

Installationsanleitung
Online USV mit SNMP Modul
auf
VMware vSphere ESXi 4.1 und 5.0
(Außer kostenlos lizenziertem ESXi Server!)

Version 1.2.3 Stand 26.11.2011

Autor:



Hr. Jörg Seibicke

Lion Hard Systems GmbH
Mannesmannstr. 13
58455 Witten

www.lion-hard-systems.de

Herausgeber:



ONLINE USV-Systeme AG
Dreimühlenstrasse 4
80469 München

www.online-usv.de

Die Texte und Abbildungen wurden mit größter Sorgfalt zusammengestellt. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Autor und Herausgeber können für fehlerhafte Angaben und deren Folgen keine Haftung übernehmen.

Für Verbesserungsvorschläge und Hinweise auf Fehler sind wir dankbar.

Autor und Herausgeber freuen sich über Ihr Interesse und stellen diese Anleitung gerne zur Verfügung. Um jedoch Missverständnisse zu vermeiden, bitten wir diese Anleitung nur im Gesamten und nicht auszugsweise zu verwenden.

Fast alle Hardware- und Software-Bezeichnungen, die in dieser Dokumentation erwähnt werden, sind gleichzeitig auch eingetragene Warenzeichen oder sollten als solche betrachtet werden.

Inhaltsverzeichnis

Inhaltsverzeichnis	3
Vorwort	5
Wie ist diese Anleitung aufgebaut?	6
Konventionen	6
1 Einbau des SNMP Moduls CS121 in die USV	7
1.1 Dip Schalter Einstellungen	7
2 Flashen der aktuellen Firmware auf das SNMP Modul CS121	8
2.1 Firmware Download.....	8
2.2 Firmware Flashen.....	9
3 Konfiguration des SNMP Moduls CS121	12
3.1 Anmeldung an das SNMP Modul	13
3.2 Einstellung der verwendeten USV	14
3.3 IP-Einstellung	16
3.4 Einstellen der RCCMD Clients auf dem SNMP Modul.....	17
3.5 Speichern der Einstellungen.....	22
3.6 Zurücksetzen der Dip Schalter und Neustart.....	22
4 Konfiguration VMware ESXi	23
4.1 Voraussetzungen.....	23
4.2 Download der benötigten Komponenten	23
4.2.1 RCCMD Client für VMware ESXi (vMA 4.1).....	23
4.2.2 Putty (SSH Client).....	27
4.2.3 WinSCP (SFTP Client).....	28
4.2.4 vMA 4.1 (virtuelle Appliance)	30
4.3 vMA 4.1 installieren	33
4.3.1 Voraussetzungen für eine Installation	33
4.3.2 Installation der vMA 4.1 auf ESXi	34
4.3.3 Konfiguration der vMA 4.1 auf ESXi	40
4.4 Kopieren von rccmdinst.tar mit dem Programm WinSCP	49
4.5 Putty starten und konfigurieren.....	52
4.6 Installation des RCCMD Clients auf vMA 4.1	56
4.7 Konfiguration des installierten RCCMD Clients auf vMA 4.1	64
4.8 Setzen der virtuellen Maschinen auf Autostart	72

5	Konfiguration der Windows-Gäste	74
5.1	Voraussetzungen.....	74
5.2	Download des RCCMD-Clients für Windows.....	74
5.3	Installation des RCCMD-Clients auf Windows 2003 Server	76
6	Testlauf.....	84
	Schlußwort.....	86
	Quellen	86

Vorwort

Jeder, der sich mit Virtualisierung und VMware beschäftigt, kennt das Problem: Wie sichere ich meine VMware gegen Stromausfall ab und wie fahre ich mein System bei Stromausfall komplett und ohne Probleme herunter?

Die Lösung heißt RCCMD von Online!

Im Nachfolgenden beschreibe ich die Installation eines Online-USV-Systems auf VMware ESXi mit Hilfe eines passenden SNMP-Moduls und der dazu gehörigen RCCMD-Clients. Mein Anliegen hierbei ist es, den Vorgang so einfach wie möglich und vor allem nachvollziehbar zu beschreiben.

Als Grundlage dieser Anleitung diente ein CS121SNMP-Einbaumodul und eine Online XANTO RS 1000 USV. Da der ESXi keine Konsole hat, bediene ich mich im Laufe dieser Installation ersatzweise der vSphere Management Assistant VM, die stellvertretend den Shutdown des ESXi ausführt.

Mit dieser Anleitung sollte es für einen geübten und erfahrenen Systemintegrator möglich sein, die Hard- und Software in etwa einer Stunde zu konfigurieren.

Ich hoffe, dass diese Anleitung zum besseren Verständnis dieses innovativen USV-Systems beiträgt.

Jörg Seibicke

Geschäftsführer

VMware Certified Professional für Virtual Infrastructure 3, vSphere 4 und vSphere 5



Lion Hard Systems GmbH

Mannesmannstr. 13

58455 Witten

Wie ist diese Anleitung aufgebaut?

Diese Anleitung ist eine „Schritt für Schritt“-Dokumentation. Jedes folgende Kapitel baut auf dem vorherigen auf.

Benötigte Dateien und Programme werden in dieser Anleitung als Internetdownload beschrieben. Die Programme für Ihre Online USV finden Sie auch auf der mitgelieferten Installations-CD.

Konventionen

Fettdruck

Fettdruck wird verwendet, um Text anzuzeigen, den Sie eingeben.



Return-Taste Ihres Computers.



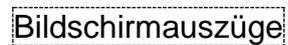
Leerzeichen eingeben.



Buttons sind mit einem schattierten Rahmen versehen.

Kursivdruck

Kommentare und Anmerkungen.



Bildschirmansichten sind mit einem gestricheltem Rahmen versehen.

1 Einbau des SNMP Moduls CS121 in die USV



Abbildung 1-1 CS 121 SNMP Einbaumodul

Bevor Sie das SNMP Modul (Artikelbezeichnung bei Online = DW7SNMP30 oder DW5SNMP30) in den dafür vorgesehenen Slot der USV stecken, muss dieses konfiguriert werden. Dazu müssen Sie den ersten Dip Schalter (Abbildung 1-3 Konfigurationsmodus) auf OFF stellen, um das SNMP Modul in den Konfigurationsmodus zu nehmen.

1.1 Dip Schalter Einstellungen

Dip Schalter 1	Dip Schalter 2	Beschreibung
ON	OFF	Normaler Betriebsmodus
OFF	OFF	Konfigurationsmodus



Abbildung 1-2 Normaler Betriebsmodus



Abbildung 1-3 Konfigurationsmodus

Nach dem Umschalten in den Konfigurationsmodus stecken Sie das SNMP Modul in den dafür vorgesehenen Slot Ihrer USV.

2 Flashen der aktuellen Firmware auf das SNMP Modul CS121

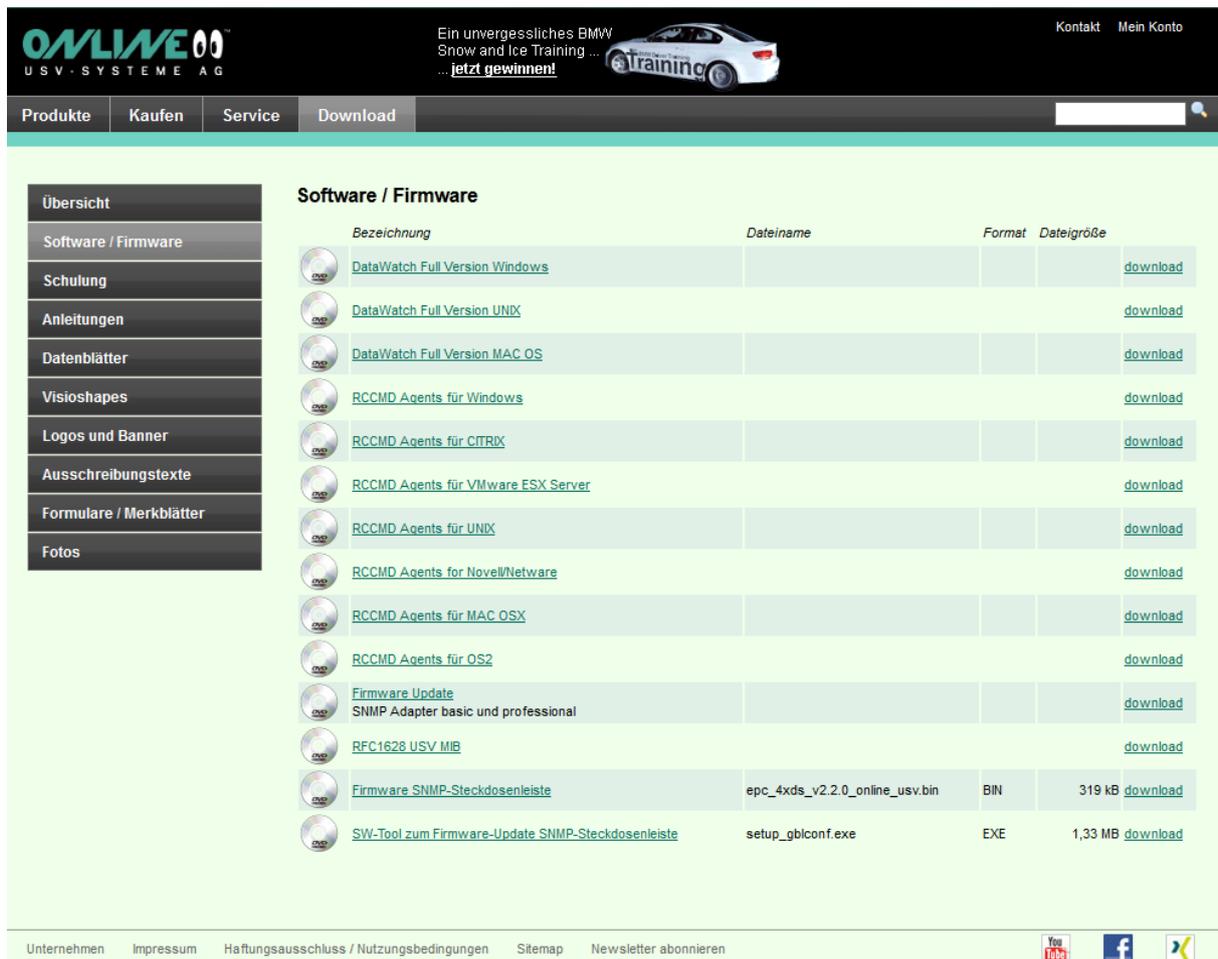
2.1 Firmware Download

Vor der Installation sollten Sie immer die aktuellste Firmware auf das SNMP Modul installieren.

Die neueste Firmware Version finden Sie unter folgendem Link:

<http://www.online-usv.de/de/download/softwarefirmware.php>

Bitte den Punkt „DataWatch Updates und Patches“ danach „Firmware Update“ und noch einmal „Firmware Update“ auswählen.



Ein unvergessliches BMW Snow and Ice Training ...
... **jetzt gewinnen!**

Kontakt Mein Konto

Produkte Kaufen Service Download

Übersicht
Software / Firmware
Schulung
Anleitungen
Datenblätter
Visioshapes
Logos und Banner
Ausschreibungstexte
Formulare / Merkblätter
Fotos

Software / Firmware

Bezeichnung	Dateiname	Format	Dateigröße
DataWatch Full Version Windows			download
DataWatch Full Version UNIX			download
DataWatch Full Version MAC OS			download
RCCMD Agents für Windows			download
RCCMD Agents für CITRIX			download
RCCMD Agents für VMware ESX Server			download
RCCMD Agents für UNIX			download
RCCMD Agents for Novell/Netware			download
RCCMD Agents für MAC OSX			download
RCCMD Agents für OS2			download
Firmware Update SNMP Adapter basic und professional			download
RFC1628 USV MIB			download
Firmware SNMP-Steckdosenleiste	epc_4xds_v2.2.0_online_usv.bin	BIN	319 kB download
SW-Tool zum Firmware-Update SNMP-Steckdosenleiste	setup_gblconf.exe	EXE	1,33 MB download

Unternehmen Impressum Haftungsausschluss / Nutzungsbedingungen Sitemap Newsletter abonnieren

Abbildung 2-1

Nach dem Download entpacken Sie das Archiv und führen das Setup (Abbildung 2-2) aus.

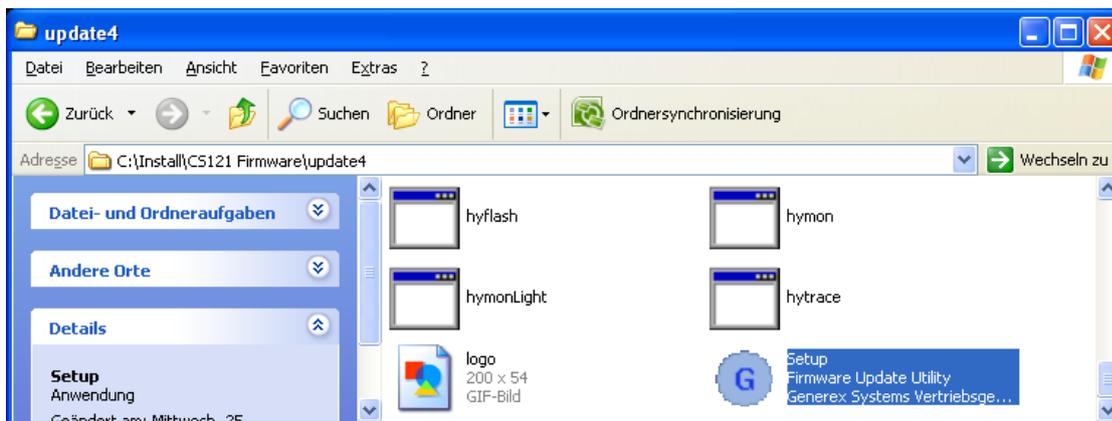


Abbildung 2-2

2.2 Firmware Flashen

Die Default IP Adresse der USV ist **10.10.10.10**.

Klicken Sie auf **Check device** und nach erfolgreicher Prüfung auf **Weiter >**.

Hinweis: Standard Passwort ist „cs121-snmp“.

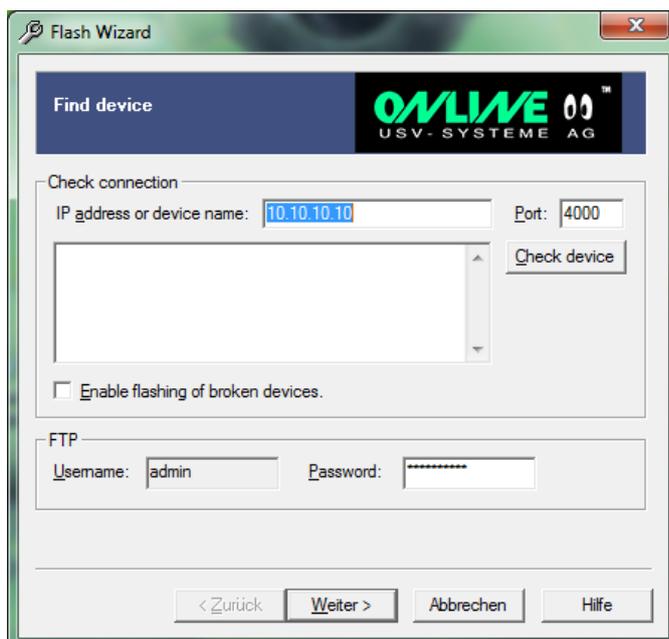


Abbildung 2-3

Bestätigen Sie im folgenden Bildschirm die Informationen über die MAC-Adresse, etc. und klicken auf **Weiter >**

Anschließend zeigt Ihnen der Bildschirm den identifizierten SNMP-Adapter, bestätigen Sie dies mit einem Klick auf **Weiter >**.

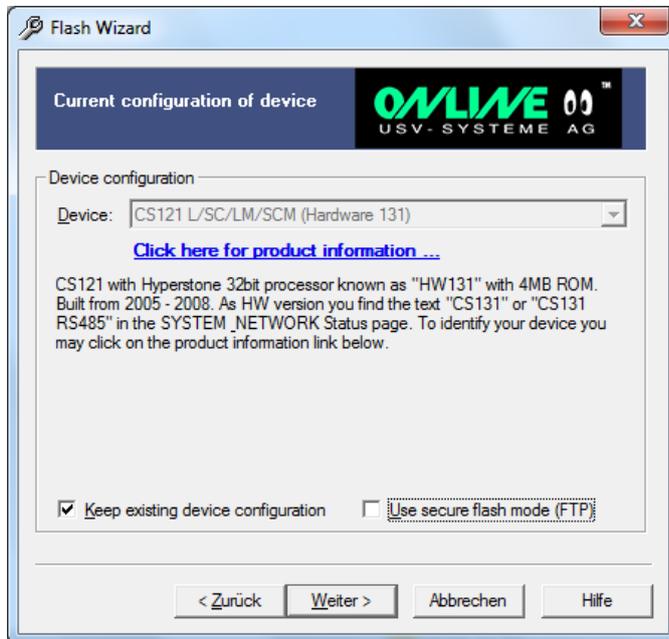


Abbildung 2-4

Bestätigen Sie Ihre Auswahl mit **Weiter >**

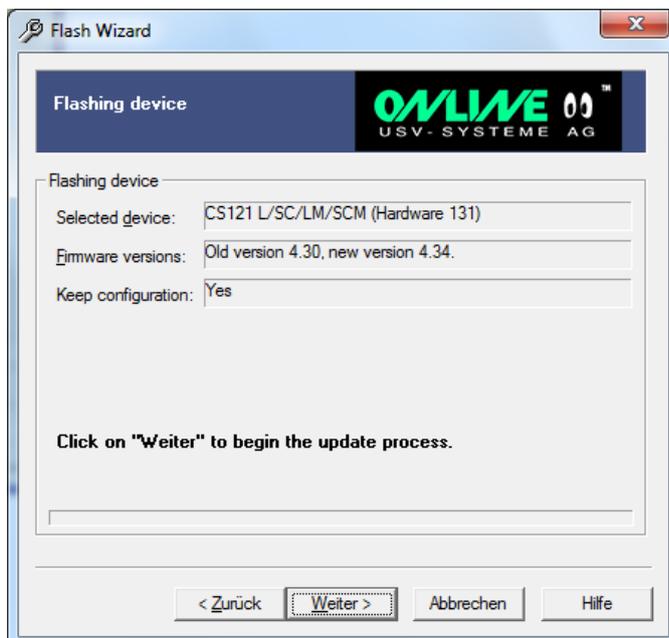


Abbildung 2-5

und klicken anschließend auf **OK**.

Schalten Sie die USV und den PC nicht aus und warten Sie bis das Update abgeschlossen ist!

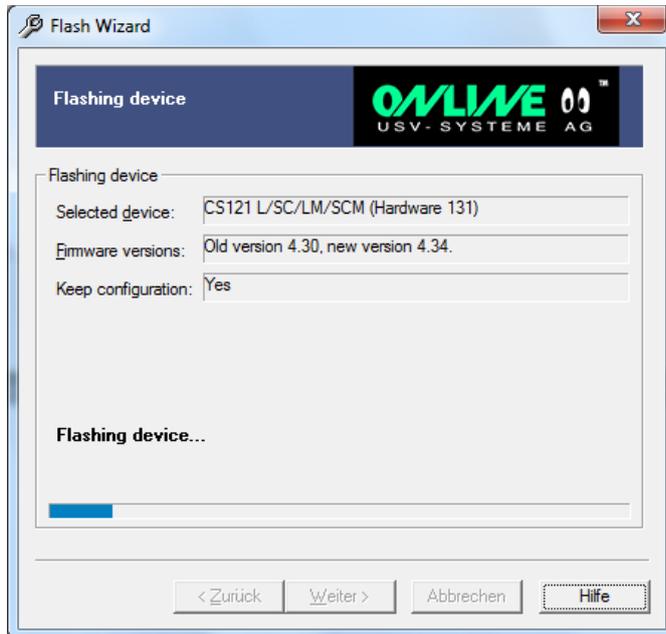


Abbildung 2-6

Abschließend warten Sie den Countdown ab und klicken dann auf **Fertig stellen**. Das SNMP Modul kann nun konfiguriert werden.

Bitte vor Ablauf des Countdown nicht das Fenster schließen.



Abbildung 2-7

3 Konfiguration des SNMP Moduls CS121

Die Konfiguration erfolgt über den integrierten Web-Server der USV. Öffnen Sie dafür auf einem an Ihr Netzwerk angeschlossenen PC einen Browser und geben als Adresse <http://10.10.10.10> ein.

Beachten Sie, dass der Web-Server auf dem SNMP Modul erst etwa zwei Minuten nach dem Einschalten der USV erreichbar sein wird. Sie sollten nun die Startseite der USV sehen (Abbildung 3-1).

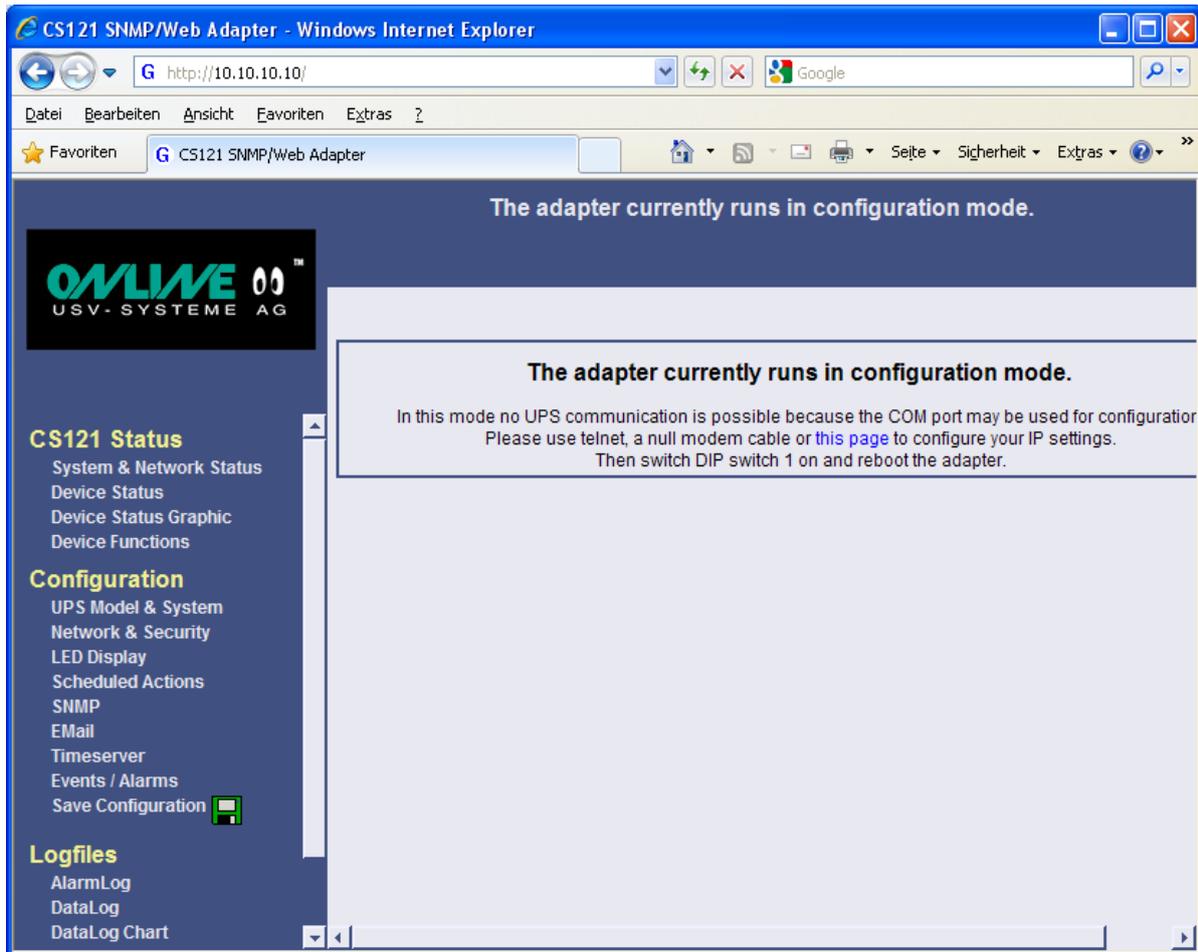


Abbildung 3-1

Klicken Sie nun den Menüpunkt **UPS Model & System** an.

3.1 Anmeldung an das SNMP Modul

Bei der ersten Auswahl eines Konfigurationspunktes erscheint zunächst die Anmeldemaske des SNMP Moduls (Abbildung 3-2).

Als Benutzernamen geben Sie **admin** und als Kennwort **cs121-snmp** ein.

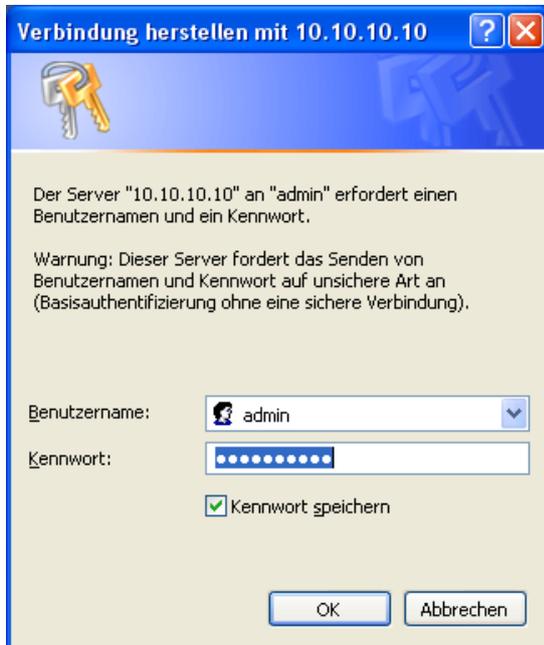


Abbildung 3-2

3.2 Einstellung der verwendeten USV

Nach erfolgreicher Anmeldung sollten Sie nun den Dialog **UPS Model & System Settings** sehen (Abbildung 3-3).

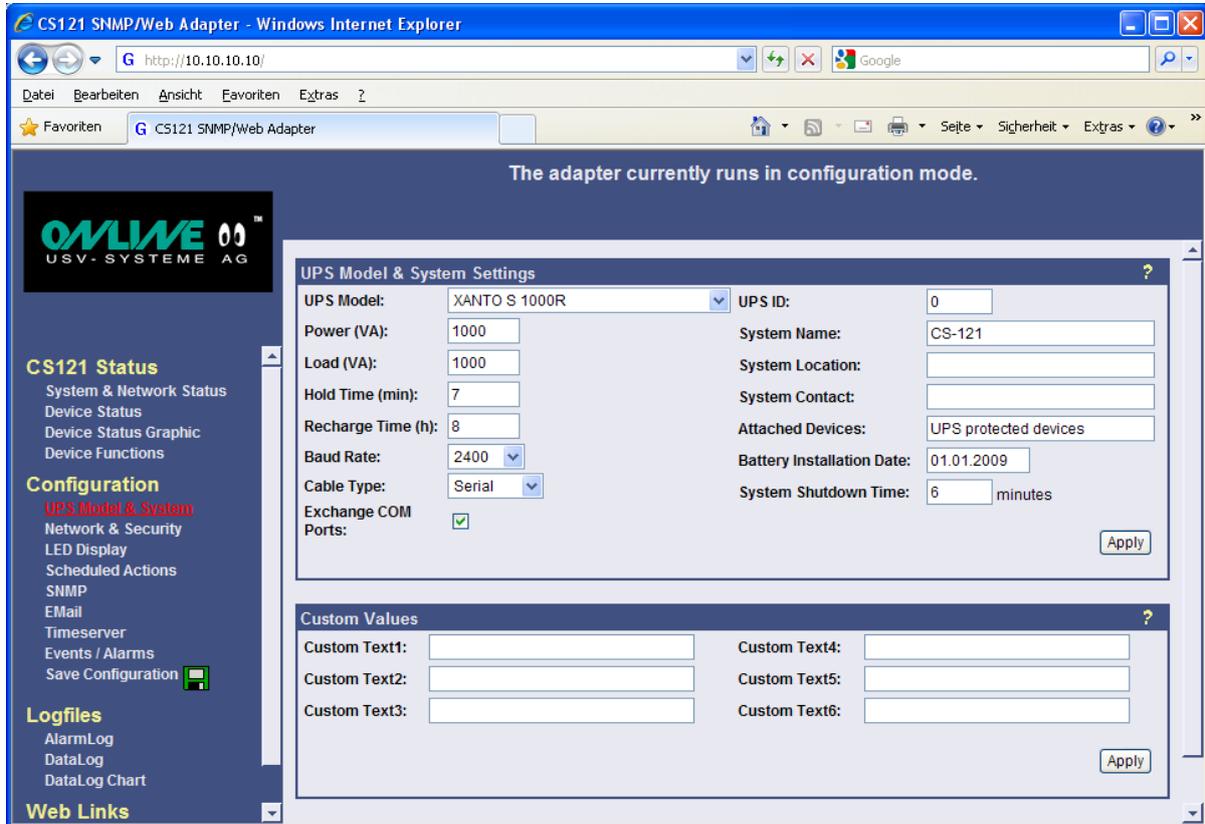


Abbildung 3-3

Hier wählen Sie bei **UPS Model:** Ihren verwendeten UPS Typen aus (Abbildung 3-4).

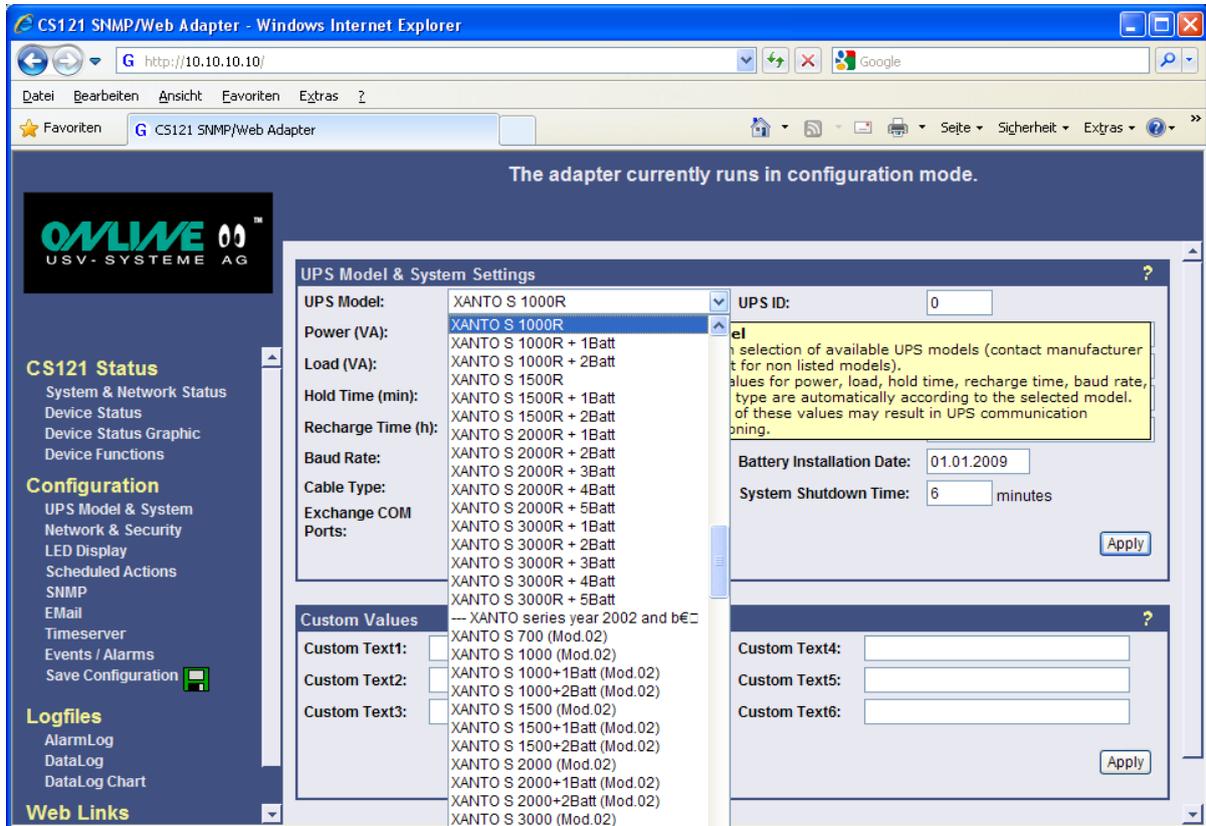


Abbildung 3-4

Klicken Sie anschließend auf **Apply**.

3.3 IP-Einstellung

Klicken Sie nun den nächsten Menüpunkt **Network & Security** an. Der Dialog **Network & Security Settings** wird aufgerufen (Abbildung 3-5).

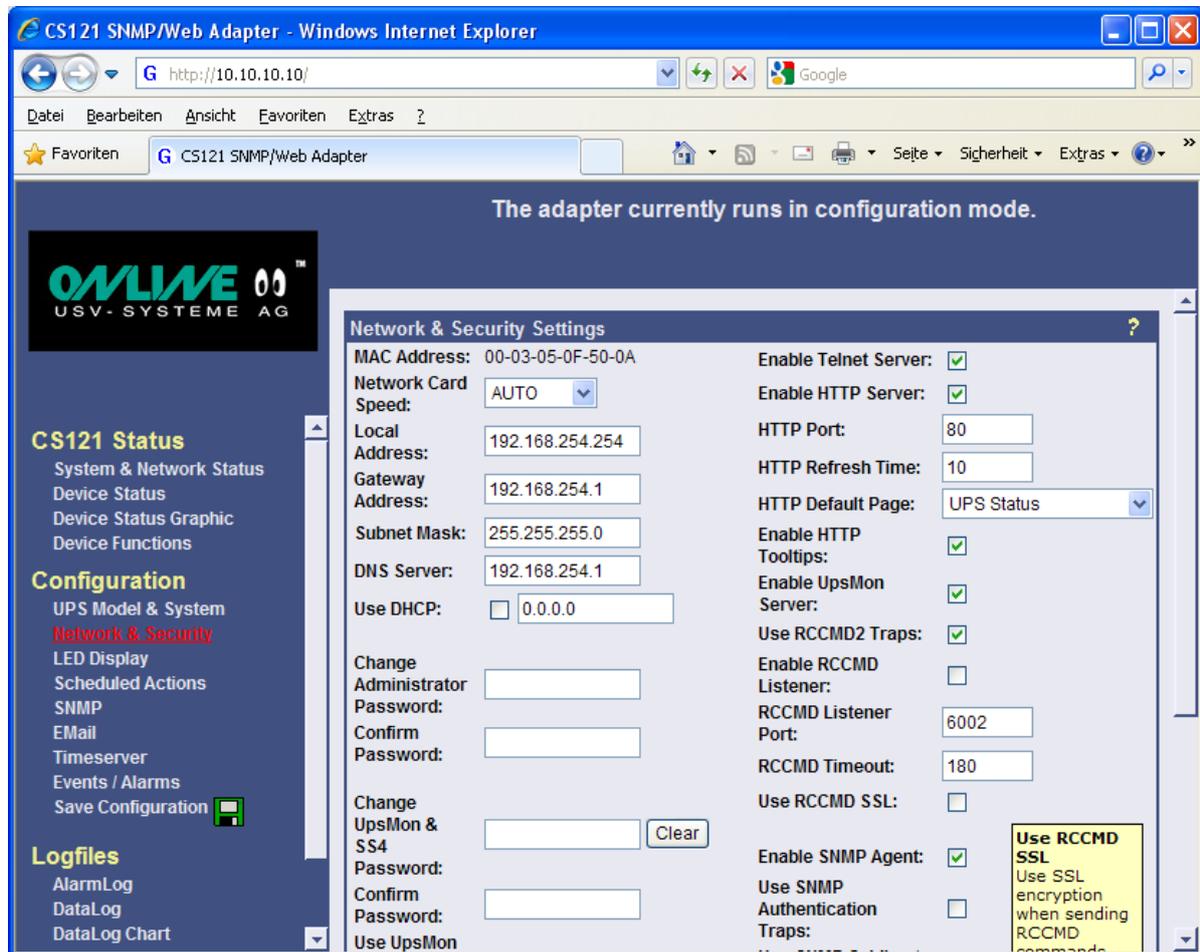


Abbildung 3-5

Geben Sie eine lokale, freie IP-Adresse **Local Address:** entsprechend Ihres lokalen Subnetzes für das SNMP Modul ein.

Hier wird zum Beispiel die IP **192.168.254.254** und die passende Subnetzmaske **Subnet Mask:** **255.255.255.0** verwendet.

Als Gateway **Gateway Address:** tragen Sie die IP-Adresse Ihres Routers ein. In diesem Beispiel ist das **192.168.254.1**.

Zum Schluss noch den **DNS Server** eintragen. Dies ist in der Regel Ihr Router oder Ihr Domänen-Controller, falls Sie Windows 200x Server mit Active Directory verwenden.

In diesem Beispiel ist das der Internetrouter mit der IP **192.168.254.1**.

Natürlich lassen sich hier noch weitere Punkte konfigurieren. Für die rudimentäre Einrichtung und einen ersten Funktionstest reichen diese Einstellungen jedoch aus.

Nach Abschluss der Konfiguration scrollen Sie das Fenster nach unten und klicken auf **Apply** (Abbildung 3-6).

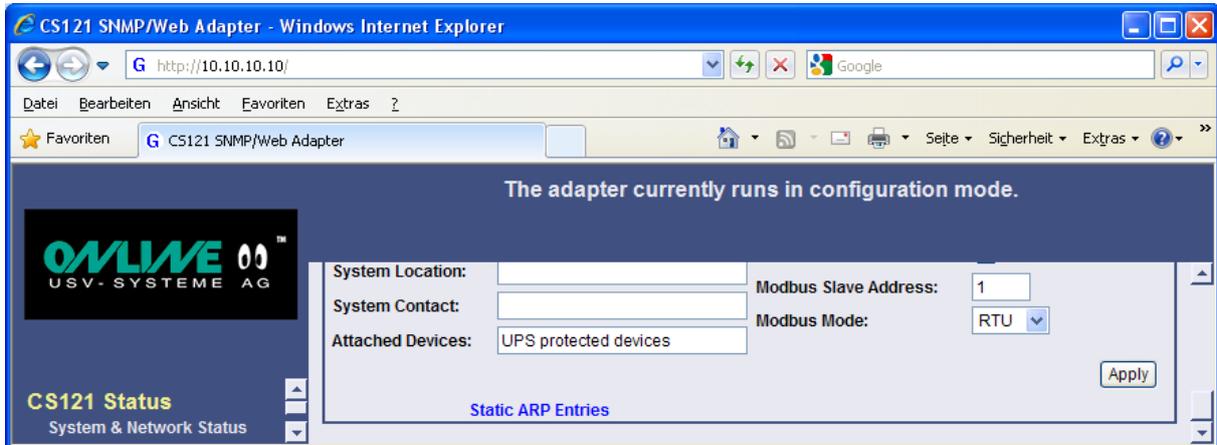


Abbildung 3-6

3.4 Einstellen der RCCMD Clients auf dem SNMP Modul

Klicken Sie auf **Events / Alarms**, um den Dialog **Event Configuration** zu öffnen (Abbildung 3-7). Wählen Sie den ersten Punkt **Powerfail**.

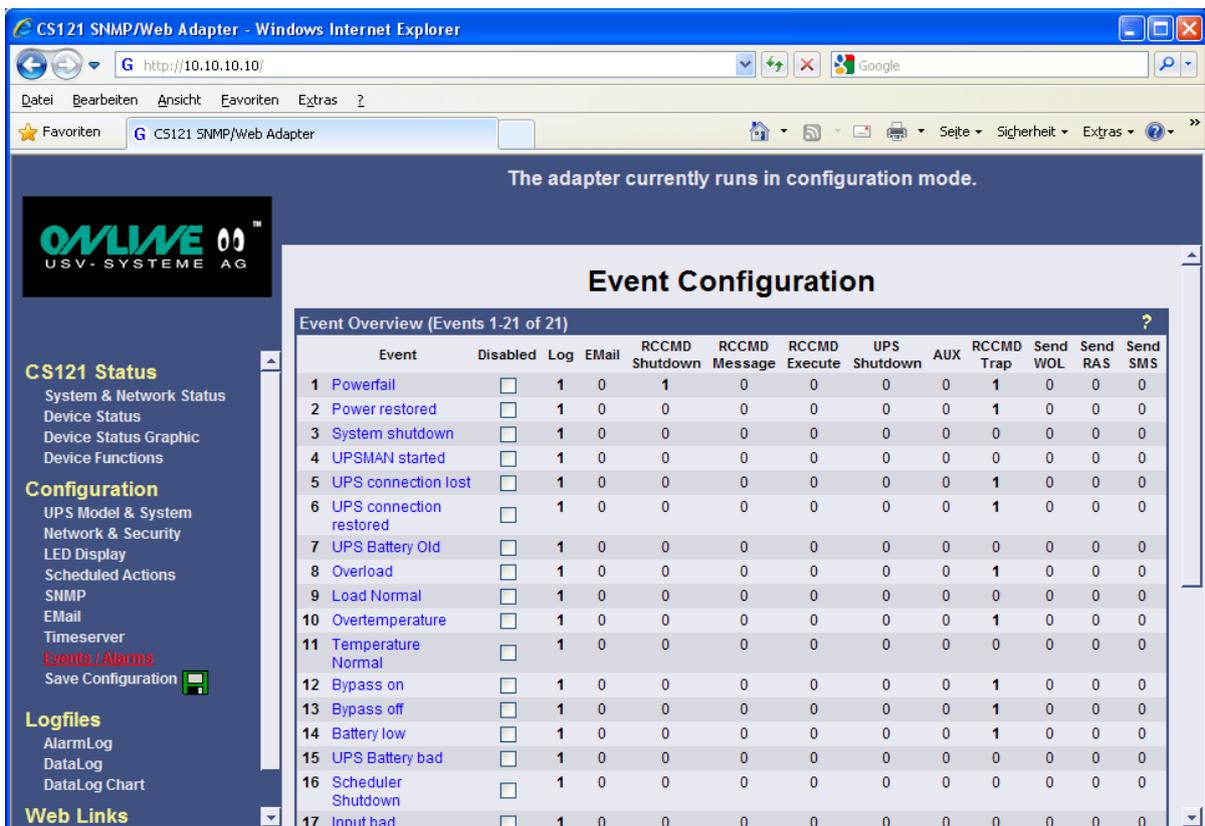


Abbildung 3-7

Die Event Jobs für Powerfail werden angezeigt (Abbildung 3-8).
 Klicken Sie auf **Add new job**.

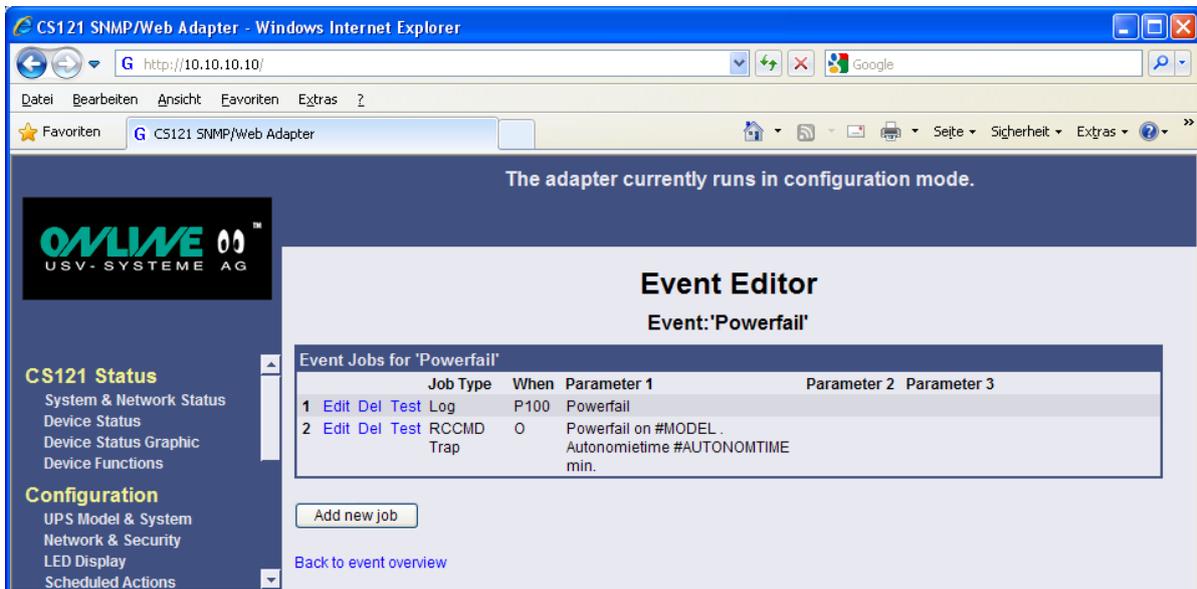


Abbildung 3-8

Der Job Editor wird geöffnet (Abbildung 3-9).

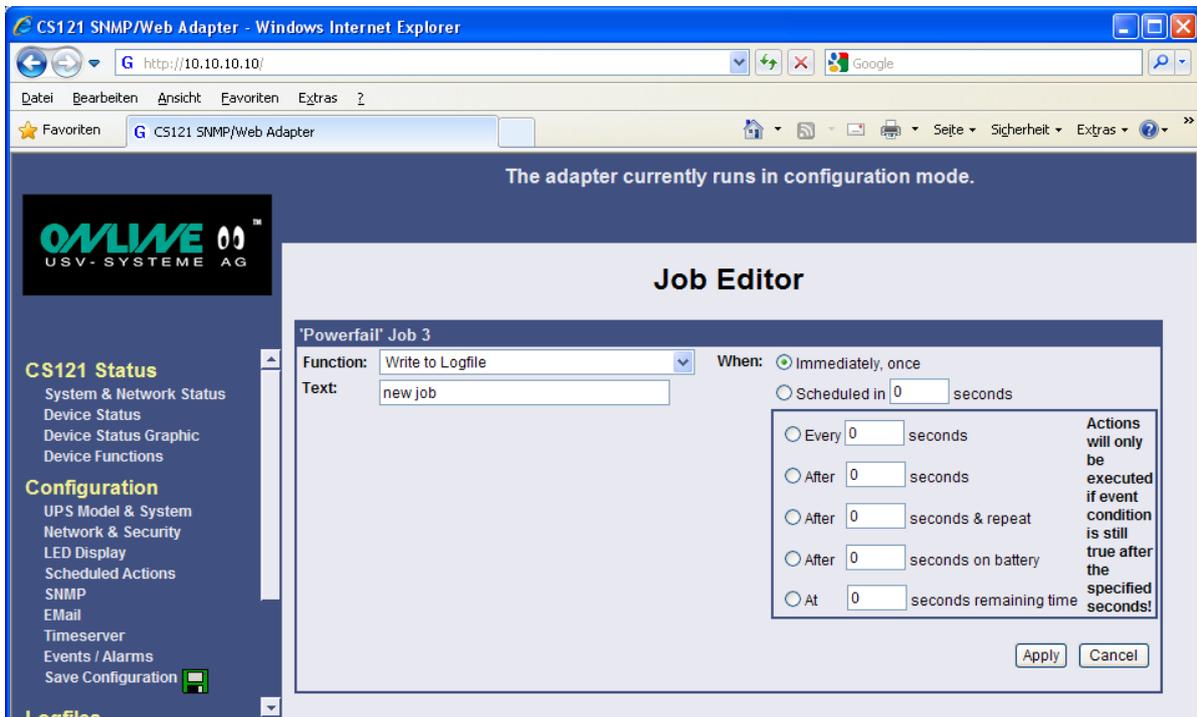


Abbildung 3-9

Wählen Sie unter **Funktion:** den Eintrag **Send RCCMD Shutdown to remote client** (Abbildung 3-10) aus.

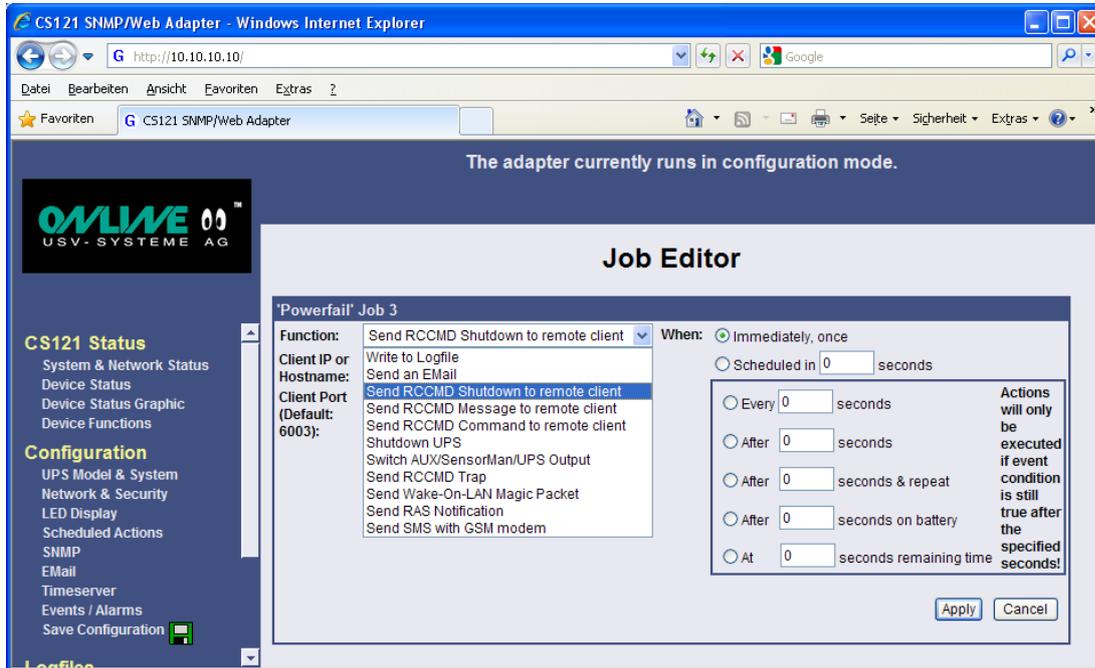


Abbildung 3-10

Zum Abschluss überlegen wir uns eine sinnvolle Strategie für das Herunterfahren aller Hosts und Clients, die mit Hilfe des SNMP Adapters heruntergefahren werden sollen.

Diese Einstellungen hängen im Wesentlichen von den verwendeten Betriebssystemen und deren Wichtigkeit für das gesamte System ab.

Ferner sollten diese Einstellungen so geplant werden, dass noch genügend Batterielaufzeit übrig ist, um auch den (die) ESX Host(s) herunterzufahren!

Für unser Beispiel nehmen wir einen VMware ESXi Host und zwei Windows-Gäste, bestehend aus einem Domänen-Controller und einem Datenbank-Server. Desweiteren installieren wir einen weiteren GastMden VMware Management Assistant (wird in der weiteren Dokumentation vMA 4.1 genannt.); der den Shutdown des VMware ESXi Servers regeln wird.

Server:	IP	Typ	Shutdown-Zeit in Sekunden?	RCCMD Client ?	Shutdown-Reihenfolge
VMware ESXi Server	192.168.254.224	Host	90	nein	4
VMware Management Assistant	192.168.254.199	Gast	90	ja	3
Windows 2003 R2 Server (DC)	192.168.254.200	Gast	90	ja	2
Windows 2003 R2 Server (Oracle DB)	192.168.254.210	Gast	180	ja	1

Tabelle 1

Gemäß der Tabelle 1 muss der DB-Server als erstes heruntergefahren werden. In unserem Beispiel beginnen wir mit dem Herunterfahren der Systeme, nachdem das System 30 Sekunden auf Batteriestrom gelaufen ist. Dazu tragen Sie unter **Client IP or Hostname:** die IP des DB-Servers **192.168.254.210** und stellen **After 30 seconds on battery** ein. Abschließend klicken Sie auf **Apply** (Abbildung 3-11).

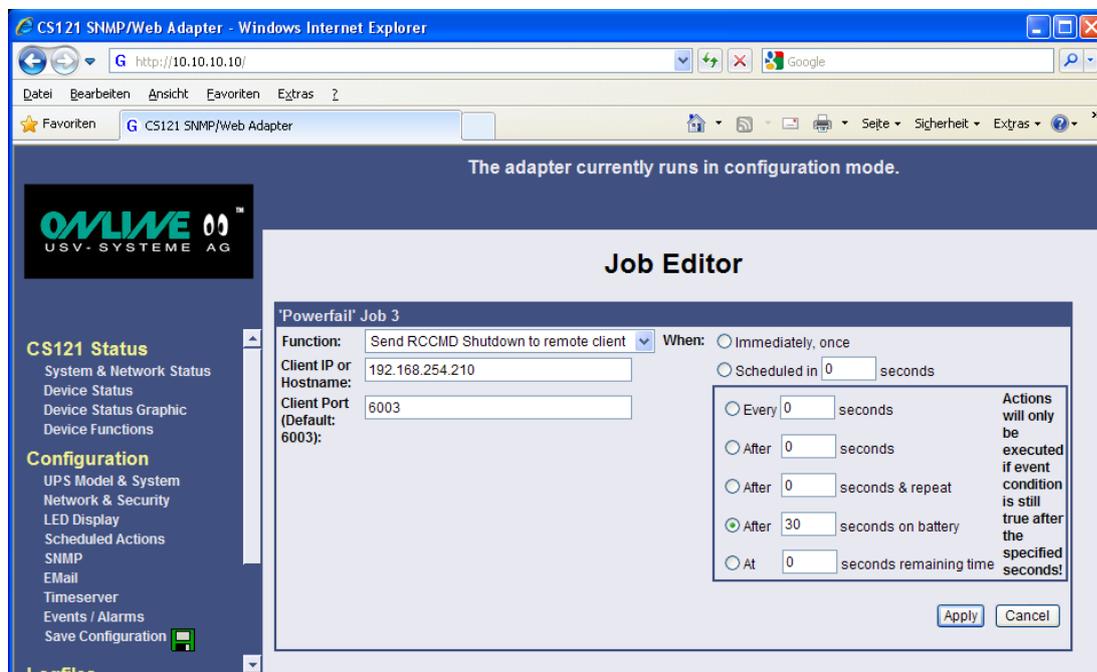
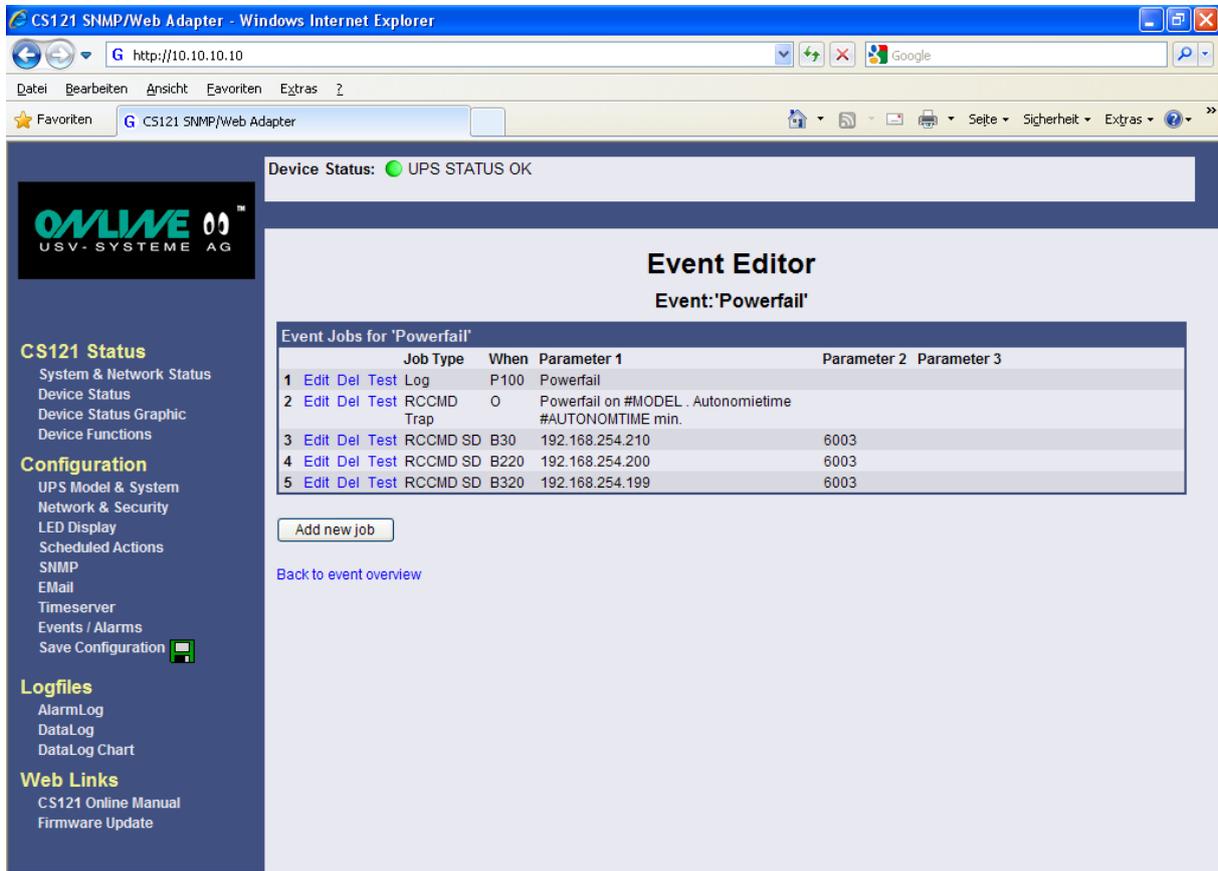


Abbildung 3-11

Für die weiteren Server addieren Sie die Zeit für das Herunterfahren des verbleibenden Gastes und des VMware ESXi Servers mit vMA 4.1 plus je zehn Sekunden. Wiederholen Sie diesen Vorgang bis die Tabelle abgearbeitet ist (Abbildung 3-12).

Der ESXi Host bleibt unberücksichtigt da er von der vMA 4.1 heruntergefahren wird.



The screenshot shows a web browser window with the URL <http://10.10.10.10>. The page title is "CS121 SNMP/Web Adapter". The device status is "UPS STATUS OK". The main content area is titled "Event Editor" and shows "Event: 'Powerfail'". Below this is a table of "Event Jobs for 'Powerfail'":

	Job Type	When	Parameter 1	Parameter 2	Parameter 3
1	Edit Del Test Log	P100	Powerfail		
2	Edit Del Test RCCMD Trap	0	Powerfail on #MODEL . Autonomietime #AUTONOMTIME min.		
3	Edit Del Test RCCMD SD	B30	192.168.254.210	6003	
4	Edit Del Test RCCMD SD	B220	192.168.254.200	6003	
5	Edit Del Test RCCMD SD	B320	192.168.254.199	6003	

Below the table, there is an "Add new job" button and a link "Back to event overview". The left sidebar contains navigation menus for "CS121 Status", "Configuration", "Logfiles", and "Web Links".

Abbildung 3-12

Natürlich ist dies nur ein Beispiel und sollte individuell auf das eigene System abgestimmt werden. Ein gleichzeitiges herunterfahren von Gästen ist möglich.

Hinweis: Anmelde-Server und Domänen-Controller sollten immer zum Schluss heruntergefahren werden. Der letzte Server, der heruntergefahren wird, muss immer der vMA 4.1 Server sein, welcher unseren Host (ESXi VMware Server) nach dem Starten des Shutdownprozesses herunterfährt.

3.5 Speichern der Einstellungen

Nachdem alle notwendigen Einstellungen konfiguriert wurden, müssen diese gespeichert und das SNMP Modul mit den neuen Werten gebootet werden.

Wählen Sie den Menüpunkt [Save Configuration](#) aus (Abbildung 3-13).

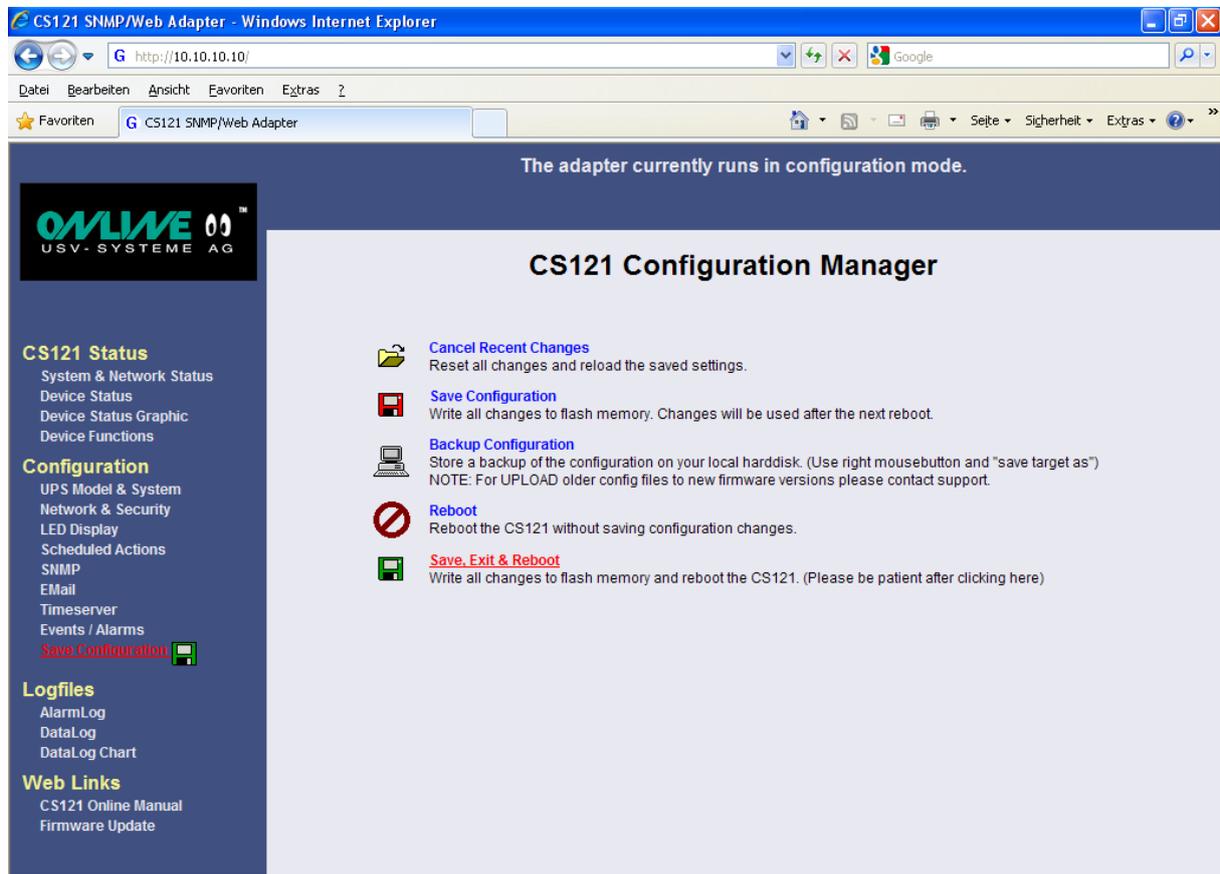


Abbildung 3-13

[Save, Exit & Reboot](#) anklicken und etwa zwei Minuten warten. Danach sollten die Einstellungen permanent vorhanden sein. Sie können diese nach einer erneuten Anmeldung überprüfen.

3.6 Rücksetzen der Dip Schalter und Neustart

Abschließend muss die USV abgeschaltet und das SNMP Modul per Dip Schalter aus dem Konfigurationsmodus genommen werden. Stellen Sie dafür den ersten Dip Schalter auf ON (Abbildung 1-2). Weitere Informationen entnehmen Sie dem Kapitel 1.1. Das SNMP Modul kann nun fest eingebaut und die USV mit konfiguriertem SNMP Modul neu gestartet werden.

Anschließend erfolgt die Client-Installation auf dem Host und den Gästen.

4 Konfiguration VMware ESXi

4.1 Voraussetzungen

Für die Konfiguration von VMware ESXi werden folgende Programme und Informationen benötigt:

- RCCMD Client für VMware ESXi 4 unter vMA 4.1
- mitgelieferter Licence code
- Putty (SSH Client)
- WinSCP (SFTP Client)
- vMA 4.1 (virtuelle Appliance)

4.2 Download der benötigten Komponenten

4.2.1 RCCMD Client für VMware ESXi (vMA 4.1)

Den aktuellen RCCMD Client für VMware ESXi finden Sie hier unter folgendem Link:

<http://www.online-usv.de/de/download/softwarefirmware.php>

Bitte den Punkt „DataWatch Updates und Patches“ danach „RCCMD Agents“ auswählen.

Wählen Sie den Punkt **RCCMD Agents** (Abbildung 4-1).

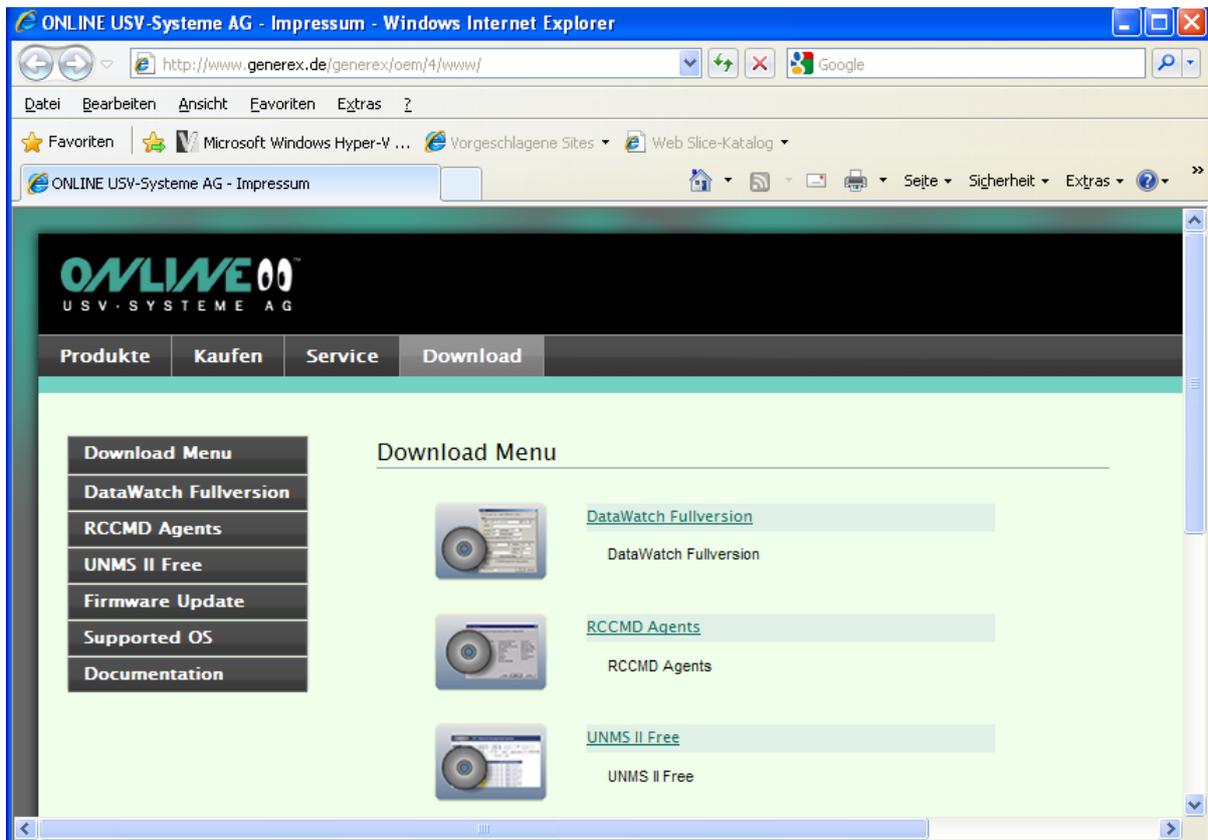


Abbildung 4-1

Wählen Sie **RCCMD for VMware ESX** (Abbildung 4-2).

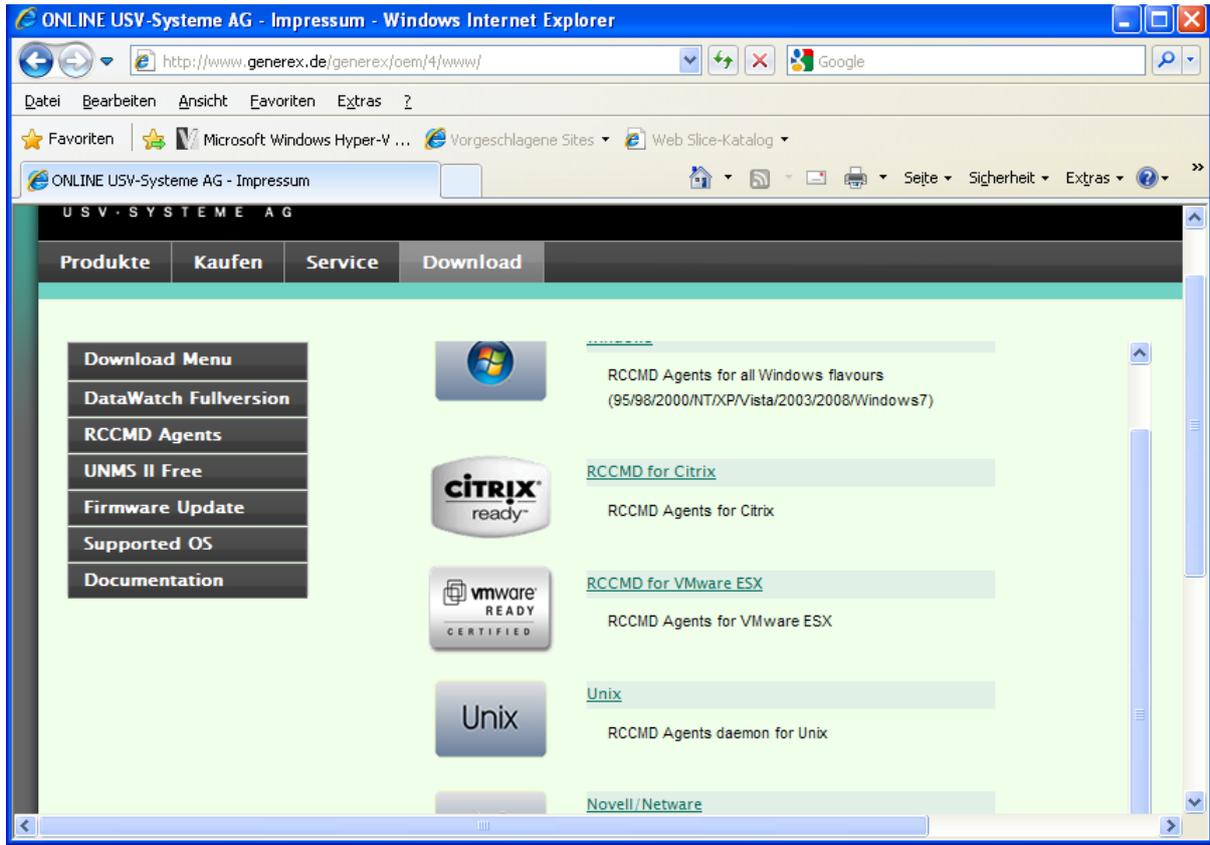


Abbildung 4-2

Geben Sie hier Ihren Licence Code ein, wählen **VMware ESXi4.x** aus und klicken auf **Create package...** (Abbildung 4-3).

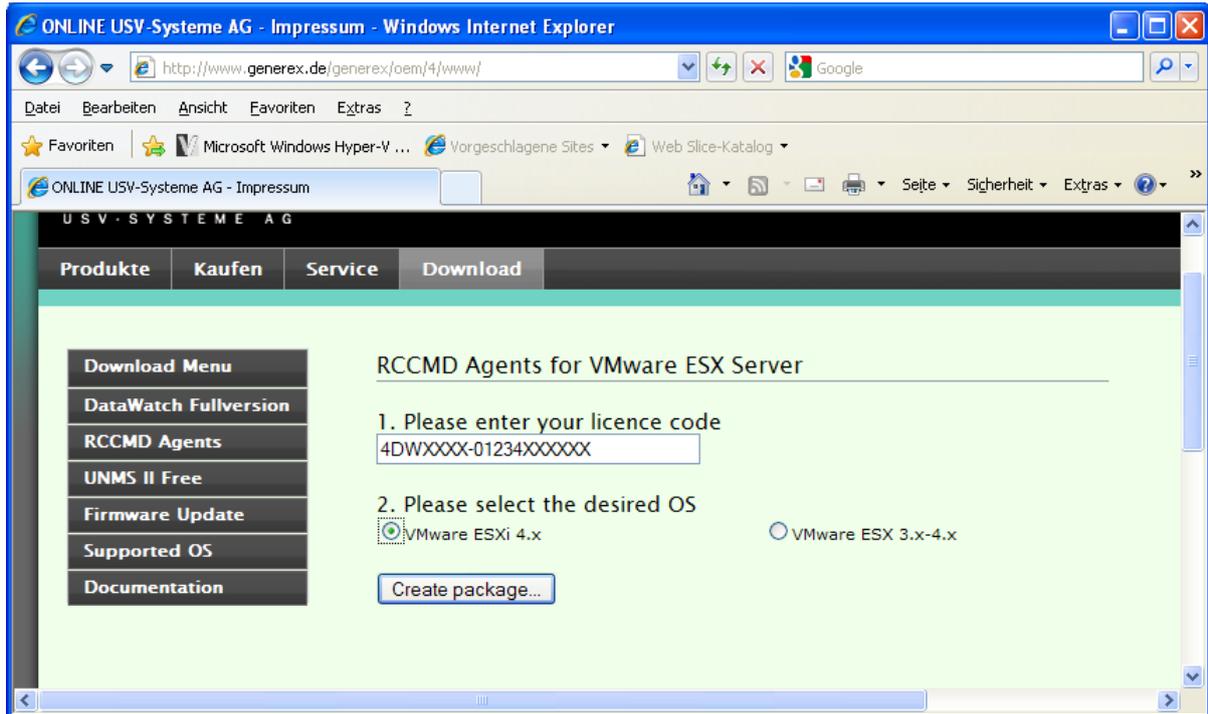


Abbildung 4-3

Klicken Sie auf **Download the software package** (Abbildung 4-4).

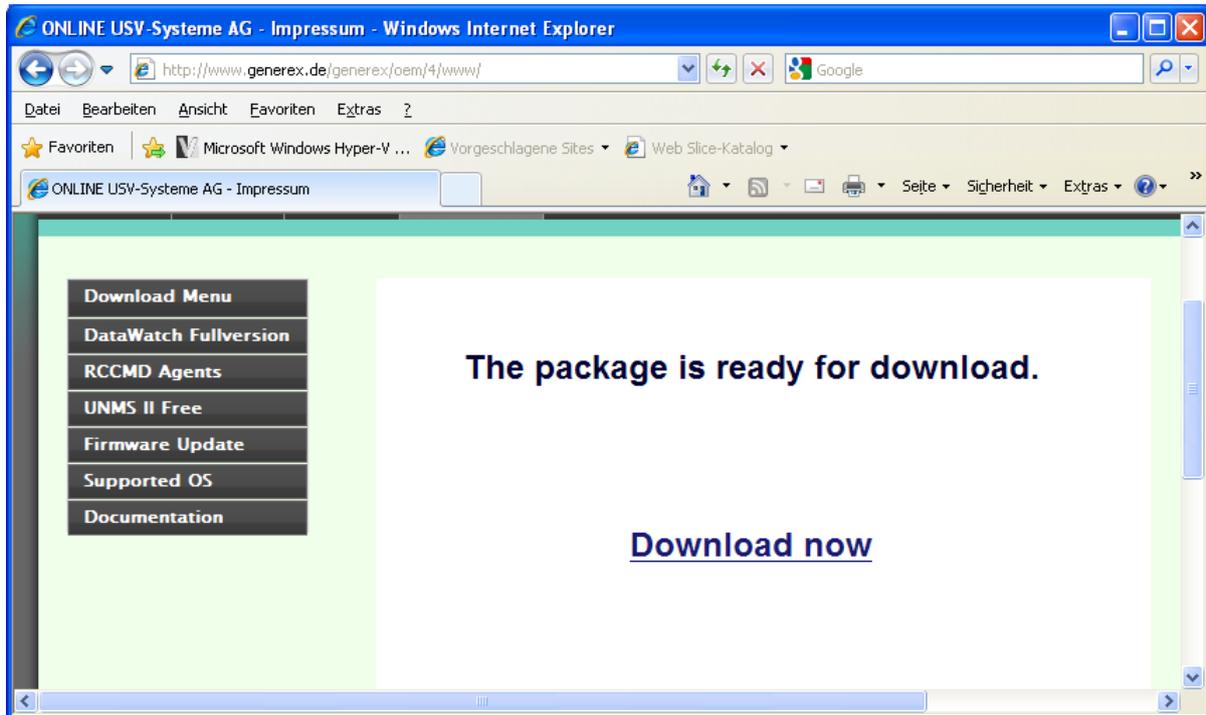


Abbildung 4-4

Klicken Sie auf **Speichern** und legen die Datei rccmdinst.tar in einem Verzeichnis Ihrer Wahl ab (Abbildung 4-5).

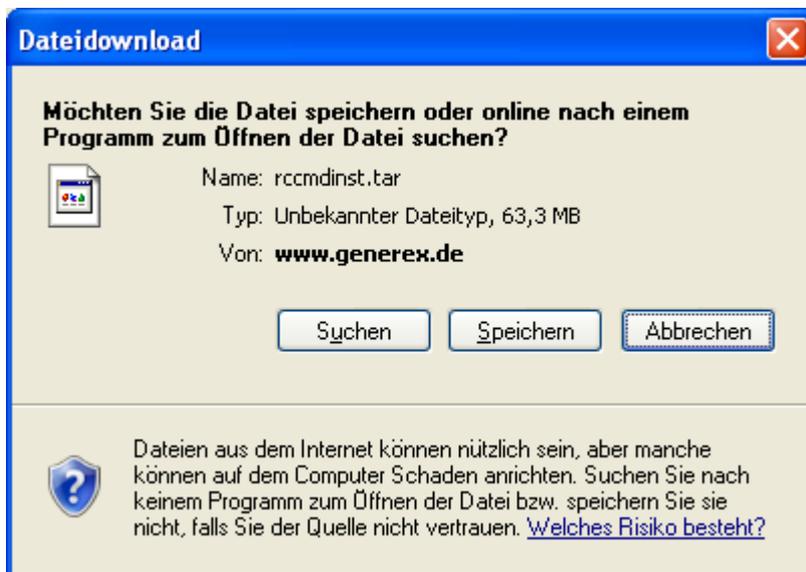


Abbildung 4-5

4.2.2 Putty (SSH Client)

Putty ist über folgenden Link zu beziehen:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

Klicken Sie auf putty.exe, um den Download zu starten (Abbildung 4-6).

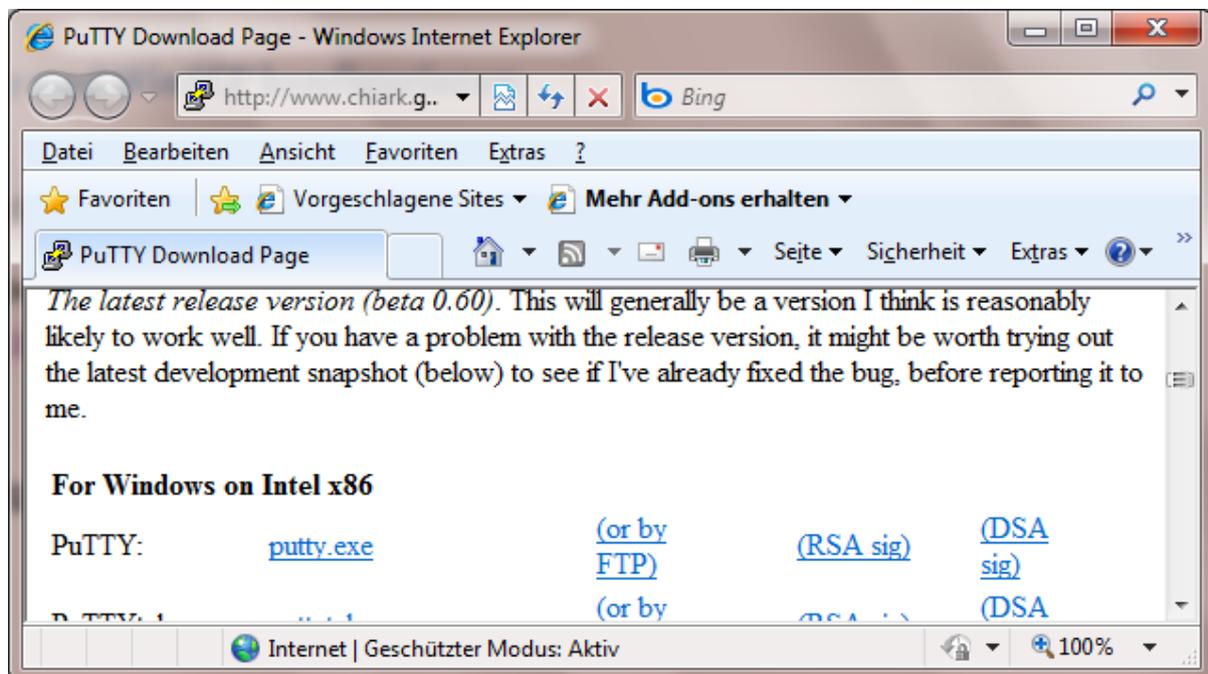


Abbildung 4-6

Klicken Sie auf **Speichern** und legen die Datei putty.exe in einem Verzeichnis Ihrer Wahl ab (Abbildung 4-7).



Abbildung 4-7

4.2.3 WinSCP (SFTP Client)

WinSCP ist über folgenden Link zu beziehen: <http://winscp.net/eng/download.php>

Über den Link **Installation package** startet der Download (Abbildung 4-8).

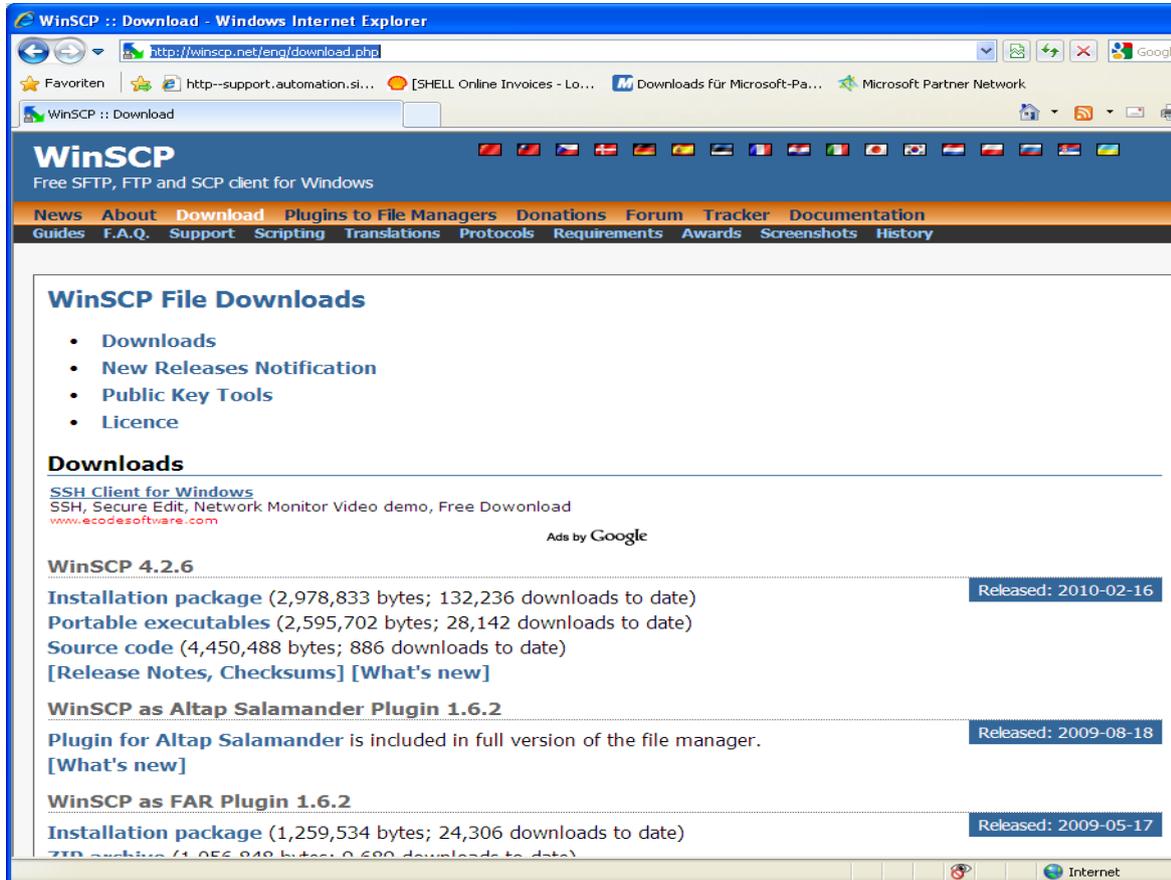


Abbildung 4-8

Klicken Sie auf **Speichern** und legen die Datei in einem Verzeichnis Ihrer Wahl ab (Abbildung 4-9).

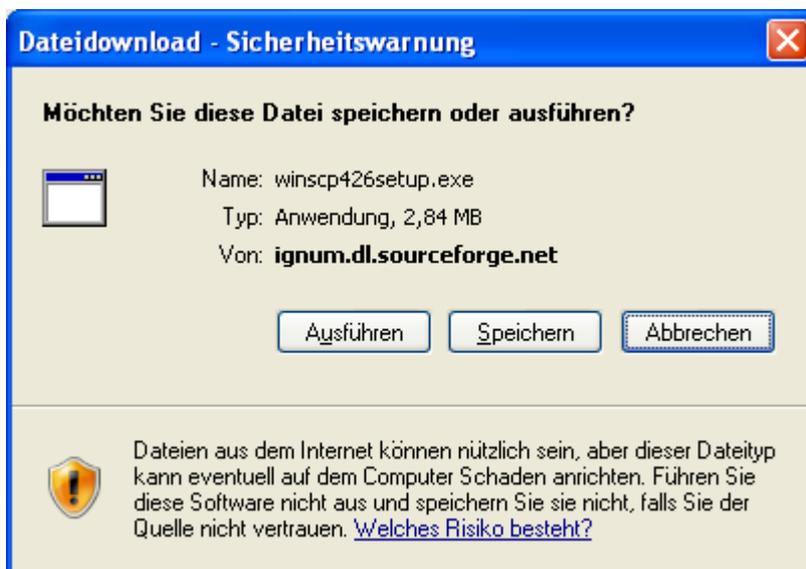


Abbildung 4-9

Öffnen Sie anschließend die Datei und führen das Setup gemäß den Programmanweisungen durch. Das Setup erstellt eine Programm-Verknüpfung auf Ihrem Desktop (Abbildung 4-10).



Abbildung 4-10

4.2.4 vMA 4.1 (virtuelle Appliance)

Downloaden Sie die vMA 4.1 von der VMware Homepage. Diese liegt dort als virtuelle Appliance (.ovf File) vor und kann über den vSphere Client auf Ihrem ESXi installiert werden.

Download Link:

<http://communities.vmware.com/community/vmtn/vsphere/automationtools/vima>

Nachdem Sie sich bei VMware angemeldet und authentifiziert haben, starten Sie den **Download** (Abbildung 4-11). Haben Sie keinen gültigen Account bei VMware, können Sie diesen auf der Download-Seite einrichten.

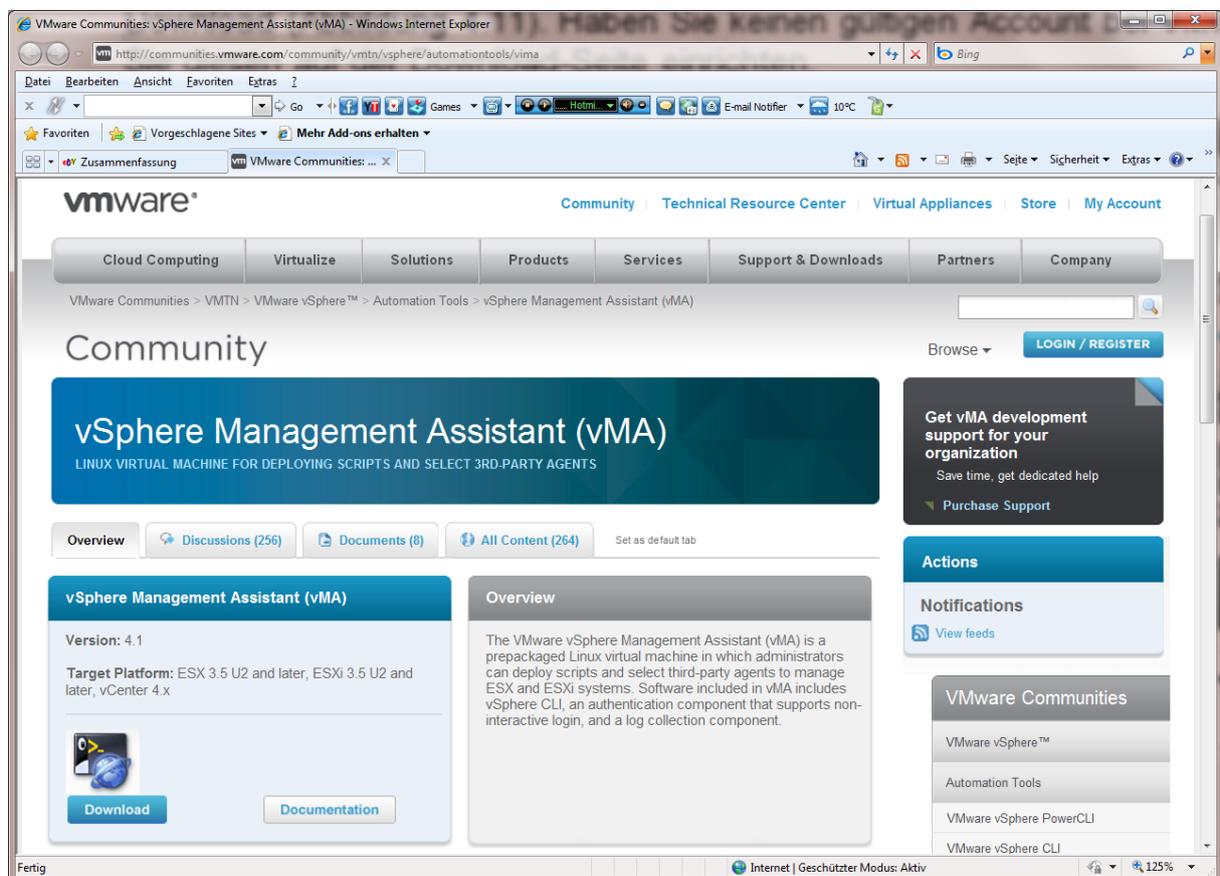


Abbildung 4-11

Bitte lesen und akzeptieren Sie das End User Licence Agreement (Abbildung 4-12) mit **Yes**.

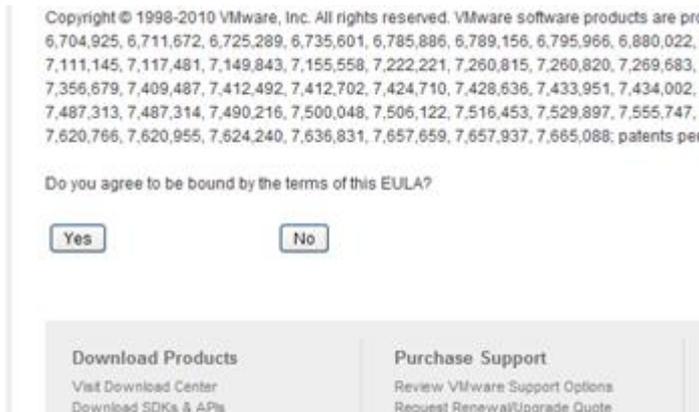


Abbildung 4-12

Wählen Sie unter **Download Options** den Punkt **Use Download Manager** aus (Abbildung 4-13) und wählen den **zip** Link.

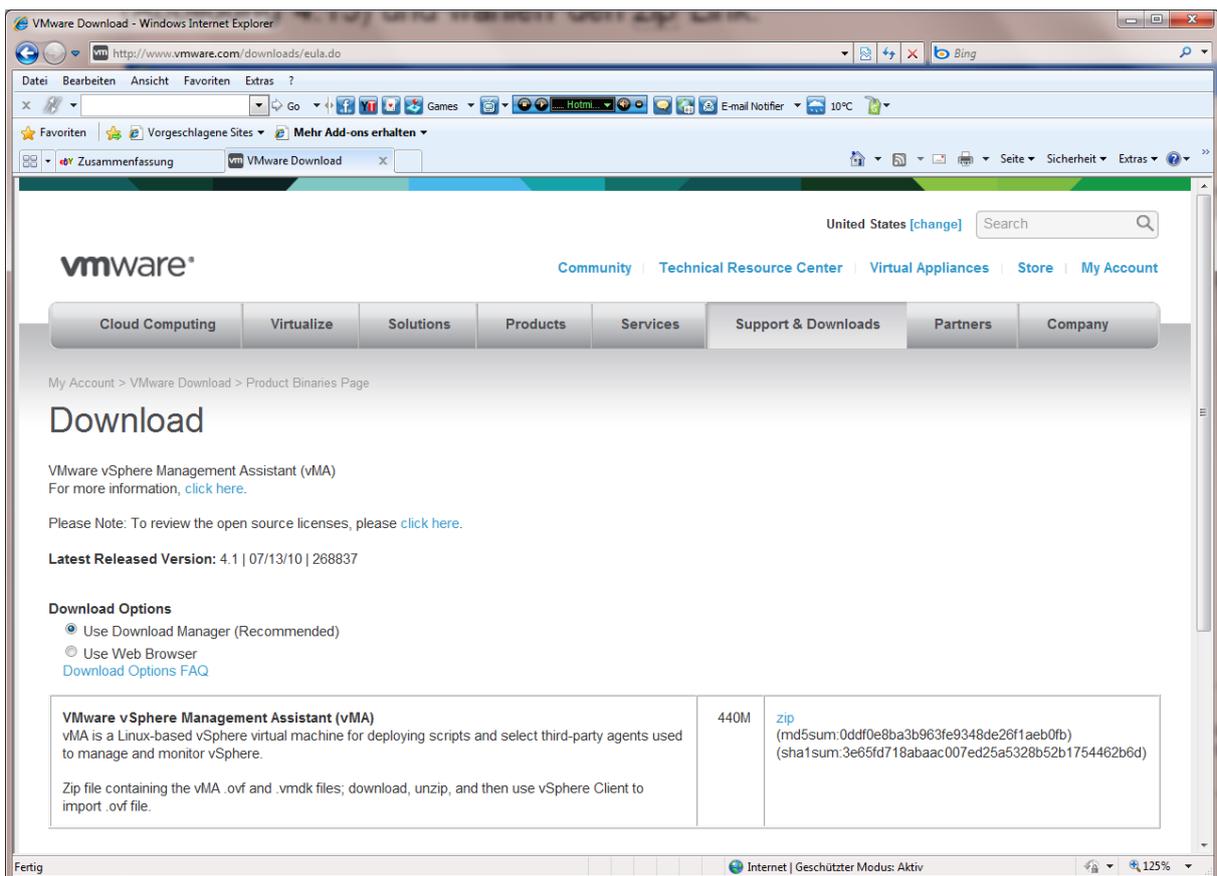


Abbildung 4-13

Speichern Sie die Datei in einem Verzeichnis Ihrer Wahl. Danach startet der VMware Download Manager (Abbildung 4-14).

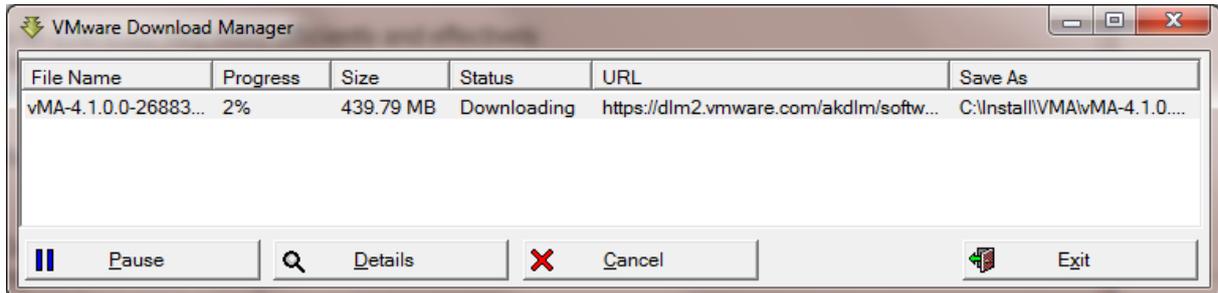


Abbildung 4-14

Entpacken Sie das Archiv (Abbildung 4-15).

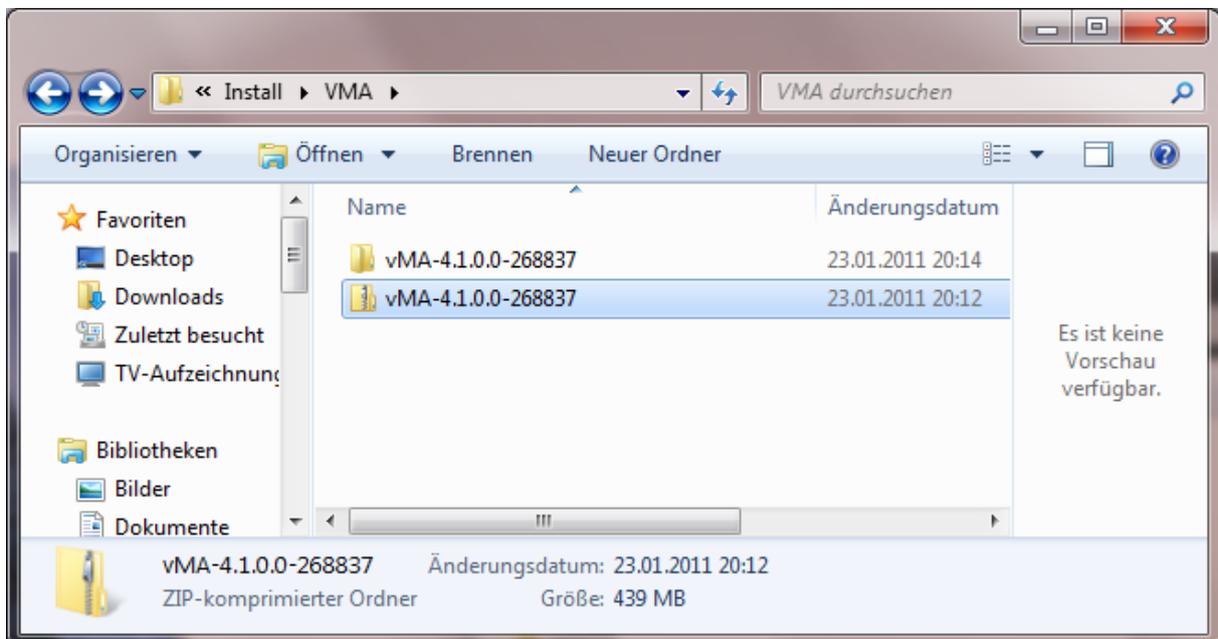


Abbildung 4-15

4.3 vMA 4.1 installieren

4.3.1 Voraussetzungen für eine Installation

Bevor Sie mit der Installation beginnen, möchte ich darauf hinweisen, dass die Installation vMA 4.1 aus lizenzrechtlichen Gründen nur auf lizenzierten ESXi ab Essentials Status erlaubt ist. Sie können die vMA 4.1 während der 60 Tage dauernden Evaluierungsphase installieren. Um eine Lizenzrechtsverletzung zu vermeiden, sollte ein Upgrade für Ihre ESXi Evaluierungslizenz auf mindestens Essential oder Foundation Status erfolgen. Die Backupfunktionalitäten für vSphere stehen nur in diesen Versionen vollständig zur Verfügung.

Die vMA 4.1 stellt bestimmte Ansprüche an die verwendete Hardware. Achten Sie darauf, dass Ihr ESXi Server den Hardware-Virtualisierungsmodus unterstützt. Diese Funktion; auch VT Modus genannt; lässt sich über das Bios Ihres Servers aktivieren.

Hinweis: vMA 4.1 ist ein 64 Bit Betriebssystem und ist daher nur auf 64 Bit Hardware lauffähig!

Eine Installation auf einem Hewlet Packard Proliant Server ab der Generation 5 mit Intel Xeon Quadcore CPU oder einem IBM xSeries eServer mit Intel Xeon Quadcore CPU (z.B. Modell x3650) sollte problemfrei nach Aktivierung des VT Modus über das Bios möglich sein.

Werden die Hardwaremindestanforderungen nicht erfüllt werden, bricht die Installation mit einer Fehlermeldung (Abbildung 4-16) ab.

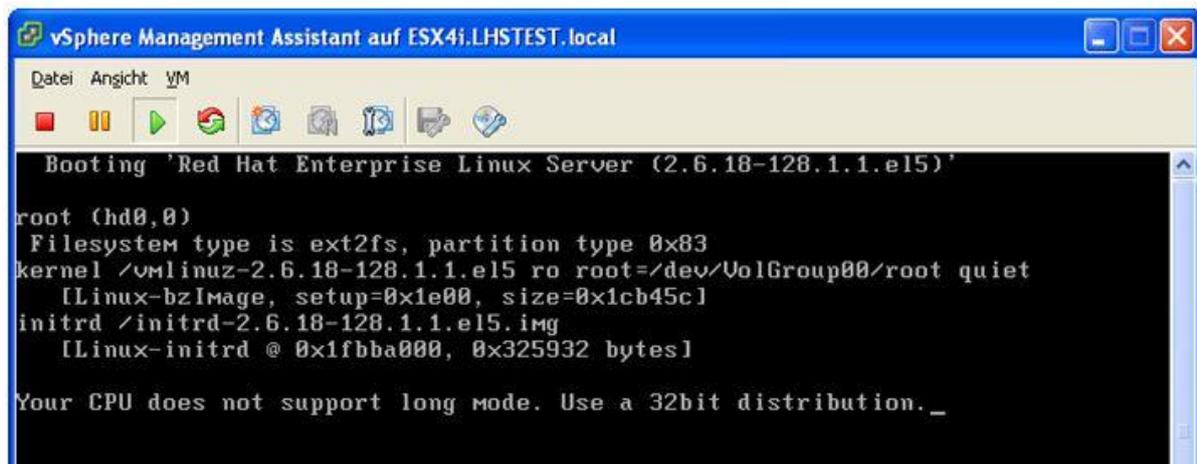


Abbildung 4-16

4.3.2 Installation der vMA 4.1 auf ESXi

Starten Sie Ihren vSphere Client und melden sich bei Ihrem ESXi an (Abbildung 4-17).



Abbildung 4-17

Bei der ersten Anmeldung erscheint eine Sicherheitswarnung (Abbildung 4-18). Klicken Sie auf **Dieses Zertifikat installieren und keine Sicherheitswarnungen für „Ihr ESXi Server“ anzeigen.** und anschliessend auf **Ignorieren**.

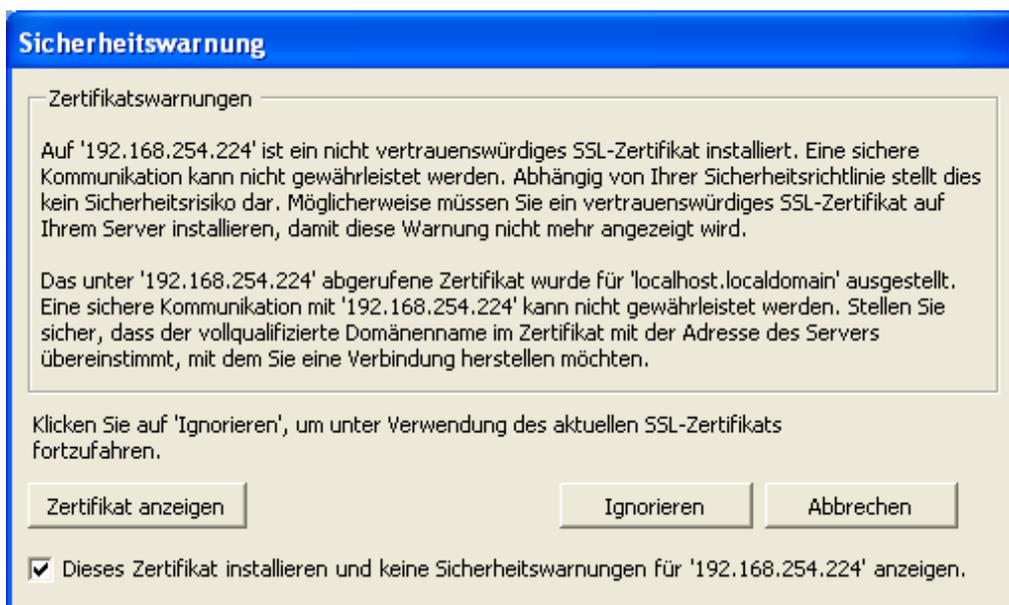


Abbildung 4-18

Nach dem Start Ihres vSphere Clients (Abbildung 4-19) wählen Sie den Menüpunkt **Datei** und wählen den Unterpunkt **OVF-Vorlage bereitstellen** aus (Abbildung 4-20).

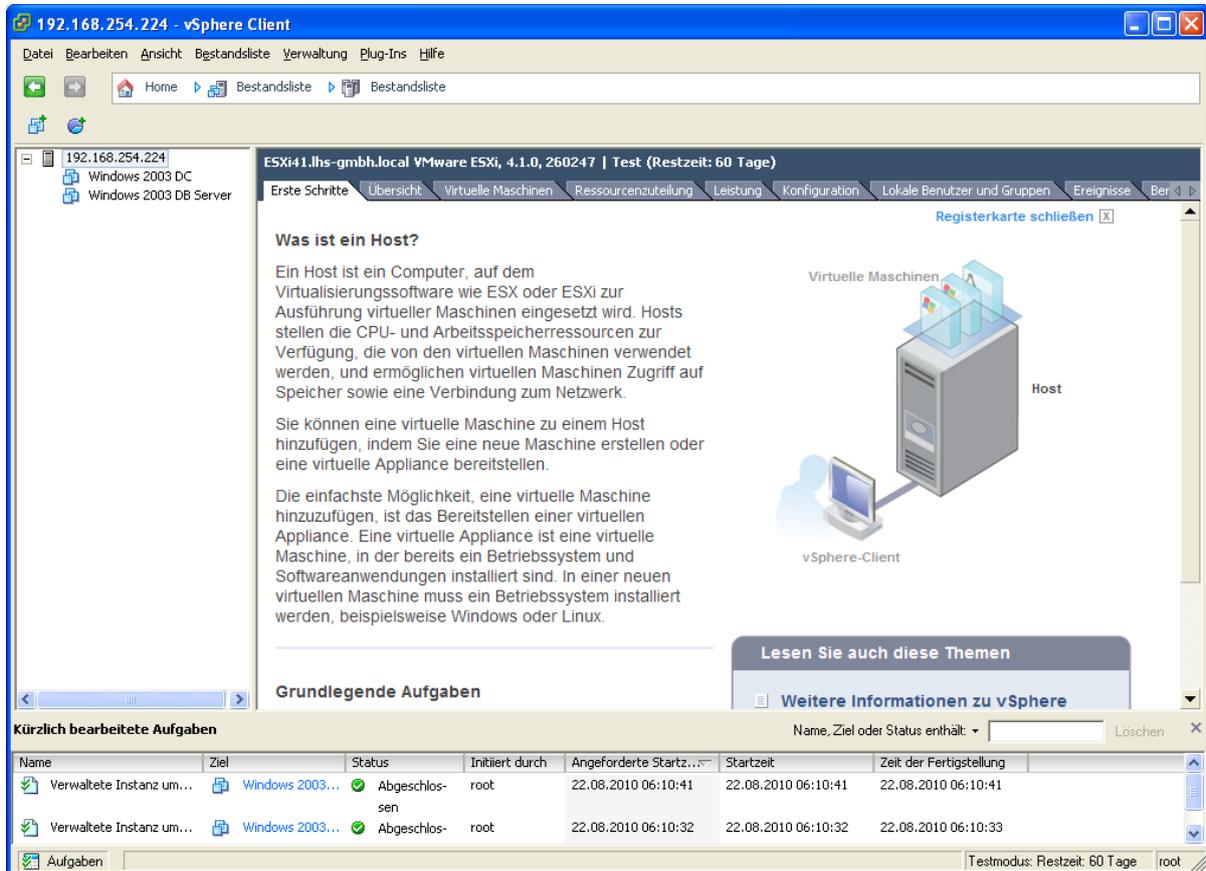


Abbildung 4-19

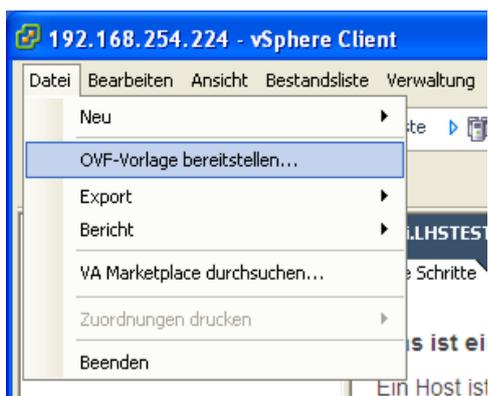


Abbildung 4-20

Es startet der OVF Vorlagen Assistent (Abbildung 4-21).

Markieren Sie den Punkt **Aus Datei bereitstellen:** und klicken auf **Durchsuchen...**

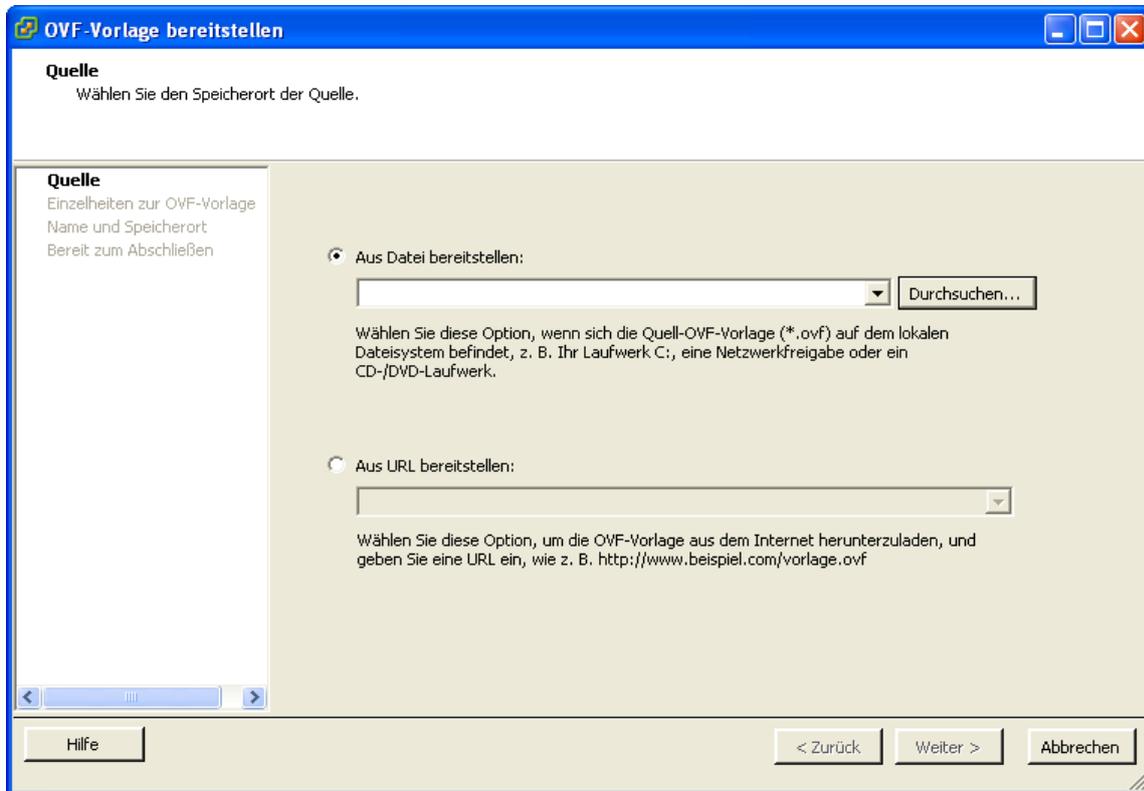


Abbildung 4-21

Wählen Sie die vMA 4.1 OVF Datei aus (Abbildung 4-22) und klicken auf **Öffnen**.

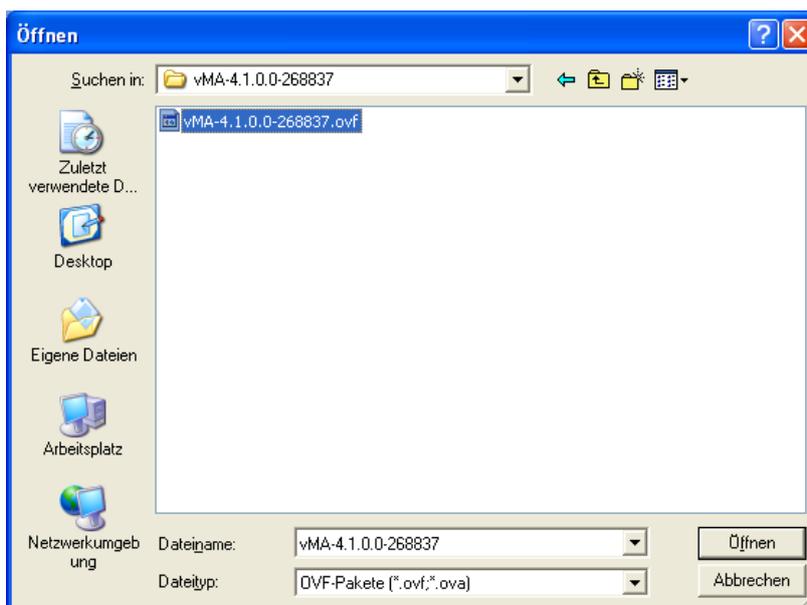


Abbildung 4-22

Bestätigen Sie die Quelle mit **Weiter** (Abbildung 4-23).

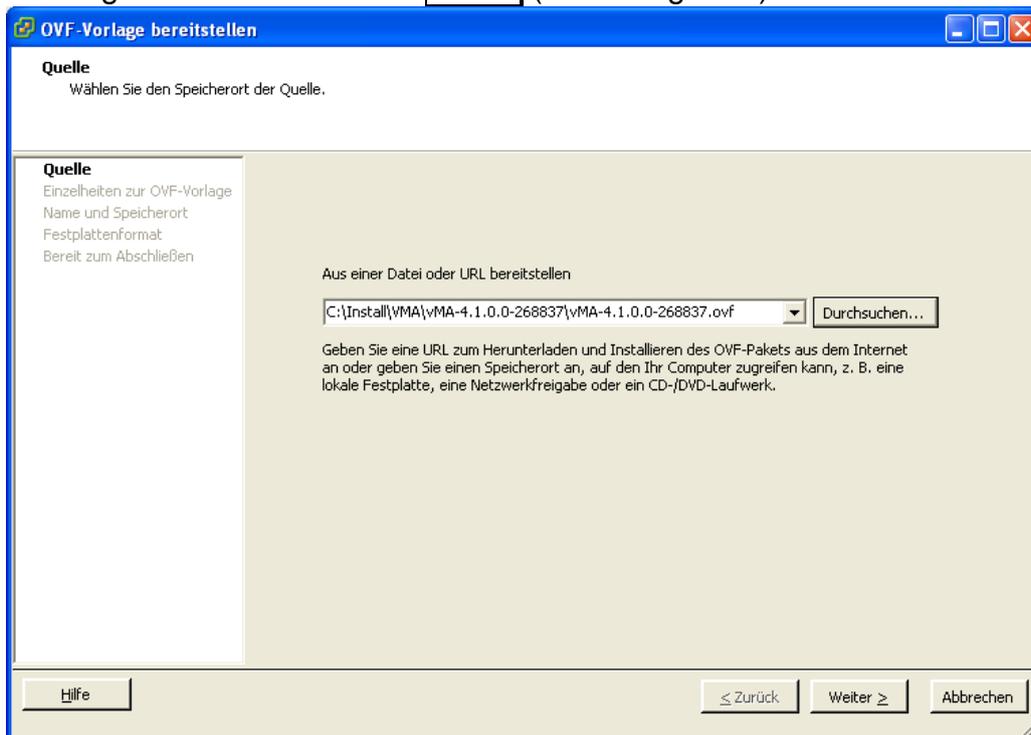


Abbildung 4-23

Klicken Sie in der nächsten Maske (Abbildung 4-24) des Assistenten auf **Weiter**.

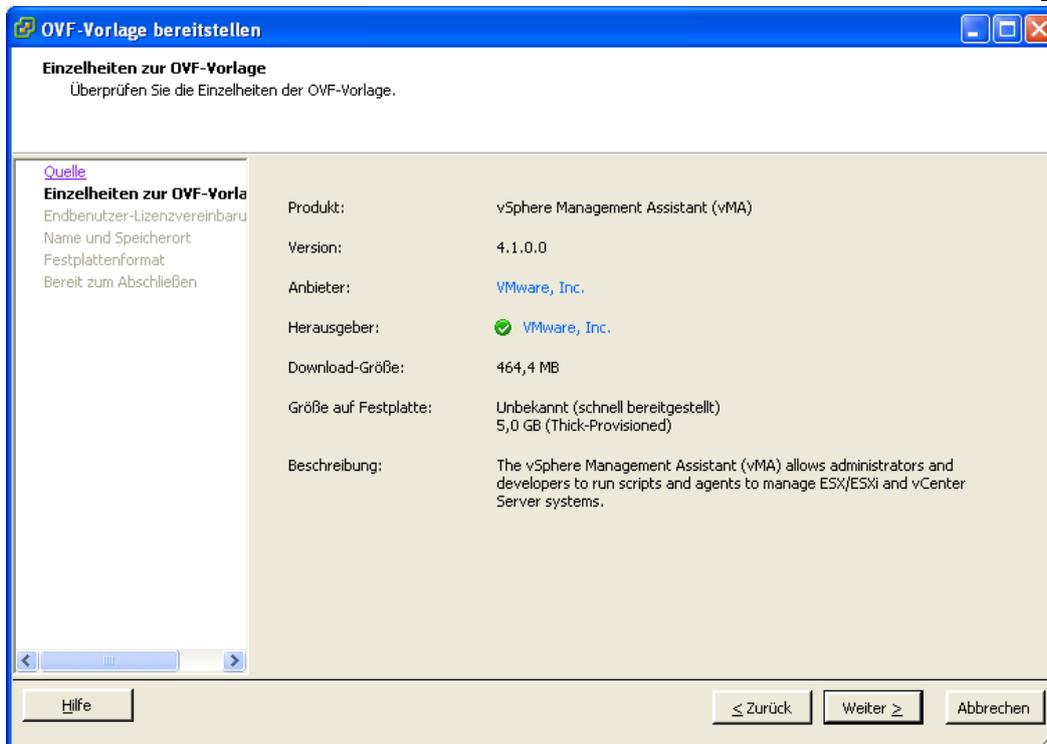


Abbildung 4-24

Akzeptieren Sie die EULA (Abbildung 4-25) und bestätigen diese mit **Weiter**.

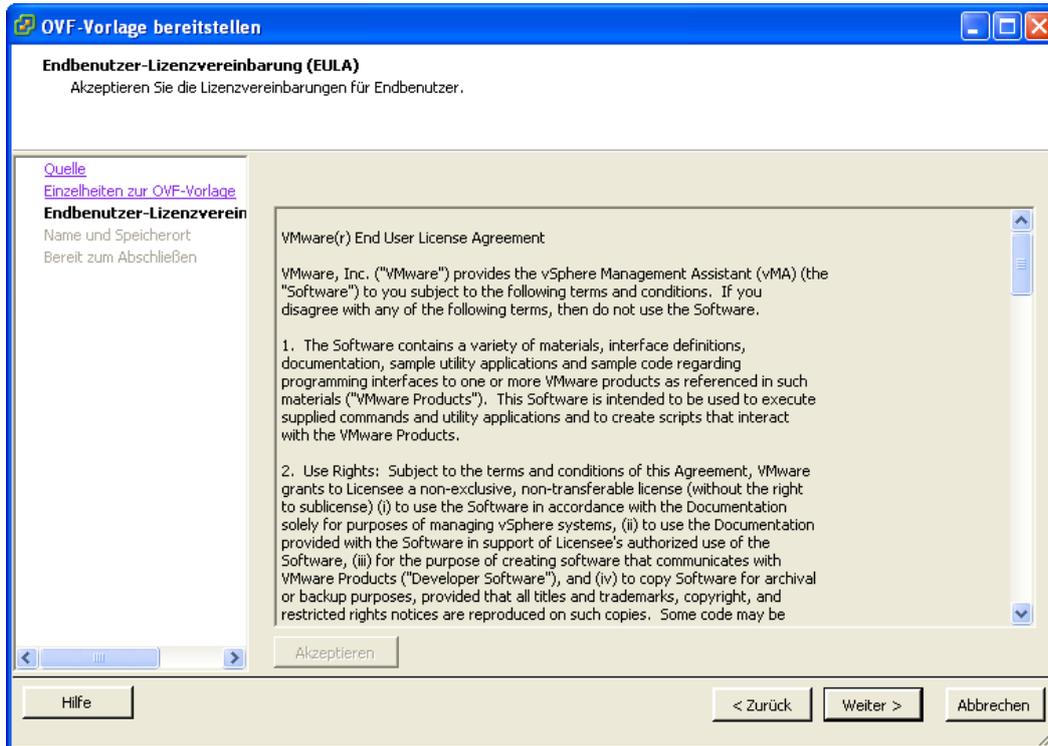


Abbildung 4-25

In der Maske **Name und Speicherort** (Abbildung 4-26) vergeben Sie einen Namen für die vMA 4.1 auf Ihrem ESXi und bestätigen diesen mit **Weiter**.

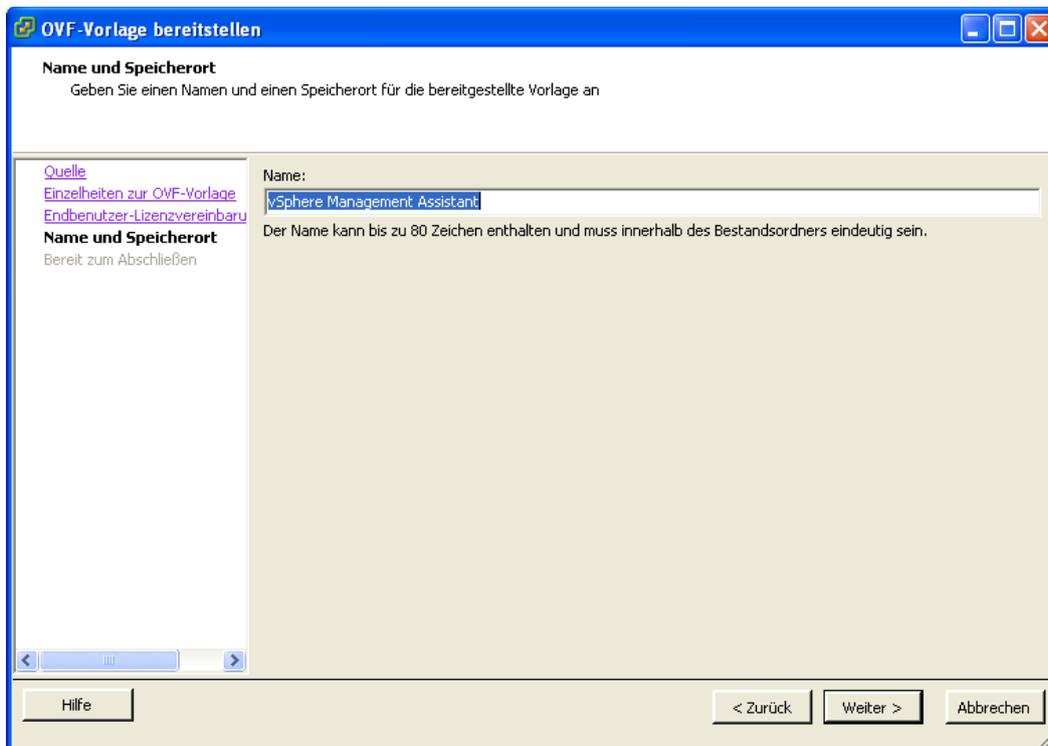


Abbildung 4-26

In der letzten Maske des Assistenten (Abbildung 4-27) werden Ihre Einstellungen zusammengefasst. Mit **Beenden** wird die Bereitstellung gestartet.

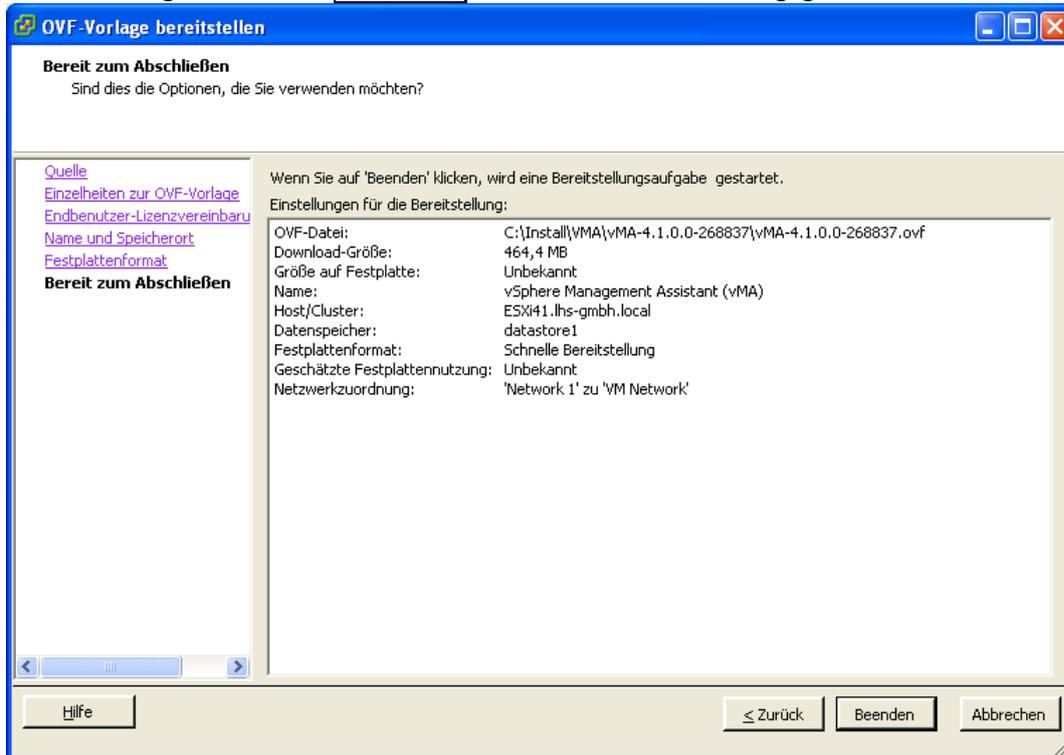


Abbildung 4-27

Klicken Sie auf **Schließen** um die Bereitstellung abzuschließen (Abbildung 4-28).

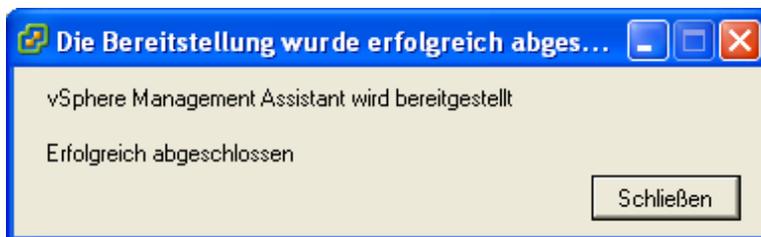


Abbildung 4-28

4.3.3 Konfiguration der vMA 4.1 auf ESXi

Starten Sie Ihre neue virtuelle vMA 4.1 (Abbildung 4-29) im vSphere Client

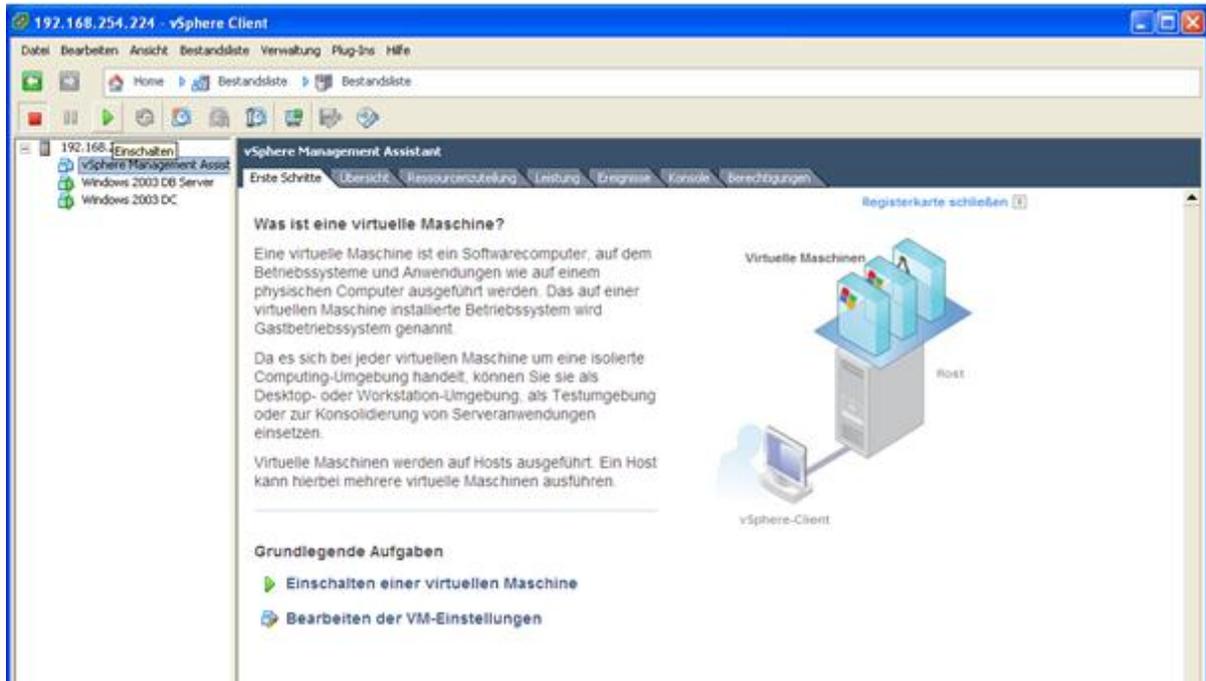


Abbildung 4-29

Öffnen Sie die Konsole der vMA 4.1 (Abbildung 4-30).

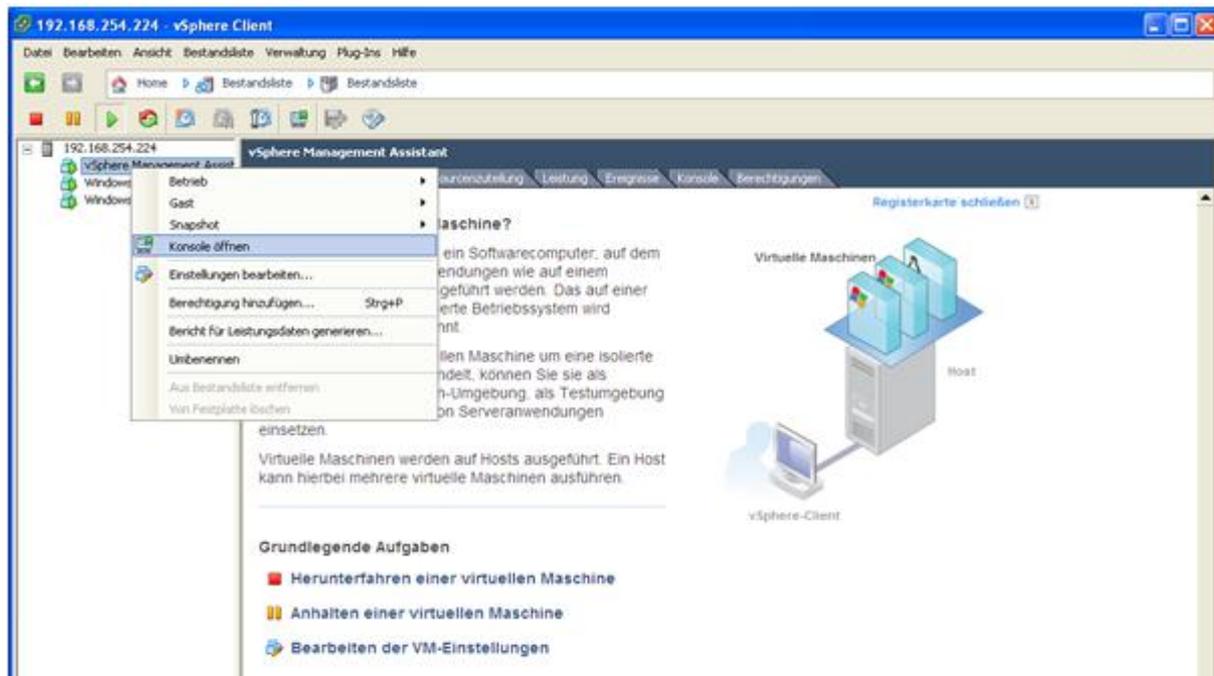


Abbildung 4-30

Es erscheint der vMA 4.1 Start Bildschirm (Abbildung 4-31).

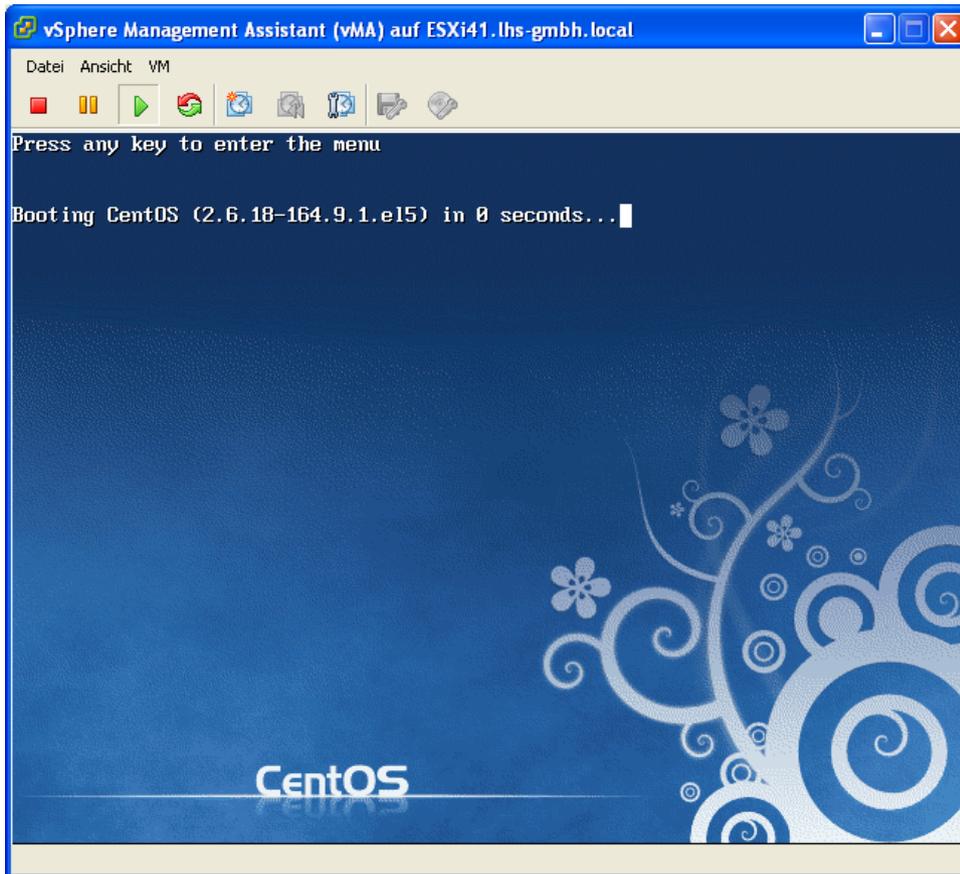


Abbildung 4-31

Entspricht der Host den Kompatibilitätsanforderungen bootet vMA 4.1 bis zur Startkonfiguration (Abbildung 4-32).

Geben Sie bei `Use DHCP to configure network` `no` ein.

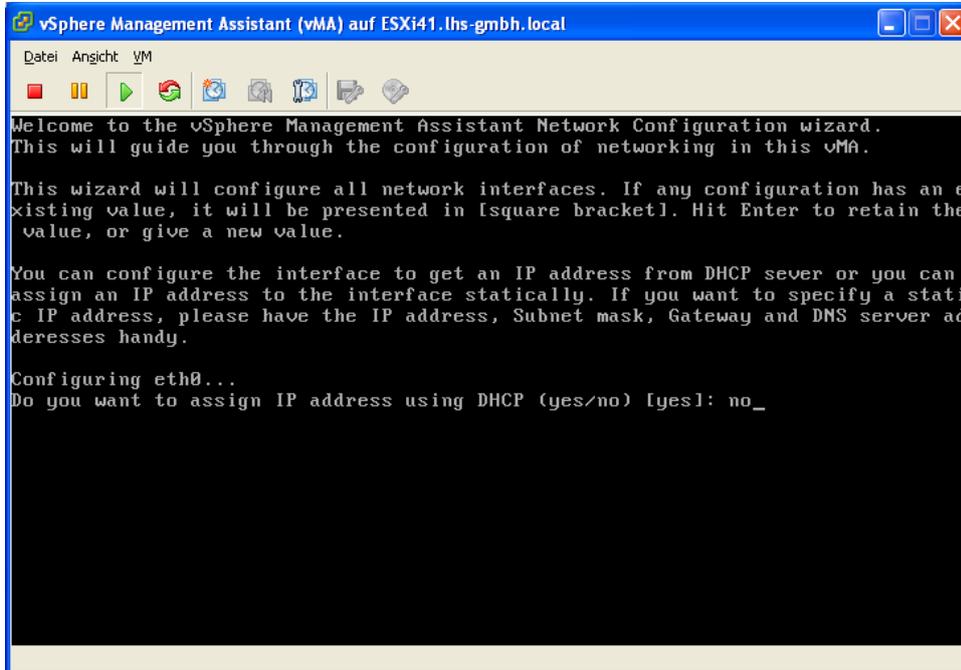


Abbildung 4-32

Geben Sie bei `Enter IP Address` die IP Adresse für die vMA 4.1 ein. In diesem Beispiel ist das die `192.168.254.199` (Abbildung 4-33).



Abbildung 4-33

Bei `Enter Subnet Mask:` geben Sie das passende Subnetz `255.255.255.0` (Abbildung 4-34) ein. Bei `Enter Gateway Address:` die Gateway IP eingeben, welches in der Regel Ihr Internetrouter ist, in unserem Beispiel ist das die `192.168.254.1`.

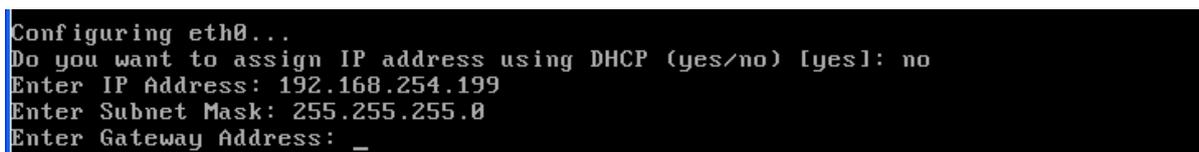


Abbildung 4-34

Bei dem Punkt `Enter Primary DNS Address` geben Sie die IP Adresse Ihres DNS Servers ein. In der Regel ist dies Ihr Internetrouter oder Domänencontroller, in unserem Beispiel ist das die **192.168.254.1** ↵ (Abbildung 4-35).

```
Configuring eth0...
Use DHCP to configure the network (yes/no) [no]: no
Enter IP Address [192.168.254.199]: 192.168.254.199
Enter Subnet Mask [255.255.255.0]: 255.255.255.0
Enter Gateway Address [192.168.254.1]: 192.168.254.1
Enter Primary DNS Address(Press Ctrl-D to clear existing value) [192.168.254.1
192.168.254.1
```

Abbildung 4-35

In dieser Installation wird kein zweiter DNS Server vergeben (Abbildung 4-36). Lassen Sie den Eintrag bei `Enter Secondary DNS Address` leer und bestätigen mit ↵.

```
Configuring eth0...
Use DHCP to configure the network (yes/no) [no]: no
Enter IP Address [192.168.254.199]: 192.168.254.199
Enter Subnet Mask [255.255.255.0]: 255.255.255.0
Enter Gateway Address [192.168.254.1]: 192.168.254.1
Enter Primary DNS Address(Press Ctrl-D to clear existing value) [192.168.254.1
192.168.254.1
Enter Secondary DNS Address(Press Enter to leave it blank):
```

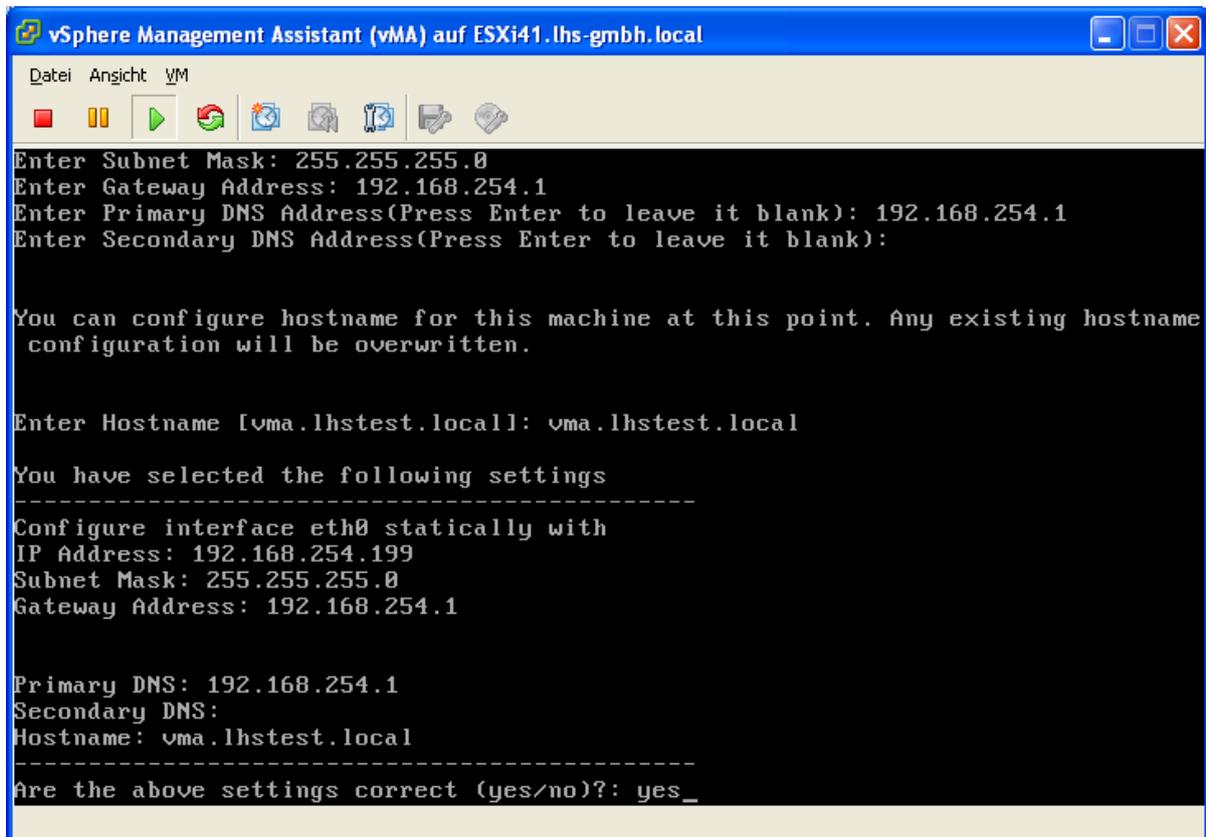
Abbildung 4-36

Geben Sie bei `Enter Hostname` einen Hostnamen (FQDN) für Ihre vMA 4.1 ein. In diesem Beispiel (Abbildung 4-37) ist das **vMA 4.1.lhstest.local** ↵.

```
Configuring eth0...
Use DHCP to configure the network (yes/no) [no]: no
Enter IP Address [192.168.254.199]: 192.168.254.199
Enter Subnet Mask [255.255.255.0]: 255.255.255.0
Enter Gateway Address [192.168.254.1]: 192.168.254.1
Enter Primary DNS Address(Press Ctrl-D to clear existing value) [192.168.254.1
192.168.254.1
Enter Secondary DNS Address(Press Enter to leave it blank):
Enter Hostname [vma.lhstest.local]: vma.lhstest.local
```

Abbildung 4-37

Abschliessend bestätigen Sie Ihre Eingaben mit **yes**↵ (Abbildung 4-38).



```

vSphere Management Assistant (vMA) auf ESXi41.lhs-gmbh.local
Datei Ansicht VM
[Icons]
Enter Subnet Mask: 255.255.255.0
Enter Gateway Address: 192.168.254.1
Enter Primary DNS Address(Press Enter to leave it blank): 192.168.254.1
Enter Secondary DNS Address(Press Enter to leave it blank):

You can configure hostname for this machine at this point. Any existing hostname
configuration will be overwritten.

Enter Hostname [vma.lhstest.local]: vma.lhstest.local

You have selected the following settings
-----
Configure interface eth0 statically with
IP Address: 192.168.254.199
Subnet Mask: 255.255.255.0
Gateway Address: 192.168.254.1

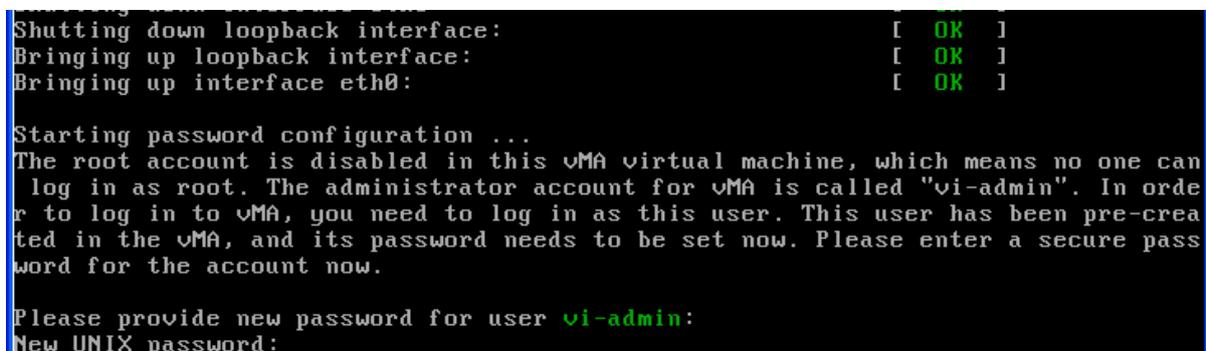
Primary DNS: 192.168.254.1
Secondary DNS:
Hostname: vma.lhstest.local
-----
Are the above settings correct (yes/no)? : yes_
  
```

Abbildung 4-38

Es folgt die Aufforderung ein Passwort für den vi-admin User zu vergeben.

Hinweis: Bei der vMA 4.1 existiert kein Username root! Der User mit diesen Rechten heisst hier vi-admin.

Geben Sie ein neues Kennwort bei `New UNIX password` ein (Abbildung 4-39) und bestätigen mit ↵.



```

Shutting down loopback interface: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface eth0: [ OK ]

Starting password configuration ...
The root account is disabled in this vMA virtual machine, which means no one can
log in as root. The administrator account for vMA is called "vi-admin". In orde
r to log in to vMA, you need to log in as this user. This user has been pre-crea
ted in the vMA, and its password needs to be set now. Please enter a secure pass
word for the account now.

Please provide new password for user vi-admin:
New UNIX password: _
  
```

Abbildung 4-39

Wiederholen Sie die Eingabe bei `Retype new UNIX password:` (Abbildung 4-40).

```
ted in the vMA, and its password needs to be set now. Please enter a secure pass
word for the account now.

Please provide new password for user vi-admin:
New UNIX password:
Retype new UNIX password: _
```

Abbildung 4-40

Um die Konfiguration abzuschliessen, drücken sie eine Taste (Abbildung 4-41).

```
Please provide new password for user vi-admin:
New password:
Retype new password:

Password for vi-admin configured
-----

Use "vi-admin" and configured password for logging into vMA!
-----

Press any key to continue..._
```

Abbildung 4-41

Sie sehen nun den Willkommensbildschirm der vMA 4.1 Durch drücken von ALT-F2 gelangen Sie in die Loginmaske.

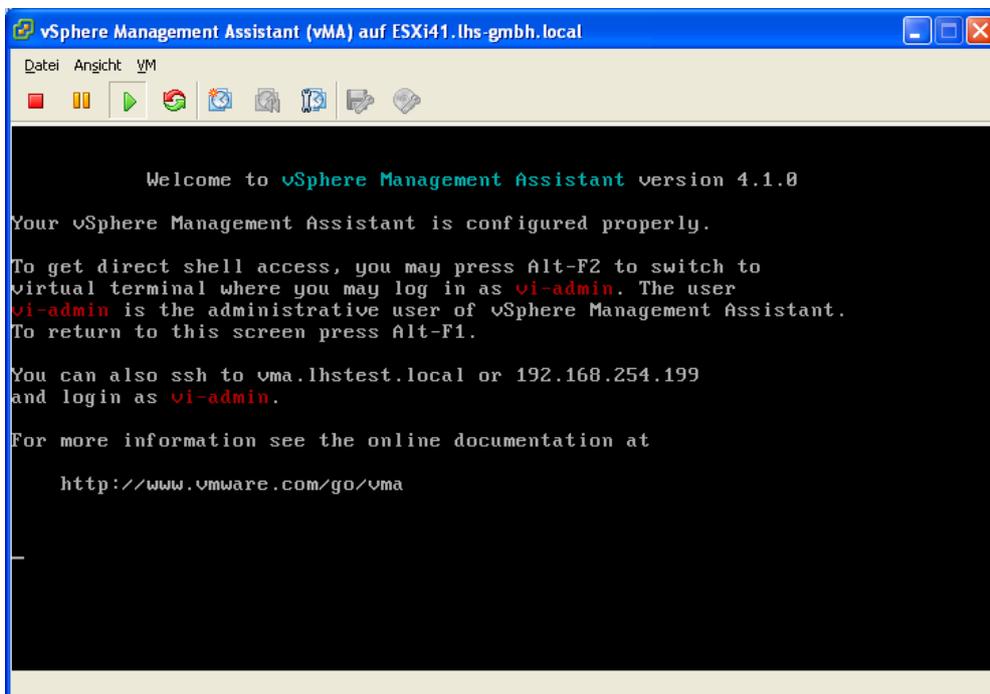


Abbildung 4-42

Sie befinden sich nun in der Loginmaske Ihrer erfolgreich installierten vMA 4.1 (Abbildung 4-43).

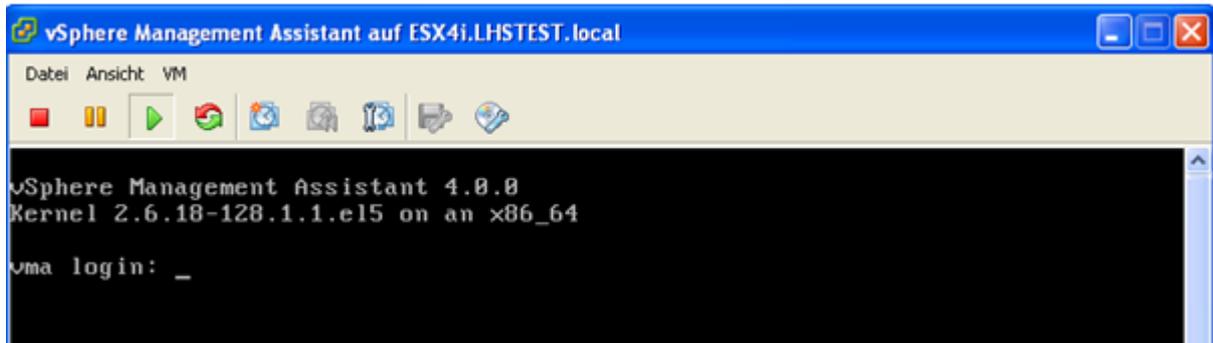


Abbildung 4-43

Melden Sie sich mit **vi-admin** und Ihrem Passwort **xxxxxx** an (Abbildung 4-44).

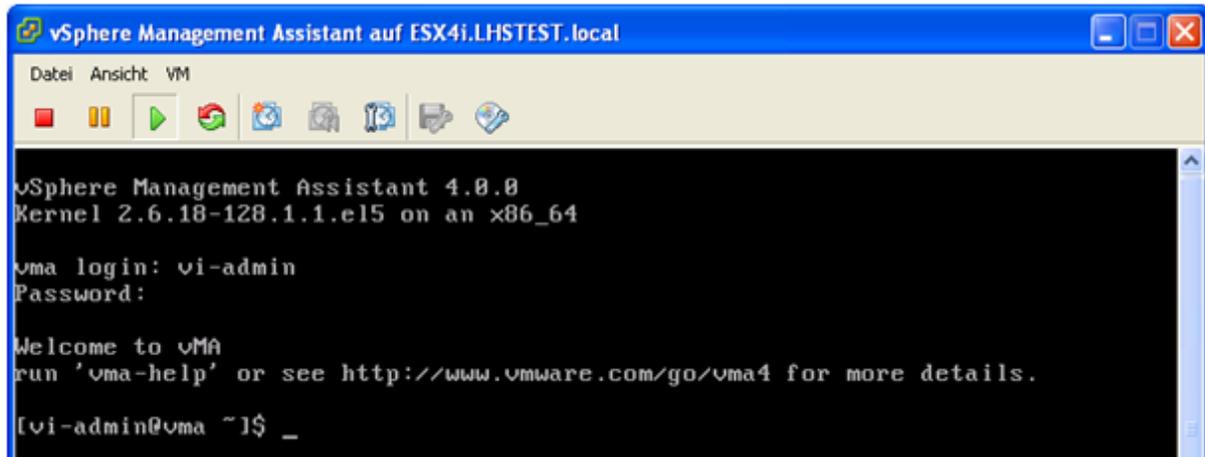


Abbildung 4-44

Als erstes müssen Sie Ihren ESXi bei der vMA 4.1 registrieren!

Dies ist zwingend notwendig, damit Befehle vom RCCMD Client über vMA 4.1 an den ESXi Server weitergeleitet werden können.

Dies geschieht mit dem Befehl `sudo vifp addserver` gefolgt von der IP Adresse oder dem Hostnamen Ihres ESXi Servers.

In unserem Beispiel: `sudo vifp addserver 192.168.254.224` (Abbildung 4-45).

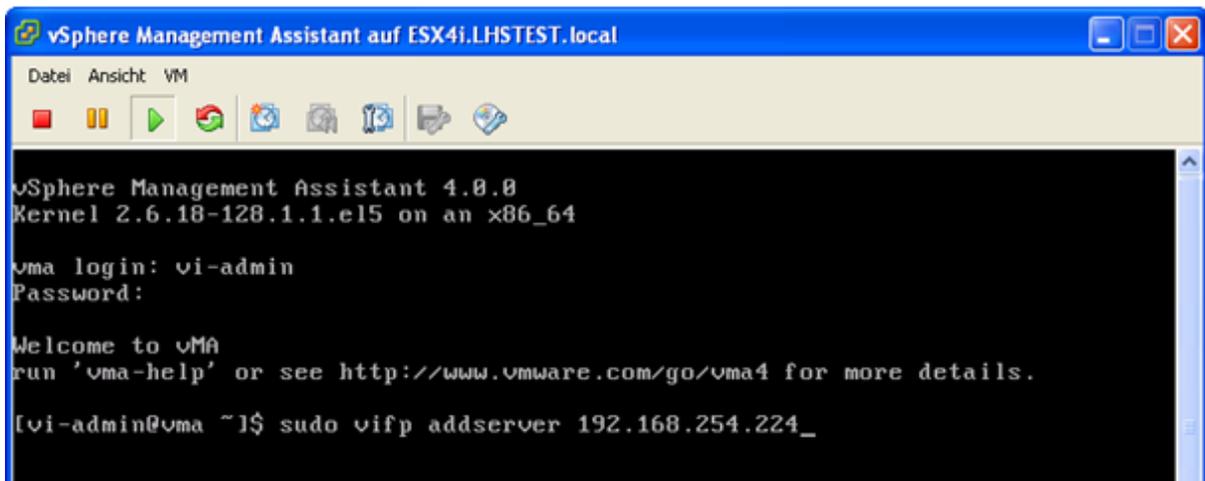
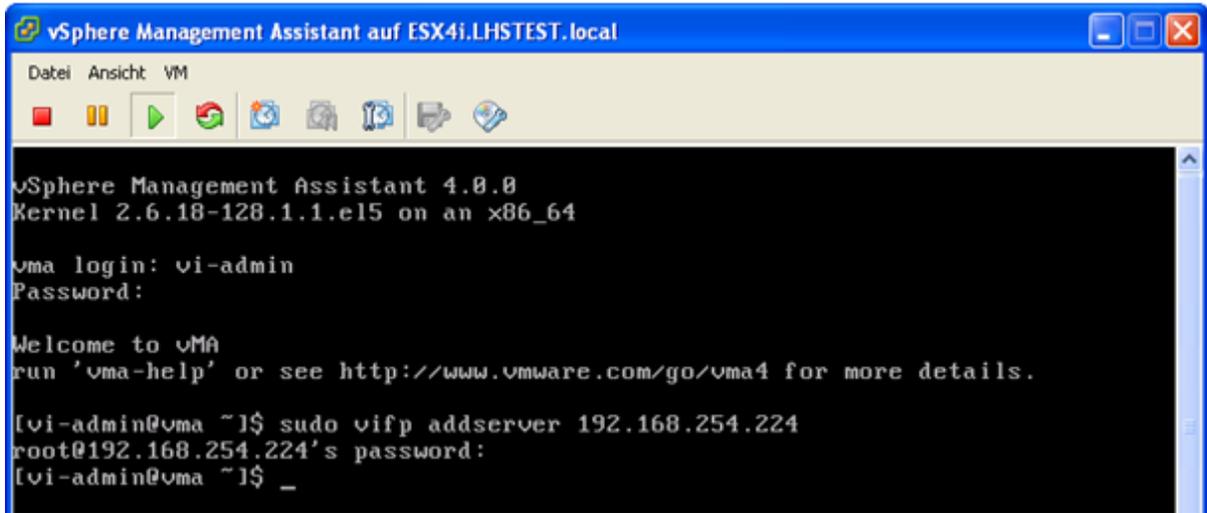


Abbildung 4-45

Zur Bestätigung der Registrierung müssen Sie das Passwort Ihres ESXi Servers eingeben und mit ↵ bestätigen (Abbildung 4-46).



```

vSphere Management Assistant auf ESX4i.LHSTEST.local
Datei Ansicht VM
vSphere Management Assistant 4.0.0
Kernel 2.6.18-128.1.1.el5 on an x86_64

vma login: vi-admin
Password:

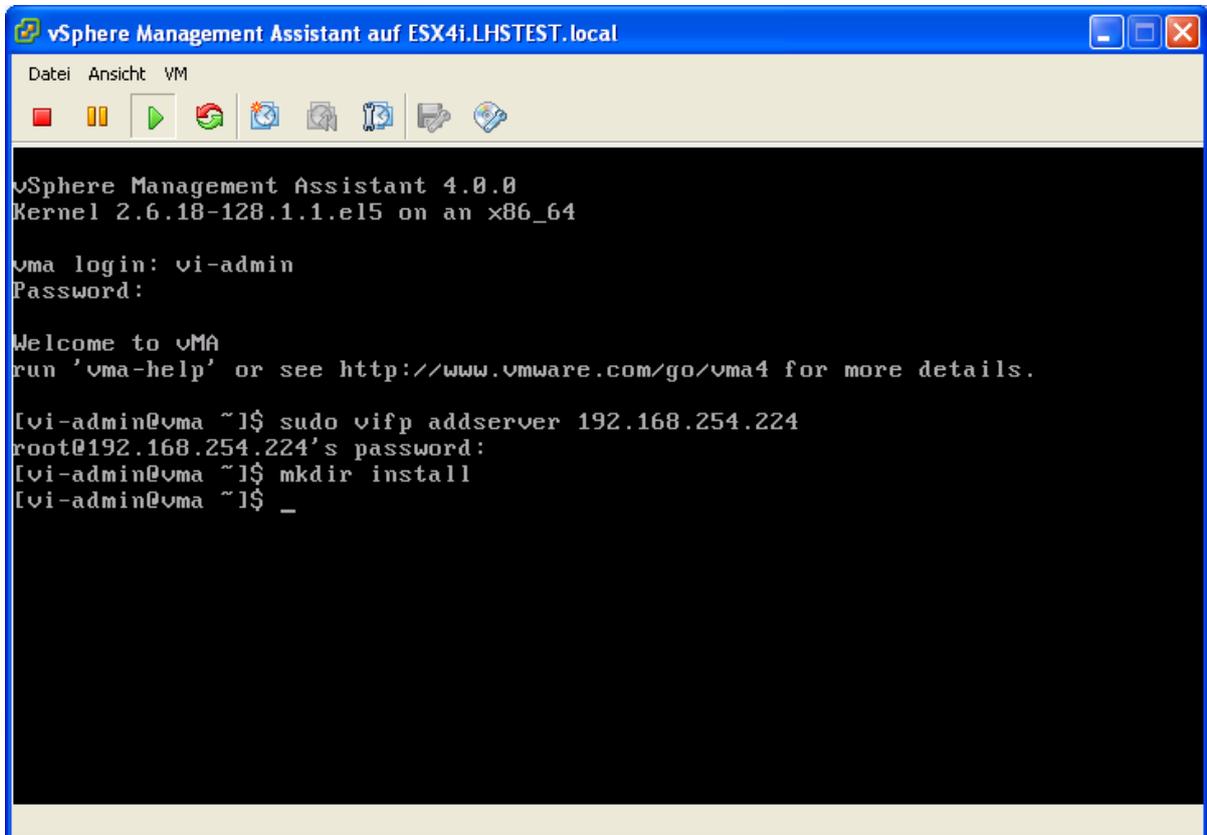
Welcome to vMA
run 'vma-help' or see http://www.vmware.com/go/vma4 for more details.

[vi-admin@vma ~] $ sudo vifp addserver 192.168.254.224
root@192.168.254.224's password:
[vi-admin@vma ~] $ _
  
```

Abbildung 4-46

Wenn keine Fehlermeldung erscheint, ist der ESXi Server bei der vMA 4.1 registriert.

Zum Abschluss dieser Installation legen Sie ein Installationsverzeichnis im Homeverzeichnis des vi-admin Users an: **mkdir install**↵ (Abbildung 4-47).



```

vSphere Management Assistant auf ESX4i.LHSTEST.local
Datei Ansicht VM
vSphere Management Assistant 4.0.0
Kernel 2.6.18-128.1.1.el5 on an x86_64

vma login: vi-admin
Password:

Welcome to vMA
run 'vma-help' or see http://www.vmware.com/go/vma4 for more details.

[vi-admin@vma ~] $ sudo vifp addserver 192.168.254.224
root@192.168.254.224's password:
[vi-admin@vma ~] $ mkdir install
[vi-admin@vma ~] $ _
  
```

Abbildung 4-47

4.4 Kopieren von rccmdinst.tar mit dem Programm WinSCP

Starten Sie das bereits installierte Programm WinSCP (siehe Kapitel 4.2.3). Klicken Sie auf **New**, um eine neue Session aufzubauen (Abbildung 4-48).

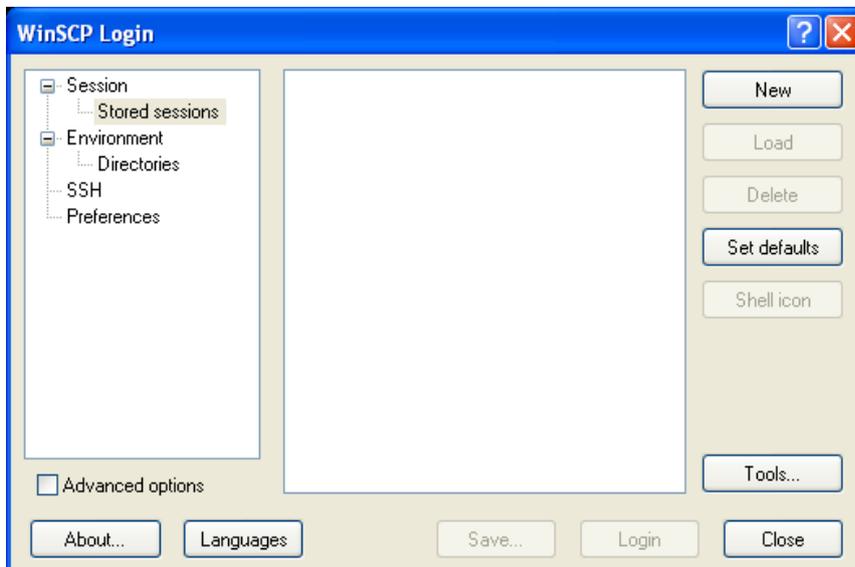


Abbildung 4-48

Hier geben Sie unter **Host name** die IP-Adresse Ihrer vMA 4.1 Appliance, unter **Port number** **22**, den **User name** **vi-admin** und das entsprechende **Password** ein. Über den Button **Login** wird die Session aufgebaut (Abbildung 4-49).

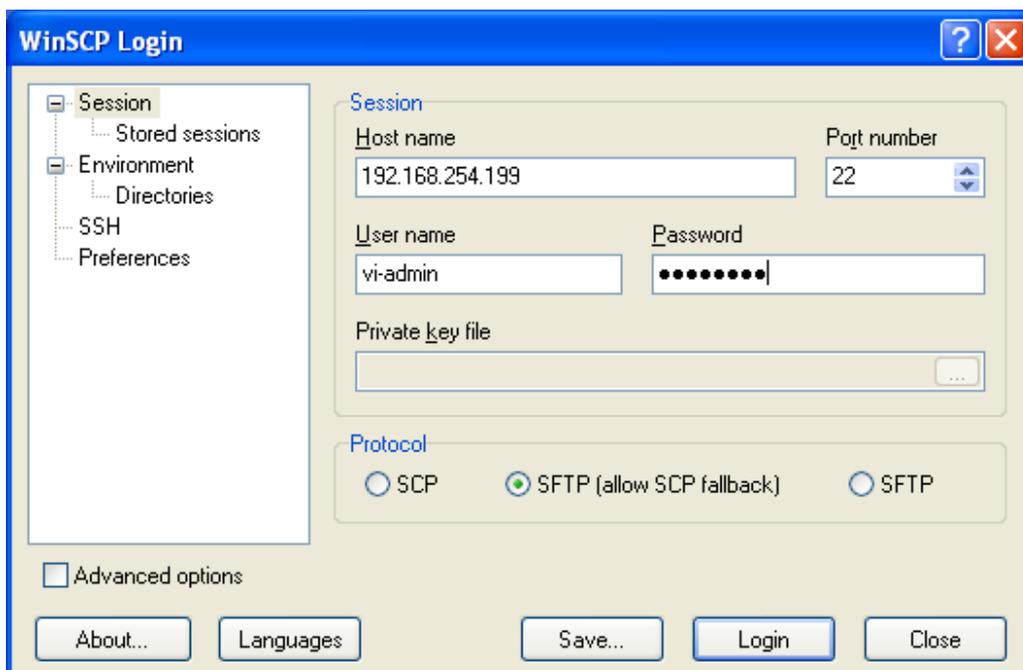


Abbildung 4-49 Loginmaske WinSCP

Bestätigen Sie die Warnung (Abbildung 4-50) mit **Yes**.

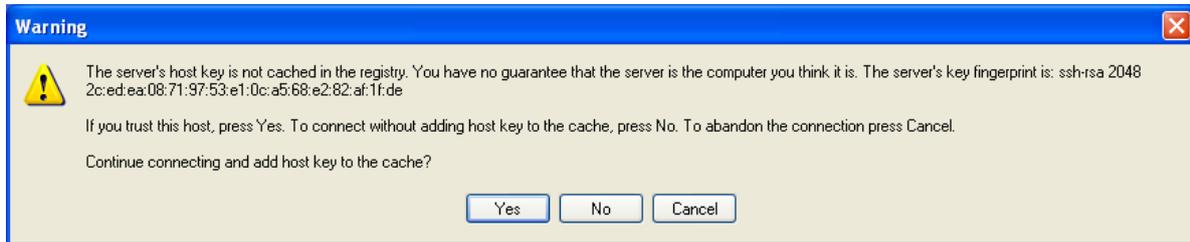


Abbildung 4-50

Kopieren Sie die Datei `rccmdinst.tar` (Kapitel 4.2.1) in das angelegte Installationsverzeichnis `install` auf dem vMA 4.1 (Abbildung 4-51). Dazu markieren Sie die Datei `rccmdinst.tar` und drücken die Taste F5.

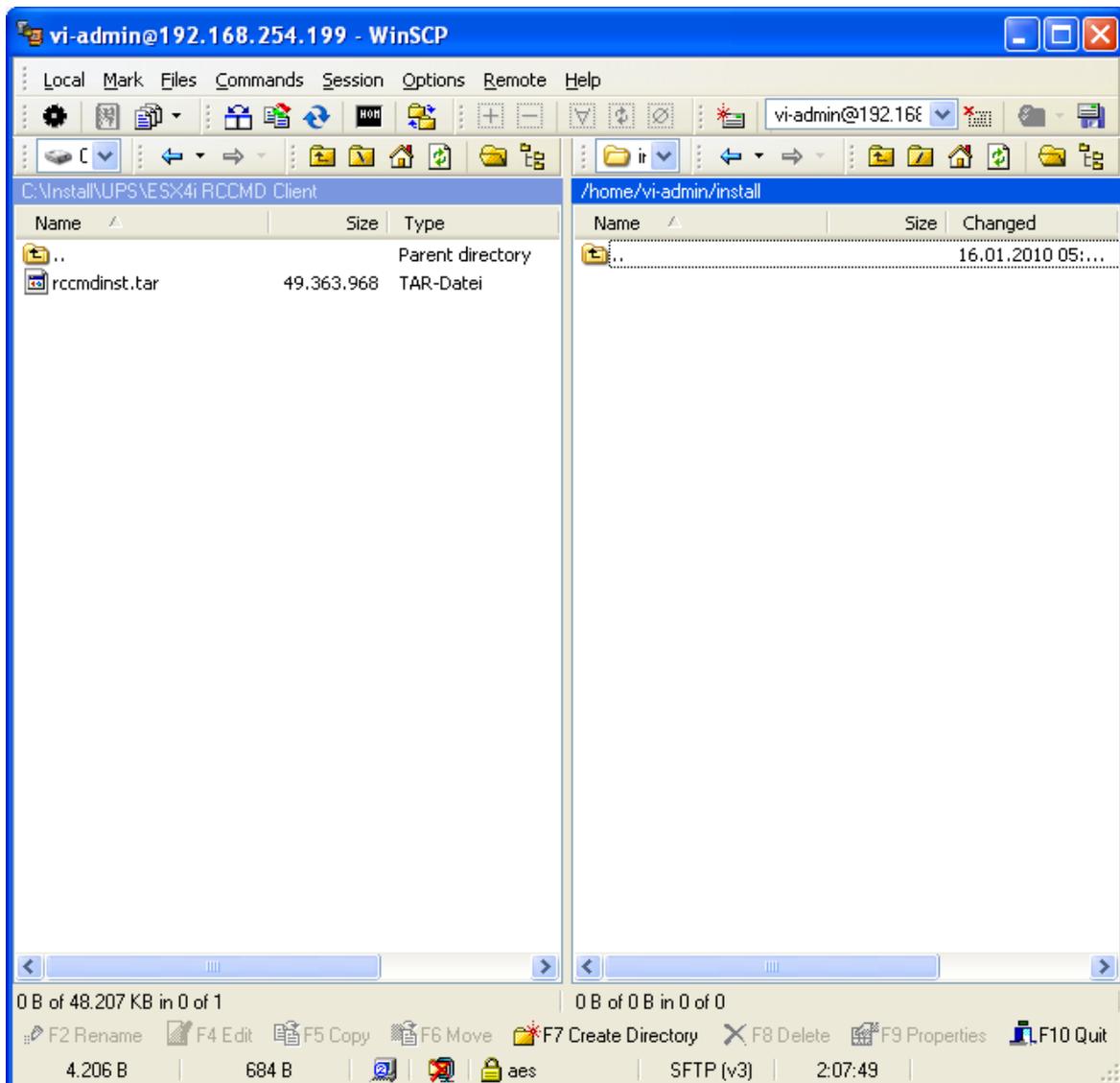


Abbildung 4-51 Transfermaske von WinSCP

Klicken Sie auf **Copy** (Abbildung 4-52).

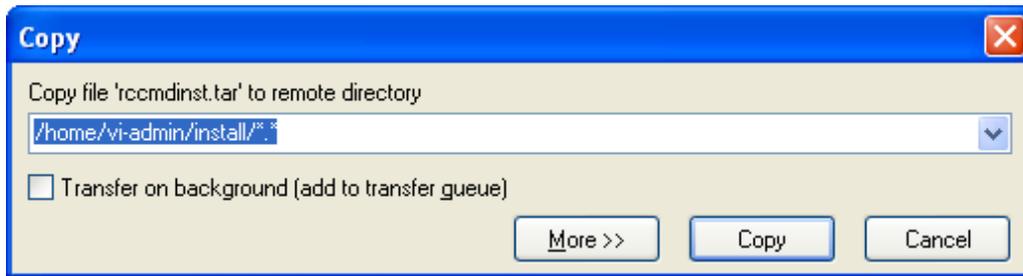


Abbildung 4-52

Die Datei **rccmdinst.tar** liegt nun auf der vMA 4.1 (Abbildung 4-53).

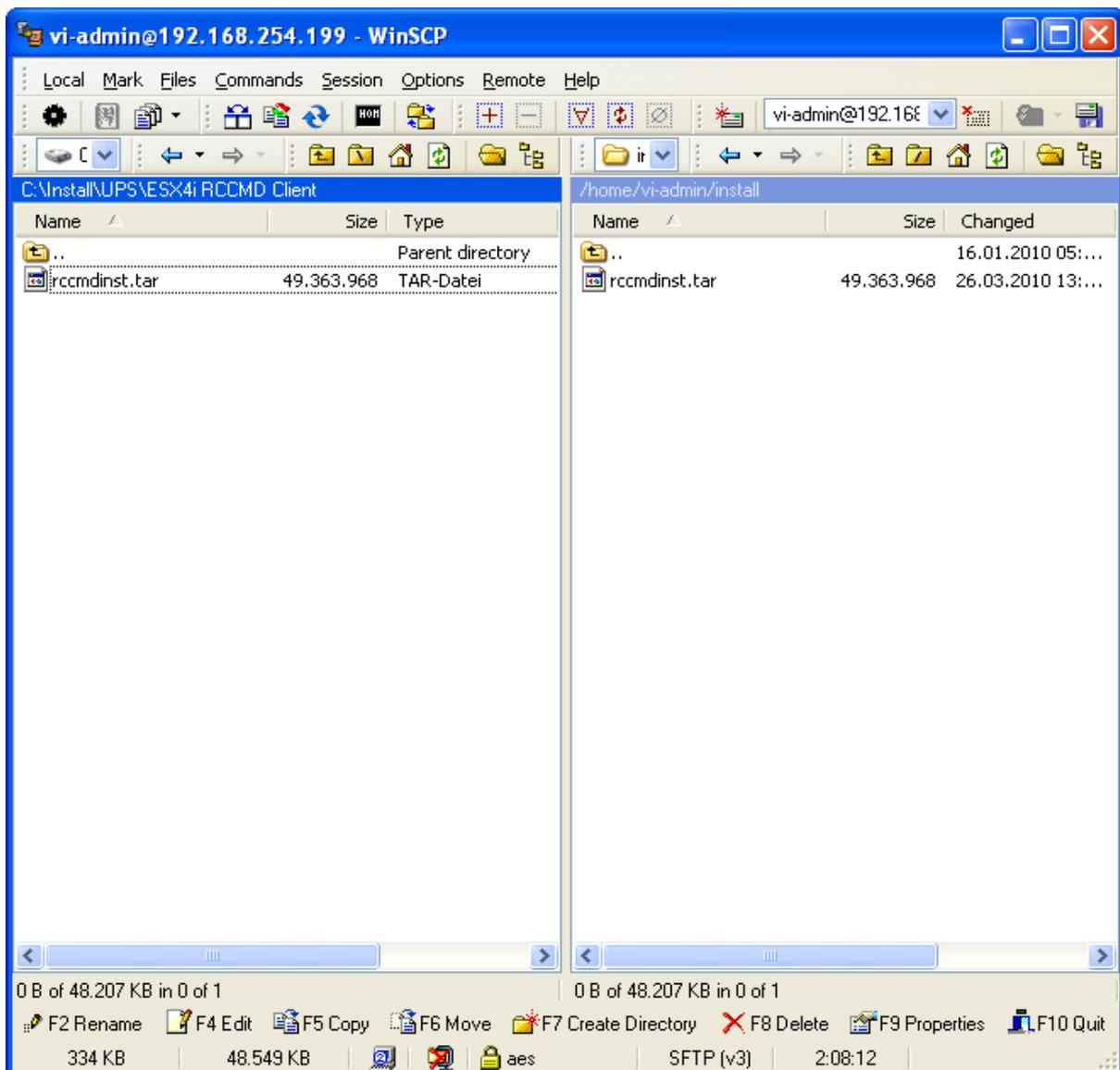


Abbildung 4-53

Das Programm WinSCP kann beendet werden.

4.5 Putty starten und konfigurieren

Starten Sie das Programm Putty (Ausführen von putty.exe. Abbildung 4-54).

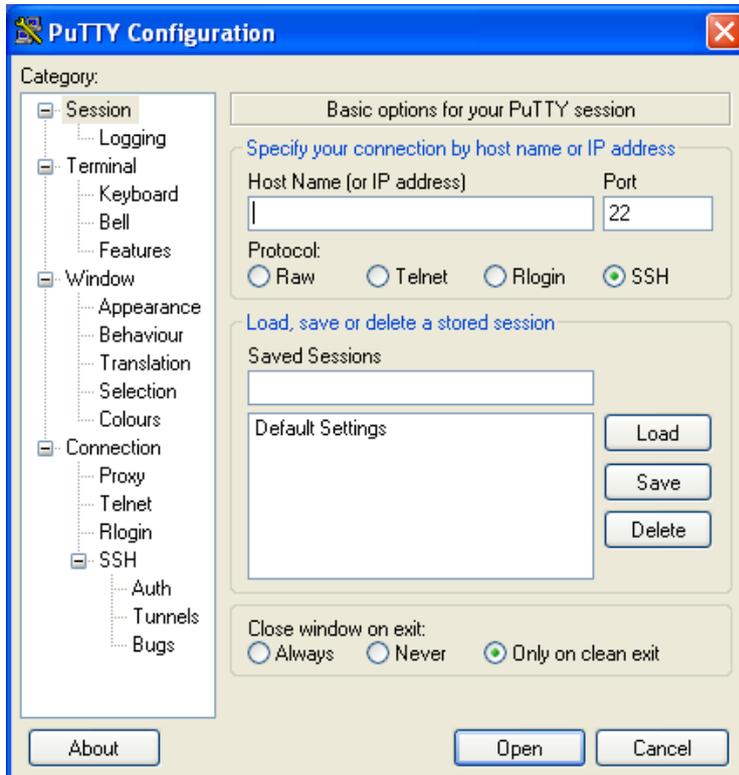


Abbildung 4-54

Im Menüpunkt **Session** sind folgende Einstellungen vorzunehmen (Abbildung 4-55):

Host Name geben Sie hier die IP-Adresse Ihres vMA 4.1 Servers ein.

Port: 22, Protocol: SSH

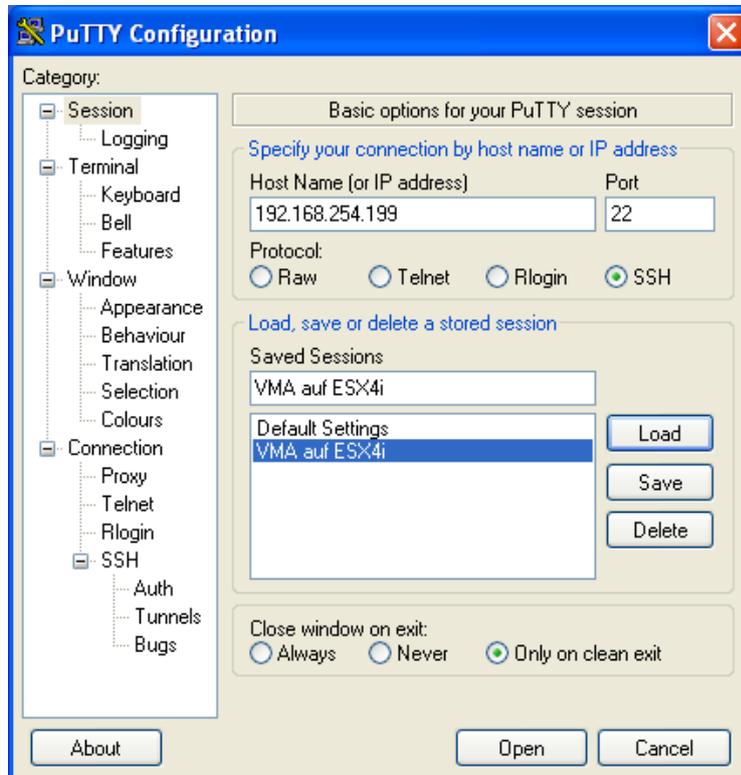


Abbildung 4-55 IP Adresse eingeben

Für eine verbesserte Darstellung wählen Sie den Menüpunkt **Windows** (Abbildung 4-56) und dort den Unterpunkt **Translation**. Setzen Sie den **Character** auf **UTF-8**.

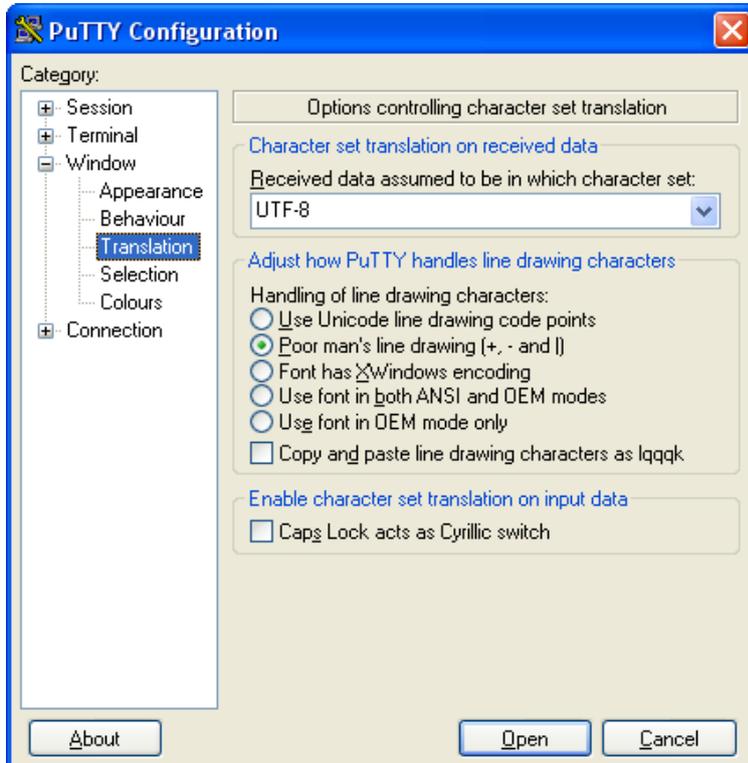


Abbildung 4-56 Character Set auswählen

Um sich via Putty auf dem VMware vMA 4.1 Server anzumelden, klicken Sie auf **Open**. Bei der ersten Verwendung erscheint ein Warnhinweis, den Sie mit **Ja** bestätigen (Abbildung 4-57).



Abbildung 4-57

Sie sollten nun wie gewohnt Ihr Login-Fenster sehen (Abbildung 4-58).



Abbildung 4-58

Melden Sie sich mit User: **vi-admin**, Password: **xxxxxx** (Abbildung 4-59) an.



Abbildung 4-59

Ihr VMware vMA 4.1 Server lässt sich via Putty (fast) genau so bedienen, wie direkt an der Konsole. (Was natürlich über den vSphere Client auch noch möglich ist).



Abbildung 4-60

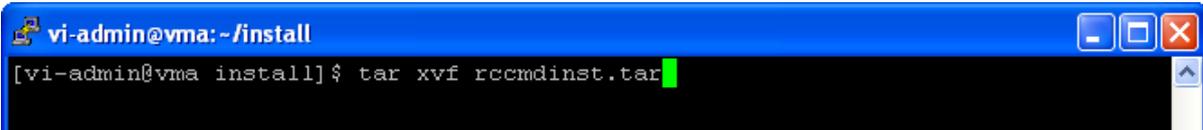
4.6 Installation des RCCMD Clients auf vMA 4.1

Wechseln Sie in das angelegte Installationsverzeichnis mit dem Befehl: **cd_install**.

```
[vi-admin@vma ~]$ cd install
[vi-admin@vma install]$
```

Abbildung 4-61

Entpacken Sie das Archiv mit **tar_xvf_rccmdinst.tar**.

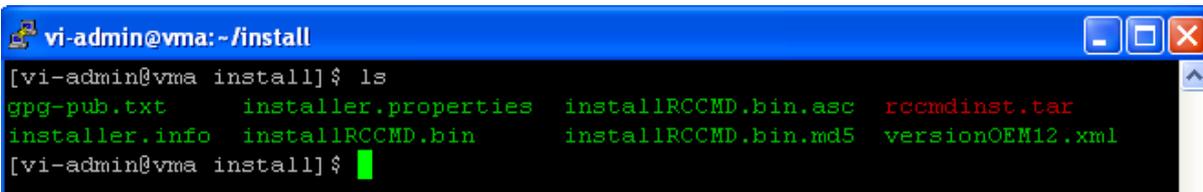


```
vi-admin@vma: ~/install
[vi-admin@vma install]$ tar xvf rccmdinst.tar
```

Abbildung 4-62

Es werden sieben Dateien entpackt.

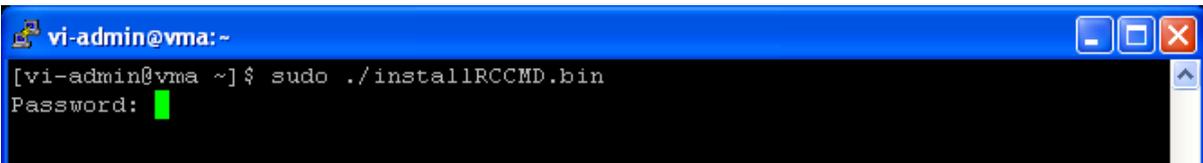
Diese können Sie sich mit dem Befehl **ls** anschauen.



```
vi-admin@vma: ~/install
[vi-admin@vma install]$ ls
gpg-pub.txt      installer.properties  installRCCMD.bin.asc  rccmdinst.tar
installer.info  installRCCMD.bin     installRCCMD.bin.md5  versionOEM12.xml
[vi-admin@vma install]$
```

Abbildung 4-63

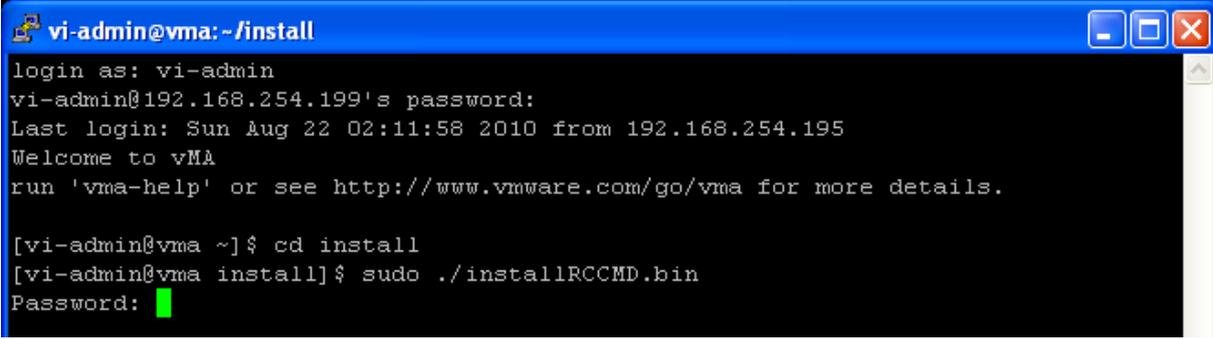
Jetzt können Sie die Installation des RCCMD Clients starten geben sie dazu folgenden Befehl ein: **sudo_./installRCCMD.bin** (Abbildung 4-64).



```
vi-admin@vma: ~
[vi-admin@vma ~]$ sudo ./installRCCMD.bin
Password:
```

Abbildung 4-64

Geben Sie nun Ihr vMA 4.1 Password ein. (Abbildung 4-65)



```
vi-admin@vma:~/install
login as: vi-admin
vi-admin@192.168.254.199's password:
Last login: Sun Aug 22 02:11:58 2010 from 192.168.254.195
Welcome to vMA
run 'vma-help' or see http://www.vmware.com/go/vma for more details.

[vi-admin@vma ~]$ cd install
[vi-admin@vma install]$ sudo ./installRCCMD.bin
Password: █
```

Abbildung 4-65

Wählen Sie die Installationsprache (Abbildung 4-66). In unserem Beispiel wählen Sie bitte die **1** für Deutsch und drücken **↵**.



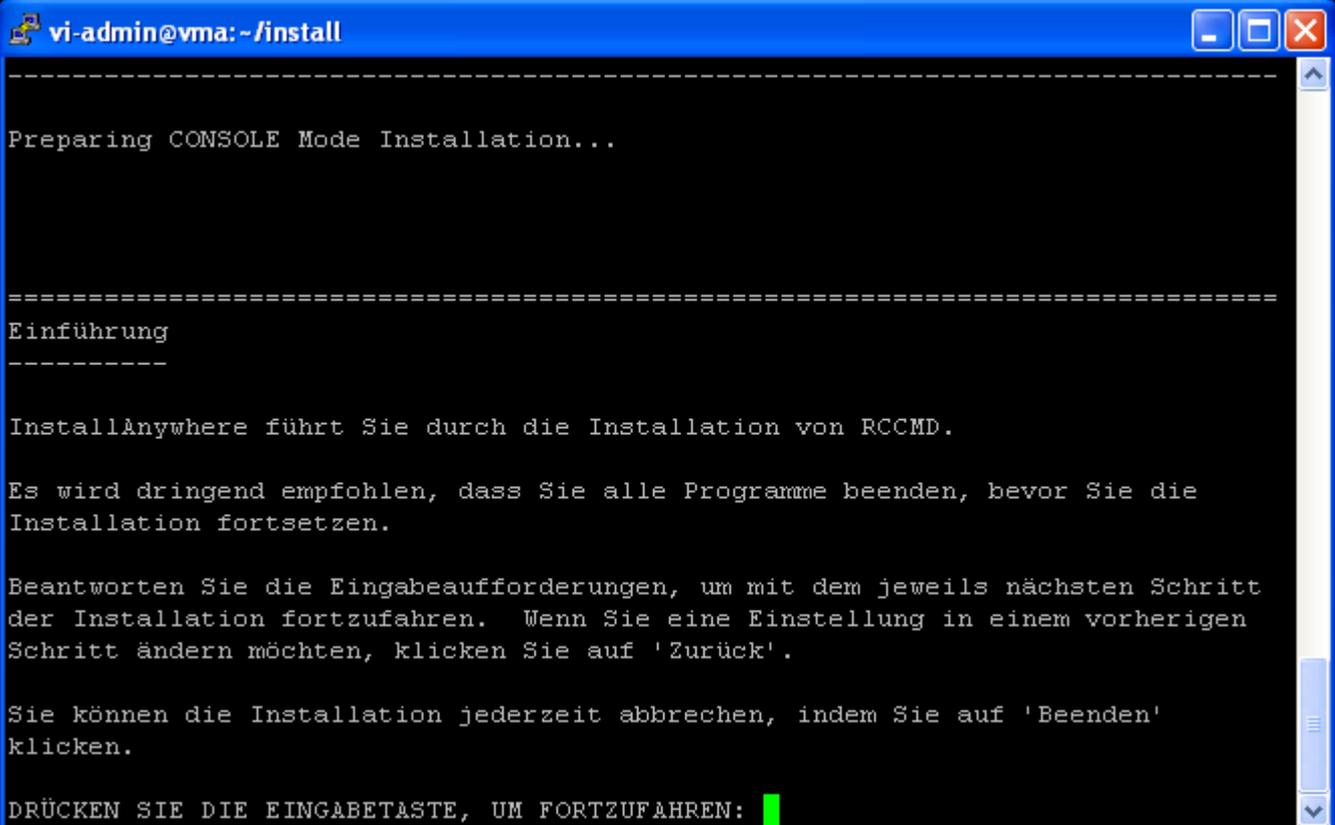
```
=====
Choose Locale...
-----

  1- Deutsch
->2- English
  3- Español
  4- Français
  5- Italiano
  6- Português

CHOOSE LOCALE BY NUMBER: 1 █
```

Abbildung 4-66

Um Fortzufahren drücken Sie ↵. (Abbildung 4-67)



```

vi-admin@vma:~/install
-----
Preparing CONSOLE Mode Installation...

-----
Einführung
-----

InstallAnywhere führt Sie durch die Installation von RCCMD.

Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die
Installation fortsetzen.

Beantworten Sie die Eingabeaufforderungen, um mit dem jeweils nächsten Schritt
der Installation fortzufahren. Wenn Sie eine Einstellung in einem vorherigen
Schritt ändern möchten, klicken Sie auf 'Zurück'.

Sie können die Installation jederzeit abbrechen, indem Sie auf 'Beenden'
klicken.

DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN: █
  
```

Abbildung 4-67

Nach erfolgter Umgebungserkennung drücken Sie ↵. (Abbildung 4-68)



```

-----
SysOS & Platform
-----

OS & CPU Architektur: x86_64 x86_64 GNU/Linux

VMware ESXi Umgebung erkannt.

DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN: █
  
```

Abbildung 4-68

Geben Sie nun Ihren RCCMD Lizenzschlüssel ein und drücken ↵. (Abbildung 4-69)



```

-----
Geben Sie ihren Lizenzschlüssel ein
-----

Geben Sie ihren Lizenzschlüssel ein
Normalerweise ist der Lizenzschlüssel im Handbuch oder auf der CD-Hülle
vermerkt.

Lizenzschlüssel eingeben: 4DWXXXX-1234XXXXXX █
  
```

Abbildung 4-69

Geben Sie die IP Adresse Ihres ESXi Servers ein. In unserem Beispiel ist das **192.168.254.224** und drücken ↵. (Abbildung 4-70)

```
=====
Wie heißt der ESXi Host?
-----

Geben Sie Namen oder IP-Adresse des ESXi Hosts ein.

Name oder IP-Adresse (DEFAULT: ): 192.168.254.224 █
```

Abbildung 4-70

Geben Sie Ihr ESXi Benutzerkennung mit Rootrechten ein. In diesem Beispiel ist das **root** und drücken ↵. (Abbildung 4-71)

```
=====
ESXi Userdetails
-----

Geben Sie eine Benutzerkennung an, die berechtigt ist den ESXi-Host herunterzufahren ( z.B. root)

Benutzername (DEFAULT: root): root █
```

Abbildung 4-71

Tippen Sie Ihr ESXi Passwort ein und drücken ↵. (Abbildung 4-72)

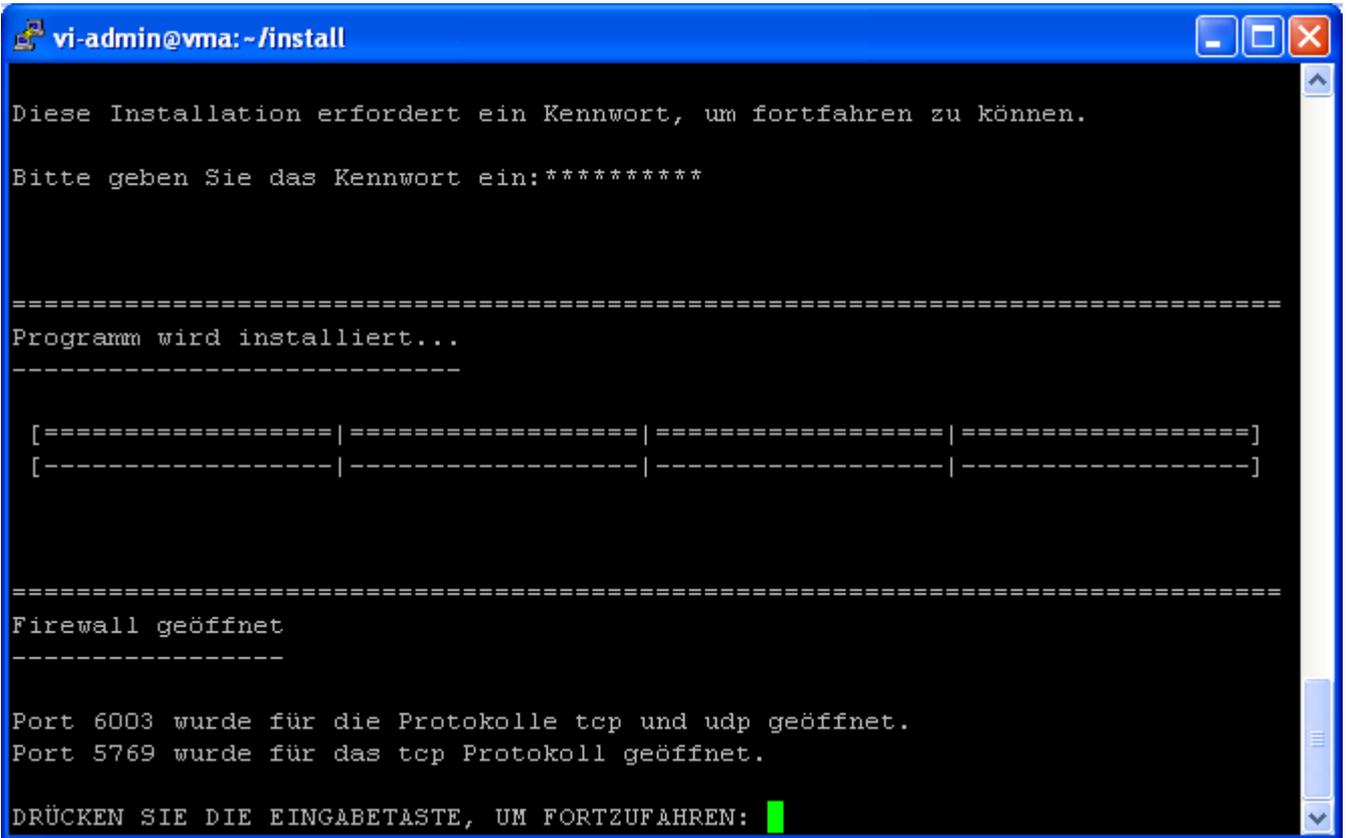
```
=====
Kennwort eingeben
-----

Diese Installation erfordert ein Kennwort, um fortfahren zu können.

Bitte geben Sie das Kennwort ein:***** █
```

Abbildung 4-72

Die Installation startet, um fortzufahren drücken Sie ↵. (Abbildung 4-73)



```

vi-admin@vma:~/install
=====
Diese Installation erfordert ein Kennwort, um fortfahren zu können.
Bitte geben Sie das Kennwort ein:*****

=====
Programm wird installiert...
-----

[=====|=====|=====|=====|=====]
[-----|-----|-----|-----|-----]

=====
Firewall geöffnet
-----

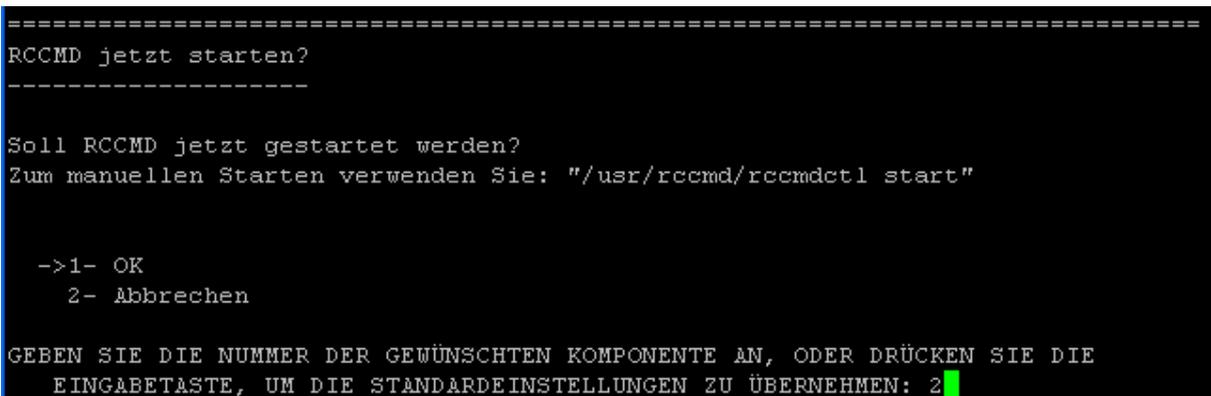
Port 6003 wurde für die Protokolle tcp und udp geöffnet.
Port 5769 wurde für das tcp Protokoll geöffnet.

DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN: █

```

Abbildung 4-73

Wählen Sie nun die 2 aus und drücken ↵. (Abbildung 4-74) Damit wird der RCCMD Client nicht gestartet! Dies erfolgt erst nach der Konfiguration des RCCMD Clients.



```

=====
RCCMD jetzt starten?
-----

Soll RCCMD jetzt gestartet werden?
Zum manuellen Starten verwenden Sie: "/usr/rccmd/rccmdctl start"

->1- OK
    2- Abbrechen

GEBEN SIE DIE NUMMER DER GEWÜNSCHTEN KOMPONENTE AN, ODER DRÜCKEN SIE DIE
EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ÜBERNEHMEN: 2 █

```

Abbildung 4-74

Um fortzufahren drücken Sie bitte ↵. Die Konfiguration des RCCMD Clients wird im nächsten Kapitel behandelt.

```
=====
RCCMD-Konfiguration erforderlich
-----

Eine Konfiguration des RCCMD ist erforderlich. Dazu muss die
"/usr/rccmd/rccmd.cfg" bearbeitet werden.

Sollten Sie entscheiden den RCCMD mit der Standardkonfiguration zu starten, ist
es von jeder Netzwerkadresse aus möglich an diesen Nachrichten zu senden.
Bitte richten Sie eine oder mehrere IP-Adressen ein, die berechtigt sein sollen
diesem RCCMD Nachrichten zu senden.

DRÜCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN: █
```

Abbildung 4-75

Um die Installation zu beenden drücken Sie ↵.

```
=====
Installation abgeschlossen
-----

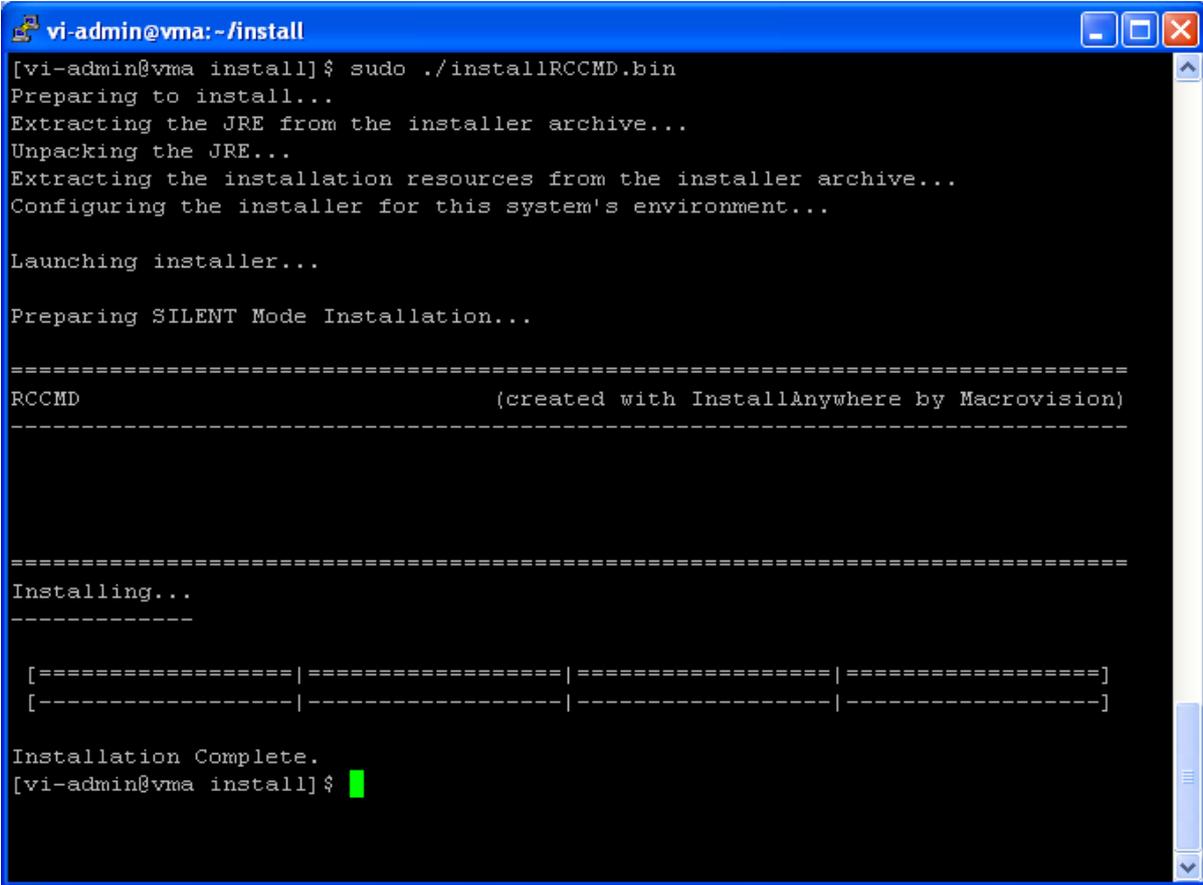
Herzlichen Glückwunsch. RCCMD wurde erfolgreich im folgenden Verzeichnis
installiert:

    /usr/rccmd

DRÜCKEN SIE DIE EINGABETASTE, UM DEN INSTALLER ZU BEENDEN:
[vi-admin@vma install]$ █
```

Abbildung 4-76

Am Ende der Bildschirmausgabe sollte der Eintrag `Installation Complete` stehen. Damit ist die Installation des RCCMD Clients abgeschlossen. (Abbildung 4-77)



```
vi-admin@vma: ~/install
[vi-admin@vma install]$ sudo ./installRCCMD.bin
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

Preparing SILENT Mode Installation...

=====
RCCMD                               (created with InstallAnywhere by Macrovision)
=====

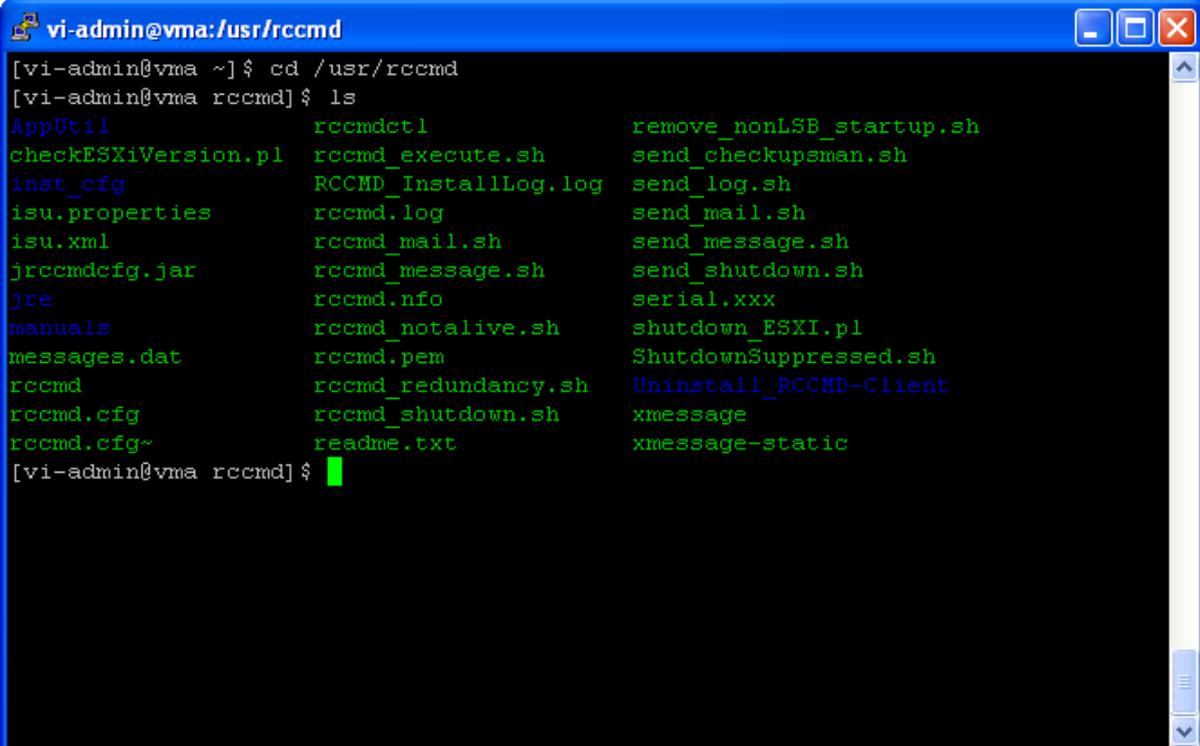
Installing...
-----

[-----|-----|-----|-----]
[-----|-----|-----|-----]

Installation Complete.
[vi-admin@vma install]$ █
```

Abbildung 4-77

Prüfen Sie ob die Dateien des RCCMD Clients ordnungsgemäß ins Zielverzeichnis geschrieben wurden .Wechseln Sie dazu mit dem Befehl `cd /usr/rccmd` in das Zielverzeichnis und geben `ls` ein. Die Auflistung sollte der wie in dargestellt entsprechen.



```

vi-admin@vma:~/usr/rccmd
[vi-admin@vma ~]$ cd /usr/rccmd
[vi-admin@vma rccmd]$ ls
AppUtil                rccmdctl                remove_nonLSB_startup.sh
checkESXiVersion.pl   rccmd_execute.sh        send_checkupsman.sh
inst_cfg               RCCMD_InstallLog.log    send_log.sh
isu.properties         rccmd.log                send_mail.sh
isu.xml                rccmd_mail.sh           send_message.sh
jrcmcdcfg.jar          rccmd_message.sh        send_shutdown.sh
jre                    rccmd.nfo                serial.xxx
manuals                rccmd_notalive.sh       shutdown_ESXI.pl
messages.dat           rccmd.pem                ShutdownSuppressed.sh
rccmd                  rccmd_redundancy.sh     Uninstall_RCCMD-Client
rccmd.cfg              rccmd_shutdown.sh       xmessage
rccmd.cfg~             readme.txt                xmessage-static
[vi-admin@vma rccmd]$

```

Abbildung 4-78

So noch nicht vorhanden, erzeugen Sie folgende Datei mittels `vi .esxi_creds`.



```
vi-admin@vma:/usr/rccmd
[vi-admin@vma rccmd] $ vi .esxi_creds
```

Abbildung 4-81

In der Datei tragen Sie die IP Adresse und die Authentifizierungsdaten des herunterzufahrenden Servers ein.

In unserem Beispiel ist das (Abbildung 4-82)

`VI_Server = 192.168.254.224`

`VI_Username = root`

`VI_Password = xxxxxx`



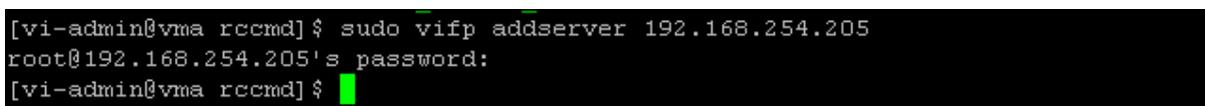
```
vi-admin@vma:/usr/rccmd
VI_SERVER = 192.168.254.224
VI_USERNAME = root
VI_PASSWORD = xxxxxx
~
```

Abbildung 4-82

Mit `wq!` abspeichern, da die Datei schreibgeschützt sein kann.

Sollen noch weitere ESXi Hosts heruntergefahren werden, melden Sie diesen zunächst bei der vMA 4.1 an.

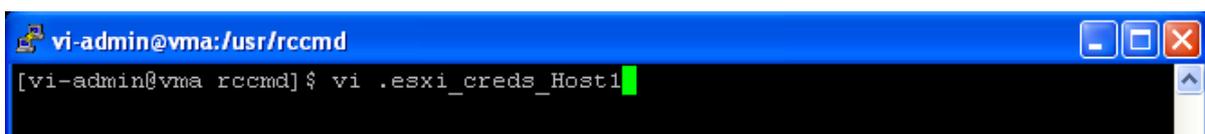
In unserem Beispiel ist das `sudo vifp addserver 192.168.254.205`.



```
[vi-admin@vma rccmd] $ sudo vifp addserver 192.168.254.205
root@192.168.254.205's password:
[vi-admin@vma rccmd] $
```

Abbildung 4-83

Erzeugen Sie eine zusätzliche Datei mittels `vi .esxi_creds_Host1`.



```
vi-admin@vma:/usr/rccmd
[vi-admin@vma rccmd] $ vi .esxi_creds_Host1
```

Abbildung 4-84

In der zusätzlichen Datei tragen Sie die IP Adresse und die Authentifizierungsdaten des herunterzufahrenden Servers ein.

In unserem Beispiel ist das:

```
VI_Server = 192.168.254.205
```

```
VI_Username = root
```

```
VI_Password = xxxxxx
```



```
vi-admin@vma: /usr/rccmd
VI_SERVER = 192.168.254.205
VI_USERNAME = root
VI_PASSWORD = [REDACTED]
```

Abbildung 4-85

Mit `:wq!` abspeichern.

Im nächsten Schritt editieren Sie die Datei `rccmd.cfg` mit dem Befehl `vi_rccmd.cfg` (Abbildung 4-87).



Abbildung 4-87

Bei `AllowedAddresses=` tragen Sie die IP-Adresse des Rccmdsender ein. In unserem Beispiel ist das **192.168.254.254**. (Abbildung 4-88). Somit stellen Sie sicher, dass kein anderer Rccmdsender den VMware ESXi Server herunterfahren kann.

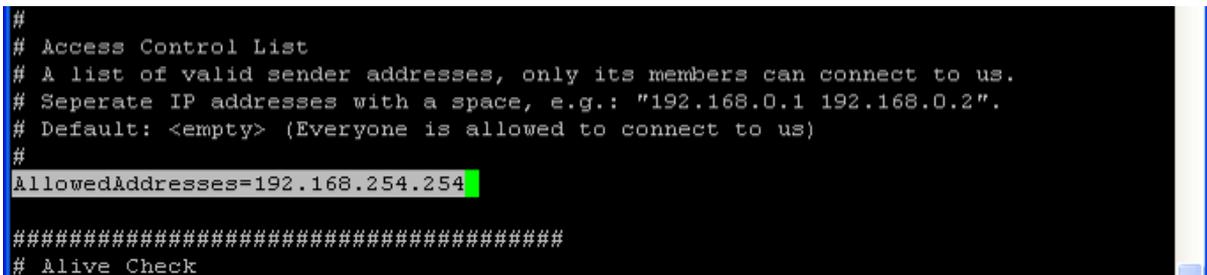


Abbildung 4-88

Setzen Sie bei `AliveEnabled=` den Wert auf **true**. Damit prüft der RCCMD Client ob die USV über das SNMP Modul erreichbar ist (Abbildung 4-89).

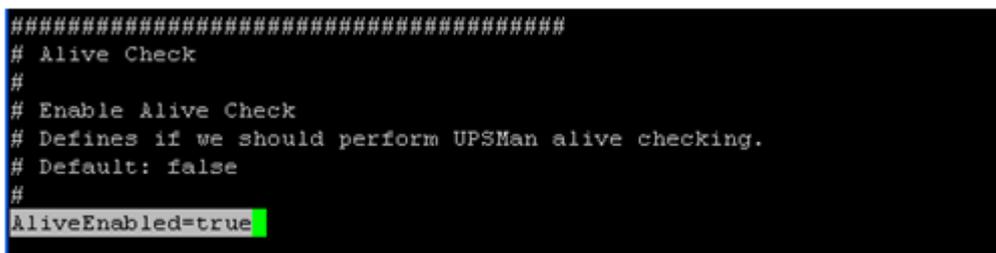


Abbildung 4-89

Tragen Sie unter `AliveAddresses=` die IP Adresse des SNMP Adapters Ihrer USV ein. In unserem Beispiel ist das die **192.168.254.254** (Abbildung 4-90).

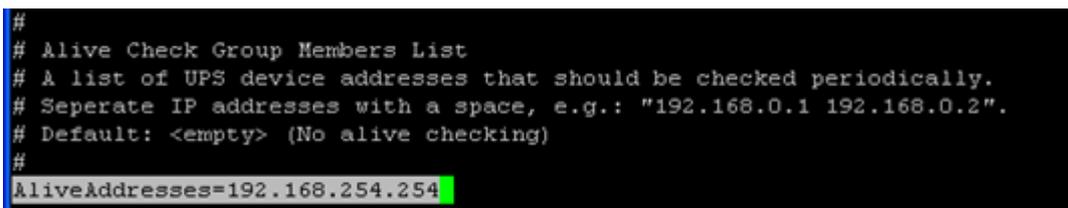


Abbildung 4-90

Zum Speichern der Änderungen drücken Sie die ESC-Taste und geben `:wq` ein (Abbildung 4-91).

```
AliveAddresses=192.168.254.254
#
# Alive Program
# Full path to script that is executed when an alive check fails.
# Default: rccmd_notalive.sh
:wq
```

Abbildung 4-91

Damit die Änderungen angewendet werden, müssen Sie den RCCMD Client neu starten. Dazu wechseln Sie mit `cd /etc/init.d` in das Dienststartverzeichnis `init.d` (Abbildung 4-92).



```
vi-admin@vma:/usr/rccmd
[vi-admin@vma rccmd]$ cd /etc/init.d
```

Abbildung 4-92

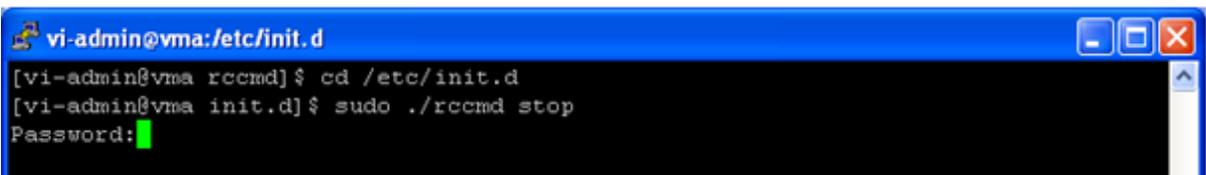
Mit `sudo ./rccmd_stop` beenden Sie den RCCMD Dienst (Abbildung 4-93).



```
vi-admin@vma:/etc/init.d
[vi-admin@vma rccmd]$ cd /etc/init.d
[vi-admin@vma init.d]$ sudo ./rccmd stop
```

Abbildung 4-93

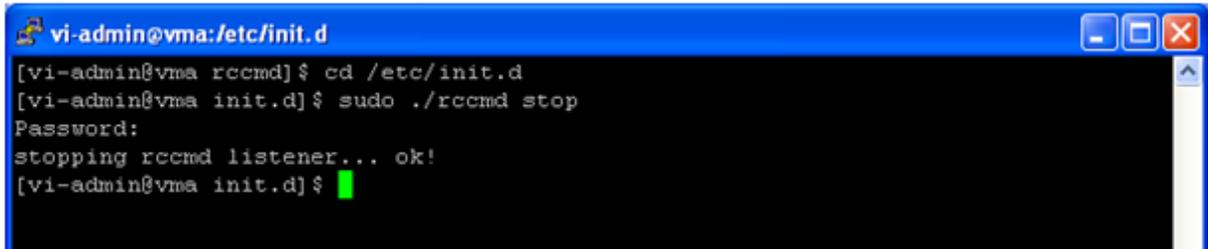
Da es sich um einen Eingriff mit erforderlichen Rootrechten handelt, geben Sie nun Ihr Passwort für die vMA 4.1 ein (Abbildung 4-94).



```
vi-admin@vma:/etc/init.d
[vi-admin@vma rccmd]$ cd /etc/init.d
[vi-admin@vma init.d]$ sudo ./rccmd stop
Password:
```

Abbildung 4-94

Der RCCMD Dienst wird gestoppt (Abbildung 4-95).

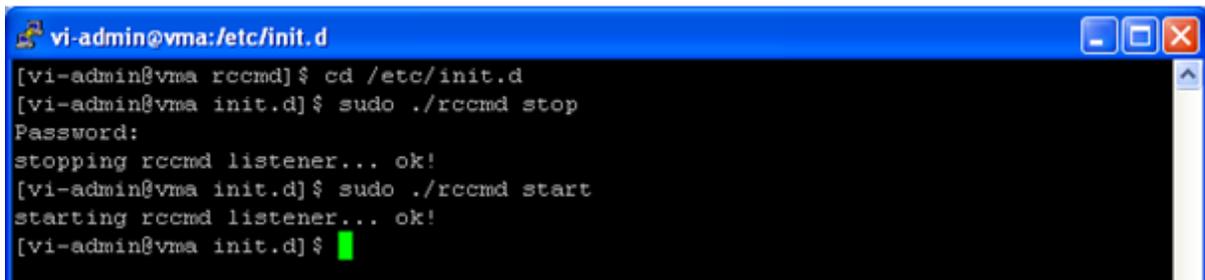


```

vi-admin@vma:/etc/init.d
[vi-admin@vma rccmd]$ cd /etc/init.d
[vi-admin@vma init.d]$ sudo ./rccmd stop
Password:
stopping rccmd listener... ok!
[vi-admin@vma init.d]$
  
```

Abbildung 4-95

Mit `sudo ./rccmd start` starten Sie den RCCMD Dienst erneut (Abbildung 4-96).



```

vi-admin@vma:/etc/init.d
[vi-admin@vma rccmd]$ cd /etc/init.d
[vi-admin@vma init.d]$ sudo ./rccmd stop
Password:
stopping rccmd listener... ok!
[vi-admin@vma init.d]$ sudo ./rccmd start
starting rccmd listener... ok!
[vi-admin@vma init.d]$
  
```

Abbildung 4-96

Prüfen Sie, ob der Daemon auch in der Prozessliste auftaucht. Dies erfolgt mit dem Befehl `ps tree` (Abbildung 4-97).



```

vi-admin@vma:~
[vi-admin@vma ~]$ ps tree
  
```

Abbildung 4-97

4.8 Setzen der virtuellen Maschinen auf Autostart

Setzen Sie die vMA 4.1 und eventuell auch andere virtuelle Maschinen auf Autostart, damit diese nach einem möglichen Stromausfall erneut gestartet werden. Im Falle der vMA 4.1 wird zudem auch das Shutdownverhalten der vMA 4.1 konfiguriert.

Hinweis: Die vMA 4.1 verfügt nicht über einen eigenen RCCMD Client und wird deshalb über die VMware Tools heruntergefahren.

Um die notwendigen Änderungen durchzuführen klicken Sie bitte über den vSphere 4 Client auf den Reiter **Konfiguration** Ihres ESXi Servers (Abbildung 4-99). Wählen Sie den Punkt **Software VM starten/herunterfahren** aus und klicken dann rechts oben auf den Punkt **Eigenschaften...**

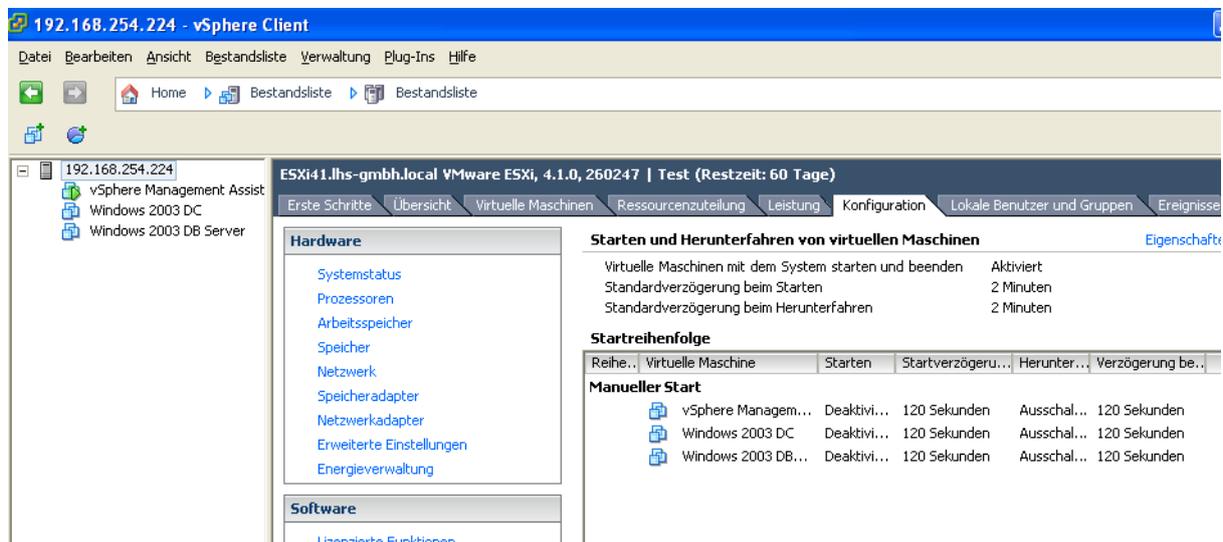


Abbildung 4-99

Aktivieren Sie den Punkt **Automatisches Starten und Herunterfahren von virtuellen Maschinen zulassen** (Abbildung 4-100).

Die Start und Stop-Verzögerungen können Sie nach Ihren Vorgaben individuell einstellen.

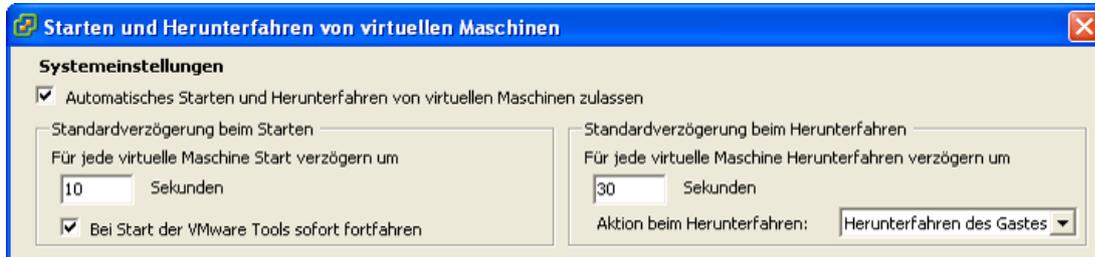


Abbildung 4-100

Klicken Sie die für den Autostart vorgesehene vMA 4.1 VM an und verschieben Sie diese mit dem **Nach oben** Button bis Sie unter **Automatischer Start** steht (Abbildung 4-101).

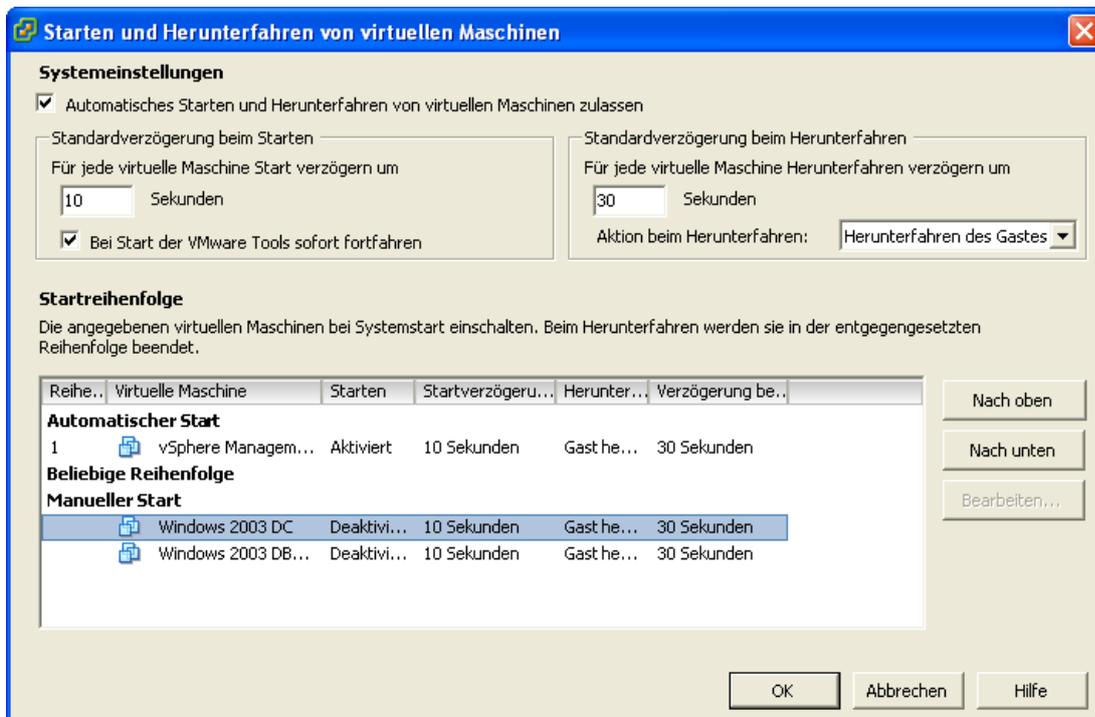


Abbildung 4-101

Bestätigen Sie mit **OK** um den Vorgang abzuschließen.

5 Konfiguration der Windows-Gäste

5.1 Voraussetzungen

Für die Konfiguration der Windows-Gäste werden folgende Programme benötigt:

- RCCMD-Client für Windows

5.2 Download des RCCMD-Clients für Windows.

Den aktuellen RCCMD-Client für Windows finden Sie unter folgendem Link:

<http://www.online-usv.de/de/download/softwarefirmware.php>

Bitte den Punkt „DataWatch Updates und Patches“ danach „RCCMD Agents“ auswählen.

Wählen Sie den Punkt RCCMD Agents.

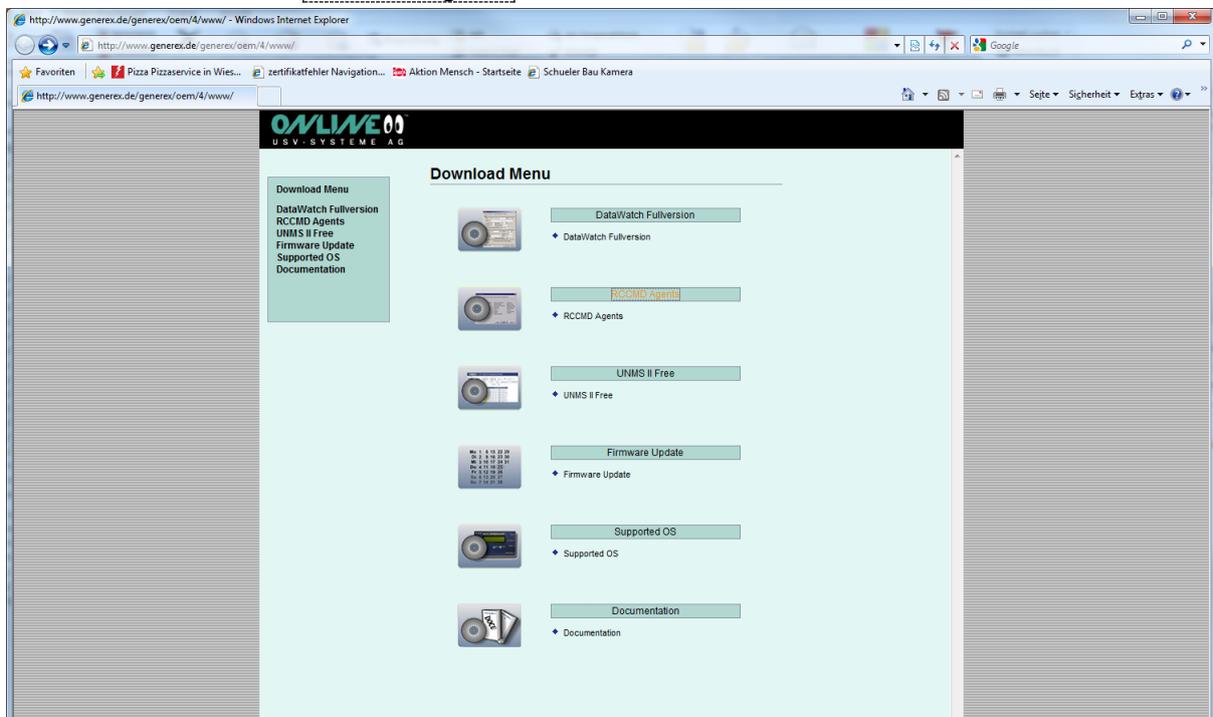


Abbildung 5-1

Wählen Sie den Punkt **Windows**.

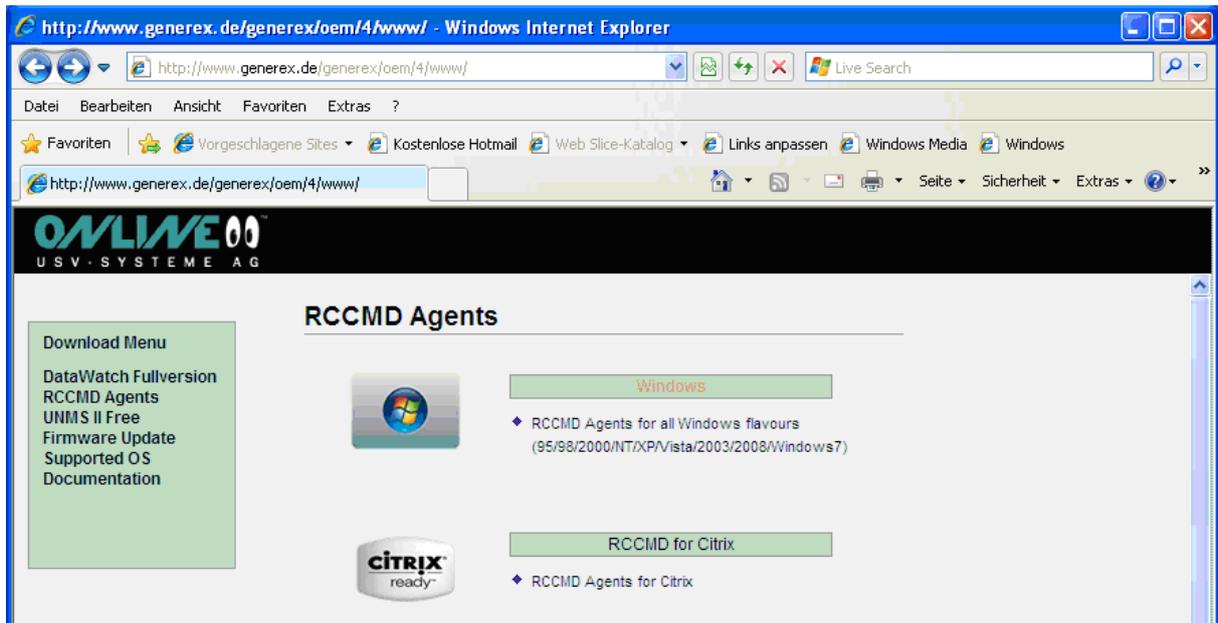


Abbildung 5-2

Speichern Sie die Archivdatei **rccmcd.zip** in einem Verzeichnis Ihrer Wahl über den Button **Speichern**.



Abbildung 5-3

Entpacken Sie anschließend die Archivdatei **rccmcd.zip**.

5.3 Installation des RCCMD-Clients auf Windows 2003 Server

Öffnen Sie das rccmdd Verzeichnis und führen `setup.exe` aus.

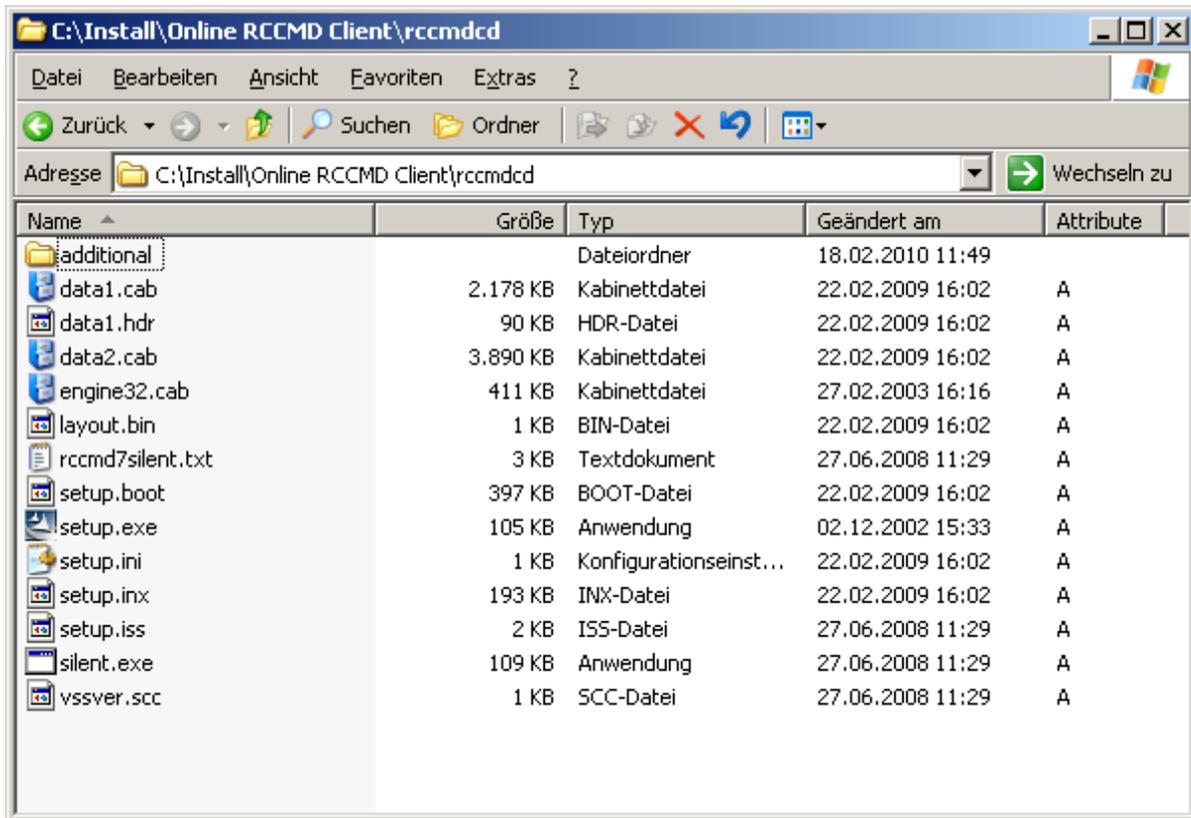


Abbildung 5-4

Wählen Sie Ihre Sprache aus. Klicken Sie auf `OK`.



Abbildung 5-5

Im Willkommensfenster klicken Sie auf **Weiter >**.

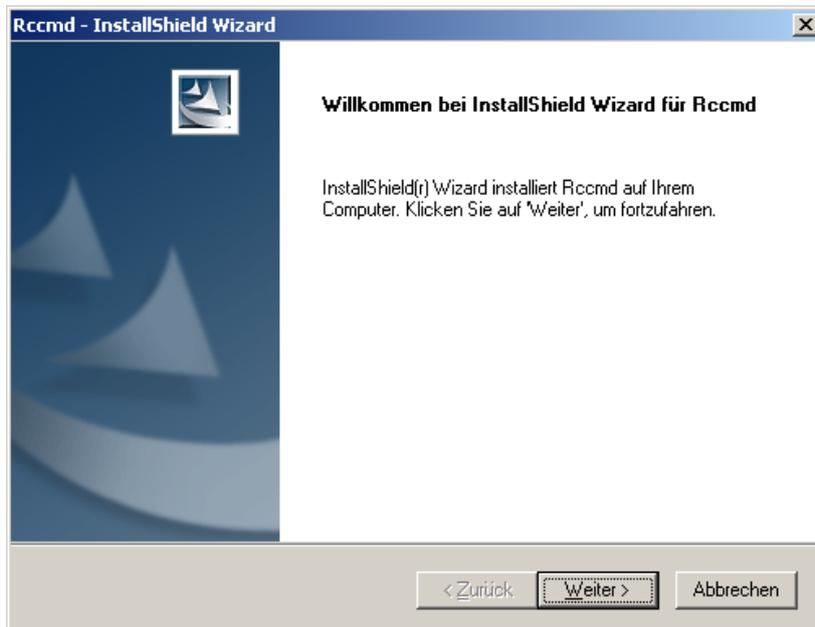


Abbildung 5-6

Geben Sie Ihren Lizenz-Schlüssel (Licence code) ein und bestätigen dies mit **Weiter >**.

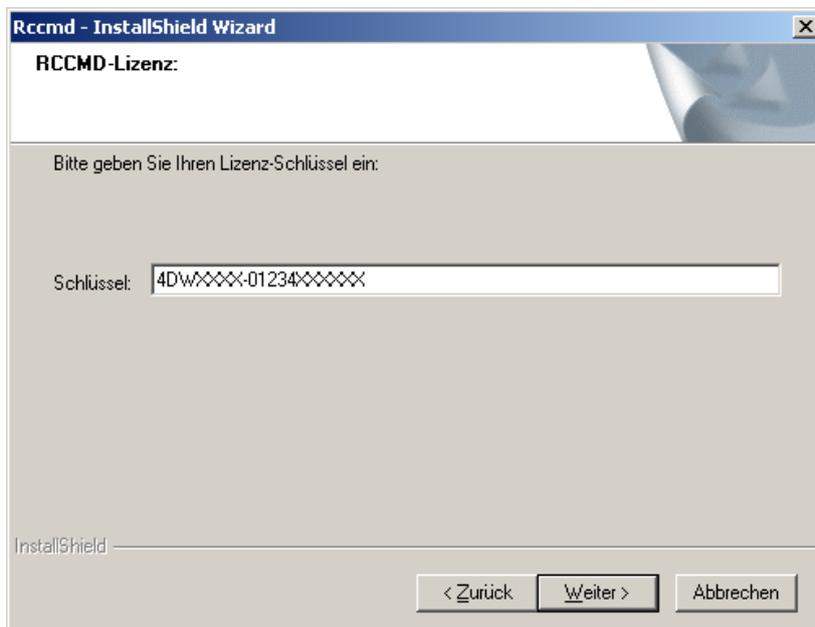


Abbildung 5-7

Bestätigen Sie, dass Sie mit der Lizenzvereinbarung einverstanden sind und klicken auf **Weiter >**.



Abbildung 5-8

Wählen Sie **Vollständig** als Setup-Typ aus und klicken auf **Weiter >**.

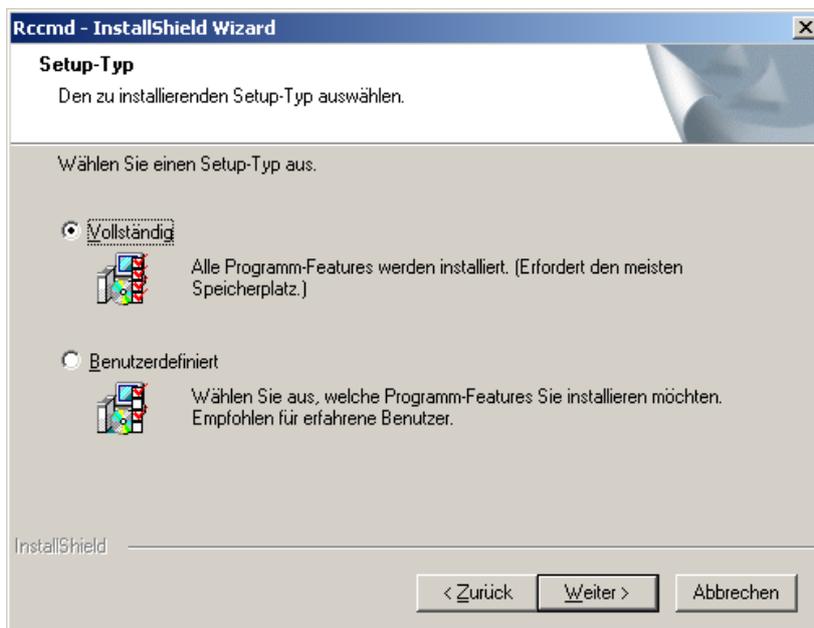


Abbildung 5-9

Klicken Sie zum Abschluss auf **Installieren**.

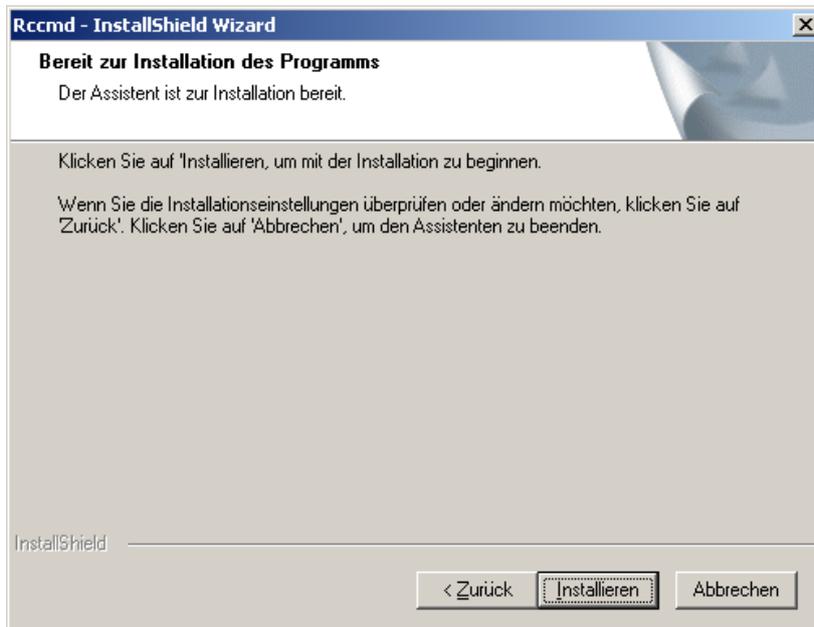


Abbildung 5-10

Das Öffnen der Firewall bestätigen Sie mit **OK**.

Schließen Sie die Installation durch Klicken des **Fertig stellen** Buttons ab.

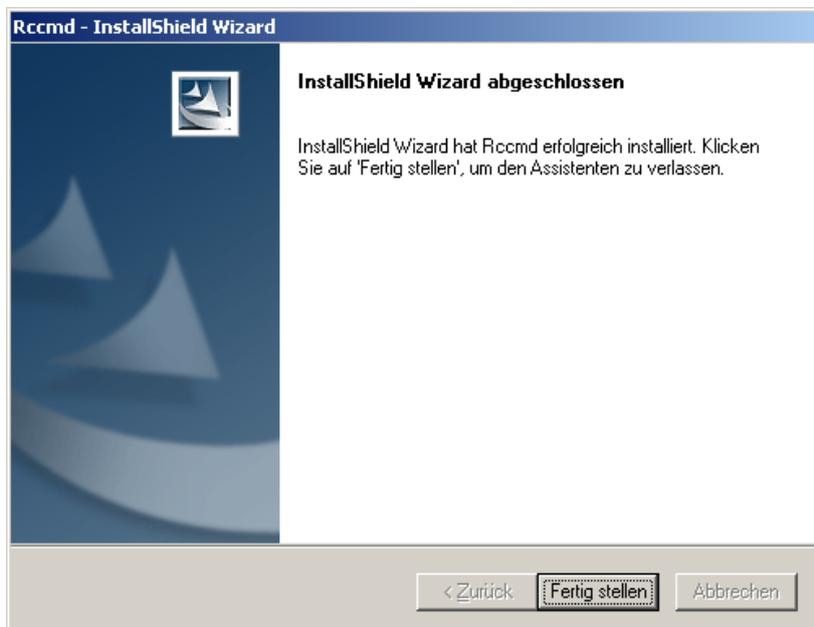


Abbildung 5-11

Geben Sie erneut den Lizenz-Schlüssel ein und klicken **Next >**.

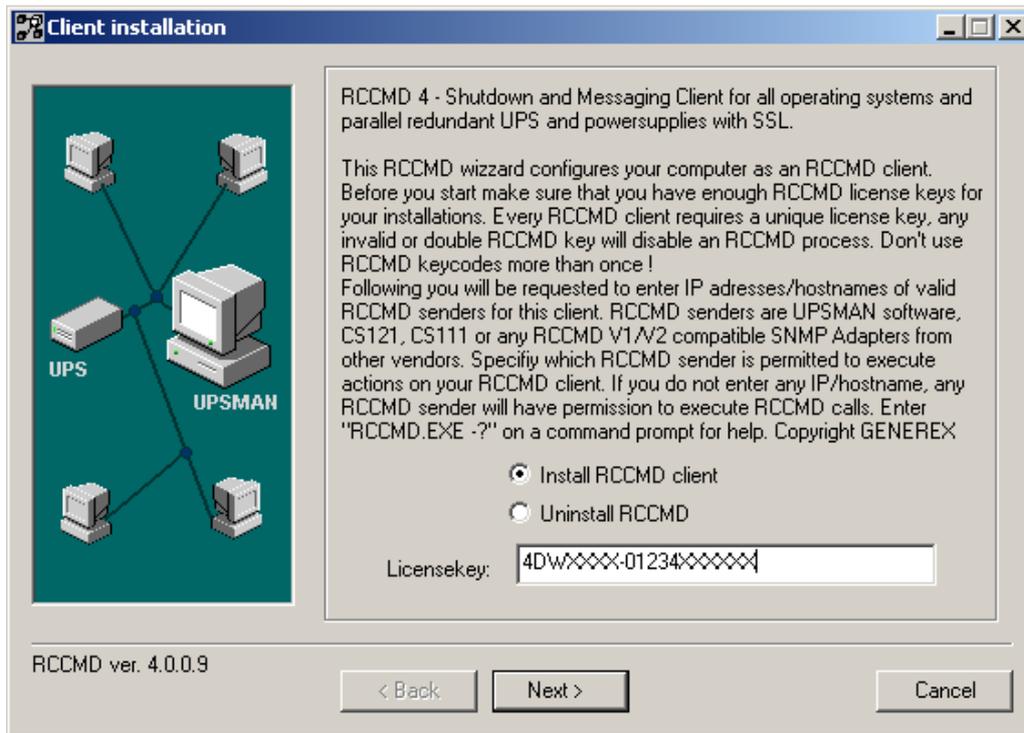


Abbildung 5-12

Klicken Sie in dem folgenden Dialog auf **Add Address ...**.

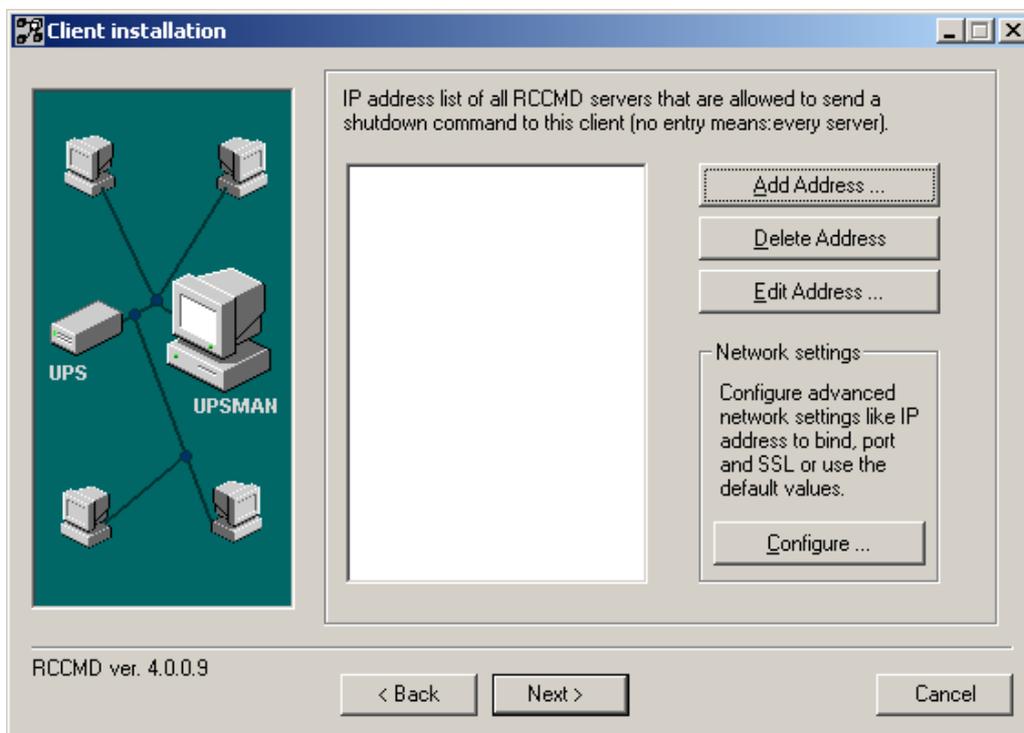


Abbildung 5-13

Geben Sie die IP-Adresse Ihres RCCMD Moduls ein (Kapitel 3.3) und klicken auf **OK**.

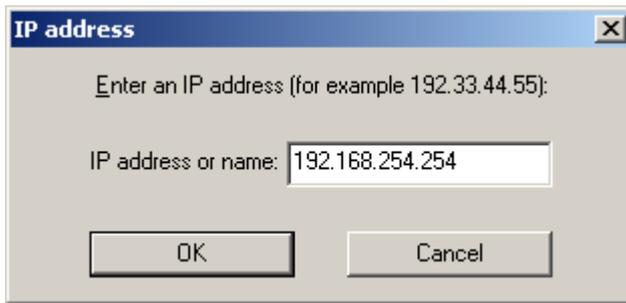


Abbildung 5-14

Klicken Sie nun **Next >**, um den nächsten Dialog anzuzeigen.

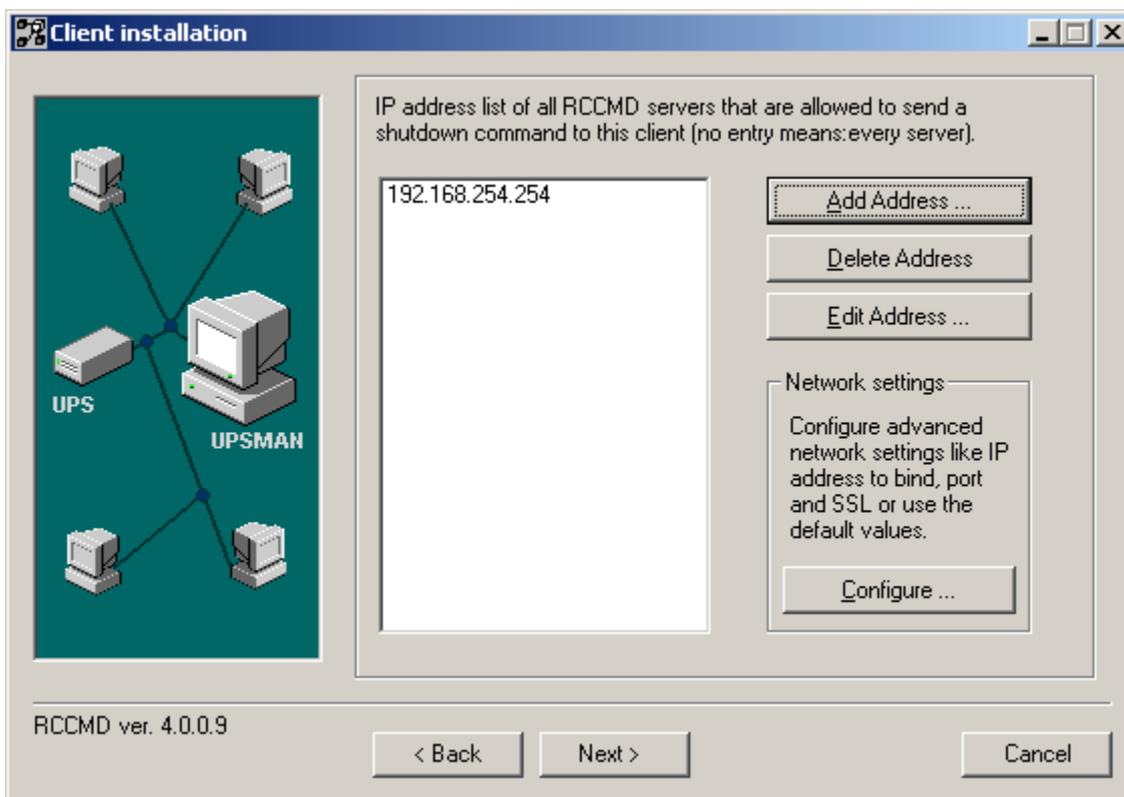


Abbildung 5-15

Aktivieren Sie Enable connection check und klicken auf .

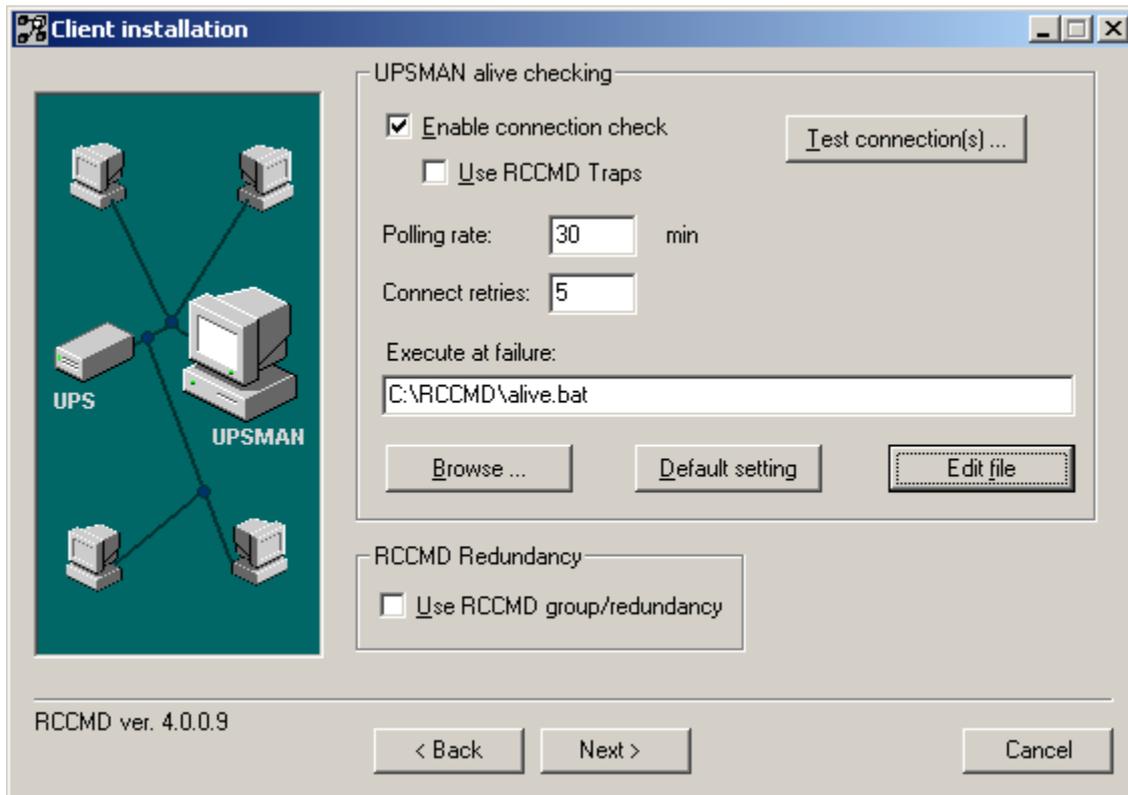


Abbildung 5-16

Es folgt der Verbindungstest des Clients an das RCCMD Modul. Bestätigen Sie den Dialog mit .

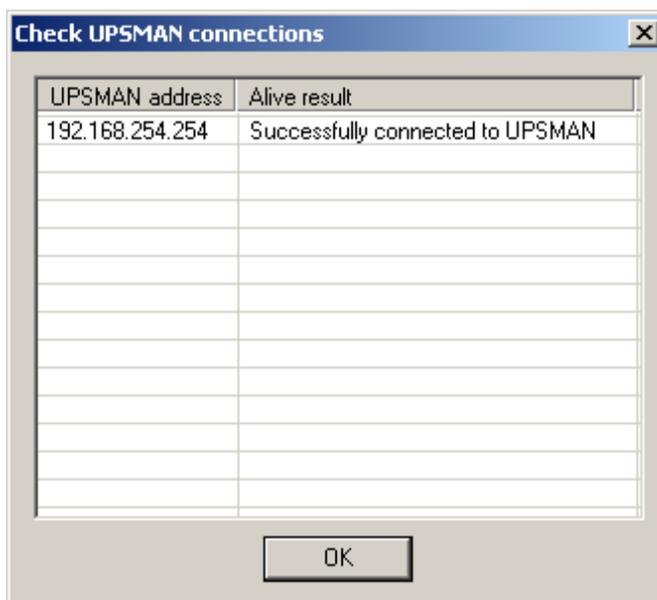


Abbildung 5-17

Auch diesen Dialog mit **OK** bestätigen.

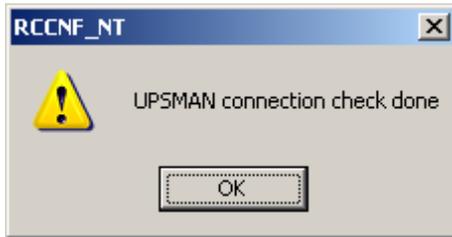


Abbildung 5-18

Behalten Sie die Standardeinstellungen bei und klicken auf **Install**.

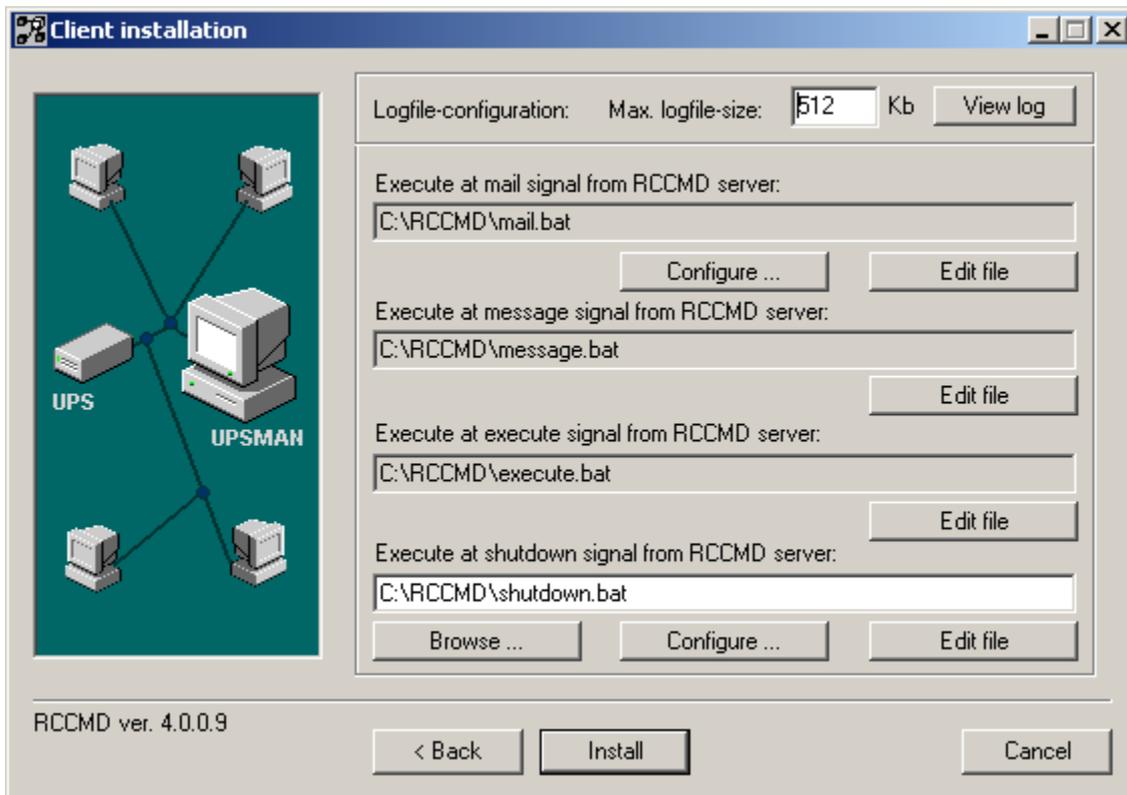


Abbildung 5-19

Nach dem erneuten Bestätigen ist die Windows-Client-Installation abgeschlossen.

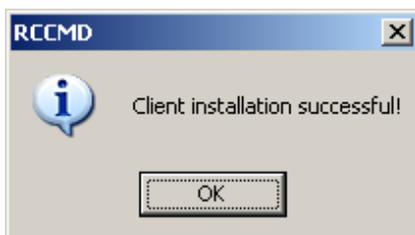


Abbildung 5-20

Wiederholen Sie die Schritte in diesem Kapitel für jeden weiteren Client.

6 Testlauf

Vor Inbetriebnahme in die Produktionsumgebung empfehle ich, die Funktion des Systems mindestens 2x zu testen. Ziehen Sie dazu den Stromversorgungsstecker der USV und kontrollieren Sie, ob das System seinen Shutdown ordnungsgemäß ausführt.

Wenn alles richtig konfiguriert wurde, sollte bei den Clients, nach Unterbrechung der Stromversorgung, der RCCMD kontrollierte Shutdownprozess stattfinden (Abbildung 6-1 und Abbildung 6-2).

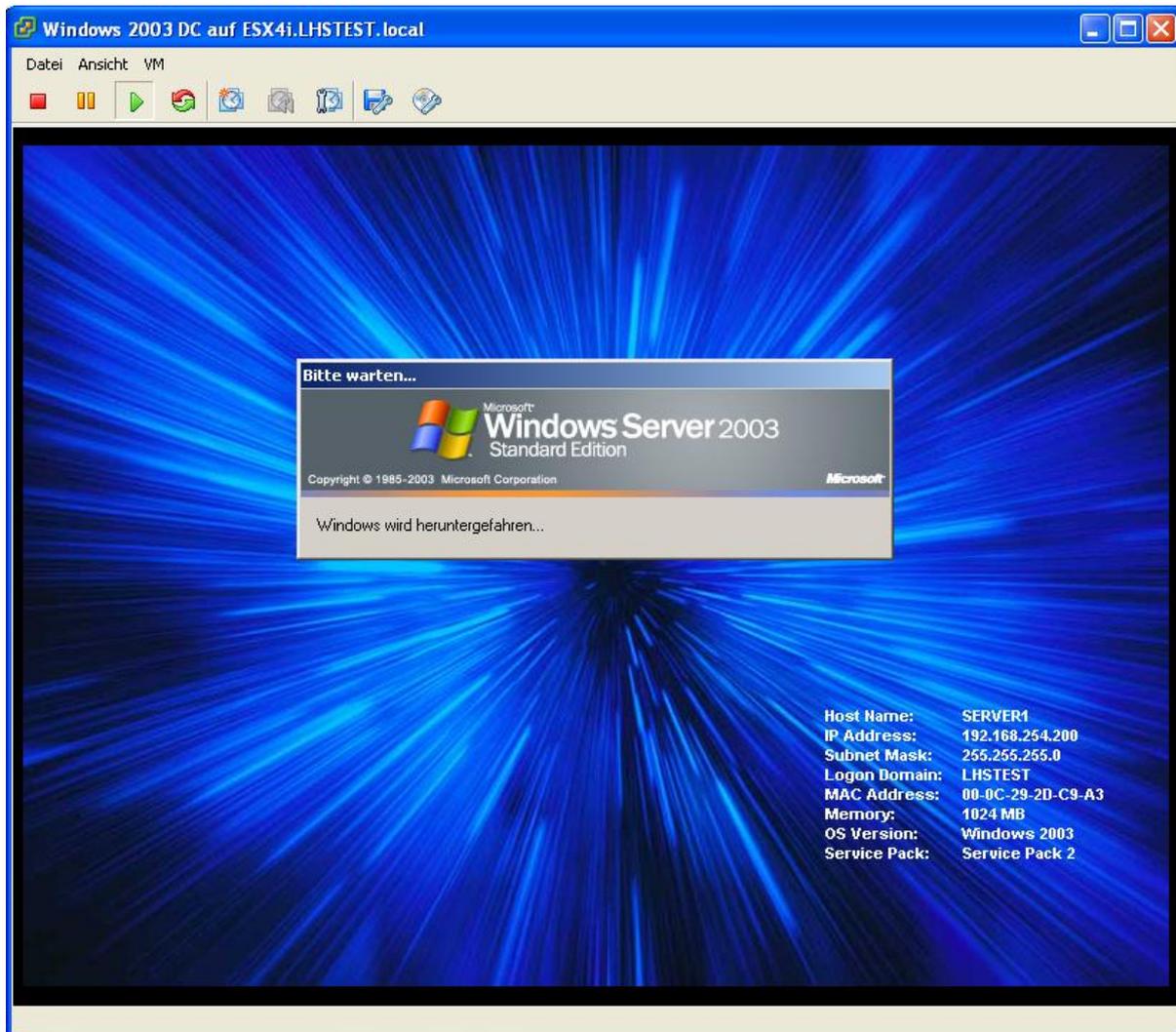


Abbildung 6-1

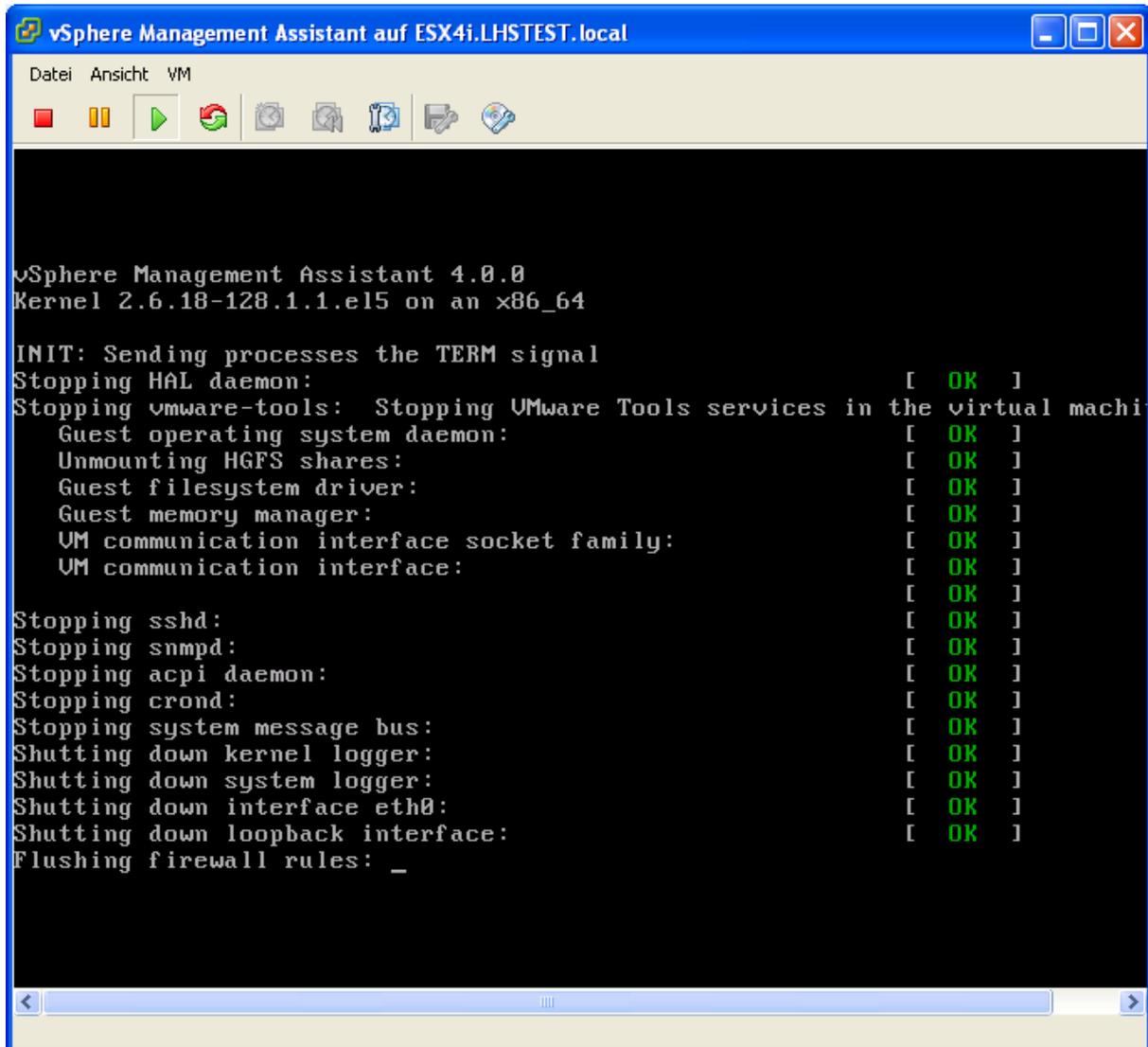


Abbildung 6-2

Sobald alle VM's beendet sind, schaltet sich auch der ESXi ab.

Hinweis: Bitte beachten Sie, dass dies beinahe unmittelbar nach Abschalten der vMA 4.1 stattfindet. Auf dem Monitor selbst ist bis zu diesem Zeitpunkt nichts zu sehen. Der gesamte Shutdownprozess Ihres ESXi Servers findet annähernd zeitgleich mit dem Shutdown der vMA 4.1 statt.

Schlußwort

Selbstverständlich kann auf die Installation der RCCMD-Clients unter Windows verzichtet werden und Sie können den VMware ESXi Server die Arbeit durchführen lassen. Dazu sind die VMware Tools auf den Gästen zu installieren und entsprechend zu konfigurieren. Desweiteren muss der VMware ESXi Server selbst korrekt konfiguriert werden, damit ein Shutdown von jedem Gast ordnungsgemäß erfolgen kann. Der Shutdown der Gäste ist dann aber nicht sichtbar und somit unkontrolliert! Dies geschieht, da der VMware ESXi - Client getrennt wird und man sich darauf verlassen muss, dass alles richtig läuft! Dieses Szenario kann ich Ihnen deshalb nicht empfehlen.

Erfahrungsgemäß geht die Installation des RCCMD-Clients schneller und ist in seiner Funktion auch wesentlich sicherer. Die bessere Kontrollierbarkeit des Shutdown-Prozesses jedes einzelnen Gastes ist ein enormer Vorteil.

Viel Erfolg beim Einsatz!

Quellen

www.online-usv.de

www.vmware.com

www.vmware.com/support/developer/vima/vima40/doc/vma_40_guide.pdf

www.chiark.greenend.org.uk

www.winscp.org