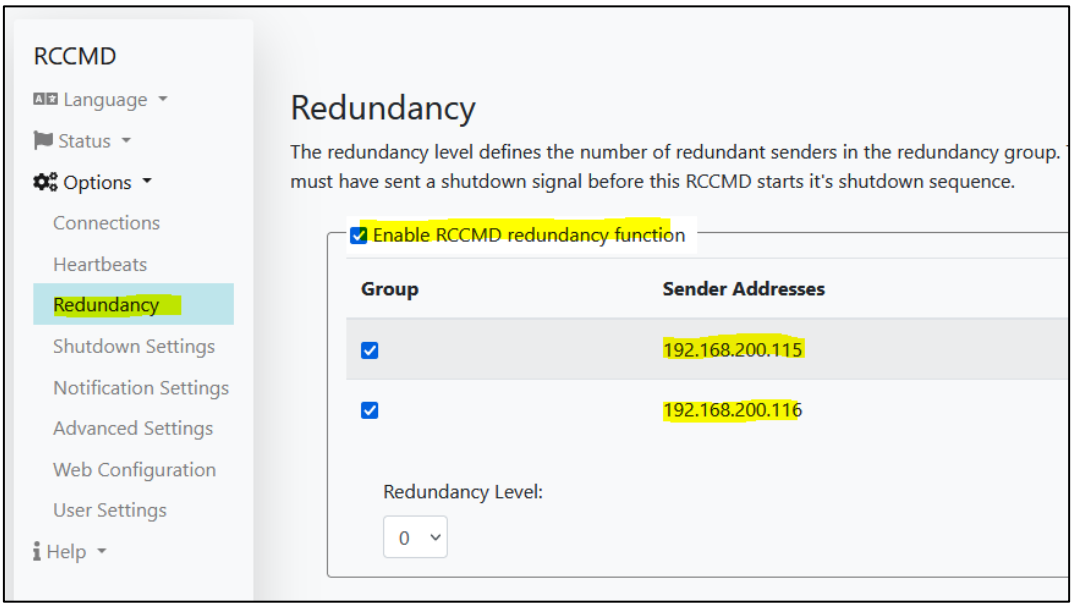
Geben Sie hier die IP-Adressen der Sender ein, in diesem Fall: die IP-Adressen der beiden CS141-WEBMANAGER. Sobald Sie diese eingetragen haben, werden nur noch eingehende Signale von genau diesen Sendern zugelassen.

Tipp: DHCP Mode

Wenn Sie die CS141 WEBMANAGER im DHCP – Modus laufen lassen, kann es sein, dass der DHCP-Server neue IP-Adressen zuteilt. Sollte dies geschehen, wird der RCCMD Client die Ausführung verweigern, da die „neuen“ IP-Adressen nicht hinterlegt sind! Achten Sie also darauf, dass die IP-Adressen beiden CS141 WEBMANAGER im DHCP-Server fest eingetragen sind. Das gillt auch umgekehrt – SOLLTE der DHCP-Server dem RCCMD Client eine neue IP-Adresse zuweisen, dann laufen die RCCMD-Shutdownbefehle ins Leere – dazu aber später noch einmal mehr…

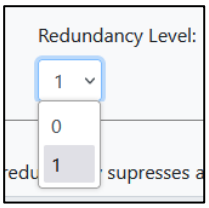
2. *Redundanz einstellen*

Nachdem Sie IP-Adressen eingetragen haben, können sie die Redundanzgruppe einstellen:



Aktivieren Sie zunächst die Redundanz-Funktion und markieren Sie die IP-Adressen, die Sie für diese Redundanz in Beziehung zueinander setzen möchten. In diesem Fall haben wir unter Connections 2 IP-Adressen eingetragen, die hier wieder auftauchen.

Wie ist der Redundanz-Level berechnet?



Der Redundanzlevel folgt einer einfachen Annahme:

Bei zwei USV-Anlagen gibt es immer 2 CS141 WEBMANAGER, von denen einer von beiden zwangsläufig als erstes einen Shutdown senden wird. Welcher der beiden WEBMANAGER das genau ist, hängt vom individuellen Ladezustand der Batterien, der Auslasung, vom Stromausfall, etc. ab. Der Shutdown wird aber so lange unterdrückt, bis alle weiteren WEBMANAGER in dieser Liste ebenfalls ein Shutdown-Befehl gesendet haben.

Daraus ergibt sich, dass der Redundanz-Level mathematisch N + 1 beträgt, wobei N generell der erste Webmanager ist, der ein Shutdown-Befehl sendet, wogegen“+1“ die Anzahl der weiteren Webmanager ist, die in dieser Gruppe einen Shutdown senden müssen.

Daraus ergeben sich folgende Werte:

0 -> Es muss kein weiterer Webmanager ein Shutdownbefehl senden.

1 -> Es muss ein weiterer WEBMANAGER ein Shutdown senden.

➔ **Da wir hier nur zwei USV-Anlagen haben, stellen Sie die Redundanz auf 1 („0“ würde keinen Sinn ergeben)**

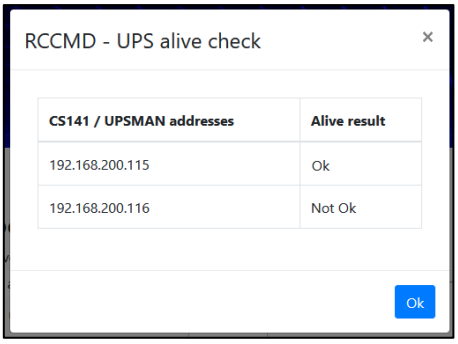
Was ist, wenn der zweite CS141 gar nicht mehr erreichbar ist, etwa durch ein Totalausfall des Switches?

RCCMD nimmt den Shutdown-Befehl unter Vorbehalt an: Wenn einer der beiden Webmanager ein Shutdownbefehl sendet, überprüft die Redundanzfunktion automatisch, ob alle weiteren WEBMANAGER, die für das Redundanz ausgewählt wurden, verfügbar ist, und die Kommunikation zur jeweiligen USV auch korrekt funktioniert:

Sollte diese Bedingung nicht erfüllt sein, wird der Shutdown ausgeführt, weil es naheliegenderweise keinen weiteren Shutdownbefehl geben kann.

3. *Testen der Verbindung*

Im letzten Schritt sollten Sie noch überprüfen, ob RCCMD beide CS141 WEBMANAGER erreichen und abfragen kann. Klicken Sie hierzu unter Heartbeats bei Test UPS Connections auf „Run alive check now…“



Da gibt es zwei Möglichkeiten:

OK -> Der CS141 ist erreichbar

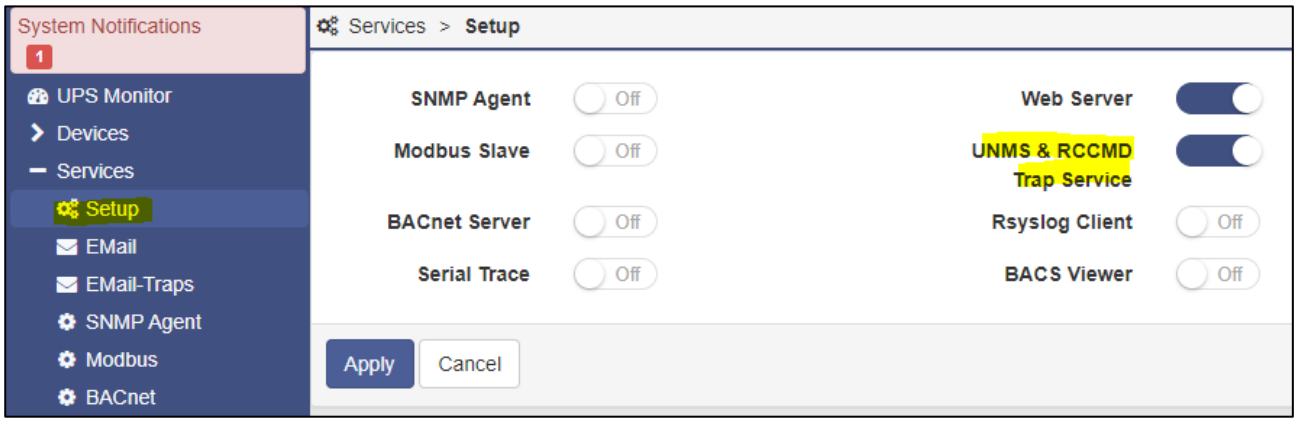
Not OK -> Der CS141 ist nicht erreichbar.

- Überprüfen Sie die Ports 5769 / 6003 TCP
- Überprüfen Sie die das Zertifikat
- Überprüfen Sie, ob TLS ON / OFF ist
- Überprüfen Sie, ob der UNMS & Trap Service auf dem CS141 aktiv ist
- Überprüfen Sie, ob Firewalls oder Virenscanner / Security-Lösungen die Kommunikation blocken.

4. Konfiguration am CS141

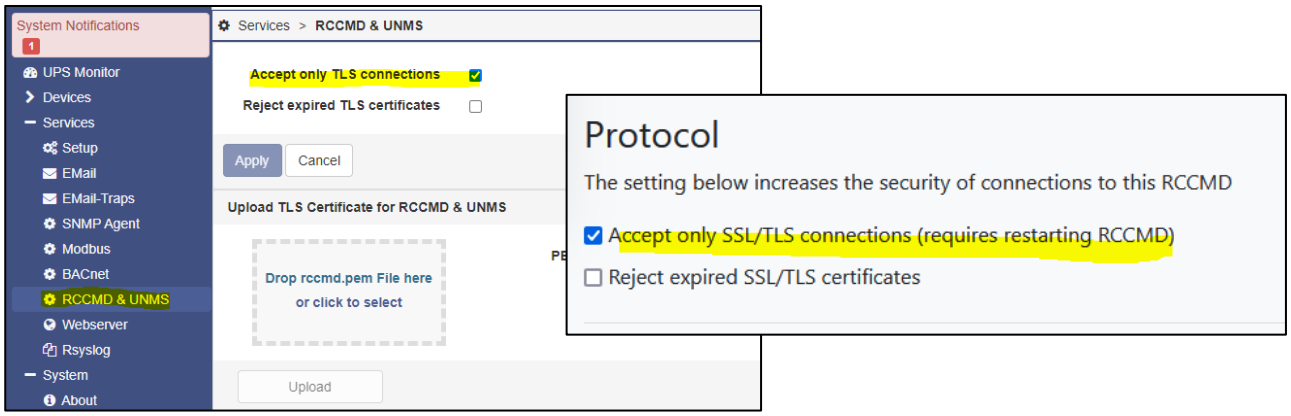
RCCMD ist jetzt so weit fertig konfiguriert und bereit für seine Aufgaben. Jetzt müssen beide CS141 identisch konfiguriert werden. Melden Sie sich beim CS141 WEBMANAGER an und führen Sie folgende Einstellungen durch:

a. Aktivieren Sie den ZNMS & RCCMD Trap Service



Dieser Schritt ist notwendig, damit RCCMD über Port 5769 TCP den CS141 abfragen kann. Ist der Service auf OFF, antwortet der CS141 und Sie erhalten beim Heartbeat Test ein Not OK.

b. Überprüfen Sie die TLS-Einstellung



Diese muss im CS141 und im RCCMD Programm (zu finden unter Options>Connections) identisch sein, da ansonsten die Kommunikation an sich nicht möglich ist.

c. Definition des Shutdown Jobs

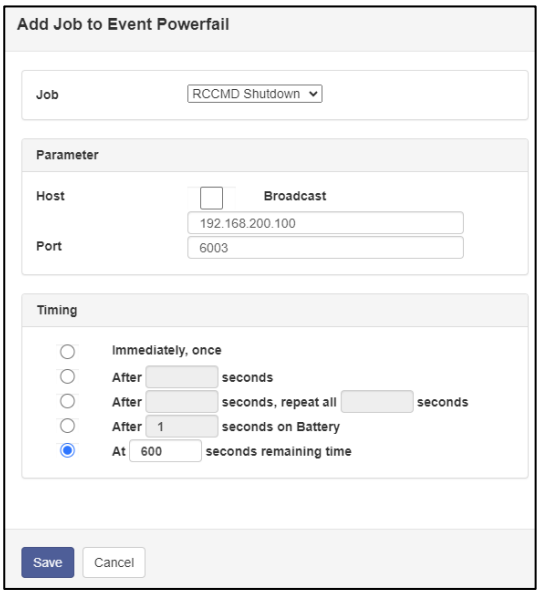
Richten Sie im CS141 bei Powerfail den Job „RCCMD Shutdown ein“

Job: Wählen Sie RCCMD Shutdown aus

Host: Geben Sie das Ziel des Jobs an, das ist die IP-Adresse des Betriebssystems oder Computers, auf dem der RCCMD Client installiert ist.

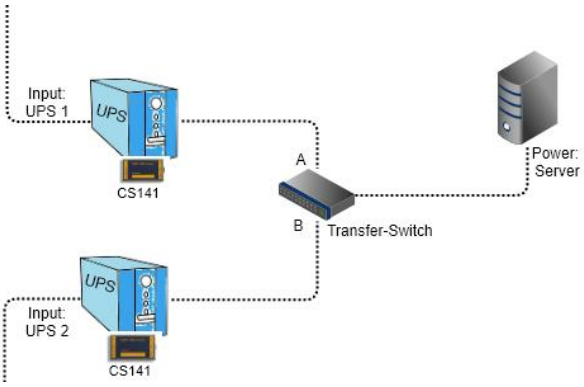
Port: Der Standard-Port ist 6003 TCP – Achten Sie darauf, dass RCCMD und CS141 auf dem selben Port senden bzw. auf ein eingehendes Signal lauschen.

Timing: Hier entscheidet sich, wann der CS141 den Job RCCMD Shutdown versendet. In diesem Beispiel wird der Job versendet, wenn ein Powerfail aktiv ist (Event Powerfail) und die USV meldet, dass noch 600 Sekunden Restlaufzeit verfügbar sind.



➔ **Achten Sie darauf, dass diese Konfiguration auf beiden CS141 durchgeführt werden muss, da ja beide CS141 WEBMANAGER ein individuell getriggertes Shutdown-Signal senden müssen. RCCMD wartet hier generell auf beide Shutdown-Befehle.**

5. Wie breche ich den Shutdown ab?



Erinnern wir uns an diese Zeichnung…

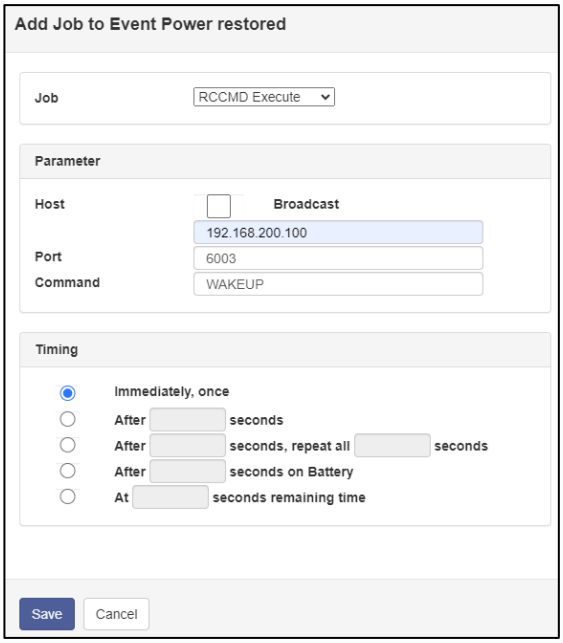
Es ist realistisch, dass UPS 1 einen Stromausfall hat, von dem UPS 2 niemals betroffen war, da es sich ja um zwei getrennte Stromkreise handelt.

Mit der aktuellen Konfiguration kann RCCMD zwar den Shutdown unterdrücken, wenn beide USV-Anlagen sonst verfügbar waren, aber nicht selbstständig herausfinden, ob der Stromausfall bei UPS 1 behoben wurde.

RCCMD führt aber akribisch Buch darüber, welche USV (bzw. welcher CS141 WEBMANAGER) bereits eine Shutdown-Anweisung ausgesprochen hat, und sobald alle USV-Anlagen dies getan haben, wird RCCMD folgerichtig aktiv, und fährt den Server herunter.

Um dem zu begegnen, bietet der CS141 einen speziellen Befehl, mit dem er seine Shutdownanweisung widerruft. RCCMD wird dem entsprechend der Shutdown-Anweisung wieder löschen und in den Regelbetrieb zurückfallen. Das Gegenereignis von Powerfail ist Power Restored. Hier definieren Sie entsprechend den Gegenjob, indem Sie einen Job hinzufügen und als Job „RCCMD Execute“ auswählen.

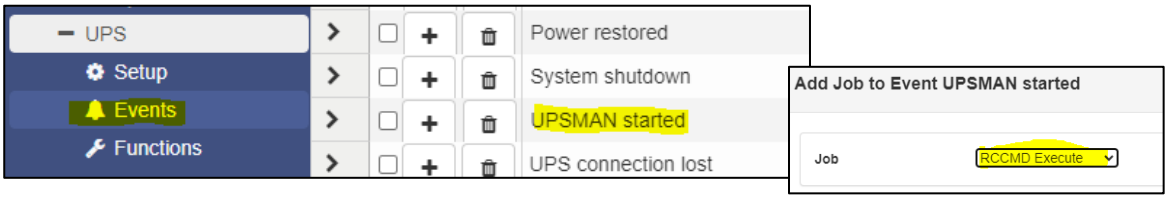
Job:	Wählen Sie RCCMD EXECUTE aus
Host:	Geben Sie das Ziel des Jobs an, das ist die IP-Adresse des Betriebssystems oder Computers, auf dem der RCCMD Client installiert ist.
Port:	Der Standard-Port ist 6003 TCP – Achten Sie darauf, dass RCCMD und CS141 auf dem selben Port senden bzw. auf ein eingehendes Signal lauschen.
Command	Schreiben Sie „WAKEUP“ in das Kommandofenster. Das ist der Befehl, mit dem ein RCCMD Shutdown mit aktiver Redundanz widerrufen wird.
Timing:	Hier entscheidet sich, wann der CS141 den Job RCCMD Shutdown versendet. In diesem Beispiel wird der Job unmittelbar versendet, wenn der Hauptstrom wiederhergestellt wird.



Sonderfall - Wenn der CS141 einen Powerfail erkennt, einen Shutdownbefehl versendet, und dann die USV herunterfährt

Die bisherige Konfiguration ist darauf eingestellt, dass der Stromausfall beendet ist, *bevor die USV sich herunterfährt*. Als Ergebnis von einem beendeten Powerfail gibt es das Gegenereignis Power Restored. Wenn der Stromausfall so lange andauert, dass die USV jedoch beschließt, sich herunterzufahren, um die Batterien vor der Tiefenentladung zu schützen, dann wäre der nächste Status beim Anfahren der USV zwangsläufig nicht „Power Restored“, weil diese Statusmeldung von der USV nur herausgegeben wird, unter der Bedingung, dass ein Stromausfall beendet ist, und die USV noch läuft.

Bei einem Neustart der USV ist das erste Ereignis, dass der CS141 WEBMANAGER triggert, das Ereignis „UPSMAN started“, und signalisiert damit, dass die Kommunikation zwischen CS141 und USV erfolgreich hergestellt wurde und der CS141 seinen Betrieb aufnimmt.



Um sicherzustellen, dass in beiden Fällen der Zähler beim jeweiligen RCCMD Client zurückgesetzt wird, sollten Sie den Job „RCCMD Execute“ mit dem Kommando WAKEUP ebenfalls bei UPSMAN startet hinterlegen.

SSL TLS ON / OFF – Warum ein RCCMD scheinbar nicht richtig kommunizieren will

TLS ist die Abkürzung für Transport Layer Security, und ermöglicht prinzipiell eine verschlüsselte Verbindung zwischen zwei IT-Systemen. Dabei ist es unerheblich, ob es sich um die Kommunikation zwischen Webbrowser und einem Server, zwei Infrastrukturgeräten oder einem Infrastrukturgerät und einem Server handelt, die Methode ist immer dieselbe: Bei einem Handshake wird überprüft, ob Sender bzw. Empfänger auch diejenigen sind, die sie vorgeben zu sein, und beide Endpunkte verschlüsseln anschließend mit vorliegenden Zertifikaten ihre Kommunikation. Da sich die Endpunkte bei diesem Vorgang gegenseitig bekannt machen, ist es für einen Hacker schwieriger, sich in die Kommunikation einzugreifen und diese zu manipulieren.

Wie funktioniert ein Zertifikat

Prinzipiell besteht ein SSL-Zertifikat immer aus zwei Teilen: einem öffentlichen Schlüssel und einem privaten. Der private Schlüssel wird verwendet, um Daten zu verschlüsseln, und der öffentliche Schlüssel, um zu entschlüsseln. Der öffentliche Schlüsselteil wird auf Anfrage nach dem Handshake dem jeweiligen Empfänger übergeben.

Jetzt gibt es mehrere Möglichkeiten:

- Das Zertifikat ist gültig
- Das Zertifikat ist ungültig, gesperrt oder beschädigt
- Das Zertifikat ist ausgelaufen
- Das Zertifikat ist grundsätzlich gültig, aber die Echtheit kann nicht bestätigt werden.
- …

Ob die Kommunikation zu Stande kommt, hängt hier oftmals von der individuellen Konfiguration der Kommunikationspartner ab:

1. SSL/TLS im Webbrowser: „Die Verbindung ist nicht sicher“

Das hängt damit zusammen, dass RCCMD im integrierten Webserver ein eigenes Werkszertifikat mitbringt, dass mehrere Attribute erfüllt:

- Nicht abgelaufener Zeitstempel
- Nicht von einer CA gesperrt
- Funktionsfähig
- Grundlegend gültig…

Aber: da es sich um ein hausinternes Zertifikat handelt, kann aus naheliegenden Gründen keine Signatur existieren, die bestätigt, dass der Webbrowser jetzt tatsächlich mit genau dem RCCMD Server kommuniziert, der er vorgibt zu sein.

Genau DAS bemängelt der Webbrowser, und warnt mit einem Dialog vor einer theoretischen Bedrohung, bevor die eigentliche Webseite (Das Webinterface) aufgerufen wird. Ob Ihnen die Option angeboten wird, dennoch fortzufahren, hängt von der individuellen Browserkonfiguration und den Netzwerkpolicen ab. Dieses Zertifikat kann in neueren Versionen von RCCMD einfach ausgetauscht werden, indem Sie unter Netz Konfiguration Ihr firmeneigenes Zertifikat als Standard PEM -File hochladen:

RCCMD wird automatisch das neue Zertifikat in den importieren und aktivieren. Wenn dieser Hinweis dennoch erscheint, bedeutet dies lediglich, dass der Webbrowser am Zertifikat etwas auszusetzen hat.

Tipp:

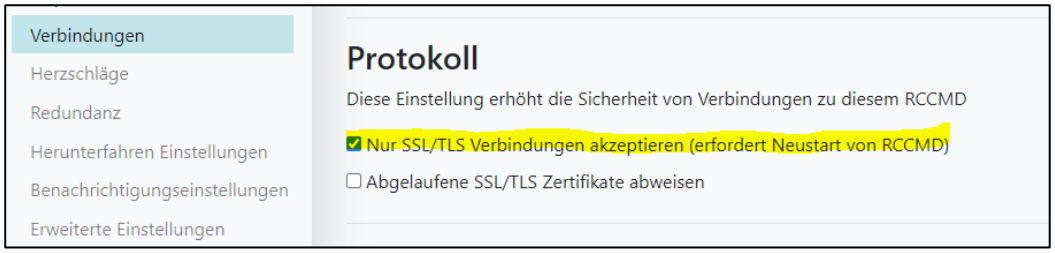
Erstellung von Zertifkaten: Im CS141 Benutzerhandbuch finden Sie ein vollständiges Tutorial über das Erstellen von PEM-Files unter Microsoft Windows. Sie können das CS141 Benutzerhandbuch jederzeit unter www.generex.de im Downloadbereich herunterladen.

2. Kommunikation RCCMD <-> CS141läuft nicht oder nicht richtig

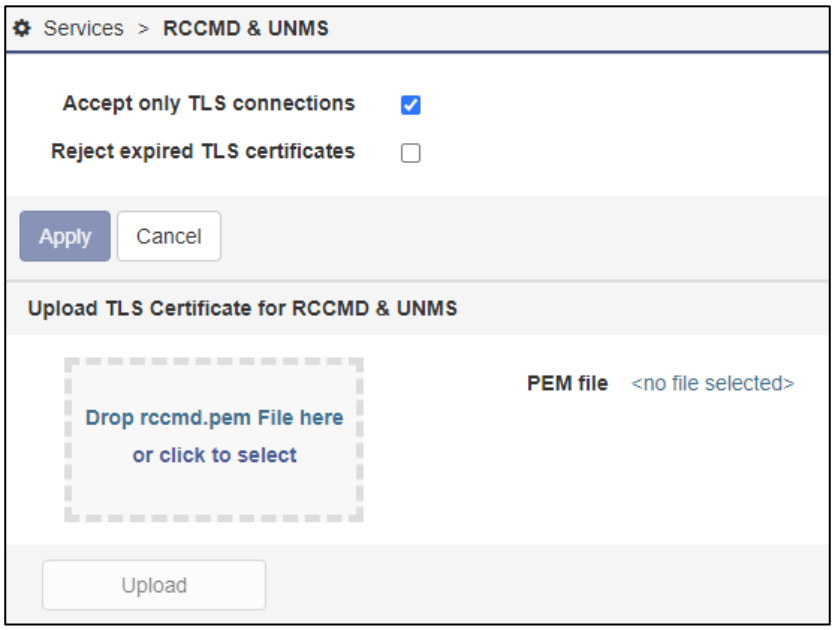
Obwohl alles richtig eingerichtet wurde, scheint RCCMD einfach eine Kommunikation abzulehnen. Hier gibt es grundlegend 2 Möglichkeiten, die RCCMD betreffen:

a. Unter Verbindungen ist nicht SSL/TLS einheitlich eingeschaltet:

Sowohl unter RCCMD:



Als auch in Ihrem CS141:



1. Problem: Die Haken sind bei SSL / TLS nicht synchron.

Es müssen auf beiden Endpunkten Accept only TLS connections entweder auf AN oder auf AUS gestellt sein.– da ansonsten eine von beiden Seiten unverschlüsselt kommuniziert, was die andere Seite folgerichtig ablehnt

2. Zertifikate sind nicht synchron

Im Installationsordner von RCCMD findet sich diese Datei:

Dies ist nicht der PEM-File für das Webinterface, sondern das Zertifikat für Kommunikation CS141 <-> RCCMD bzw. anderen RCCMD-Installationen in Ihrem Netzwerk. Um die TLS / SSL – Kommunikation zu verwenden, muss das Zertifikat bei allen Teilnehmern identisch sein – sollten Sie es geändert haben, müssen sie dies dem entsprechend bei allen anderen Teilnehmern ebenfalls tun.

Austausch bei RCCMD: Benennen Sie die rccmd.pem um in rccmd.pem1 und kopieren Ihr Zertifikat als PEM-File an diese Stelle. Benennen Sie Ihre PEM-Datei in rccmd.pem um. Starten Sie RCCMD neu.

Austausch bei einem CS141: Bennen Sie Ihren PEM-File in rccmd.pem um und ziehen sie die Datei in die vorbereitete Box. Drücken Sie auf Upload. Der CS141 wird die Datei automatisch hochladen und aktivieren.

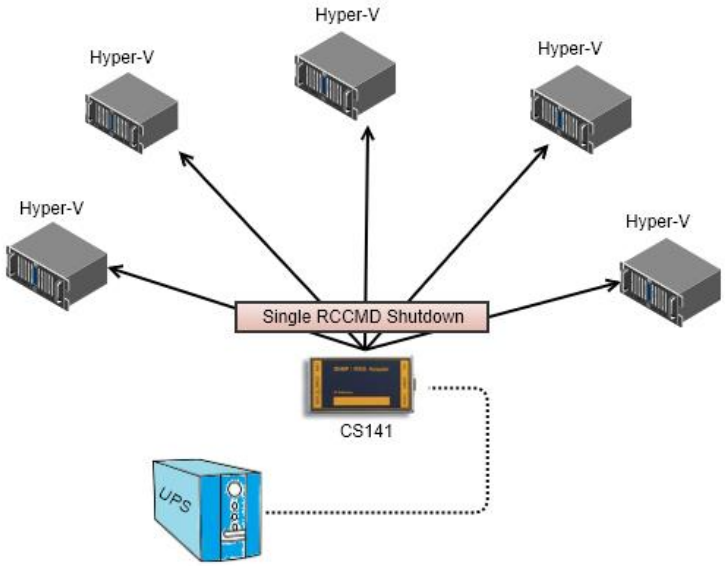
Einstieg in RCCMD mit Windows PowerShell und Hyper-V

Basic: Eine Einführung in Hyper-V

HYPER-V ist die Virtualisierungstechnologie von Microsoft, bei der neben einzelnen Workstations auch ganze Server-Infrastrukturen innerhalb einer virtuellen Umgebung betrieben werden können. Ein nicht zu vernachlässigender Unterschied zu VMware besteht dabei in der Tatsache, dass es bei Hyper-V kein komfortables vCenter gibt, sondern stattdessen über PowerShell und Skripten bzw. Skriptbefehlen direkt administriert wird, wodurch ziemlich spezielle Vor- und Nachteile entstehen.

Fall 1: Das Stand-Alone Betriebsszenario ohne interne Abhängigkeiten:

Es gibt beliebig viele Hyper-V- Server, die nicht miteinander verbunden sind. a, es wäre hier sogar möglich, mit einem RCCMD Client und den passenden Skripten die gesamte Hyper-V – Umgebung herunterzufahren, aber es ist in dieser Konstellation nur bedingt empfehlenswert, da die Vertrauensstellung der Server untereinander sehr empfindlich reagiert, wenn man versucht, ein Skript von einem Node auf einem anderen auszuführen.



Sinnvoller ist es hier, auf jeden Hyper-V Node einen eigenen RCCMD – Client zu installieren, der die notwendigen Skripte dann mit lokalen Admin-Rechten direkt ausführt (Bei einem Failover-Cluster ändern sich hier die Spielregeln, dazu aber später noch einmal mehr).

Wenn man einen Hyper-V Server in seiner Standardkonfiguration lokal herunterfährt, werden die virtuellen Maschine angehalten, der jeweilige Betriebszustand gespeichert und danach der Hauptserver heruntergefahren. Nach dem Start werden die Betriebsdaten wieder geladen und der Server weiter ausgeführt. Ob Anhalten und Speichern funktioniert, hängt also davon ab, was in der virtuellen Maschine betrieben wird:

- Speicherabbilder können sehr groß werden

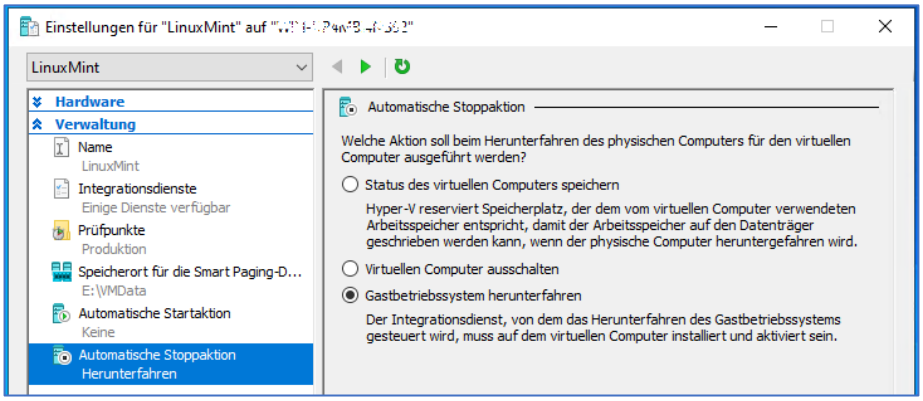
  Es könnte passieren, dass der vorhandene Speicherplatz auf dem Hauptserver gar nicht ausreicht, um die Betriebsdaten aller virtuellen Maschinen aufzunehmen.

- Programmbedingt geht das nicht

  Buchungssysteme, Rendering Systeme, Programme mit speziellen Shutdownroutinen, etc…. es gibt viele Anwendungen, die im Shutdownfall sauber ausgeschaltet und heruntergefahren werden müssen.

Sauberen Shutdown einleiten

Bekommt RCCMD die Anweisung von einem CS141 / BACS System, gibt es dem lokalen Computer zwar den Shutdown-Befehl, hat aber keinen Einfluss darauf, was mit den Maschinen passiert, wenn das Host-Betriebssystem die Shutdown-prozedur startet!



Sollten Sie die Windows PowerShell nicht installiert oder deaktiviert haben, können Sie die Shutdownkontrolle an den Hyper-V Manager übertragen, und dort einstellen, was geschehen soll, wenn der Server heruntergefahren wird:

Status des virtuellen Computers speichern

Im Fall eines Shutdowns wird ein vollständiges Speicherabbild erstellt. Prüfen Sie bitte zwei Dinge: Erstens, ob der Server überhaupt genug Speicher bereitstellen kann, und zweitens, ob generell die Programme innerhalb der virtuellen Maschine diese Funktion überhaupt unterstützen.

Virtuellen Computer ausschalten

Der klassische Hard-OFF auf die virtuelle Maschine, je nach Betriebssystem und Verwendung kann das zu unterschiedlichen Problemen führen

Gastbetriebssystem herunterfahren.

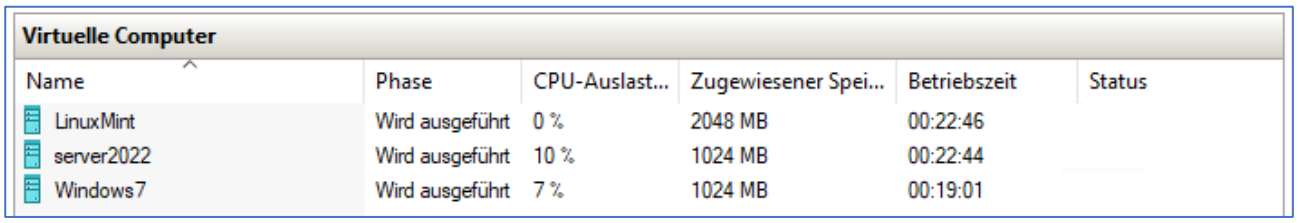
Das Betriebssystem innerhalb der virtuellen Maschine wird angewiesen sich selber herunterzufahren.

Fall 2: Interne Abhängigkeiten bei virtuellen Servern auf einem Hyper-V

Das ist prinzipiell die logische Erweiterung von Fall 1 – was ist, wenn auf einem Hyper-V – Node mehrere virtualisierte Systeme laufen, die eine gegenseitige Abhängigkeit haben oder eine spezielle Shutdownreihenfolge benötigen?

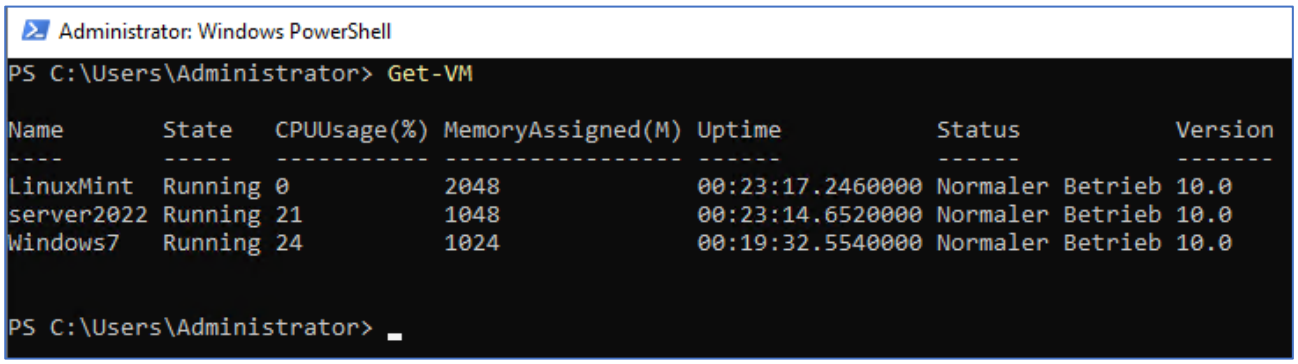
Jetzt zeigt sich der Unterschied zu VMware: Anstelle eines grafischen Verwaltungsmenüs wie es bei VMware verwendet wird, ist bei Hyper-V die WindowsPowerShell im Einsatz, um derartige Konfigurationen zu realisieren.

In diesem Beispiel laufen jetzt 3 virtuelle Systeme:

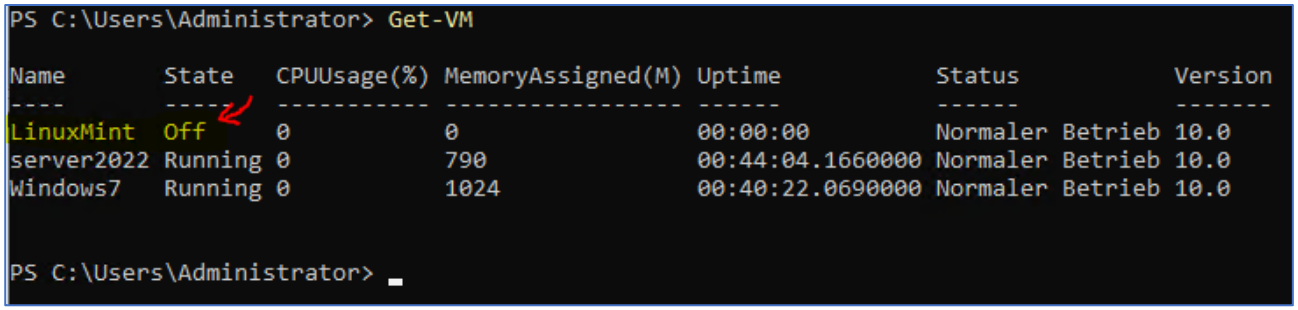


Wenn man den Hyper-V herunterfahren würde, würden alle 3 Betriebssysteme auf jeden Fall beendet werden. Zwei werden heruntergefahren, während Windows 7 „gespeichert und beendet“ wird. Als Benutzer macht die PowerShell einem dieses relativ einfach:

Mit dem Befehl **Get-VM** holt man sich zunächst einen Überblick aller aktuell laufenden virtuellen Maschinen:

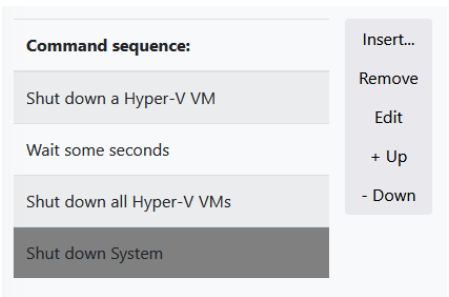


Die Maschinen lassen sich anschließend mit dem Befehl **Stop-VM [Name der Maschine]** herunterfahren:



Für die Realisierung des individuellen Shutdowns bietet RCCMD 3 Befehle, mit denen Sie einen struktruierten Server Shutdown umsetzen können:

- Shutdown a Hyper-V VM: Bennen Sie eine VM zum Heruterfahren
- Wait some seconds: Definieren Sie ein Zeitfenster bis zum nächsten Job
- Shutdown all Hyper-V VMs: Fahren Sie alle virtuellen Maschinen runter
- Shutdown System: Fahren Sie den Server herunter

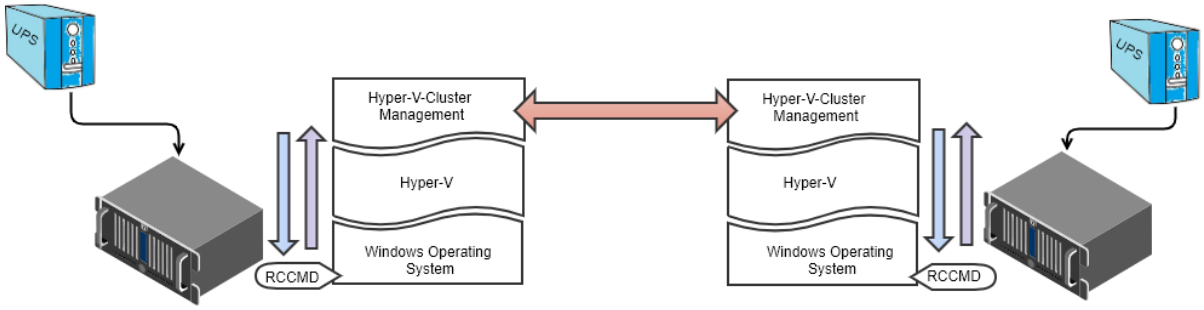


Mit der korrekten Sequenz und Zeitfenstern können Sie so alle virtuellen Maschinen strukturiert herunterfahren, und anschließend den Server ausschalten.

Einzige Bedingung: Windows PowerShell muss installiert und aktiviert sein.

Hyper-V mit Clustermanagement (PowerShell wird vorausgesetzt)

Die Kommunikation bei Hyper-V ist sehr strukturiert, so dass RCCMD ohne weitere Probleme betrieben werden kann:



Es wird immer zunächst die übergeordnete Instanz informiert und entsprechend auf die Freigabe gewartet. Das bedeutet bei einem Shutdown via RCCMD, dass das Betriebssystem den Shutdown bim Hyper-V ankündigt. Dieser organisiert das strukturierte herunterfahren von virtuellen Maschinen. Im Anschluss wird das Trägersystem heruntergefahren.

Sollte es einen Hyper-V-Cluster Manager geben, informiert Hyper-V zunächst diesen, welcher mit anderen Cluster Managern in Verbindung steht und die Migration von virtuellen Maschinen organisiert. Sind alle Maschinen auf einen anderen Server umgezogen, speichert ein Hyper-V anschließend die verbliebenen virtuellen Maschinen und fährt sie runter. Ist dies geschehen, wird das Trägersystem regulär heruntergefahren.

Geplantes vs. ungeplantes Failover – den simultanen Shutdown vorbereiten bei 2 Hosts

Schwieriger wird es, wenn man bei einem Powerfail beide Nodes (oder Hosts) herunterfahren will. Um die Schwierigkeit dahinter zu verstehen, muss man grob wissen, wie die Wanderung von virtuellen Maschinen zwischen zwei Nodes geschieht:

Bei zwei Nodes gibt es hier den Zugang zum VM-Speicher, die Kommunikation zwischen den Cluster-Nodes und einen Witness-Server, über den beide Nodes ausmachen, wer das sog. „Quorum“ innehat, also den aktuelleren Betriebszustand stellen wird.

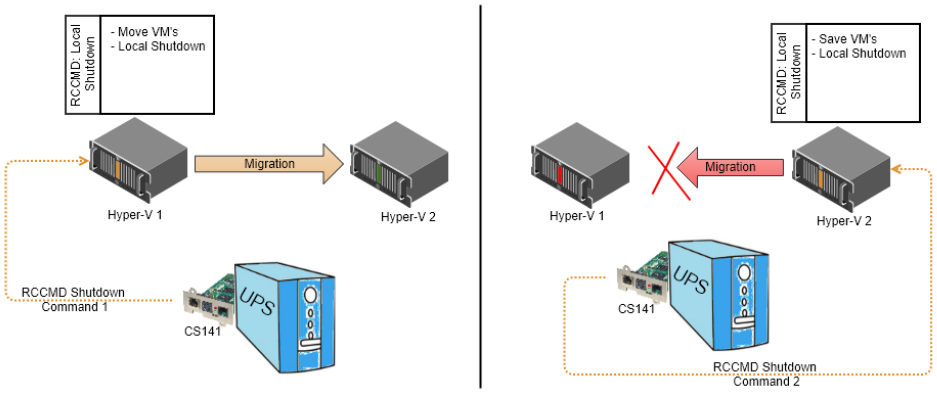
Bei einem Failover-Cluster wird in der Regel ein Primärserver konfiguriert, wo die VMs beheimatet laufen sollen, und einen Gast, auf dem diese ggfs. aktuell ausgeführt wird. Bei einem Failover-Cluster wird dabei die für den virtuellen Server zuständige VHD – Datei repliziert, an den eingetragenen Gast übertragen und regelmäßig mit aktuellen Betriebsdaten abgeglichen und aktualisiert, wobei der ausführende Node die Daten an seine eingetragenen Partner sendet:

- Bei einem geplanten FailOver (z.B. eine Life-Migration oder der Shutdown eines der beiden Nodes) wird dem Clustermanager genug Zeit eingeräumt, seine Betriebsdaten zu senden, und erst danach wird der Shutdown durchgeführt
- Bei einem ungeplanten FailOver wird von der letzten verfügbaren Aktualisierung ausgegangen, es kann also ggfs. zu einem gewissen Datenverlust gekommen sein.
- Wenn beide Nodes ungeplant „aus“ gehen, dann zählt laut Quorum letzte gespeicherte aktuelle Betriebszustand, der verfügbar ist.

Das Problem liegt hier im Detail versteckt:

Die Standard-Konfiguration eines FailOver-Clusters geht gar nicht davon aus, dass beide Nodes geplant herunterfahren. Bei einem geplanten Shutdown durch das Betriebssystems wird etwa 120 Sekunden angesetzt, bevor das Betriebssystem herunterfährt, um die Betriebsdaten zu aktualisieren und auf einem anderen Node die virtuelle Maschine zum Laufen zu bringen. Der Haken ist, dass bei zwei Nodes, die gleichzeitig *geplant* herunterfahren sollen, zwangsläufig ein Interessenkonflikt entstehen könnte: Node A wird versuchen, alle seine Maschinen und Betriebsdaten an Node B zu verschieben, und umgekehrt. Die Maschinen bleiben damit ggfs. unglücklich in der Schwebe hängen und werden dann entsprechend ruppig durch den Shutdown des Node-Betriebssystems abgewürgt. Je nach Größe und Komplexität gibt es hier nun unterschiedliche Verfahrensweisen:

Beispiel: Der ganz einfache Fall

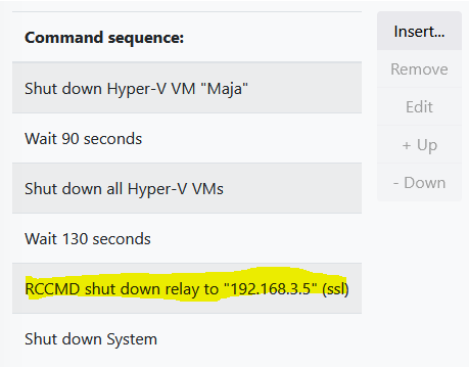


Im einfachen Fall sind es zwei Nodes, die einen Fail-Over-Cluster bilden, und beide Nodes könnten alle virtuellen Maschinen beherbergen (oder einzelne Maschinen sind vom Migrationsprozess ausgenommen). Wenn Sie PowerShell nicht installiert / aktiviert haben, fahren Sie die Nodes in sequenziell runter: Node A überträgt seine Daten an Node B, übergibt die virtuellen Maschinen und schaltet sich danach aus. Im Anschluss wird Node B feststellen, dass der Cluster zusammengefallen ist (Node A ist ja schon aus oder am Herunterfahren) und gar nicht versuchen, die virtuellen Maschinen zu migrieren. Die lokalen Hyper-V's übernehmen in dem Fall hier die lokale Shutdownroutine.

Empfehlenswerter ist hier jedoch der Shutdown via PowerShell:

Für die Realisierung des individuellen Shutdowns bietet RCCMD 3 Befehle, mit denen Sie einen strukturierten Server Shutdown umsetzen können:

- Shut down a Hyper-V VM: Bennen Sie eine VM zum Heruterfahren
- Wait some seconds*: Definieren Sie ein Zeitfenster bis zum nächsten Job
- Shut down all Hyper-V VMs: Fahren Sie alle virtuellen Maschinen runter
- Wait some seconds*: Zeitfenster für die virtuellen Maschinen.
- RCCMD shut down relay: Senden Sie den Shutdown an den 2. Node**
- Shutdown System: Fahren Sie den Server herunter



*Definieren Sie die Zeitfenster so, dass die virtuellen Maschinen genug Zeit haben, eigenständig herunterzufahren und auszuschalten. Ob die virtuellen Maschinen gespeichert oder heruntergefahren werden, legen Sie in den Eigenschaften der virtuellen Maschine fest.

**Auf dem zweiten Server benötigen Sie lediglich noch den Job Shut down System, da bereits alle virtuellen Maschinen sauber heruntergefahren wurden, und nur noch der Server herunterfahren muss.

Advanced: Eigene Hyper-V Befehle für das Herunterfahren von virtuellen Maschinen auf mehreren Nodes und Quorum erstellen

Wichtig: Für die folgenden Befehle ist die Installation / Aktivierung von PowerShell notwendig:

PowerShell hat sich als **zentrale Komponente** in der Microsoft-Umgebung etabliert und ist für Administratoren und Entwickler gleichermaßen unverzichtbar. Die **Automatisierung administrativer Aufgaben** durch Skripte ermöglicht eine effizientere und zeitsparendere Arbeitsweise. **PowerShell 7 / Core** erweitert die Möglichkeiten der Skripterstellung und -ausführung mit neuen Funktionen, die speziell auf die **Serveradministration** zugeschnitten sind. Die plattformübergreifende Verfügbarkeit und die Integration mit anderen Microsoft-Produkten machen PowerShell zu einem **universellen Tool** für die Automatisierung und Optimierung von IT-Prozessen.

Folgende Versionen sind derzeitig im Umlauf:

- **Windows Server 2012 R2:** PowerShell 3.0 ist vorinstalliert, jedoch nicht standardmäßig aktiviert.
- **Windows Server 2016:** PowerShell 5.1 ist standardmäßig installiert und aktiviert.
- **Windows Server 2019:** PowerShell 5.1 ist standardmäßig installiert und aktiviert.
- **Windows Server 2022:** PowerShell 7.0 ist standardmäßig installiert und aktiviert.

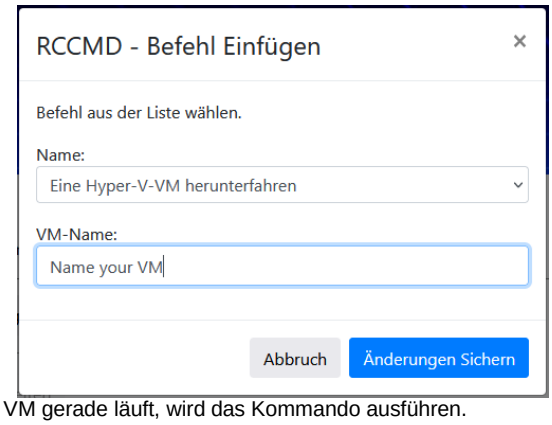
Hinweis:

- Windows Server 2012 und ältere Versionen enthalten keine standardmäßige Installation von PowerShell. Sie können PowerShell jedoch manuell auf diesen Systemen installieren.
- Die neueste Version von PowerShell kann jederzeit manuell auf jedem Windows-System installiert werden, unabhängig von der Serverversion.

Nachdem Sie PowerShell installiert haben, können Sie auf zwei spezielle Hyper-V – Befehle zurückgreifen, die RCCMD zur Verwaltung von virtuellen Maschinen innerhalb einer Hyper-V – Umgebung anbietet:

Eine spezifische Hyper-V VM herunterfahren

Mit diesem PowerShell-Befehl können Sie eine spezifische virtuelle Maschine herunterfahren. Im Eingabedialog wird hierzu der Name der virtuellen Maschine angegeben.



Hier gibt es zwei unterschiedliche Anwendungsfälle:

1. Lokaler Hyper-V

Der lokale Hyper-V Manager wird genau diese eine VM herunterfahren und beenden. Hierzu muss im

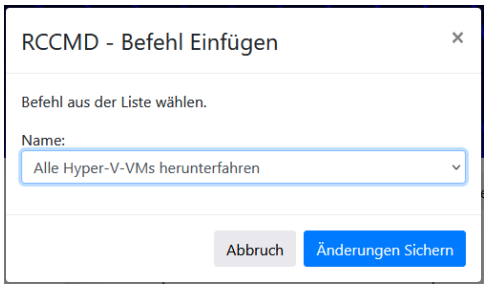
2. RCCMD ist auf dem Clustermanager installiert

Sollte sich RCCMD auf dem Clustermanager befinden, wird dieses Kommando an das Hyper-V Netzwerk übertragen, und der Node, auf dem die VM gerade läuft, wird das Kommando ausführen.

Wichtig: Sollte die virtuelle Maschine auf einen Node migrieren, der nicht Bestandteil dieses Clusters ist, wird die Maschine nicht mehr heruntergefahren, selbst wenn der Clustermanager weiß, wo sich aktuell die virtuelle Maschine aufhält.

Alle virtuellen Maschinen herunterfahren

Der Unterschied zu einer virtuellen Maschine ist, dass hier vom Hyper-V Manager eine Liste aller virtuellen Maschinen mit dem Status „running“ abgefragt wird und anschließend über das Kommando „stop-vm“ geziehlt heruntergefahren werden.



Auch hier gibt es wieder zwei Anwendungsmöglichkeiten:

1. Lokaler Hyper-V (Ohne Clustermanager!)

In diesem Fall werden alle lokal laufenden virtuellen Maschinen strukturiert heruntergefahren und die virtuelle Maschine ordnungsgemäß beendet.

2. Auf dem Clustermanager

Es wird vom Clustermanager alle virtuellen Maschinen angefordert, die den Status „running“ haben, mit dem Befehl stop-vm werden die virtuellen Maschinen im Cluster regulär heruntergefahren und die VMs beendet.

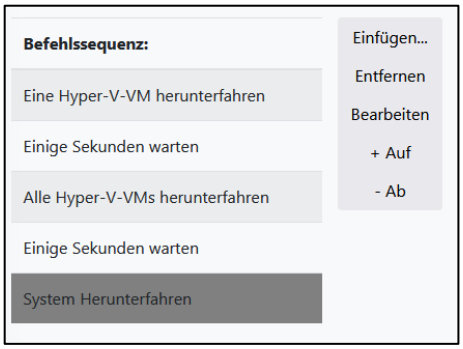
Tipp: Hyper-V funktioniert Kontext-Bezogen

Diese beiden Kommandos erlauben einen strukturierten Shutdown aller virtuellen Maschinen auf einem einem Hyper-V Server oder einem ganzen Hyper-V Cluster, was davon ausgeführt wird, hängt stark vom jeweiligen Kontext ab.

Shutdown Befehlssequenz mit RCCMD bei einem Hyper-V mit 3 virtuellen Maschinen

1. Bei einem Hyper-V Server

Bei dieser Konstellation wird auf jedem Windows Host ein eigener RCCMD Client benötigt. Der Shutdown wird dabei lokal getriggert, und die virtuellen Maschinen sollen heruntergefahren werden:



1. Eine Hyper-V-VM herunterfahren

Das wäre z.B. der Management Server, der vor dem Datenbankserver heruntergefahren werden muss. Geben Sie hierbei den Namen der virtuellen Maschine an, den Sie beim Anlegen gewählt haben.

2. Einige Sekunden warten

In diesem Beispiel wurden 90 Sekunden eingetragen. RCCMD wird also dem Betriebssystem 90 Sekunden einräumen, bevor der nächste Punkt in der Liste gestartet wird.

3. Alle Hyper-V-VMs herunterfahren

RCCMD fordert vom Hyper-V Manager eine Liste alle virtuellen Maschinen mit dem Status „Running“ ab und weist den Hyper-V-Manager an, die Betriebssysteme herunterzufahren.

4. Einige Sekunden warten

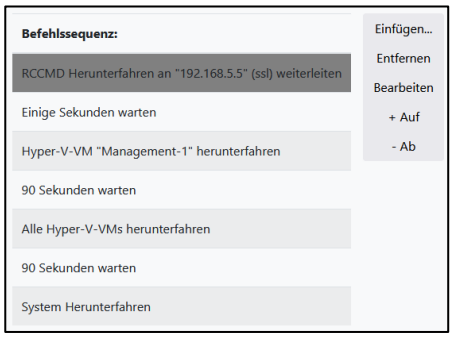
Geben Sie den Betriebssystemen Zeit, das Herunterfahren zu organisieren und die virtuellen Maschinen geordnet zu beenden.

5. System herunterfahren

Der Hyper-V Server wird heruntergefahren, und der Server schaltet sich aus. Beachten Sie bitte, dass dieser Befehl die virtuellen Maschinen hart abschaltet, die jetzt noch laufen. Planen Sie unter Punkt 5 ein entsprechend großes Zeitfenster mit ein.

Sollten Sie eine VM laufen haben, die eine spezielle Shutdownroutine benötigt

Leiten Sie als Vorbereitende Maßnahme das RCCMD Signal an das Betriebssystem der entsprechenden virtuellen Maschine direkt weiter, und verzögern den Shutdown um ein entsprechendes Zeitfenster. Den individuellen Shutdown konfigurieren Sie in dem Fall innerhalb des RCCMD Clients, an den Sie den Shutdown weitergeleitet haben.



Beachten Sie bitte, dass für diese Funktion auf dem Gastsystem ein RCCMD Client installiert sein muss.

In diesem Fall wird zuerst ein Gastsystem zum Herunterfahren angewiesen, bevor der oben beschriebene lokale Shutdown greift.

2. Bei einem Hyper-V Cluster mit mehreren Nodes und Clustermanager

Bei mehreren Nodes mit Clustermanager ist es wichtig, von wo die Shutdownbefehle kommen: Einfach Nodes in einem Cluster lokal herunterzufahren ist hier nicht empfehlenswert, weil es zu Datenverlust und Beschädigungen bei den auf dem Node laufenden virtuellen Maschinen und dem Betriebssystem kommen kann. Das Problem potenziert sich mit der Anzahl an Nodes, die einfach heruntergefahren werden. Hier empfiehlt es sich, über den Clustermanager zu gehen, der – anders als z.B. bei VMware – als Dienst auf jedem Node läuft: Man kann also von jedem Node, das Mitglied ist, einen strukturierten Cluster-Shutdown einleiten. Entscheidend ist also nicht, von welchem Node der Clustermanager seine Befehle bekommt, sondern in welcher Reihenfolge die Befehle gegeben werden:

1. Alle Hyper-V-VMs herunterfahren

```
Get-VM | Where-Object {$_.State -eq "Running"} | Stop-VM
```

Der Clustermanager fordert von den Nodes in diesem Cluster alle virtuellen Maschinen mit dem Status „running“ an und organisiert ein jeweils lokales herunterfahren.

2. Cluster-Zustand sichern:

```
Save-ClusterCheckpoint <Production_1>
```

Mit diesem Befehl wird der Zustand des Clusters gesichert und kann auf diese Weise später bei Bedarf wiederhergestellt werden.

3. Cluster Stop und local shutdown

```
Get-ClusterNode | Where-Object {$_.State -eq "Up"} | Stop-ClusterNode
```

Nachdem alle virtuellen Maschinen heruntergefahren sind, können Sie mit Cluster Stop den Hyper-V Cluster gefahrlos anhalten und die Nodes herunterfahren.

Tipp: Geladene Module beachten

Einige Befehle sind nur ausführbar, wenn die Windows PowerShell die jeweiligen Module installiert sind und geladen wurden.

So passen Sie die Shutdown.bat im RCCMD an:

Teil 1: Anlegen des ersten Hyper-V – Befehls:

1. Nutzen Sie in den RCCMD Shutdown-Optionen den Hyper-V – Befehl „Eine Hyper-V-VM herunterfahren“ und geben Sie unter VM-Name den Namen einer VM ein.

2. Ändern Sie die Sicherungen

3. Legen Sie noch den Job „Ein paar Sekunden warten“ an, und vergeben Sie z.B. 90 Sekunden.

4. Drücken Sie oben rechts auf Speichern, um Ihre Änderungen in die Batch-Datei in die Batch-Datei zu schrieben. Der Neustart von RCCMD ist in diesem Fall nicht notwendig, da Sie noch weitere Einstellungen vornehmen müssen.

5. Drücken Sie F5, um die Webanzeige zu aktualisieren.

Im Anschluss können Sie die Einstellungsdatei direkt im Webbrowser editieren, indem Sie auf „Datei bearbeiten“ klicken.

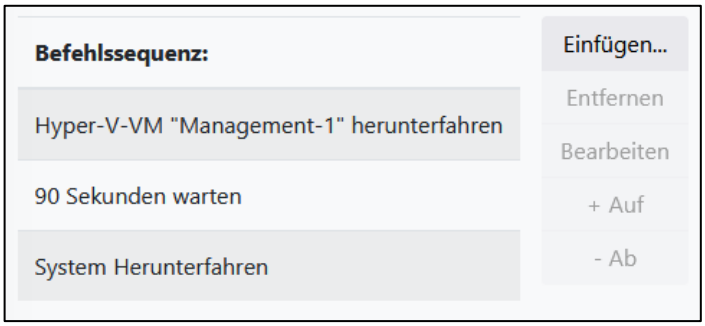
Teil 2: Anpassen Shutdownreihenfolge

Die Befehlssequenz sollte jetzt 3 Zeilen enthalten:

1. Hyper-V-VM „XXXX“ herunterfahren

2. 90 Sekunden warten

3. System herunterfahren



Diese Befehle werden in genau der Reihenfolge von oben nach unten ausgeführt. Wichtig ist zu wissen: Alles, was nach System Herunterfahren steht, kann nicht mehr ausgeführt werden, weil das lokale Betriebssystem herunterfährt. Drücken Sie anschließend auf Datei bearbeiten, und fügen Sie die gewünschten Befehle hinzu – die vorher eingegebenen Kommandos können als Blaupause dienen, um erweitert zu werden. Fügen Sie die benötigten Befehle einfach hinzu:

Beispiel 1: Hyper-V OHNE: Clustermanager

```
rem created by setup
@echo off
set path=%path%;C:\Program Files (x86)\RCCMD
@cls

PowerShell.exe Stop-VM "Management-Server-1"
gxSleep.exe 90
PowerShell.exe Stop-VM "Database-Server-1"
gxSleep.exe 90
PowerShell.exe Get-VM | Where-Object {$_.State -eq "Running"} | Stop-VM
gxSleep.exe 90
ExitWin.exe shutdown force
```

Abbruch | Änderungen Sichern

Die Befehlssequenz würde von oben nach unten in dieser Reihenfolge ausgeführt werden:

1. PowerShell.exe Stop-VM “Management-Server-1“ :	Der Management Server 1 wird heruntergefahren
2. gxSleep.exe 90	RCCMD wird 90 Sekunden warten
3. PowerShell.exe Stop-VM “Database-Server-1“	Der Database Server 1 wird heruntergefahren
4. gxSleep.exe 90	RCCMD wartet 90 Sekunden
5. PowerShell.exe Get-VM | Where-Object {$_.State -eq "Running"} | Stop-VM	Alle VM’s werden heruntergefahren, die noch als aktiv gekennzeichnet sind
6. gySleep.exe 90	RCCMD wartet 90 Sekunden
7. ExitWin.exe shutdown force	Der Host fährt runter

Beispiel 2: Hyper-V mit mehreren Nodes : und Clustermanager

Hier wären ein paar weiterführende Anpassungen notwendig:

```
rem created by setup
@echo off
set path=%path%;C:\Program Files (x86)\RCCMD
@cls

PowerShell.exe Stop-VM "Management-Server-1"
gxSleep.exe 90
PowerShell.exe Stop-VM "Database-Server-1"
gxSleep.exe 90
PowerShell.exe Get-VM | Where-Object {$_.State -eq "Running"} | Stop-VM
gxSleep.exe 180
PowerShell.exe Save-ClusterCheckpoint <Production_1>
gxSleep.exe 90
PowerShell.exe Get-ClusterNode | Where-Object {$_.State -eq "Up"} | Stop-ClusterNode
```

Abbruch | Änderungen Sichern

1. PowerShell.exe Stop-VM “Management-Server-1“ :	Der Management Server 1 wird heruntergefahren
2. gxSleep.exe 90	RCCMD wird 90 Sekunden warten
3. PowerShell.exe Stop-VM “Database-Server-1“	Der Database Server 1 wird heruntergefahren
4. gxSleep.exe 90	RCCMD wartet 90 Sekunden
5. PowerShell.exe Get-VM | Where-Object {$_.State -eq "Running"} | Stop-VM	Alle VM’s werden heruntergefahren, die noch als aktiv gekennzeichnet sind
6. gxSleep.exe 180	RCCMD wartet 180 Sekunden
7. PowerShell.exe Save-ClusterCheckpoint <Production_1>	Der aktuelle Zustand des Clusters „Production_1“ wird gespeichert.
8. gxSleep.exe 90	RCCMD wartet 90 Sekunden
9. PowerShell.exe Get-ClusterNode | Where-Object {$_.State -eq "Up"} | Stop-ClusterNode	Alle Nodes, die laufen, werden heruntergefahren. Das schließt den Node mit ein, über den die Befehle eingegeben wurden.

➔ **Der Befehl ExitWin.exe shutdown force entfällt, da über Stop-ClusterNode der Server heruntergefahren wird.**

Tipp: Zeitfenster planen

Diese Beispiele gehen von idealisierten Zeitfenster aus (gxSleep.exe) – Passen Sie die Zeitfenster an die jeweiligen Shutdownrealistäten an, um Probleme zu vermeiden.

Wichtige PowerShell Hyper-V Befehle:

1. Get-VM:	Zeigt alle virtuellen Maschinen auf dem Hyper-V-Server an.
2. Start-VM:	Startet eine virtuelle Maschine.
4. Stop-VM:	Fährt eine virtuelle Maschine herunter.
7. Save-VM:	Speichert den Status einer virtuellen Maschine.
8. Restore-VM:	Stellt den Status einer virtuellen Maschine aus einem Snapshot wieder her.
9. Export-VM:	Exportiert eine virtuelle Maschine in eine Datei.
10. Import-VM:	Importiert eine virtuelle Maschine aus einer Datei.

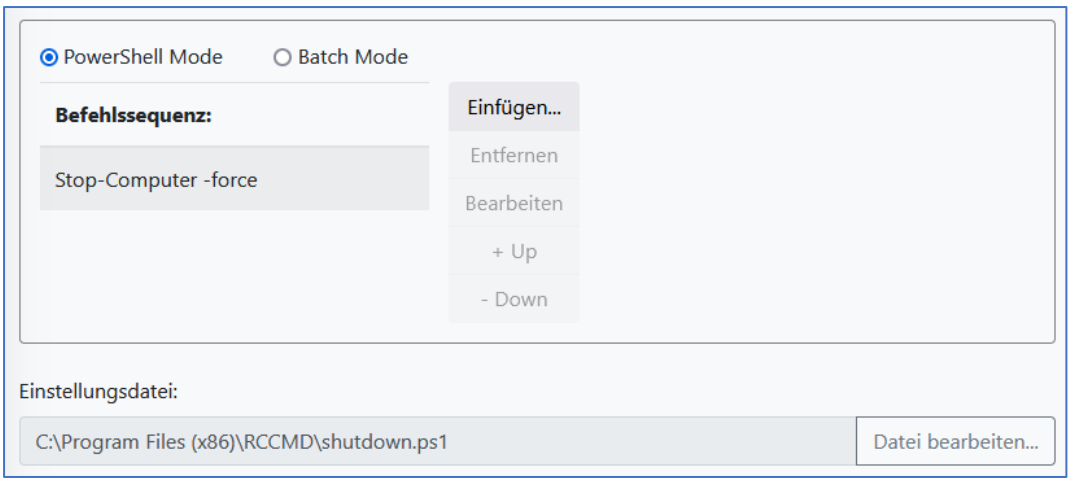
Wichtige Hyper-V Cluster-Manager Befehle in PowerShell:

1. Get-Cluster:	Zeigt Informationen zu allen Clustern im Failovercluster-Manager an.
2. Get-ClusterNode:	Zeigt Informationen zu allen Nodes in einem Cluster an.
3. Get-ClusterResource:	Zeigt Informationen zu allen Ressourcen in einem Cluster an.
4. Start-ClusterNode:	Startet einen Node in einem Cluster.
5. Stop-ClusterNode:	Fährt einen Node in einem Cluster herunter.
6. Stop-Cluster:	Hält einen Cluster an und migriert VMs auf andere Nodes.
7. Resume-Cluster:	Setzt ein angehaltenes Cluster fort.
9. Move-ClusterResource:	Verschiebt eine Ressource auf einen anderen Node im Cluster.

Skripting mit PowerShell unter RCCMD: Der Windows PowerShell- Mode

Diese Funktion ist bei RCCMD für Windows ab Version 4.57.12 240417 oder neuer verfügbar-

Unter „Herunterfahren Einstellungen“ können Sie ab der Version 4.57.x 240417 zwischen einem nativen PowerShell Modus* und dem Batch-Modus wählen:



**) Windows PowerShell vorausgesetzt, nur bei RCCMD für Windows*

Der Unterschied ist, dass an Stelle der „shutdown.bat“ (Batch Mode) das Skript „shutdown.ps1“ mit den notwendigen lokalen administrativen Freigaben gestartet wird – Befehle werden jetzt über die modernere Windows PowerShell direkt an das Betriebssystem gegeben, was zahlreiche Optionen ermöglicht, die innerhalb des Batchfiles mitunter nur sehr aufwändig realisiert werden können.

- Wie auch im Batch-Mode finden Sie unter „Einfügen“ vorgefertigte Modulbefehle, welche Sie direkt verwenden können, um das Betriebssystem herunterzufahren.
- Erfahrene Systemintegratoren finden mit „Datei bearbeiten“ einen schlanken Webeditor, mit der sie die shutdown.ps1 direkt an die jeweiligen Anwendungsszenarien anpassen können.

Tipp: Mischen von Batch-Dateien und PowerShell-Skripten

Wenn Sie PowerShell-Skripte und Batchfiles miteinander kombinieren möchten, empfehlen wir über den PowerShell-Mode zu gehen, da es sehr viel einfacher ist, eine Batchdatei als Subprozess in ein PowerShell-Skript zu integrieren. Ein Batch-File würde zwar auch ein PowerShell Skript starten, es ist sehr aufwändig, den Prozess hinterher zu überwachen.

Der Hauptunterschied zum Batch-Mode ist, dass die Windows PowerShell speziell für die Verwaltung von Servern ausgelegt ist, wodurch Sie nativ und transparent einen komplexen Serverstrukturen bei Problemen automatisiert verwalten und bei Bedarf strukturiert herunterfahren können.

Ich lese immer wieder Java in Verbindung mit RCCMD – ist das denn überhaupt sicher?

Berechtigte Fragen – Ja, für interne Prozesse verwendet der integrierte Webserver eine spezielle Java Runtime Umgebungen. Man muss hier jedoch wie in vielen Fällen im IT-Bereich differenzieren, denn „Java" ist nicht gleichzusetzen mit dem „dem unsicheren Java aus der Presse" oder „dem lizenzkostenpfichtigen Java" .

Was genau benutzt RCCMD?

Das Webinterface von RCCMD verwendet eine Java Runtime Envirommemt (JRE) für bestimmte **interne** Prozesse – es gibt keine Möglichkeit, „von außen" auf diese internen Prozesse zu gelangen, um alternative Prozesse zu starten, ausgenommen natürlich grobe Fahrlässigkeit wie das Behalten der Standardpassworten …

Sind Lizenzgebühren wegen der Verwendung von Java fällig?

Nein, die Java Runtime Environment hat aktuell nichts mit dem zu tun, was Sie unter „Java.com" herunterladen und installieren können. und wofür Unternehmen Lizenzgebühren bezahlen müssen. RCCMD bringt Out-Of-The-Box alles mit, was Sie für den sicheren Betrieb benötigen.

Mein Security Programm zeigt den Hinweis, „dass eine veraltete Java-Version gefunden wurde mit dem Vermerk eines „potenziellen Sicherheitsrisikos".

Viele meist günstige Security-Programme degradieren standardmäßig ältere Software zu einer potentiellen Schwachstelle - und ignorieren neben dem Einsatzgebiet dieser Software z.B. auch, ob ein Entwicklerteam bei GENEREX spezielle Anpassungen vorgenommen hat, um professionelle Software wie RCCMD abzusichern – Experten schätzen Betriebsstabilität und höchste Sicherheitsstandards: Die neueste Programmversion ist nicht immer die beste Wahl, wenn es um Stabilität und Leistungsfähigkeit geht, ganz zu schweigen von innovativen neuen Sicherheitsproblemen, die vorher gar nicht existierten. Aus diesem Grund findet Screening Software die (zumindest als diese FAQ entstanden sind) Version 11, und beschwert sich, dass es keine Version 18 ist.

Kann ich eine Liste bekommen mit den Modulen, die Ihre JRE benutzt?

Nein (und da diskutieren wir auch nicht…). Was wir Ihnen anbieten können, ist, dass Sie uns einen Auszug Ihres Security-Audits zukommen lassen, und dann können wir Ihnen genau erklären, was Ihr Security Scanner da gefunden hat. Wenden Sie sich hierzu einfach an Support@generex.de

Glossar – wichtige Abkürzungen

- **RCCMD:** Remote Control and Command, ein Softwaretool zur Fernverwaltung und Abschaltung von Computern und Servern.
- **VM:** Virtuelle Maschine.
- **ESXi:** VMware ESXi, ein Hypervisor für die Virtualisierung von Servern.
- **OVA:** Open Virtual Appliance, ein Format für virtuelle Maschinen, das von vielen Anbietern unterstützt wird.
- **vCenter:** VMware vCenter, ein Tool zur Verwaltung von virtuellen Maschinen in einer VMware-Umgebung.
- **HA:** High Availability, ein Verfahren zur Sicherstellung der Verfügbarkeit von Servern im Falle eines Ausfalls.
- **DHCP:** Dynamic Host Configuration Protocol, ein Protokoll zur automatischen Vergabe von IP-Adressen an Computer in einem Netzwerk.
- **DNS:** Domain Name System, ein System zur Übersetzung von Domainnamen in IP-Adressen.
- **TLS:** Transport Layer Security, ein Protokoll zur Verschlüsselung von Daten im Internet.
- **HTTP:** Hypertext Transfer Protocol, ein Protokoll zur Übertragung von Webinhalten.
- **IP:** Internet Protocol, ein Protokoll zur Adressierung von Computern in einem Netzwerk.
- **GUI:** Graphical User Interface, eine grafische Benutzeroberfläche.
- **CLI:** Command Line Interface, eine Befehlszeilenoberfläche.
- **SSH:** Secure Shell, ein Protokoll zur sicheren Fernverwaltung von Computern.
- **VMA:** Virtual Media Assistant, ein Tool von VMware zum Verwalten von virtuellen Medien.
- **IPv4:** Internet Protocol Version 4, ein Protokoll zur Adressierung von Computern in einem Netzwerk.
- **IPv6:** Internet Protocol Version 6, ein neues Protokoll zur Adressierung von Computern in einem Netzwerk.
- **vSAN:** Virtual SAN, ein Software-defined Storage-System von VMware.
- **RAID:** Redundant Array of Independent Disks, ein Verfahren zur Erhöhung der Datensicherheit und -verfügbarkeit durch die Verwendung mehrerer Festplatten.
- **NFS:** Network File System, ein Protokoll zur Freigabe von Dateien und Verzeichnissen über ein Netzwerk.
- **iSCSI:** Internet Small Computer System Interface, ein Protokoll zur Speicherung von Daten auf einem Server über ein Netzwerk.
- **USB:** Universal Serial Bus, ein Standard für den Anschluss von Geräten an Computer.
- **PCI:** Peripheral Component Interconnect, ein Busstandard für den Anschluss von Geräten an Computer.
- **BIOS:** Basic Input/Output System, ein Softwareprogramm, das bei jedem Start eines Computers ausgeführt wird.
- **UEFI:** Unified Extensible Firmware Interface, ein neues BIOS-Standard.
- **MBR:** Master Boot Record, ein Bootloader auf Festplatten im MBR-Partitionsstil.
- **GPT:** GUID Partition Table, ein neuer Partitionsstil für Festplatten.
- **PKS-1:** Public Key Cryptography Standard 1, ein asymmetrisches Verschlüsselungsverfahren.
- **PKS-8:** Public Key Cryptography Standard 8, ein Format für die Speicherung von privaten Schlüsseln.
- **CS141:** Ein von GENEREX hergestellter vollqualifizierter Webmanager. Dient als RCCMD Server für den RCCMD Client.
- **BACS: B**attery **A**nalyse **a**nd **C**are **S**ystem: Ein von GENEREX hergestelltes vollqualifiziertes und skalierbares aktives Batteriemanagementsystem. Ein BACS WEBMANAGER erfüllt auch die Funktion eines RCCMD Servers für RCCMD Steuersignale.
- **Hyper-V**: Eine von Microsoft entwickelte freie Virtualisierungsplatform, welche innerhalb eines Microsoft Windows Betriebssystems verfügbar ist. Hyper-V kann über die Features bei Bedarf nachinstalliert werden und beliebige Betriebssysteme virtualisieren.
- **MAC-OS:** Ein von Apple entwickeltes und vertriebenes Betriebssystem. Läuft üblicherweise nur auf einem Apple-Computer.

Urheberrechts-Erklärung zum geistigen Eigentum und Umgang mit vertraulichen Informationen

Die Informationen in diesem Benutzerhandbuch sind nicht bedingte Anweisungen und können ohne Ankündigung verändert werden. Obwohl GENEREX versucht hat, präzise Informationen in diesem Dokument bereitzustellen, übernimmt GENEREX keine Verantwortung für die Genauigkeit dieser Informationen.

GENEREX ist nicht verantwortlich für jeden indirekten, speziellen, daraus folgenden oder unbeabsichtigten Schaden, ohne Einschränkungen, verlorener Gewinne oder Einkommen, Kosten von Austausch Gütern, Verlust oder Beschädigung von Daten, die sich durch den Gebrauch dieses Dokumentes oder das hier beschriebenen Produkt ergeben.

GENEREX als Hersteller der genannten Produkte, übernimmt keine Verpflichtungen mit diesen Informationen. Die Produkte, die in diesem Handbuch beschrieben werden, wurden auf der alleinigen Basis von Informationen für Geschäftspartner gegeben, damit diese ein besseres Verständnis für die GENEREX Produkte erhalten.

GENEREX erlaubt seinen Geschäftspartnern die Informationen, die in diesem Dokument enthalten sind, an Dritte weiterzugeben, ebenso an das Personal in deren Firma oder ihren eigenen Kunden, elektronisch, manuell, in Form von Fotokopien oder Ähnlichem. GENEREX gibt an, dass der Inhalt nicht verändert oder angepasst werden darf, ohne schriftliche Genehmigung von GENEREX.

Alle Rechte, Titel und Interessen am GENEREX Markenzeichen BACS oder Firmenzeichen (registriert oder nicht registriert) oder der Geschäftswert bzw. das geistige Eigentum von GENEREX, das Urheberrecht und die Produkt-Patente sind exklusiv und ohne Einschränkungen im Eigentum von GENEREX.

GENEREX wird jede Beanstandung über den Inhalt dieses Dokumentes zeitnah abwickeln. Kommentare oder Beanstandungen zu diesem Dokument sollten an die GENEREX Systems Vertriebsgesellschaft mbH adressiert werden.

Das Urheberrecht der Europäischen Union ist gültig (Copyright EU).

Urheberrecht und Lizenzen

Die Copyright-Autorisierung von GENEREX und anderen relevanten Softwareanbietern muss respektiert werden.
GENEREX und ihre Lieferanten behalten sich die Rechte an den Softwarekomponenten vor.
Insbesondere sind verboten:

Kopieren und Verteilen, Modifikationen und Ableitungen, Dekompilieren, Reverse Engineering.
Komponenten, die unter die GNU General Public License und weitere Open Source Lizenzen fallen, sind in die Software integriert.

Eine Übersicht über die integrierten Open Source-Komponenten und eine Kopie der aktuellen Lizenz erhalten Sie unter www.generex.de/legal/sla.

GENEREX wird den Quellcode für alle Komponenten von Software bereitstellen, die unter der GNU General Public License und vergleichbaren Open Source-Lizenzen lizenziert sind.

Für Quellcode-Anfragen senden Sie bitte eine E-Mail an info@generex.de