



Benutzerhandbuch für Linux-Produkte

NCP engineering GmbH

2020-04-20 (r47326)

Inhaltsverzeichnis

1	Einleitung	1
1.1	Gültigkeitsbereich dieses Dokuments	1
1.2	Wie dieses Dokument zu lesen ist	1
1.3	Unterstützte Linux-Distributionen	2
1.4	Firewall	2
1.5	Besonderheit beim NCP Virtual Secure Enterprise VPN Server	2
2	Umstellung von älteren Versionen von NCP-Software	2
3	Installation	3
3.1	Ausführen des Installationsprogramms	3
3.2	Ein typischer Installationsvorgang	5
3.3	Aktualisierung bestehender Installationen	7
3.3.1	Aktualisierungen von alten Versionen, die eine inkompatible Dateistruktur verwenden	9
	Aktualisierung alter Installationen von NCP Secure Enterprise Server, die auch NCP Secure Enterprise HA Server installiert haben	10
3.4	Produkt-spezifische Installationsfunktionen	11
3.4.1	NCP Secure Enterprise Management Server	11
3.4.2	NCP Secure Client	11
3.5	Benutzer- und Gruppenkonten	11
3.6	Deinstallation	11
3.7	Liste der Dateipfade	12
3.8	Automatische Installation	13
3.9	Umgang mit Installationsfehlern	13
4	Starten und Stoppen des Produkts	13
4.1	Manuelles Hoch- und Herunterfahren	13
4.2	Hoch- und Herunterfahren über das Linux-Init-System	14
5	Kommandozeilenwerkzeuge	17
5.1	Die Programme <code>sentinel</code> und <code>control</code>	17
5.1.1	Konfiguration der gestarteten Dienste	18
5.1.2	Operationen auf individuellen Daemon-Prozessen	18
5.1.3	Einfluss darauf nehmen, wie <i>sentinel</i> mit Abstürzen umgeht	19
5.1.4	Übergabe von benutzerdefinierten Parametern an <i>Daemons</i>	21
5.1.5	Zugriff auf <i>Daemon</i> -Logdateien	21
5.2	Startkonfiguration mit dem Programm <code>initconfig</code>	21
5.2.1	Einsehen der aktuellen Konfiguration	22
5.2.2	Interaktion mit dem Init-System	22
5.3	Umgang mit Softwareabstürzen: Das Programm <code>crash</code>	23
5.3.1	Löschen alter Absturzberichte	23
5.4	Produktlizenz und -version mit dem Programm <code>license</code>	24

6	Produktspezifische Konfiguration	24
6.1	NCP Secure Client	24
6.1.1	Hinzufügen von Desktopsymbolen und Menüeinträgen mit <code>clnt-desktopconfig</code>	24
6.2	NCP Secure Enterprise Server	25
6.2.1	Einrichtung von SNMP	25
6.3	NCP Secure Enterprise HA Server	26
6.3.1	Einrichtung von SNMP	26
6.4	NCP Secure Enterprise Management Server	26
6.4.1	Datenbankkonfiguration	27
	Einrichtung der Datenbank	27
	Datenbankkonfiguration unter Verwendung der nativen Schnittstelle für MariaDB bzw. MySQL	28
	Datenbankkonfiguration unter Verwendung von unixODBC	30
	Verbindungstest über die Kommandozeile	32
6.4.2	Dienste-Konfiguration	32
6.4.3	Konfiguration der Betriebsart	34
	Umschalten zwischen Backup- und Failsafe-Modus im Batchmodus	35

Dieses Dokument erklärt die Installation und Benutzung von NCP-Produkten auf dem Linux-Betriebssystem.

1 Einleitung

1.1 Gültigkeitsbereich dieses Dokuments

Diese Dokumentation gilt für folgende NCP-Produkte:

- NCP Secure Enterprise Server Version 12.00 und höher
- NCP Virtual Secure Enterprise VPN Server Version 12.00 und höher
- NCP Secure Enterprise HA Server Version 11.00 und höher
- NCP Virtual Secure Enterprise HA Server Version 12.00 und höher
- NCP Friendly Net Detection Server Version 2.20 und höher
- NCP Secure Client Version 5.20 und höher
- NCP Secure Enterprise Management Server Version 5.30 und höher

Dieses Handbuch deckt nicht die komplette Verwendung dieser Produkte ab, sondern nur Funktionen, die spezifisch für das Linux-Betriebssystem sind. Insbesondere die Installation der Software und ihre Integration in Linux.

Manche Produkte enthalten besondere Funktionen, die nicht in anderen Produkten verfügbar sind. Beachten Sie außerdem, dass einige Details, die in dieser Dokumentation erklärt werden, sich zwischen unterschiedlichen Software-Versionen unterscheiden können wenn neue Funktionalität hinzugefügt wird, oder Fehler behoben werden.

Um vollen Nutzen aus diesem Dokument zu ziehen sind Grundlagenwissen über das Linux-Betriebssystem und die Linux-Kommandozeile hilfreich.

1.2 Wie dieses Dokument zu lesen ist

Innerhalb dieses Dokuments werden Sie den Begriff `<prod>` in Kommandonamen oder Dateinamen wiederfinden. Dieser wird als Platzhalter verwendet, für die individuelle Abkürzung, die für jedes NCP-Produkt zum Einsatz kommt. Die [folgende Tabelle](#) zeigt die `<prod>`-Werte für die unterschiedlichen NCP-Produkte.

Tabelle 1: Vorsilben für NCP-Produkte

Produkt	Wert für <prod>
NCP Secure Enterprise Server	ses
NCP Virtual Secure Enterprise VPN Server	vses
NCP Secure Enterprise HA Server	has
NCP Virtual Secure Enterprise HA Server	vhas
NCP Friendly Net Detection Server	fnd
NCP Secure Client	clnt
NCP Secure Enterprise Management Server	sem

Wenn zum Beispiel in dieser Dokumentation ein Programm als `<prod>-uninstall` erscheint dann ist damit im Fall des NCP Secure Enterprise Server ein Programm namens `ses-uninstall` gemeint. Entsprechend für die anderen Produkte, wie oben aufgeführt.

Alle Kommandos und Beispiele, die in diesem Dokument aufgeführt sind, sind dafür vorgesehen von einer Linux-Konsole aus ausgeführt zu werden. Andere Begriffe für *Konsole* in diesem Dokument sind *Terminal* oder *Kommandozeile*. Im Allgemeinen können Sie für jedes Konsolenkommando `<cmd>` eine kurze Hilfe erhalten indem Sie `<cmd> --help` oder `<cmd> -h` eingeben.

Die meisten Beispielausgaben in diesem Dokument sind der Installationsroutine und den Werkzeugen des NCP Friendly Net Detection Server entnommen. Sie treffen jedoch weitgehend auch für alle anderen unterstützten NCP-Produkte zu.

1.3 Unterstützte Linux-Distributionen

NCP-Produkte laufen auf allen wichtigen Linux-Distributionen, insbesondere den folgenden:

- Debian GNU/Linux,
- Ubuntu,
- Red Hat Enterprise Linux (oder CentOS) und
- SUSE Linux Enterprise.

1.4 Firewall

Bitte beachten Sie dass alle Produkte außer dem NCP Secure Client eingehende Netzwerkverbindungen benötigen, um richtig zu funktionieren. Daher kann es notwendig sein, eine bestehende Firewallkonfiguration anzupassen oder die Firewall zu deaktivieren. Die notwendigen Ports entnehmen Sie der allgemeinen Produktdokumentation.

1.5 Besonderheit beim NCP Virtual Secure Enterprise VPN Server

Beim NCP Virtual Secure Enterprise VPN Server, welcher auch den NCP Virtual Secure Enterprise HA Server enthält, gilt es grundsätzlich zu beachten: Sämtliche Hinweise in diesem Dokument, die die Systemumgebung betreffen (beispielsweise die unterstützten Linux-Distributionen) haben keine Gültigkeit, da es sich um eine virtuelle Appliance handelt. Diese bringt naturgemäß ihr eigenes System mit. Zur Installation der virtuellen Appliance lesen Sie bitte die Installationsanleitung, die sich im doc-Unterverzeichnis des ISO-Images befindet.

Die Aktualisierung erfolgt über das Debian-Paketmanagement-System über speziell dafür zur Verfügung gestellte Paketquellen. Insofern verliert auch das Kapitel über die Installation in diesem Dokument seine Gültigkeit.

Trotzdem basieren natürlich beide Produkte auf den gleichen Mechanismen und bringen die gleichen Kommandozeilenwerkzeuge mit, weshalb auch diese Dokumentation ausgeliefert wird. Im Normalfall sollten Sie aber sämtliche Funktionalität über die Weboberfläche bzw. den Management-Server erreichen.

2 Umstellung von älteren Versionen von NCP-Software

Falls Sie ein NCP-Produkt aktualisieren, dass älter ist als [hier](#) aufgelistet, dann werden Sie einige wesentliche Änderungen betreffen:

- Eine neue Installationsroutine wird verwendet und die Ablageorte von Dateien haben sich verändert. Sie finden [allgemeine Informationen über den Installationsvorgang](#) und Informationen spezifisch für [Aktualisierungen alter Versionen](#) in diesem Dokument.
 - Die Art wie NCP-Programme gestartet werden und in das Linux-Init-System integriert werden hat sich verbessert. Sie finden weitere Informationen in [Starten und Stoppen des Produkts](#).
 - Eine Reihe neuer und standardisierter Kommandozeilenprogramme sind nun Teil jedes NCP-Produktes. Informationen darüber finden Sie in dem Abschnitt über [Kommandozeilenwerkzeuge](#).
-

Anmerkung

Die Änderungen zwischen alten und neuen Versionen der NCP-Software sind signifikant. Es wurde Sorge getragen, dass Sie sich nicht zu sehr darum kümmern müssen, wenn Sie aktualisieren. Aufgrund der Komplexität des Vorgangs und der individuellen Situation können jedoch Fehler auftreten. Bitte nehmen Sie sich die Zeit die Veränderungen, die in diesem Dokument beschrieben sind zu verstehen, um Fehler zu vermeiden.

3 Installation

3.1 Ausführen des Installationsprogramms

Jedes NCP-Linux-Produkt wird als binäres Installationsprogramm ausgeliefert, dass auf die Dateiendung `.bin` endet. Um die Installation auszuführen müssen Sie erst das Installationsprogramm an einen geeigneten Ort auf der Zielfmaschine kopieren. Für den Zweck dieser Dokumentation nehmen wir an, dass das Installationsprogramm `fnd_linux_x86-64_200_rev16909.bin` heißt, wie es der Fall wäre für NCP Friendly Net Detection Server für 64-Bit-Linux, Version 2.00, Revision 16909.

Um das Programm auszuführen müssen Sie unter Umständen erst das *executable bit* für die Datei setzen. Die folgende Auflistung zeigt, wie man das Installationsprogramm daraufhin prüft, ob es ein *executable bit* hat, und wie man es hinzufügt, falls nötig.

Hinzufügen des executable bit zum Installationsprogramm

```
$ ls -l fnd_linux_x86-64_200_rev16909.bin
-rw-rw-r-- ❶ 1 user user 27887112 30. Apr 13:50 fnd_linux_x86-64_200_rev16909.bin

$ chmod +x fnd_linux_x86-64_200_rev16909.bin

$ ls -l fnd_linux_x86-64_200_rev16909.bin
-rwxrwxr-x ❷ 1 user user 27887112 30. Apr 13:50 fnd_linux_x86-64_200_rev16909.bin
```

- ❶ Falls hier ein `x` sichtbar ist, ist das *executable bit* bereits gesetzt (was hier nicht der Fall ist)
- ❷ Hier ist das Bit gesetzt, nachdem es ausdrücklich mittels `chmod` hinzugefügt wurde

Anmerkung

Das *executable bit* wird vom Betriebssystem benötigt, um das Ausführen der Datei als Programm zu erlauben. Es kann verloren gehen, wenn das Installationsprogramm in ZIP-Archiven gespeichert, aus dem Internet heruntergeladen oder auf einem Wechseldatenträger abgespeichert wird.

Sobald Sie sichergestellt haben, dass das *executable bit* für das Installationsprogramm gesetzt ist, versuchen Sie es auszuführen. Für den Anfang lassen Sie uns nur den Hilfetext des Programms anzeigen:

Ausgeben der Programmhilfe des Installationsprogramms (Auszug)

```
$ ./fnd_linux_x86-64_200_rev16909.bin -h

Aufruf:

./fnd_linux_x86-64.bin [--restore <Pfad>] [--verify] [-k]
                        [--tempdir <Pfad>] [-x <Pfad>] [-i] [--relaxed]
                        [--compatibility] [-v] [-d <Pfad>] [-n] [-b]
                        [--su] [--sudo] [--] [--version] [-h]

[...]
```

Dieser Hilfetext kann als Quelle für Online-Dokumentation genutzt werden. In ihm werden die Parameter die an das Installationsprogramm übergeben werden können, erklärt. Diese Parameter beeinflussen, wie gewisse Details der Installation durchgeführt werden. Im Normalfall können Sie das Installationsprogramm ohne zusätzliche Parameter ausführen.

Wenn Sie zum Beispiel Details über das NCP-Produkt erfahren möchten, das im Installationsprogramm enthalten ist, übergeben Sie den `--info`-Parameter.

Informationen über die Installation

```
$ ./fnd_linux_x86-64_200_rev16909.bin --info
-----
> NCP Friendly Net Detection Server <
-----
```

Dies ist ein Installationspaket für:

```
Codename des Produktes: fnd
Voller Produktname: NCP Friendly Net Detection Server
Version des Produktes: 2.00
Ziel-Architektur: x86_64
Ziel-Betriebssystem: linux
Bauart: debug
Bibliotheksart: shared
Größe der enthaltenen Daten: 3840972 bytes (3.66 MB)
```

Umgebungsdaten:

```
Erkannte Linux-Distribution: Gentoo
Erkannte Linux-Version: Gentoo 2.2
Erkanntes Init-System: OpenRC
Werkzeug zum Erlangen von Root-Rechten: su
```

Durch Übergabe des `--info`-Parameters gibt das Installationsprogramm Informationen über die enthaltenen Daten aus, und über das Linux-System, dass es erkannt hat. Danach beendet sich das Programm ohne weitere Aktionen auszuführen.

Wenn die Installation tatsächlich gestartet wird benötigen Sie ausreichende Berechtigungen, um die Installation durchzuführen. Wenn Sie die Installation als der *root*-Benutzer ausführen besteht kein Problem. Wenn Sie die Installation als normaler Benutzer ausführen, benötigt das Installationsprogramm jedoch *root*-Rechte um fortzufahren.

Um *root*-Rechte zu erhalten wird das Installationsprogramm das Programm *su* oder *sudo* aufrufen, welches Sie wiederum nach dem *root*- oder Benutzerpasswort fragen wird, abhängig von der Systemkonfiguration. Im Erfolgsfall wird das Installationsprogramm sich selbst erneut mit *root*-Rechten aufrufen.

Damit die Programme *su* und *sudo* richtig funktionieren müssen sie korrekt konfiguriert sein. Jede Linux-Distribution benutzt eine andere Voreinstellung und Strategie, wie dies gelöst ist. Für die typischen Linux-Distributionen und in den meisten gängigen Fällen wird das Programm, dass vom NCP-Installer gewählt wird, korrekt sein. In machen Fällen kann es jedoch für Sie nötig werden explizit das Werkzeug zu wählen, dass für diesen Zweck verwendet wird. Tun Sie dies indem Sie den Schalter `--su` oder `--sudo` als Parameter and das Installationsprogramm übergeben.

Nachfolgend ein Beispiel dafür, wie *root*-Rechte beim Start des NCP-Installers erlangt werden:

Erlangen von root-Rechten während der Installation

```
-----
> NCP Friendly Net Detection Server <
-----

Entpacke Installationsdateien... erfolgreich

Es sind Root-Rechte notwendig, um die Installation fortzusetzen.
Das 'su'❶-Hilfsprogramm wird nun gerufen, um das Installationsprogramm mit
```

```
erhöhten Rechten neu zu starten.
```

Bitte geben Sie die benötigten Anmeldedaten ein

Passwort:

=== Rufe Installationsroutine ===

[...]

- ❶ Hier wird das Werkzeug angezeigt, dass zur Erlangung von *root*-Rechten verwendet wird

3.2 Ein typischer Installationsvorgang

Um tatsächlich eine Installation auszuführen rufen Sie einfach das Installationsprogramm ohne Argumente auf. Der Installer wird Sie durch eine Reihe von Schritten führen bis das NCP-Produkt vollständig auf Ihrem System installiert ist. Im ersten Schritt werden die im Installer enthaltenen Daten in ein temporäres Verzeichnis entpackt. Dann werden einige Kompatibilitäts-Überprüfungen durchgeführt. Diese stellen sicher, dass das Linux-System kompatibel mit der enthaltenen Software ist.

Falls diese Schritte erfolgreich sind gibt der Installer Informationen über die Software aus, die installiert werden soll. Das Programm bittet dann um Bestätigung, ob die Installation fortfahren soll. Wenn Sie eine Neuinstallation eines NCP-Produkts vornehmen sieht die Ausgabe ähnlich wie nachfolgend aus:

Überprüfungen und Informationsübersicht

```
$ ./fnd_linux_x86-64_200_rev16909.bin
-----
> NCP Friendly Net Detection Server <
-----

Entpacke Installationsdateien... erfolgreich

=== Rufe Installationsroutine ===

Prüfe Kompatibilität... erfolgreich

Keine bestehende Installation dieses Produkts wurde gefunden.

Sie sind im Begriff die folgende Produktversion zu installieren:

    Codename des Produktes: fnd
    Voller Produktname: NCP Friendly Net Detection Server
    Version des Produktes: 2.00
    Ziel-Architektur: x86_64
    Ziel-Betriebssystem: linux
    Bauart: debug
    Bibliotheksart: shared
    Baubezeichnung: release+fnd-200
    Gebaute Revision: rev16909

Wollen Sie diese Installation durchführen?

(ja/j/nein/n):
```

Eine Reihe Fragen wie diese werden vom Installer gestellt. Geben Sie Ihre Antwort an der Eingabeaufforderung (ja/j/nein/n) : ein. Die Werte in Klammern sind die möglichen Antworten in diesem Fall. Sie können also entweder j oder ja eingeben, um eine positive Antwort zu geben. Oder n oder nein um eine negative Antwort zu geben.

Diese erste Frage ermöglicht es Ihnen zu überprüfen, welche Software gleich installiert werden soll und gibt Ihnen die Möglichkeit zu überdenken, ob Sie wirklich die Installation ausführen wollen.

Anmerkung

NCP-Software wird durch eine Versionsnummer und eine Revisionsnummer identifiziert. Die Versionsnummer ist in diesem Fall *2.00*. Die Revisionsnummer ist *rev16909*. Diese beiden Nummern bilden die eindeutige Identifikation eines NCP-Software-Stands. In älteren NCP-Versionen wurden stattdessen Build-Nummern verwendet, wie *Build 039*.

Nachdem Sie *j* oder *ja* eingegeben haben wird der Installer mit den nächsten Schritten der Installation fortfahren. Erst werden die *Voraussetzungen* geprüft. Dieser Schritt stellt sicher, dass etwaige Abhängigkeiten, die das NCP-Produkt hat erfüllt sind. Ein Beispiel für eine solche Abhängigkeit ist, dass NCP Secure Enterprise HA Server erfordert, dass NCP Secure Enterprise Server installiert ist, und zwar in der richtigen Version. Andernfalls kann die Installation nicht fortgesetzt werden.

Nachdem diese Überprüfung ausgeführt wurde bittet Sie der Installer den NCP Lizenztext zu lesen und zu akzeptieren. Nachdem die erste Frage zum Betrachten des Lizenztextes akzeptiert wurde, wird ein Textbetrachtungsprogramm gestartet, dass es Ihnen erlaubt den Lizenztext zu lesen und in ihm zu navigieren. Wenn Sie damit fertig sind verlassen Sie das Betrachtungsprogramm indem Sie die *q*-Taste drücken. Damit werden Sie zum Installationsvorgang zurückgebracht. Die nächste Frage ist, ob Sie dem Lizenztext zustimmen, was notwendig ist, damit die Installation fortfahren kann.

Folgendes zeigt die Ausgabe des Installationsvorgangs, wie er bislang beschrieben wurde:

Lizenzabfrage während der Installation

```
Wollen Sie diese Installation durchführen?
```

```
(ja/j/nein/n): j
```

```
Prüfe Voraussetzungen... erfolgreich
```

```
Als nächstes wird der Lizenztext für dieses NCP-Produkt in einem externen  
Programm angezeigt. Sie können durch den Text mit Hilfe der Pfeiltasten und  
Bild auf/ab navigieren. Um das Lesen zu beenden drücken Sie 'q'. Ihre  
Zustimmung zum Lizenztext ist notwendig, um die Installation fortzusetzen.
```

```
Sind Sie bereit den Lizenztext anzusehen?
```

```
(ja/j/nein/n): j
```

```
Stimmen Sie dem Lizenztext zu?
```

```
(ja/j/nein/n): j
```

```
Sie haben den NCP Software-Lizenz-Text akzeptiert
```

Nachdem die Lizenz betrachtet und akzeptiert wurde fragt der Installer nach dem Installationsverzeichnis für das NCP-Produkt. Standardmäßig ist dies `/opt/ncp/<prod>`, was an der Eingabeaufforderung in eckigen Klammern angezeigt wird wie `[/opt/ncp/`. Wählen Sie einen beliebigen gültigen Dateisystempfad als Installationsverzeichnis. Das Zielverzeichnis darf jedoch noch keine Daten enthalten, um Datenverlust zu verhindern. Wenn Sie mit dem vorgegebenen Pfad einverstanden sind, akzeptieren Sie ihn, in dem Sie einfach *ENTER* drücken.

Anmerkung

Das Installationsverzeichnis kann nachträglich nicht auf einfachem Weg geändert werden, daher wählen Sie es bitte sorgfältig.

Nachdem Sie das Installationsverzeichnis gewählt haben beginnt die eigentliche Installation. Der Installer gibt eine Reihe von Punkten (.) aus während er alle notwendigen Dateien in das Zielverzeichnis kopiert. Dann erfolgt die Integration in das Linux-System:

- das installierte Produkt, seine Version und Installationsort werden verzeichnet
-

- die Programme, die mit dem Produkt ausgeliefert werden, werden zu der PATH-Variable des System hinzugefügt, so dass Sie sie direkt von der Kommandozeile zugreifen können (Sie müssen sich jedoch neu am System anmelden, um die neuen Kommandos sichtbar zu machen)
- das Produkt wird dem Linux-Init-System hinzugefügt, so dass es während dem Bootvorgang des Systems gestartet werden kann

Die letzten Fragen betreffen das Starten der neu installierten Software. Entscheiden Sie sich, ob Sie sie beim Systemstart hochfahren wollen und ob es jetzt sofort gestartet werden soll. Sie können das Produkt zu einem späteren Zeitpunkt zum Systemstart hinzufügen, wie es in [Starten und Stoppen](#) beschrieben ist.

Die abschließenden Installationsschritte die besprochen wurden sehen wie folgt aus:

Finale Installationsschritte

```
Bitte wählen Sie ein Installationsverzeichnis

[/opt/ncp/fnd]:

Das Installationsverzeichnis ist /opt/ncp/fnd

Installiere Daten..... erfolgreich

Speichere Installations-Informationen... erfolgreich

Passe die PATH-Variable des Systems an... erfolgreich

Konfiguriere Init-System... erfolgreich

Wollen Sie NCP Friendly Net Detection Server zum Systemstart hinzufügen?

(ja/j/nein/n): n

Wollen Sie NCP Friendly Net Detection Server jetzt sofort starten?

(ja/j/nein/n): n

NCP Friendly Net Detection Server kann gestartet werden durch den Aufruf

    /etc/init.d/ncp-fnd start

und gestoppt werden durch den Aufruf

    /etc/init.d/ncp-fnd stop

=== Installationsroutine wurde verlassen ===

Räume temporäre Dateien auf... erfolgreich
```

Falls einer der Schritte der Installation bei Ihnen fehlgeschlagen ist werfen Sie einen Blick in die [Fehlerbehandlung](#).

3.3 Aktualisierung bestehender Installationen

Das Installationsprogramm kann natürlich auch bestehende Installationen aktualisieren. Der Vorgang wie er für Neuinstallationen im vorherigen Abschnitt beschrieben wurde unterscheidet sich nur in manchen Aspekten, die in diesem Abschnitt behandelt werden.

Während dem Installationsschritt *Prüfe Kompatibilität* prüft der Installer, dass die bereits installierte Version mit der neuen Version aktualisiert werden kann, die im Installer enthalten ist. In manchen Fällen kann eine besondere Aktualisierungsreihenfolge

über eine Zwischenversion nötig sein. In einem solchen Fall wird eine entsprechende Fehlermeldung ausgegeben werden und die Installation wird abgebrochen.

Im Erfolgsfall zeigt der Installer Informationen über die bereits installierte und die neue Softwareversion an, wie hier gezeigt:

Beispiel einer Aktualisierung von NCP Friendly Net Detection Server

```
-----
> NCP Friendly Net Detection Server <
-----

Entpacke Installationsdateien... erfolgreich

=== Rufe Installationsroutine ===

Prüfe Kompatibilität... erfolgreich

Sie haben bereits folgende Version dieses Produkts installiert:

    Codename des Produktes: fnd
    Voller Produktname: NCP Friendly Net Detection Server
    Version des Produktes: 2.00
    Ziel-Architektur: x86_64
    Ziel-Betriebssystem: linux
    Bauart: debug
    Bibliotheksart: shared

Sie sind im Begriff die folgende Produktversion zu installieren:

    Codename des Produktes: fnd
    Voller Produktname: NCP Friendly Net Detection Server
    Version des Produktes: 2.00
    Ziel-Architektur: x86_64
    Ziel-Betriebssystem: linux
    Bauart: debug
    Bibliotheksart: shared
```

Der Installer prüft Unterschiede zwischen der alten und der neuen Version der Software. Festgestellte Unterschiede werden in Farbe in der Ausgabe angezeigt. Wenn sich zum Beispiel die Produktversion von 2.00 nach 2.01 ändert, dann wäre die 2.01 in Farbe, zur einfacheren Erkennung.



Warnung

Eine Zurückstufung einer NCP-Installation auf eine ältere Version oder Revision ist möglicherweise nicht vollständig unterstützt und der Installer gibt in solchen Fällen eine Warnung aus. Wenn Sie sich unsicher darüber sind kontaktieren Sie den NCP-Support für detaillierte Informationen.

Einige Installationsfragen werden während Aktualisierungen übersprungen. Zum Beispiel ist das Installationsverzeichnis bereits durch die existierende Installation festgelegt und muss nicht nochmals abgefragt werden. Außerdem werden Sie auch nicht nochmals gefragt, ob Sie die Software dem Systemstart hinzufügen wollen.

Während der Aktualisierung werden jedoch einige **zusätzliche** Schritte durchgeführt:

- Falls das zu aktualisierende Produkt gerade gestartet ist, dann wird es angehalten. Sie werden allerdings zunächst danach gefragt, ob Sie das auch tun wollen.
- Der Schritt *Aktualisierung der Installationsstruktur* führt etwaige Schritte aus, die nötig sind, um die bestehende Installation kompatibel mit der neuen Version der Software zu machen. Zum Beispiel können sich die Ablageorte von Dateien ändern oder Konfigurationsdateien müssen angepasst werden.

Die Dateien der neuen Software überschreiben alte Versionen dieser Dateien im Installationsverzeichnis. Konfigurationsdateien die dafür gedacht sind vom Benutzer bearbeitet zu werden, werden nicht überschrieben, stattdessen befinden sich Dateien die in `.sam` enden daneben, die eine Beispielkonfiguration enthalten, die nach einer Aktualisierung auf Änderungen überprüft werden kann.

Falls eine Aktualisierung wesentliche Änderungen mit sich bringt, von denen der Benutzer Kenntnis haben muss, werden besondere Hinweis-Nachrichten während der Installation angezeigt.

3.3.1 Aktualisierungen von alten Versionen, die eine inkompatible Dateistruktur verwenden

Ältere Versionen von NCP-Produkten haben eine andere Installationsroutine verwendet, die weniger flexibel als die aktuelle war. Außerdem verwenden alte Versionen eine unterschiedliche Dateistruktur. Während in aktuellen Versionen die meisten Daten in einem Installationsverzeichnis gespeichert werden, waren die Daten in alten Versionen über mehrere Pfade verteilt.

Diese älteren Versionen von NCP-Produkten können ebenso auf die neue Dateistruktur aktualisiert werden. Einige Vorkehrungen müssen jedoch getroffen werden. Die Aktualisierung der alten auf die neue Struktur kann nur von bestimmten Versionen aus ausgeführt werden:

- NCP Secure Enterprise Server kann von Version 8.11 auf Version 8.14 aktualisiert werden
- NCP Secure Enterprise HA Server kann von Version 3.04 auf Version 3.05 aktualisiert werden
- NCP Friendly Net Detection Server kann von Version 1.01 auf Version 2.00 aktualisiert werden
- NCP Secure Client kann von Version 3.25 auf Version 3.30 aktualisiert werden
- NCP Secure Enterprise Management Server kann von Version 3.02 auf Version 3.03 aktualisiert werden

Falls die Version Ihres NCP-Produkts älter ist als hier gezeigt ist es notwendig, dass Sie erst auf die hier gelistete Version aktualisieren und erst dann die Aktualisierung auf die Installation neuer Art vornehmen.

Die aktuelle Installationsroutine wird diese Bedingungen überprüfen und nur Aktualisierungen von den oben genannten Versionen erlauben. Falls die Aktualisierung als durchführbar eingestuft wird zeigt der Installer eine etwas andere Versionsinformation:

Aktualisierungs-Information für Aktualisierungen von alten Installationen

Für dieses Produkt wurde folgende Installation alter Art gefunden:

```
NCP Friendly Net Detection Server 1.00 Build 006
Version: 1.00
```

Sie sind im Begriff die folgende Produktversion zu installieren:

```
Codename des Produktes: fnd
Voller Produktname: NCP Friendly Net Detection Server
Version des Produktes: 2.00
Ziel-Architektur: x86_64
Ziel-Betriebssystem: linux
Bauart: debug
Bibliotheksart: shared
```

Außerdem wird der Installer Sie informieren, dass diese Aktualisierung wesentliche Änderungen mit sich bringen wird. Später wird Ihnen der Installer die Möglichkeit geben das Installationsverzeichnis der Software zu ändern. In alten Installationen von NCP-Produkten außer bei NCP Secure Enterprise Management Server war das Installationsverzeichnis festgelegt auf den Pfad `/usr/local/ncp/<prod>`. Deshalb gibt Ihnen der Installer die Möglichkeit die Installation an einen anderen Ort zu verschieben. Dies ist das einzige Mal, dass Sie sich für einen anderen Installationspfad entscheiden können. Sie können jedoch den alten Installationspfad beibehalten, indem Sie den vorgegebenen Installationspfad, der vom Installer angezeigt wird, auswählen.

Falls Sie sich entscheiden das Installationsverzeichnis zu wechseln kann es notwendig werden, dass Sie Konfigurationsdateien des NCP-produkts anpassen, um den neuen Installationspfaden gerecht zu werden, obwohl der Installer sich Mühe gibt alles

entsprechend anzupassen. Hier ist die diesbezügliche Ausgabe während der Installation bezüglich der Auswahl eines neuen Installationsverzeichnisses:

Auswahl eines neuen Installationsverzeichnisses während der Aktualisierung alter Installationen

Beginnend mit diesem Update von NCP Friendly Net Detection Server ist es möglich benutzerdefinierte Installationspfade auszuwählen. Standardmäßig wird der bisherige Installationspfad beibehalten. Sie können einen anderen auswählen wenn Sie mögen.

Bitten geben Sie den Installationspfad an oder drücken Sie Eingabe, um den aktuellen beizubehalten.

(drücken Sie Eingabe, um den Vorschlag, der in Klammern angezeigt wird zu akzeptieren)

```
[/usr/local/ncp/fnd]:
```

Im alten Installationskonzept wurden Dateien oft flach in das Installationsverzeichnis gelegt. In der neuen Installation sind die Dateien in Unterverzeichnisse des Installationsverzeichnisses strukturiert wie `bin`, `sbin` und `etc`. Daher muss der Installer während der Aktualisierung entscheiden, welche existierenden Dateien in welche Unterverzeichnisse gehören. Alle Dateien die der Installer kennt werden automatisch an die richtige Stelle verschoben.

Es kann jedoch auftreten, dass einige Dateien dem Installer nicht bekannt sind. Dies kann zum Beispiel der Fall sein, wenn der Benutzer benutzerdefinierte Dateien zu der Installation hinzugefügt hat. Da die Installationsroutine nicht wissen kann, was mit solchen Dateien zu tun ist, legt sie sie an einem sicheren Ort unterhalb des Unterverzeichnisses `old` ab. In diesem Fall gibt der Installer eine **Warnmeldung** während der Aktualisierung aus. Sie müssen sich um die in das `old`-Verzeichnis abgelegten Dateien per Hand kümmern und entscheiden, wo sie hingehören, oder was mit ihnen zu tun ist.

Warnmeldung, die während der Aktualisierung angezeigt wird wenn unbekannte Dateien gefunden wurden

```
Installationsstruktur wird aktualisiert... erfolgreich
```

```
HINWEIS: 1 Dateien, die diese Installationsroutine nicht zuordnen
konnte wurde nach '/usr/local/ncp/fnd/old' verschoben. Bitte untersuchen Sie
diese Dateien und entfernen Sie sie oder verschieben Sie sie an die richtigen
Stellen.
```

```
HINWEIS: Sie müssen unter Umständen Konfigurationsdateien des
Produkts in '/usr/local/ncp/fnd/etc' anpassen, um den neuen Dateipfaden gerecht
zu werden. Bitte überprüfen Sie sie um Konfigurationsfehler zu vermeiden.
```

```
Die alte Installationsstruktur wurde entfernt.
```

Aktualisierung alter Installationen von NCP Secure Enterprise Server, die auch NCP Secure Enterprise HA Server installiert haben

Wenn Sie eine alte Installation von NCP Secure Enterprise Server und NCP Secure Enterprise HA Server haben, die Sie aktualisieren wollen dann muss ein besonderes Vorgehen eingehalten werden. NCP Secure Enterprise HA Server kann nur installiert werden, wenn NCP Secure Enterprise Server bereits installiert ist, weil er davon abhängt. Zur Aktualisierung auf die neue Installationsroutine ist es notwendig erst NCP Secure Enterprise HA Server auf die neue Version zu aktualisieren. Erst danach aktualisieren Sie NCP Secure Enterprise Server ebenso.

Es ist nicht möglich nur NCP Secure Enterprise HA Server auf die neue Version zu aktualisieren, weil er nicht funktioniert bis Sie auch NCP Secure Enterprise Server aktualisiert haben.

Die Installationsroutine wird Sie informieren, falls die vorgesehene Aktualisierungs-Reihenfolge nicht eingehalten wird und eine Aktualisierung in diesem Fall ablehnen.

3.4 Produkt-spezifische Installationsfunktionen

Einige NCP-Produkte haben besondere Funktionen während der Installation. Diese Fälle werden in diesem Abschnitt behandelt.

3.4.1 NCP Secure Enterprise Management Server

Im Falle des NCP Secure Enterprise Management Server wird Sie der Installer während der Installation nicht fragen, ob Sie die Software direkt starten möchten, da hierfür [eine Datenbankverbindung](#) konfiguriert sein muss, bevor erfolgreich gestartet werden kann.

3.4.2 NCP Secure Client

Für den NCP Secure Client wird ein Gruppenkonto - standardmäßig mit dem Namen *ncp* - während der Installation angelegt. Nur Benutzer die Mitglieder dieser Gruppe sind können erfolgreich die grafische Monitor-Anwendung des VPN-Clients verwenden.

Die Installationsroutine fügt keine Benutzer automatisch zu dieser Gruppe hinzu. Wie Sie einen Benutzer zur Gruppe *ncp* hinzufügen, können Sie in der Dokumentation Ihres Linux-Systems in Erfahrung bringen.

Das Programm *clnt-monitor* kann verwendet werden, um die graphische Oberfläche zu starten.

3.5 Benutzer- und Gruppenkonten

Einige der NCP-Produkte wie NCP Secure Enterprise Server und NCP Secure Client erzeugen spezielle Benutzer- und Gruppenkonten zum Betrieb der Software. Diese sind notwendig für die Rechteverwaltung. Diese ermöglicht einigen der Dienste, als gewöhnlichen Benutzer ohne Root-Rechte laufen zu lassen, um die Auswirkungen möglicher Sicherheitslücken zu reduzieren.

Standardmäßig werden der Benutzer und die Gruppe *ncp* für diesen Zweck verwendet. Sie können außerdem einen benutzerdefinierten Benutzer- und Gruppennamen angeben, indem Sie die Schalter `--user` und `--group` an das Installationsprogramm übergeben. Der Benutzer und/oder die Gruppe, die Sie angeben muss bereits existieren, bevor Sie dies tun. Nur der Standardbenutzer und die -gruppe *ncp* werden automatisch durch den Installer angelegt. Um ein Benutzer- oder Gruppenkonto anzulegen können Sie die üblichen Linux-Administrationswerkzeuge verwenden. Verwenden Sie die Dokumentation Ihres Linux-Systems, um genaueres darüber zu erfahren.

Falls mehrere NCP-Produkte auf derselben Linux-Maschine installiert sind muss der Name der Gruppe, die für den Betrieb der Programme verwendet wird für alle Produkte gleich sein. Dies ist notwendig, da NCP-Programme auf gemeinsame Dateien korrekt zugreifen können müssen, wie zum Beispiel auf die Datei `/etc/ncp.db`.

3.6 Deinstallation

Zur Deinstallation existiert ein separates Programm `<prod>-uninstall` für jedes NCP-Produkt. Das Deinstallations-Programm wird Sie über das Produkt, dass Sie deinstallieren wollen informieren und darüber, welche Pfade von der Deinstallation betroffen sind. Dann werden Sie gefragt, ob Sie wirklich mit dem Deinstallationsvorgang fortfahren wollen.

Das Deinstallations-Programm wird alle Dateien die zum Produkt gehören entfernen, genauso wie verschiedene Systemeinstellungen die für die Software angepasst wurden, wie zum Beispiel das Linux-Init-System, Gruppenkonten usw. Die einzigen Daten, die nicht entfernt werden sind die Folgenden:

- Die Datei `/etc/ncp.db` wird nicht entfernt, weil sie mit anderen möglichen Installationen von NCP-Produkten geteilt wird und NCP-Lizenzdaten enthält, die Sie gegebenenfalls registriert haben.

Falls Sie ein NCP-Produkt automatisch ohne eine interaktive Abfrage entfernen wollen, können Sie die Option `--force` an das Programm `<prod>-uninstall` übergeben, so dass es keine Fragen stellt.

Beispielausgabe des Programms `fnd-uninstall`

Dieses Programm wird das folgende Produkt von Ihrem System entfernen. Dies schließt Ihre benutzerdefinierte Konfiguration, Sicherungsdaten und Logdateien mit ein:

```
Codename des Produktes: fnd
Voller Produktname: NCP Friendly Net Detection Server
Version des Produktes: 2.00
Ziel-Architektur: x86_64
Ziel-Betriebssystem: linux
Bauart: debug
Bibliotheksart: shared
```

Die folgenden Pfade werden entfernt:

```
- /opt/ncp/fnd
- /var/adm/ncp/fnd
- /var/log/ncp/fnd
```

Wollen Sie die Deinstallation wirklich ausführen?

```
(ja/j/nein/n): j
```

```
Austragen aus dem Init-System... erfolgreich
Entferne PATH-Einstellung aus dem System... erfolgreich
Entferne Installationsdateien... erfolgreich
Säubere globale Produktkonfiguration... erfolgreich
```



Warnung

Keine Sicherungskopie wird nach der Installation zurückbleiben, so dass alle Ihre Daten verloren sind. Seien Sie vorsichtig mit der Deinstallations-Routine in produktiven Umgebungen.

3.7 Liste der Dateipfade

Abgesehen vom Haupt-Installationsverzeichnis benutzt NCP-Software einige andere Pfade im Linux-Dateisystem, um Daten abzulegen. Hier ist ein Überblick über diese Stellen:

Tabelle 2: Zusätzliche Dateisystempfade

Ort	Beschreibung
/etc/ncp.db	Eine Datenbank-Datei, die zwischen allen Installationen von NCP-Software geteilt wird. Sie enthält einige Softwareeinstellungen und Lizenz- und Versionsdaten für jedes installierte Produkt.
/etc/ncp.info	Eine Konfigurationsdatei, in der alle Installationen von NCP-Produkten, ihre Installationsverzeichnisse und Versionen verzeichnet werden.
/var/log/ncp/<prod>	Logdateien die von NCP-Programmen erzeugt werden, werden je Produkt in einem gesonderten Verzeichnis an diesem Ort abgelegt.
/var/adm/ncp/<prod>/crashes	Informationen über Programmabstürze werden hier gesammelt.

3.8 Automatische Installation

Sie können ein NCP-Produkt automatisch installieren ohne jegliche Benutzerinteraktion. Dies ist nützlich zum schnellen Testen, oder wenn Sie NCP-Software über Skripte verteilen möchten.

Um den automatischen Installationsmodus einzuschalten ist der grundlegende Parameter, der zum Aufruf der Installationsroutine hinzugefügt werden muss `--batch`. In diesem Modus werden jegliche interaktive Fragen als positiv beantwortet angenommen. Für etwaige Konfigurationswerte, die vom Benutzer abgefragt würden, werden Standardwerte ausgewählt.

Sie können immer noch das Installationsverzeichnis auswählen, auch wenn Sie den *automatischen Installationsmodus* verwenden, indem Sie den Parameter `--dir` an das Installationsprogramm übergeben, gefolgt vom gewünschten Installationspfad.

Eine automatische Installation kann nur durch den *root*-Benutzer ausgeführt werden, da das Passwort zur Rechteerhöhung nicht ohne Nutzerinteraktion eingelesen werden kann.

3.9 Umgang mit Installationsfehlern

Die Installation von Software auf einer großen Bandbreite unterschiedlicher Linux-Distributionen, Versionen und Konfigurationen ist eine komplexe Aufgabe. Deshalb können Probleme entstehen beim Versuch ein NCP-Produkt zu installieren oder zu aktualisieren. Es gibt eine Reihe von Dingen, die Sie ausprobieren können, um das Problem zu beheben, bevor Sie den NCP-Support kontaktieren. Das Installationsprogramm bietet einige Schalter, die helfen können Installationsfehler zu untersuchen oder sogar zu beheben.

Zunächst können Sie die Integrität der im Installationsarchiv enthaltenen Daten überprüfen. Dies wird gemacht indem die Option `--verify` übergeben wird. Dies veranlasst den Installer sich selbst zu verifizieren und Erfolg oder Fehler zu melden. Keine Installationsschritte werden ausgeführt. Falls die Verifikation fehlschlägt, dann hat das Installationsprogramm selbst Schaden genommen, vermutlich während es auf die Zielmaschine übertragen wurde. In diesem Fall beziehen Sie eine korrekte Version des Installationsprogramms und versuchen Sie es erneut.

Einige kleinere Probleme können vermieden werden, indem der Schalter `--compatibility` an den Installer übergeben wird. Dies ändert das Verhalten des Installers in einigen Details, um kompatibler mit unerwarteten Linux-Umgebungen zu sein, wobei manche Überprüfungen nicht mehr so gut ausgeführt werden können, wie ursprünglich geplant.

Der Schalter `--relaxed` ignoriert einfach gewisse Arten von Fehlern. Falls zum Beispiel die Integration des NCP-Produkts in das Linux-Init-System fehlschlägt, wird diese Tatsache ignoriert und die Installation wird fortgesetzt. Dies gilt nur für Installationsschritte, die nicht wesentlich für die Grundfunktion der Software sind. Sie können dann versuchen die verbleibenden Probleme manuell zu beheben oder ohne die fehlenden Funktionen auskommen.

Schließlich veranlasst der Schalter `--verbose` den Installer dazu mehr Informationen darüber auszugeben, was hinter den Kulissen geschieht. Die angezeigte Information kann Ihnen einen Hinweis darauf geben, warum die Installation nicht funktioniert. Auf der anderen Seite kann die umfangreiche Ausgabe wertvoll für den NCP-Support sein, um Ihr Problem zu untersuchen. Wenn Sie den verbose-Modus einschalten wird zum Beispiel jede Datei und ihr Zieltort angezeigt, die der Installer installiert.

4 Starten und Stoppen des Produkts

In diesem Abschnitt erfahren Sie, wie das Starten und Stoppen von NCP-Produkten unter Linux gehandhabt wird.

4.1 Manuelles Hoch- und Herunterfahren

Jedes NCP-Produkt besteht aus einem oder mehreren Hintergrundprozessen, die im System laufen, um die Funktionalität des jeweiligen Produkts zur Verfügung zu stellen. Solche Hintergrundprozesse werden in Linux *Daemon* genannt.

Das Programm `<prod>-sentinel` ist dafür zuständig alle *Daemons*, die zu einem NCP-Produkt gehören zu starten. Es kann verwendet werden, um die Software manuell zu starten, um zum Beispiel um zu überprüfen, ob alles korrekt funktioniert, bevor die Software automatisch während dem Systemstart hochgefahren wird.

Als ersten Test rufen Sie das Programm *sentinel* mit dem Schalter `-f` auf, so dass es nicht in den Hintergrund verschwindet und Informationen auf die Konsole ausgibt. Dabei werden Sie sehen, dass das *sentinel*-Programm damit beginnt das komplette

NCP-Produkt hochzufahren. Wenn ein Fehler auftritt wird das *sentinel*-Programm alles wieder herunterfahren und mit einem Fehler zurückkehren. Andernfalls läuft das Programm weiter, bis eine Aufforderung zum Herunterfahren auftritt, zum Beispiel indem *Strg* + *C* gedrückt wird. Siehe [die Ausgabe des fnd-sentinel](#) für ein Beispiel, wie man *sentinel* manuell laufen lässt.

Ein Beispielaufwurf des Programms fnd-sentinel von NCP Friendly Net Detection Server

```
$ fnd-sentinel -f
Setze core_pattern auf '|/opt/ncp/fnd/bin/fnd-crash --dump %p;%u;%g;%s;%t;%h;%e;%%E;%c -- ↵
downstream core'
Starte Daemon für Erkennung befreundeter Netze ... okay
product started
fnd-sentinel: wurde gestartet am Mo 26 Mai 2014 14:53:46 CEST
Listen Port 12521
Start FND Listener

❶ ^CANforderung zum Herunterfahren empfangen.
Fahre alle Dienste herunter
Stoppe Daemon für Erkennung befreundeter Netze ... Stop FND Listener
zurückgekehrt
Aufräumen von VPN-Einstellungen im System...
    Räume iptables mangle-Regeln auf
    Räume unbenutzte Shared-Memory-Segmente auf
    Räume unbenutzte Semaphoren auf
    Räume unbenutzte Nachrichtenschlangen auf
fnd-sentinel: beendet am Mo 26 Mai 2014 14:53:50 CEST
```

- ❶ Beim Drücken von *Strg* + *C* wird das *sentinel*-Programm das Produkt wieder herunterfahren und zurückkehren nachdem einige Aufräumarbeiten durchgeführt wurden.

Anmerkung

Einige NCP-Produkte wie NCP Secure Enterprise Management Server können direkt nach der Installation nicht erfolgreich gestartet werden, wenn sie nicht zuvor korrekt konfiguriert wurden.

Sie finden weitere Informationen über das *sentinel*-Programm [hier](#).

4.2 Hoch- und Herunterfahren über das Linux-Init-System

Im Normalbetrieb werden Sie typischerweise wollen, dass NCP-Software während dem normalen Startvorgang des Betriebssystems hochgefahren wird. In Linux ist ein *Init-System* dafür zuständig Dienste während dem Startvorgang in Betrieb zu nehmen. Derzeit gibt es eine Reihe unterschiedlicher *Init-Systeme* die in den verbreiteten Linux-Distributionen zum Einsatz kommen (siehe [Vergleich von Init-Systemen](#)).

Tabelle 3: Init-Systeme die in Linux-Distributionen verwendet werden

Name	Beschreibung	Verwendet in
SystemV	Dies ist das klassische UNIX-artige Init-System, dass Shell-Skripten und Abhängigkeiten zwischen ihnen verwendet.	Debian bis zu Version 7, openSUSE vor Version 12.3, SLES vor Version 12, Rückwärtskompatibilität in CentOS 6 and RHEL 6
Upstart	Ein fortgeschrittenes, ereignis-orientiertes Init-System, dass für Ubuntu-Linux entwickelt wurde.	Ubuntu-Versionen bis zu Version 14, grundlegende Unterstützung in CentOS 6 und RHEL 6

Tabelle 3: (continued)

Name	Beschreibung	Verwendet in
systemd	Ein modernes, ereignis-orientiertes Init-System mit Unterstützung für viele moderne Linux-Funktionen, entwickelt durch die Linux-Gemeinde.	openSUSE beginnend von Version 12.3, SLES ab Version 12
OpenRC	Ein Nischen-Init-System, entwickelt von der Gentoo-Linux-Gemeinde.	Aktuelles Gentoo Linux

NCP-Software unterstützt alle diese verbreiteten Init-Systeme und kann NCP-Programme so einrichten, dass sie während dem Systemstart hochgefahren werden. Während der Installation von NCP-Software wird diese Integration standardmäßig durchgeführt. Der Installer fragt Sie nur, ob Sie das NCP-Produkt während des Startvorgangs hochfahren möchten, oder nicht. Um diese Autostart-Einstellung später zu ändern, benutzen Sie das Programm `<prod>-initconfig`.

Da unterschiedliche *Init-Systeme* in Linux verwendet werden, unterscheiden sich auch die Kommandos, um ein NCP-Produkt zu starten oder zu stoppen von Fall zu Fall. Wenn Sie nicht wissen, welche die korrekten Kommandos für Ihren spezifischen Fall sind, lassen Sie sich vom Programm `<prod>-initconfig` weiterhelfen. Übergeben Sie ihm die Parameter `--show-start-cmd` und `--show-stop-cmd`, um die Kommandos zum Starten bzw. Stoppen der NCP-Software auszugeben.

Jedes *Init-System* benutzt einen grundlegenden Skript- oder Dienstnamen, um die unterschiedlichen Programme, die verwaltet werden, zu unterscheiden. Bei NCP-Software lautet dieser Basisname `ncp-<prod>`. Beachten Sie das [Beispiel des Startens von NCP Friendly Net Detection Server](#) bei Verwendung des SystemV-Init-Systems auf Debian.

Starten und Stoppen von NCP Friendly Net Detection Server unter Debian-Linux (SystemV-Init)

```
$ fnd-initconfig --show-start-cmd ❶
/etc/init.d/ncp-fnd start

$ /etc/init.d/ncp-fnd start ❷
Starting NCP Friendly Net Detection Server
Starting Friendly Net Detection Daemon ... okay

$ /etc/init.d/ncp-fnd status ❸
Current operational status of NCP Friendly Net Detection Server

Friendly Net Detection Daemon
=====

Status: running since Mo 12 Mai 2014 04:07:16 CDT
Command Line: /usr/local/ncp/fnd/sbin/ncpfndd -f
Process ID: 5010
```

- ❶ Dies ermittelt das Kommando, um NCP Friendly Net Detection Server über das Debian-Init-System zu starten
- ❷ Unter Verwendung des Startkommandos fahren wir NCP Friendly Net Detection Server hoch
- ❸ Sie können auch den aktuellen Betriebszustand von NCP Friendly Net Detection Server ausgeben lassen. Das Kommando, um dies zu erreichen unterscheidet sich zwischen Init-Systemen.

Falls Sie sich nicht entschlossen haben den Autostart der NCP-Software während der Installation einzuschalten, ändern Sie diese Einstellung nachträglich durch Verwendung von `<prod>-initconfig -a 1`, um den Autostart einzuschalten, oder `<prod>-initconfig -a 0`, um ihn entsprechend wieder auszuschalten. Wenn der Autostart aktiviert ist, sollte die NCP-Software während dem normalen Systemstart des Linux-Systems hochgefahren werden.

Anmerkung

Sie können die Autostart-Einstellung auch mittels der Mechanismen ändern, die von Ihrem *Init-System* zur Verfügung gestellt werden, falls Sie damit vertraut sind. Unter Debian-Linux können Sie zum Beispiel NCP Friendly Net Detection Server zum Autostart hinzufügen, indem Sie `insserv --add ncp-fnd` aufrufen. Das `<prod>-initconfig`-Werkzeug bringt lediglich den Vorteil, dass es unabhängig vom darunterliegenden Init-Systems ist.

Anmerkung

Wenn Sie NCP Secure Enterprise HA Server installiert haben, der von NCP Secure Enterprise Server abhängt, dann werden sie beide unabhängig im *Init-System* konfiguriert. Bei manchen *Init-Systemen* wird beim Start von NCP Secure Enterprise HA Server automatisch auch NCP Secure Enterprise Server gestartet, um sicherzustellen, dass diese Abhängigkeit erfüllt ist. In machen Fällen müssen Sie selbst sicherstellen, dass beide zum Autostart hinzugefügt sind, um die Behandlung dieser Abhängigkeit korrekt vorzunehmen.

Teil der Integration von NCP-Produkten in das Linux-Init-System ist eine Konfigurationsdatei, die es erlaubt auf einfache Art Startparameter zu konfigurieren. Die folgende Tabelle zeigt den Ort dieser Konfigurationsdatei für die verschiedenen Init-Systeme:

Tabelle 4: Konfigurationsdateien der Init-Systeme

Init System	Ort der Konfiguration
SystemV	/etc/default/ncp-<prod>
Upstart	/etc/init/ncp-<prod>.override
systemd	/etc/sysconfig/ncp-<prod> or /etc/conf.d/ncp-<prod> (unerscheidet sich zwischen Linux-Distributionen)
OpenRC	/etc/conf.d/ncp-<prod>

Im Falle des NCP Friendly Net Detection Server kann ein solche Konfigurationsdatei wie folgt aussehen (kann sich aber wegen Unterschieden zwischen Init-Systemen leicht unterscheiden):

Init-Konfigurations-Skript für NCP Friendly Net Detection Server auf Debian-Linux in /etc/default/ncp-fnd

```
# this is an automatically generated init script for NCP Friendly Net
# Detection Server

# You can add command line switches to this variable that shall be passed to
# the sentinel program
SENTINEL_OPTS=""

# You can add command line switches to this variable that shall be passed to
# the control program
CONTROL_OPTS=""

# Allows to pass custom arguments to the ncpfndd daemon process
ncp_args_ncpfndd=""
```

Die Variablen `ncp_args_*` dienen dazu zusätzliche Parameter an den jeweiligen Daemon zu übergeben, wie [hier](#) erklärt. Die Variablen `SENTINEL_OPTS` und `CONTROL_OPTS` erlauben es benutzerdefinierte Parameter an Aufrufe der Programme *sentinel* und *control* zu übergeben, wenn Sie über das Init-System ausgeführt werden.

Sie können weiterführende Informationen über `<prod>-initconfig` [hier](#) finden.

5 Kommandozeilenwerkzeuge

Hier finden Sie Dokumentation über Kommandozeilenwerkzeuge, die zusammen mit NCP-Produkten unter Linux installiert werden. Die folgende Tabelle gibt einen Überblick über verfügbare Hilfsprogramme:

Tabelle 5: Überblick über Kommandozeilenwerkzeuge

Programm	Beschreibung
<prod>-config	Ein Konfigurations-Werkzeug, das nur für manche NCP-Produkte installiert wird und es ermöglicht interaktive und nicht-interaktive Konfiguration diverser Software-Einstellungen vorzunehmen. Siehe produktspezifische Konfiguration für weitere Informationen.
<prod>-control	Das Gegenstück zum <prod>-sentinel, das es ermöglicht eine laufende Instanz eines NCP-Produkts zu steuern.
<prod>-crash	Ein Werkzeug das verwendet wird, um Informationen über Abstürze von NCP-Programmen zu erzeugen und zu verwalten.
<prod>-desktopconfig	Ein Werkzeug, dass nur in NCP Secure Client enthalten ist, um die Integration der grafischen Programmteile in die Desktop-Oberfläche vorzunehmen.
<prod>-initconfig	Verwaltung der Integration in und Einstellungen für das Linux-Init-System.
<prod>-log	Ein Entwicklungswerkzeug zum Abrufen von Analyse-Informationen von NCP-Software zur Laufzeit.
<prod>-license	Anzeige und Verwaltung aktiver Softwarelizenzen.
<prod>-sentinel	Verwaltungsprozess für alle <i>Daemon</i> -Prozesse eines NCP-Produktes.
<prod>-uninstall	Deinstallations-Programm.

5.1 Die Programme *sentinel* und *control*

In [manuelles Hoch- und Herunterfahren](#) haben Sie erfahren, wie das <prod>-sentinel verwendet werden kann, um ein NCP-Produkt manuell zu starten. In diesem Abschnitt lernen Sie mehr darüber, was Sie mit den Programmen <prod>-sentinel und <prod>-control tun können.

Das Programm *sentinel* ist das Hauptprogramm, dass dafür zuständig ist alle Hintergrundprozesse (*Daemons*) zu starten und zu beenden, die zu einer NCP-Software-Lösung gehören. Einige einfachere NCP-Produkte wie NCP Friendly Net Detection Server bestehen nur aus einem einzelnen *Daemon*-Prozess, aber die meisten bestehen aus einer Gruppe von fünf oder mehr *Daemon*-Prozessen die laufen müssen, um die volle Funktionalität der Software zur Verfügung zu stellen. Auch wenn NCP-Software über das Linux-Init-System gestartet wird kommt das *sentinel*-Programm zum Einsatz.

Das Programm <prod>-control ist das Gegenstück zum Programm *sentinel* und wird verwendet, um mit einem im Hintergrund laufenden *sentinel*-Prozess zu interagieren. Zum Beispiel erhalten Sie Informationen über den aktuellen Betriebszustand des NCP-Produkts, indem Sie <prod>-control -s aufrufen, wie im [Beispiel für NCP Friendly Net Detection Server](#) gezeigt. Die Ausgabe zeigt Informationen über jeden derzeit laufenden *Daemon*-Prozess, seit wann er läuft, die Parameter die verwendet wurden, um ihn zu starten und seine Prozess-ID.

Überprüfung des Betriebszustands von NCP Friendly Net Detection Server mittels *fnd-control*

```
$ fnd-control -s
Gegenwärtiger Betriebszustand von NCP Friendly Net Detection Server

Daemon für Erkennung befreundeter Netze
=====
```

```
Zustand: läuft seit Mo 26 Mai 2014 14:57:10 CEST
Kommandozeile: /opt/ncp/fnd/sbin/ncpfndd -f
Prozess ID: 6180
```

Das Programm `<prod>-control` ermöglicht es Ihnen alle *Daemon*-Prozesse die vom *sentinel* ausgeführt werden zu stoppen oder neuzustarten. Dies wird erreicht, indem die Schalter `--shutdown` bzw. `--restart` übergeben werden.

Anmerkung

Wenn Sie ein NCP-Produkt über das Linux-Init-System oder das `<prod>-initconfig`-Werkzeug gestartet haben, sollten Sie es nicht auf diesem Weg herunterfahren, weil es das Init-System verwirren kann. Das Init-System könnte dann denken, dass NCP-Programm sei abgestürzt, da es sich beendet hat, ohne dazu vom Init-System aufgefordert worden zu sein.

5.1.1 Konfiguration der gestarteten Dienste

Über die Konfigurationsdatei `sentinel.conf` können die vom Sentinel standardmäßig gestarteten Dienste konfiguriert werden:

Konfiguration des Sentinel (`sentinel.conf`)

```
daemons :
{
    sem-nginx = false;
};
```

Aktuell kommt diese Datei lediglich beim NCP Secure Enterprise Management Server zum Einschalten des standardmäßig deaktivierten Webservers für das Ausrollen der TOTP-Zugangsdaten zum Einsatz.

Der bevorzugte Weg, die Konfigurationsdatei zu bearbeiten, sind die Optionen `--enable` und `--disable` des `<prod>-sentinel`:

Webserver für den NCP Secure Enterprise Management Server aktivieren

```
# sem-sentinel --enable sem-nginx
```

Falls ein Dienst deaktiviert ist, wird dies beim Auflisten der einzelnen Dienste angezeigt, was im nächsten Abschnitt beschrieben wird.

5.1.2 Operationen auf individuellen Daemon-Prozessen

Weiterhin können Sie Aktionen auf jeden einzelnen *Daemon*-Prozess ausführen, die der *sentinel* ausführt. Um eine List aller *Daemon*-Prozesse die *sentinel* kennt zu erhalten, rufen Sie einfach `<prod>-sentinel -l`:

Liste aller Daemon-Prozesse für NCP Friendly Net Detection Server

```
$ fnd-sentinel -l
Daemon für Erkennung befreundeter Netze
=====

Programmpfad: ncpfndd -f
Beschreibung: Der einzige Daemon zur Erkennung befreundeter Netze
```

Um eine Operation auf einem *Daemon*-Prozess auszuführen müssen Sie ihn durch seinen Basisnamen identifizieren, welcher im Falle von NCP Friendly Net Detection Server, wie oben gezeigt, `ncpfndd` ist, der einzige *Daemon* der in NCP Friendly Net Detection Server verfügbar ist. Die Operationen die Sie auf *Daemon* durch Verwendung des Werkzeugs `<prod>-control` ausführen können sind die folgenden:

- Neustarten des angegebenen Daemons durch Angabe von `--restart-daemon <Basisname>`
- Ausschalten des angegebenen Daemons durch Angabe von `--disable <Basisname>`
- Einschalten eines zuvor ausgeschalteten Daemons durch Angabe von `--enable <Basisname>`
- Überprüfung, ob der angegebene Daemon gerade läuft durch Angabe von `--runs <Basisname>`

Standardmäßig wartet das Programm *control* bis die angeforderte Operation abgeschlossen ist, bevor es sich beendet. Fügen Sie den Parameter `--nowait` hinzu, um es sofort zurückkehren zu lassen, ohne auf das Ergebnis der Operation zu warten. Weiterhin können Sie den Parameter `--timeout <Sekunden>` angeben, um eine Obergrenze für die Zeit zu setzen, die darauf gewartet wird, dass ein *Daemon* zurückkehrt, wenn er aufgefordert wurde herunterzufahren (dies sind standardmäßig 60 Sekunden). Fall diese Zeit überschritten wird, wird der betroffene *Daemon*-Prozess zwangsweise beendet.

Sie können das Programm *sentinel* auch so konfigurieren, dass bestimmte *Daemon*-Prozesse von Anfang an vom Starten ausgenommen sind, indem Sie `-x <Basisname>` oder `-o <Basisname>` an den *sentinel* übergeben. `-x` schließt den angegebenen *Daemon* vom Start aus während `-o` ausschließlich den angegebenen *Daemon* startet.

Anmerkung

Die Operationen auf einzelnen *Daemon*-Prozessen sind nur für die fortgeschrittene Verwendung oder zur Fehlersuche notwendig. Sie werden diese in der Regel nicht verwenden müssen.

Anmerkung

Manche *Daemon*-Prozesse werden in mehreren verschiedenen Konfigurationen gleichzeitig gestartet. Dies ist derzeit der Fall bei *ncprsd* in NCP Secure Enterprise Management Server. In diesem Fall reicht die Angabe des `<Basisnamen>` nicht aus, um eine bestimmte Instanz eines *Daemon* zu identifizieren. In diesem Fall wird dem *Daemon* eine *Persönlichkeit* hinzugefügt. In solchen Fällen können Sie die unterschiedlichen Persönlichkeiten in Erfahrung bringen, indem Sie die Liste die von `<prod>-sentinel -l` erzeugt wird einsehen. Die Identifikation auf der Kommandozeile erfolgt dann über `<Basisname>:<Persönlichkeit>`. Geben Sie zum Beispiel `ncprsd:radius` an, um die *radius*-Persönlichkeit des *Daemon* *ncprsd* von NCP Secure Enterprise Management Server auszuwählen.

5.1.3 Einfluss darauf nehmen, wie *sentinel* mit Abstürzen umgeht

Wenn einer der Dienste die vom Programm *sentinel* gestartet werden sich unerwartet beendet (zum Beispiel, weil er abgestürzt ist), wird der *sentinel* standardmäßig alle verbleibenden *Daemon*-Prozesse herunterfahren und sich beenden. Dies wird getan, um zu verhindern, dass ein unvollständiger Satz von Diensten läuft und somit immer ein sauberer Betriebszustand herrscht.

Sie können genauer beeinflussen, was *sentinel* in solchen Fällen tut indem Sie Parameter an ihn übergeben. Der Schalter `--max-crashes` bestimmt, wie viele Abstürze der *sentinel* insgesamt erlaubt, bevor er aufgibt. Wenn Sie `--max-crashes 5` übergeben und mehr als fünf Abstürze aufgetreten sind (jegliche *Daemons* die sich fehlverhalten haben zählen), wird der *sentinel* alle Prozesse herunterfahren. Andernfalls wird der abgestürzte *Daemon* neu gestartet.

Während dies erlaubt robust gegen selten auftretende Programmabstürze zu sein eignet es sich nicht so gut für den Fall wenn ein *Daemon* ständig Fehler verursacht (zum Beispiel, weil eine Konfigurationsdatei fehlerhaft ist). Für diesen Fall können die Schalter `--max-crashes-per-time` und `--crash-timebase` zusätzlich verwendet werden. Diese Schalter erlauben es eine *maximale Anzahl von Abstürzen innerhalb eines Zeitraums* zu konfigurieren. `--max-crashes-per-time` bestimmt die maximale Anzahl von Abstürzen und `--crash-timebase` bestimmt den Zeitraum in Minuten. Wenn Sie also `--max-crashes-per-time 5 --crash-timebase 15` angeben bedeutet dies, dass wenn innerhalb von 15 Minuten mehr als fünf Abstürze von *Daemons* stattgefunden haben der *sentinel* aufgeben wird, unabhängig von der Einstellung `--max-crashes`.

Wenn Sie noch genaueren Einfluss darauf nehmen wollen, was in Fehlerfällen geschieht können Sie ein benutzerdefiniertes Skript konfigurieren, dass gerufen wird um zu entscheiden, wie mit der Situation umgegangen werden soll. Hierfür übergeben Sie den Parameter `--script <Programmpfad>`, wobei `<Programmpfad>` der Pfad zu dem ausführbaren Skript ist, dass gerufen werden soll für den Fall, dass ein *Daemon* sich fehlverhält. Dem Skript werden eine Reihe von Umgebungsvariablen mitgegeben, die die gegebene Situation beschreiben. Die folgende Tabelle führt diese auf:

Tabelle 6: Umgebungsvariablen für Absturz-Skripte

Variable	Beschreibung	Beispielwert
ncp_service	Der NCP- <i>Daemon</i> der abgestürzt ist	ncpfndd
ncp_crash_code	Der Rückgabewert des abgestürzten <i>Daemons</i>	1
ncp_crash_signal_nr	Falls der <i>Daemon</i> sich beendet hat, weil er ein Signal empfangen hat wird dessen Nummer in dieser Variable zur Verfügung gestellt	9
ncp_crash_signal_name	Wie ncp_crash_signal_nr, enthält aber eine menschenlesbare Bezeichnung für das Signal	SIGKILL
ncp_exit_restart	Der Rückgabewert, den das Skript zurückgeben sollte, um den abgestürzten <i>Daemon</i> neu starten zu lassen	n.A.
ncp_exit_restart_product	Der Rückgabewert, den das Skript zurückgeben sollte, um das komplette Produkt auf geordnete Weise neu zu starten	n.A.
ncp_exit_shutdown	Der Rückgabewert, den das Skript zurückgeben sollte, um den <i>sentinel</i> zu veranlassen alle verbleibenden Prozesse zu beenden und zurückzukehren	n.A.
ncp_exit_disable	Der Rückgabewert, den das Skript zurückgeben sollte, um den <i>sentinel</i> zu veranlassen den abgestürzten Prozess zu deaktivieren, die restlichen Prozesse jedoch unverändert weiterlaufen zu lassen. Dies hinterlässt das Produkt in einem fehlerhaften Zustand.	n.A.
ncp_exit_internal	Der Rückgabewert, den das Skript zurückgeben sollte, um den <i>sentinel</i> zu veranlassen den Absturz gemäß der internen Logik zur Behandlung von Abstürzen gemäß den Schaltern <code>--max-crashes</code> , <code>--max-crashes-per-time</code> und <code>--crash-timebase</code> zu behandeln.	n.A.

Sie könnten auf diesem Weg zum Beispiel eine E-Mail verschicken, um sich über den aufgetretenen Fehler zu informieren. Oder Sie könnten sich entscheiden das Linux-System neuzustarten. Beachten Sie jedoch, dass das Programm *sentinel* keine weiteren Operationen ausführen kann, bis das Absturz-Behandlungs-Skript zurückgekehrt ist. Hier folgt ein Beispiel eines *bash*-Skripts, dass mit `--script <Programmpfad>` verwendet werden könnte:

```
#!/bin/bash

if [ $ncp_crash_code -ne 0 ]; then
    # verschicke generell eine E-Mail wenn ein Prozess mit einem
    # Fehlercode zurückgekehrt ist
    sendmail emergency@mycompany.com <<<"$ncp_service crashed with $ncp_crash_code!"
fi

if [ $ncp_service = "ncpfndd" ]; then
    # ncpfndd ist abgestürzt

    if [ $ncp_crash_code -eq 0 ]; then
        # wenn ncpfndd erfolgreich zurückgekehrt ist, starte ihn
        # einfach neu
        exit $ncp_exit_restart
    fi

    # andernfalls wird FND herunterfahren
    exit $ncp_exit_shutdown
fi
```

Während des Beendens des *sentinel* selbst führt dieser eine Reihe von Aufräumschritten durch, um sicherzustellen, dass kein globaler Zustand von abgestürzten *Daemon*-Prozessen zurückbleibt. Dies könnten zum Beispiel gemeinsame Speicherbereiche für die Inter-Prozess-Kommunikation sein. Falls solche Daten zurückbleiben könnte das Starten des NCP-Produkts das nächste Mal fehlschlagen, weil unerwartete globale Daten gefunden wurden.

Dies wird durch den *sentinel* verhindert, indem er seine Aufräumarbeiten durchführt. Sie können den *sentinel* auch ausdrücklich veranlassen eine Aufräumaktion durchzuführen, indem Sie den Parameter `--clean` übergeben. Dann wird *sentinel* nach globalen, nicht verwendeten Zustandsdaten suchen, diese entfernen und zurückkehren ohne weitere Aktionen auszuführen.

5.1.4 Übergabe von benutzerdefinierten Parametern an *Daemons*

Sie können *sentinel* zusätzliche Parameter an die einzelnen *Daemon*-Prozesse übergeben lassen. Dies kann nützlich sein zu Zwecken der Fehlersuche oder in anderen, außergewöhnlichen Situationen. Zum Beispiel unterstützen die meisten NCP-*Daemon*-Prozesse eine Option `--verbose`, die sie detailliertere Ausgaben auf die Kommandozeile machen lässt.

Der Weg um solche zusätzlichen Parameter zu übergeben ist es Umgebungsvariablen nach dem Muster `ncp_args_<Basisname>` zu setzen, wobei `<Basisname>` der Basisname des *Daemons* ist, der zusätzliche Parameter erhalten sollte. Hier ist ein Beispiel für NCP Friendly Net Detection Server:

```
$ export ncp_args_ncpfndd="--verbose"
$ fnd-sentinel -f
```

In diesem Fall wird dem *ncpfndd* der Parameter `--verbose` zur Kommandozeile hinzugefügt, wenn dieser durch `fnd-sentinel` gestartet wird. Fügen sie mehr als einen Parameter hinzu, indem Sie diese durch Leerzeichen in der Umgebungsvariable trennen.

In der [Konfigurationsdatei für das Init-System](#) besteht bereits ein Eintrag, um zusätzliche Parameter zu *ncpfndd* übergeben. Ebenso ist in anderen NCP-Produkten für jeden *Daemon*-Prozess eine Umgebungsvariable vordefiniert, um zusätzliche Parameter an diese zu übergeben. Daher müssen Sie lediglich die Parameter an dieser Stelle hinzufügen, um Sie wirksam zu schalten wenn die NCP-Software über das Init-System gestartet wird.

Anmerkung

Wie [hier](#) beschrieben, werden manche *Daemons* als unterschiedliche Persönlichkeiten gestartet, so wie der Fall beim *ncprsd* in NCP Secure Enterprise Management Server. Für diese Fälle ist das Namensmuster für Umgebungsvariablen `ncp_args_<daemon>_<personality>`, wie etwa `ncp_args_ncprsd_radius` für die Radius-Persönlichkeit von *ncprsd*.

5.1.5 Zugriff auf *Daemon*-Logdateien

Jeder *Daemon* der durch *sentinel* gestartet wird bekommt seine eigene Logdatei in `/var/log/ncp/<prod>/<daemon>.log` zugewiesen. Für *ncpfndd* wird zum Beispiel eine Logdatei in `/var/log/ncp/fnd/ncpfndd.log` angelegt. Alle Ausgaben, die ein *Daemon* sonst auf die Konsole schreiben würde, landen in dieser Logdatei. Die Logausgaben werden zu dieser Datei nur hinzugefügt, so dass die Datei beim neustarten des *Daemons* nicht überschrieben wird. Der *sentinel* selbst schreibt Logs nach `/var/log/ncp/<prod>/sentinel.log`.

Wenn Sie den *sentinel* im Vordergrund starten, indem Sie die Option `-f` übergeben, werden diese Logdateien nicht erzeugt, sondern die Ausgabe aller *Daemon*-Prozesse wird auf die Konsole geschrieben.

5.2 Startkonfiguration mit dem Programm *initconfig*

In [Hoch- und Herunterfahren über das Linux-Init-System](#) haben Sie bereits die grundlegende Verwendung des Programms `<prod>-initconfig` kennengelernt. In diesem Abschnitt betrachten wir weitere Funktionalität, die von diesem Werkzeug zur Verfügung gestellt wird.

Das Programm `<prod>-initconfig` ist ein Werkzeug, um die unterschiedlichen Linux-Init-Systeme abzudecken, ohne mit diesen im Detail vertraut zu sein. Es ermöglicht:

- festzustellen, wie die aktuelle Konfiguration eines NCP-Produkts bzgl. des Init-Systems aussieht
- abzufragen, ob ein NCP-Produkt gerade läuft
- ein NCP-Produkt über das Init-System zu starten oder zu stoppen
- die Integration des NCP-Produkts in das Init-System vorzunehmen oder zu entfernen.

5.2.1 Einsehen der aktuellen Konfiguration

Indem Sie `<prod>-initconfig -i` aufrufen erhalten Sie eine Zusammenstellung von Informationen über den Konfigurationszustand des NCP-Produkts bezüglich dem Init-System. Dies umfasst:

- ob das Produkt überhaupt in das Init-System integriert ist
- ob automatisches Hochfahren beim Systemstart aktiviert ist
- ob das Produkt derzeit hochgefahren ist

Wenn Sie wissen möchten welche Dateien im Init-System für Ihr NCP-Produkt installiert wurden übergeben Sie `--show-files`. Dies ist auch hilfreich, um den Ort der [Init-Konfigurations-Datei](#) festzustellen, falls nötig.

Es folgt eine Beispielausgabe für NCP Friendly Net Detection Server:

Informationen über die Init-System-Konfiguration für NCP Friendly Net Detection Server auf Debian-Linux

```
$ fnd-initconfig -i
Standard-Runlevel: 2
NCP Friendly Net Detection Server ist derzeit in UNIX System V integriert
Automatisches Hochfahren bei Systemstart ist eingeschalten
Das Produkt läuft derzeit

$ fnd-initconfig --show-files
/etc/default/ncp-fnd
/etc/init.d/ncp-fnd
```

Wie Sie sehen können kann manche für das Init-System spezifische Information ein Bestandteil sein, wie hier der Standard-Runlevel für das Init-System.

Sie können auch programmatisch überprüfen, ob das Produkt integriert oder am laufen ist, indem Sie die Schalter `--configured` oder `--running` übergeben und den Rückgabewert von `<prod>-initconfig` überprüfen.

5.2.2 Interaktion mit dem Init-System

Anstatt das Init-System direkt über die Kommandos aufzurufen, die in der Ausgabe von `<prod>-initconfig --show-start-c` und `<prod>-initconfig --show-stop-command` angezeigt werden können Sie `<prod>-initconfig` aufrufen, um dasselbe zu erreichen. Um die NCP-Software über das Init-System zu starten geben Sie den Parameter `--start` und um es zu stoppen den Parameter `--stop` ein.

Um die Autostart-Einstellung zu ändern sehen Sie bitte [hier](#) nach.

Schließlich können Sie die Integration der NCP-Software in das Init-System komplett über den Schalter `--remove` entfernen und es wieder integrieren über den Schalter `--integrate`. Sie sollten dies normalerweise nicht ohne guten Grund tun. Ein denkbar Einsatz dafür ist es, die originalen Init-Skripte und Init-Konfigurationsdateien wiederherzustellen, die während der Installation des NCP-Produkts angelegt wurden.

5.3 Umgang mit Softwareabstürzen: Das Programm `crash`

Obwohl NCP-Software sorgfältig gestaltet ist können Programmabstürze in unerwarteten Situationen auftreten. Im Falle eines Programmabsturzes ist es wichtig für den NCP-Support alle verfügbaren Informationen vom Kunden zu erhalten. Nur dann können unsere Softwareentwickler schnell eine Lösung für das Problem zur Verfügung stellen.

Zu diesem Zweck wird das Programm `<prod>-crash` mit jedem NCP-Produkt ausgeliefert. Es hat mehrere Einsatzgebiete. Zum einen registriert es sich im Linux-System, so dass es im Falle von Programmabstürzen gerufen wird und alle notwendigen Informationen einsammeln kann, falls es sich um den Absturz eines NCP-Prozesses gehandelt hat. Der andere Zweck ist es, es dem Endbenutzer leicht zu machen solche Absturzinformationen zu sammeln und an NCP zu senden.

Um einen Überblick über Abstürze zu erhalten, die für ein bestimmtes NCP-Produkt stattgefunden haben rufen Sie `<prod>-crash -i`. Wenn wenigstens ein Absturz vorliegt wird die Ausgabe wie folgt aussehen:

Beispielliste von Programmabstürzen für NCP Friendly Net Detection Server

```
$ fnd-crash -i
Liste aufgezeichneter NCP-Programm-Abstürze für NCP Friendly Net Detection Server

Absturz von Prozess ncpfndd
=====
Ort: /var/adm/ncp/fnd/crashes/ncpfndd.0
Datum: Mo 26 Mai 2014 08:26:08 CDT
```

In diesem Fall können wir sehen, dass ein Absturz für einzigen *Daemon*-Prozess von NCP Friendly Net Detection Server vorhanden ist. Das Basisverzeichnis für Absturzinformationen ist `/var/adm/ncp/<prod>/crashes`. Für jeden Absturz wird ein separates Verzeichnis erstellt, in welchem Absturzinformationen vom Linux-Betriebssystem und zusätzliche NCP-Logdateien gesammelt werden.

Sie können das Programm `<prod>-crash` ein komprimiertes Archiv erzeugen lassen, das alle derzeit bekannten Informationen über Abstürze für das jeweilige Produkt enthält. Dies wird erreicht, indem der Schalter `--report` und der Pfad, wohin das Archiv geschrieben werden soll, übergeben werden. Zum Beispiel:

Generieren eines Absturzbericht-Archivs für NCP Friendly Net Detection Server

```
$ fnd-crash --report /tmp
Die Fehlerberichts-Datei wurde erfolgreich in '/tmp/fnd_crash_report1.tar.bz2'
erstellt.
```

Sie können die resultierende Datei wie sie ist an den NCP-Support senden wenn Sie Fehlersituationen haben.

Teil der Absturzberichte können auch sensible Informationen wie Benutzernamen, E-Mail-Adressen oder gar Teile von geheimen Schlüsselmaterial sein. Zu Ihrer Sicherheit werden deshalb in neueren Version von NCP-Produkten diese Absturzberichte verschlüsselt abgelegt, so dass nur autorisierte NCP-Mitarbeiter diese Daten einsehen können. Diese Dateien können Sie daher bedenkenlos per E-Mail oder auf anderen Wegen über das Internet an den NCP-Support senden.

Sollten Sie diese Verschlüsselung abschalten wollen übergeben Sie den Parameter `--no-encryption`.

Das Programm `<prod>-crash` ermöglicht auch die Ausgabe von Daten über das laufende System. Dies können vorab nützliche Informationen für den NCP-Support sein. Sie erhalten diese Informationen über den Aufruf `<prod>-crash --system-info`.

5.3.1 Löschen alter Absturzberichte

Damit das Sammeln von Absturzberichten nicht zuviel Speicherplatz in Anspruch nimmt, werden beim Auftreten neuer Abstürze automatisch alte Berichte gelöscht. Dieses Löschen kann auch manuell mit `<product>-crash --delete-old` angestoßen werden. Gelöscht werden alle Berichte, die die Anzahl `max_count` überschreiten oder älter als `max_age` Tage sind.

Diese Werte können in der Konfigurationsdatei `global.conf` des entsprechenden Produkts angepasst werden. Wenn beide Werte auf 0 gesetzt sind, werden niemals Absturzinformationen gelöscht. Das Listing zeigt die Voreinstellung der Parameter.

Konfiguration der maximal verfügbaren Absturzberichte (global.conf)

```
crashdump:
{
    max_count = 20; ❶
    max_age = 30; ❷
};
```

5.4 Produktlizenz und -version mit dem Programm `license`

Die meisten NCP-Produkte erfordern einen erworbenen Lizenzschlüssel für die volle Funktionalität. Eine Ausnahme hierfür ist der NCP Friendly Net Detection Server, welcher keine Lizenz benötigt. Alle Produkte enthalten einen 30-Tage-Testzeitraum während dem Sie das Produkt ausprobieren können. Danach ist es notwendig, dass Sie eine gültige Lizenz für das Produkt registrieren, damit es weiter funktioniert.

Um die aktuellen Lizenzdaten einzusehen wird ein separates Hilfsprogramm namens `<prod>-license` bereitgestellt. Das Werkzeug zeigt den verbleibenden Zeitraum an, den die Lizenz noch gültig ist und einige weitere Informationen, die von der aktiven Lizenz und dem Produkt abhängen. Hier folgt ein Beispiel für NCP Secure Enterprise Server unter Verwendung einer Testlizenz, die noch für fünf weitere Tage gültig ist:

Einsehen der verwendeten Lizenz für NCP Secure Enterprise Server

```
$ ses-license

>>>> Aktuelle Lizenzdaten <<<<
Software-Version: NCP Secure Enterprise Server 8.14 (experimental)
Lizenzierte Version: Testversion
Gültig für weitere: 5 Tage
```

In allen Produkten außer NCP Secure Enterprise Management Server wird eine vollwertige Lizenz nicht über die Kommandozeile, sondern über die Weboberfläche (im Fall von NCP Secure Enterprise Server, NCP Secure Enterprise HA Server) oder über die Monitoranwendung (im Falle von NCP Secure Client) aktiviert.

Für NCP Secure Enterprise Management Server wird jedoch die Lizenz über das Programm `sem-license` aktiviert oder aktualisiert. Sie können es entweder mit dem Parameter `--activate` aufrufen, was das Programm veranlasst Sie interaktiv nach den Lizenzdaten zu fragen, die Sie aktivieren wollen. Alternativ können Sie die Lizenzdaten über den Parameter `--license` angeben, welche die Lizenz in der Form `<schlüssel>:<seriennummer>` entgegennimmt, wobei `<schlüssel>` ein 5 x 4-stelliger Schlüssel ist, der durch Minuszeichen getrennt wird und `<seriennummer>` eine 8-stellige Seriennummer.

Neuere Versionen von NCP Secure Client erlauben ebenfalls die Eingabe des Lizenzschlüssels auf diesem Wege als Alternative zur Eingabe über die grafische Benutzeroberfläche.

6 Produktspezifische Konfiguration

Dieser Abschnitt behandelt Hilfsprogramme und Konfigurationsaufgaben, die speziell für das jeweilige NCP-Produkt sind. Jedes Produkt wird in einem eigenen Unterabschnitt behandelt, sofern überhaupt vorhanden.

6.1 NCP Secure Client

6.1.1 Hinzufügen von Desktopsymbolen und Menüeinträgen mit `clnt-desktopconfig`

Das Werkzeug `clnt-desktopconfig` führt die Integration von NCP Secure Client in die grafische Desktopumgebung aus. Abhängig von dem Desktop den Sie verwenden umfasst dies die Erzeugung von Desktopsymbolen und Menüeinträgen, um die grafische Monitoranwendung zu starten.

Jeder Benutzer im System, der NCP Secure Client verwenden möchte kann `clnt-desktopconfig` aufrufen vorausgesetzt, dass der Benutzer ein Mitglied der Installationsgruppe von NCP Secure Client ist, welches standardmäßig `ncp` ist. Das Programm führt die Integration in die Desktopumgebung für den aufrufenden Benutzer aus. Das bedeutet, dass Sie keine Desktopsymbole als `root` für einen anderen Benutzer anlegen können.

Die wesentlichen Programmschalter, die `clnt-desktopconfig` unterstützt sind `--remove` und `--integrate`, die jeweils die Integration von NCP Secure Client in den Desktop des Aufrufers entfernen bzw. ausführen.

Anmerkung

Sie können die grafische Monitoranwendung nur ausführen, wenn die *Daemon-Prozesse* des NCP Secure Client im Hintergrund laufen.

6.2 NCP Secure Enterprise Server

6.2.1 Einrichtung von SNMP

Sie können das SNMP-Protokoll (Simple Network Management Protocol) verwenden, um Informationen über den Betriebszustand des NCP Secure Enterprise Server über das Netzwerk abzufragen und weiterzuverarbeiten. Dies kann zum Beispiel zur Überwachung dienen.

Unter Linux ist hierfür die Installation des Dienstes `snmpd` (es wird auch die Bezeichnung `net-snmp` verwendet) notwendig, der das SNMP-Protokoll implementiert. Diesen installieren Sie über die Paketverwaltung Ihrer Linux-Distribution. Zur allgemeinen Einrichtung und Verwendung des `snmpd` finden Sie Informationen in der Dokumentation Ihres Linux-Systems oder auf den Projektseiten im Internet.

Damit der `snmpd`-Dienst Daten aus dem NCP Secure Enterprise Server erhalten kann ist es notwendig einen Konfigurationseintrag vorzunehmen. Typischerweise befindet sich die relevante Konfigurationsdatei für `snmpd` unter `/etc/snmp/snmpd.conf`. Dort ist folgende Zeile einzufügen:

Eintrag des NCP Secure Enterprise Server SNMP-Plugins in die `snmpd.conf`

```
dlmod ncpSecureServer /opt/ncp/ses/lib/libncpsrvagent.so
```

Bitte beachten Sie, dass Sie diesen Pfad anpassen müssen, falls Sie NCP Secure Enterprise Server in ein anderes Verzeichnis installiert haben.

Nach der vollständigen Konfiguration von `snmpd` müssen Sie den Dienst starten bzw. neu starten. Sofern die Konfiguration und die Zugriffsrechte korrekt eingerichtet wurden sollte folgendes Kommando eine Liste mit Statuswerten des NCP Secure Enterprise Server liefern:

Testabfrage von NCP SNMP-Daten nach erfolgter Einrichtung von `snmpd`

```
snmpwalk -v 2c -c public localhost iso.3.6.1.4.1.1213.8
```

Eine MIB-Definitionsdatei ist verfügbar um die numerischen OIDs in menschenlesbare Namen zu konvertieren.

```
snmpwalk -v 2c -m /opt/ncp/ses/etc/snmp/ncpmibs/ses.mib -c public localhost ncpSecureServer
```

Die folgenden Untereinträge sind unterhalb des `ncpSecureServer` Eintrags verfügbar: `ncpSESSystemInfo`, `ncpSESLocalSystemStat`, `ncpSESLinkStatusLocal`, `ncpSESLinkStatusRadius`, `ncpSESSslVpnSessionStat`, `ncpSESDomainGroupStat`, `ncpSESServerCertificateStat`. Sie entsprechen den Einträgen in der Statistik des Secure Servers.

6.3 NCP Secure Enterprise HA Server

6.3.1 Einrichtung von SNMP

Die Einrichtung von SNMP für den NCP Secure Enterprise HA Server erfolgt analog zu der Erläuterung für [SNMP für NCP Secure Enterprise Server](#). Sie müssen lediglich als Plugin in der Konfiguration folgende Zeile verwenden:

Eintrag des NCP Secure Enterprise HA Server SNMP-Plugins in die `snmpd.conf`

```
dlmod ncpHaSrv /opt/ncp/has/lib/libncphasrvagent.so
```

6.4 NCP Secure Enterprise Management Server

Der NCP Secure Enterprise Management Server erfordert etwas mehr lokale Konfiguration als die anderen Produkte, da eine Datenbankverbindung zwingend erforderlich ist, damit der Server überhaupt startet. Deshalb muss die Konfiguration auch lokal erfolgen und nicht etwa in der Management-Konsole.

Die Grundeinstellungen des NCP Secure Enterprise Management Server können mit Hilfe des Programms `sem-config` vorgenommen werden. Das Programm erfordert Root-Rechte, ggf. wird beim Start nach dem Root-Passwort bzw. dem eigenen Passwort gefragt. Wir haben uns bewusst für ein semi-grafisches Werkzeug statt einer grafischen Benutzeroberfläche entschieden, da dieses auch über eine SSH-Verbindung oder direkt auf der Linux-Konsole funktioniert und somit auch auf Servern nutzbar ist, welche gar keine grafische Oberfläche eingerichtet haben.

Hinweis zur Aktualisierung von älteren Versionen

Das hier beschriebene semigrafische Konfigurationstool `sem-config` wurde in Version 5.30 des NCP Secure Enterprise Management Server neu eingeführt. Das Programm gab es zwar schon vorher, konnte aber nur den Wechsel der Betriebsart durchführen, sowohl textbasiert interaktiv als auch im Batch-Modus. Sämtliche andere Einstellungen mussten in der Konfigurationsdatei manuell vorgenommen werden.

Für ältere Versionen konsultieren Sie bitte die Dokumentation, welche mit der jeweiligen Version mit ausgeliefert wurde. Die Beschreibung der Konfigurationsdatei wurde in dieser Version der Dokumentation entfernt. Natürlich ist es aber nach wie vor möglich, die Datei von Hand zu editieren.

Der Batch-Modus des Tools zum Umschalten der Betriebsart funktioniert wie gewohnt, wo dass Skripte nicht angepasst werden müssen.

Das Programm orientiert an der Management-Konfiguration unter Windows. Die Anordnung der Bedienelemente und die Begrifflichkeiten sind diesem Werkzeug angelehnt. Nach dem Start erscheint zunächst das Hauptmenü. Dieses Menü entspricht den Tabs der Windows-Oberfläche.

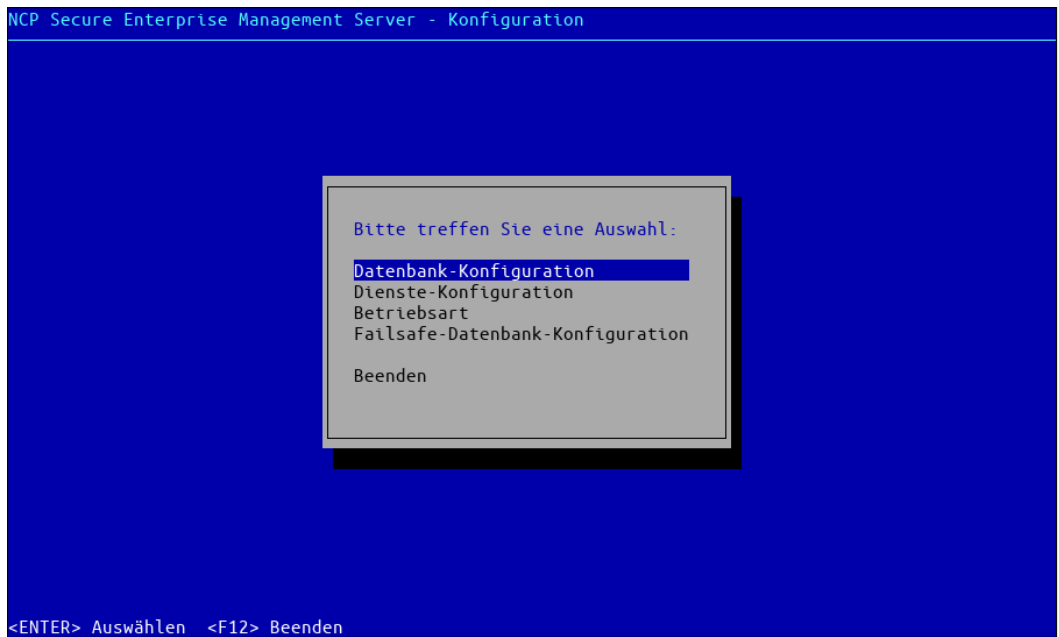


Abbildung 1: Hauptmenü

Wählen Sie mit den Cursortasten einen Menüeintrag aus und bestätigen Sie ihre Auswahl mit der Eingabetaste. Zum Beenden können Sie entweder *Beenden* wählen und mit der Eingabetaste bestätigen oder die F12-Taste drücken.

Zunächst einige Worte zur Bedienung: Grundsätzlich können die Cursortasten zur Navigation verwendet werden. Die Tab-Taste springt zum nächsten Eingabefeld, Optionsfeld oder zur nächsten Schaltfläche. Die Leertaste wählt eine Option aus, die Eingabetaste führt die Selektion aus. Ganz unten wird jeweils die Belegung der Funktionstasten dargestellt, mit denen die Bedienung wesentlich beschleunigt werden kann. Alle Funktionen sind allerdings zusätzlich über Schaltflächen verfügbar, falls die Funktionstasten (zum Beispiel über SSH) wider erwarten nicht funktionieren. Bei manchen Tastaturen, insbesondere bei Notebooks, muss zur Funktionstaste zusätzlich eine Fn-Taste betätigt werden, weil die Tasten standardmäßig anderweitig belegt sind.

6.4.1 Datenbankkonfiguration

Das Programm ermöglicht sowohl die Konfiguration der primären Datenbank als auch der Datenbank für den Failsafe-Server. Die Einstellungen sind identisch, daher wird an dieser Stelle jeweils nur die primäre Datenbank gezeigt; sie gelten für Failsafe-Server analog.

Es werden zwei Schnittstellen unterstützt, auf die Datenbank zuzugreifen:

1. die native Anbindung für *MariaDB*- bzw. *MySQL*-Datenbanken
2. die ODBC-Schnittstelle über die Kompatibilitätsschicht *unixODBC*

Bevor allerdings mit Hilfe von `sem-config` die Datenbank konfiguriert und getestet werden kann, muss erst einmal prinzipiell eine Datenbank erstellt werden. Dies wird im nächsten Abschnitt beschrieben. Falls die Datenbank schon existiert, können Sie den Abschnitt überspringen.

Einrichtung der Datenbank

Egal ob der Zugriff über den nativen Connector oder über ODBC konfiguriert wurde, muss die Datenbank an sich noch eingerichtet werden. Die vollständige Einrichtung der MySQL-Datenbank sprengt den Rahmen dieser Dokumentation. Bitte nutzen Sie die Dokumentation Ihrer Linux-Distribution für den MySQL-Server für weitere Informationen über dieses Thema. Nur so viel: Ein einfaches Programm zur Ersteinrichtung namens `mysql_secure_installation` existiert, dass sinnvolle Initial-einstellungen vornimmt und ein Passwort für den *root*-Benutzer des MySQL-Servers einrichtet.

**Wichtig**

Benutzer mit leeren Passwörtern werden vom NCP Secure Enterprise Management Server nicht unterstützt.

Unter der Annahme, dass Ihr MySQL-Server korrekt eingerichtet ist und läuft müssen Sie sich nun in die MySQL-Server-Konsole einloggen und die Datenbank anlegen. Dies wird wie folgt erreicht:

Anlegen einer leeren Datenbank namens „semdb“

```
$ mysql -u root -p
Enter password: <password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
[...]
```

```
mysql> create database semdb;
Query OK, 1 row affected (0.00 sec)
```

```
mysql> quit
Bye
```

Schließlich können Sie mit der Konfiguration des NCP Secure Enterprise Management Server fortfahren, was in den nächsten beiden Abschnitten beschrieben wird. Dort wird auch beschrieben, wie Sie eine Datenbankverbindung testen.

Datenbankkonfiguration unter Verwendung der nativen Schnittstelle für MariaDB bzw. MySQL

Bei dieser Variante wird der **MariaDB Connector/C** bzw. **MySQL Connector/C** (beide sind schnittstellenkompatibel) verwendet, um mit der Datenbank zu kommunizieren.

Dies ist die empfohlene Variante, falls eine MariaDB- bzw. MySQL-Datenbank verwendet wird. Nur bei anderen Datenbanken sollte auf die unixODBC-Schnittstelle zurückgegriffen werden.

In der Konfigurationsoberfläche stellt sich das Ganze wie in Abbildung 2 gezeigt dar.

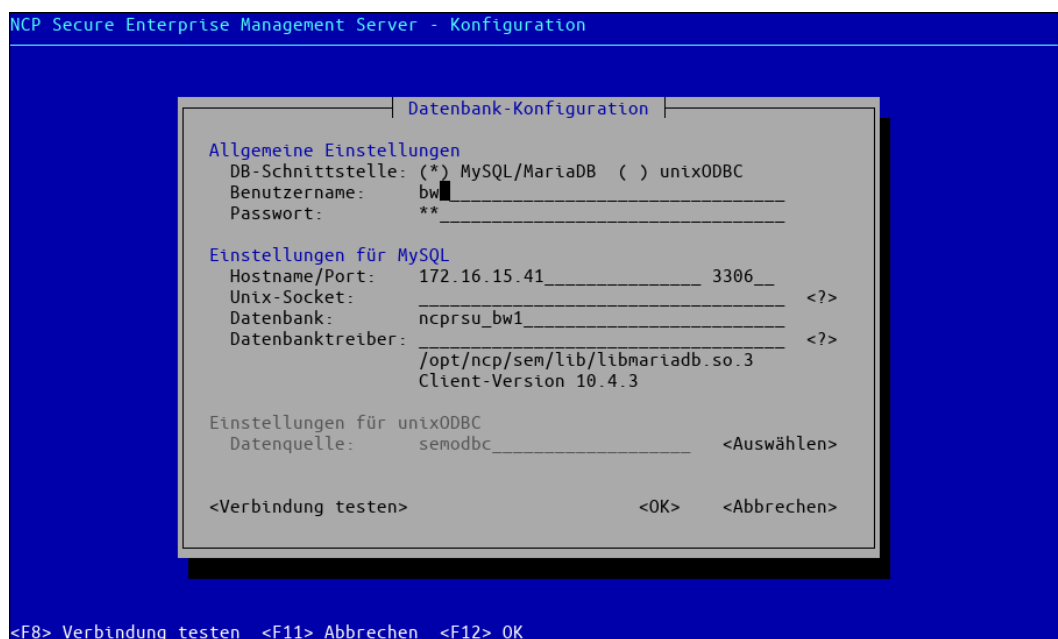


Abbildung 2: Konfiguration einer MariaDB-Datenbank

Falls nicht bereits ausgewählt selektieren Sie die MariaDB-Schnittstelle, indem Sie das Optionsfeld (*) MySQL/MariaDB mit der Tab-Taste selektieren und mit der Leertaste aktivieren. Die Einstellungen für *Benutzername*, *Passwort*, für den *Hostnamen* (ggf. localhost), den *Port* sowie für die *Datenbank* sollten selbsterklärend sein.

Der *Unix-Socket* ist eine zu TCP/IP alternative Kommunikationsmöglichkeit, wenn sich die Datenbank und der Management-Server auf dem selben Rechner befinden. In dieses Feld wird der Pfad zu einem Unix-Domain-Socket eingetragen. Dieser ist spezifisch für die jeweilige Linux-Distribution. Falls die Kommandozeilenwerkzeuge `mysql` bzw. `mariadb` eingerichtet sind, kann der Pfad des Sockets damit herausgefunden werden:

Ermitteln des Pfades des Unix-Domain-Sockets mit `mysql`

```
$ mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
...

mysql> show variables like 'socket';
+-----+-----+
| Variable_name | Value                               |
+-----+-----+
| socket        | /var/lib/mysql/mysql.sock         |
+-----+-----+
1 row in set (0.00 sec)

mysql> Bye
```

Damit der Unix-Domain-Socket verwendet wird, muss als Hostname `localhost` konfiguriert werden. Ist dieses Feld leer, so wird eine lokale TCP/IP-Kommunikation verwendet.

Der *Datenbanktreiber* ist eine Bibliothek (Shared Object) die die Kommunikation mit der MariaDB- bzw. MySQL-Datenbank implementiert. Es handelt sich um den Connector/C. Seit Version 5.30 des NCP Secure Enterprise Management Server liefert NCP den *MariaDB Connector/C* in der jeweils neuesten Version mit aus. Wird in dieses Feld nichts eingetragen, so wird dieser mit ausgelieferte Treiber verwendet. Dennoch kann ein manuell oder über die Linux-Distribution installierter Treiber konfiguriert werden. Tragen Sie hierfür in dieses Feld den absoluten Pfad oder nur den Dateinamen (dann wird in den System-Bibliotheksverzeichnissen gesucht) zum Datenbanktreiber mit ein. Wenn Sie dieses Feld verlassen wird sofort geprüft, ob es sich um einen gültigen Datenbanktreiber handelt und die Version angezeigt. Eine Kommunikation mit der Datenbank erfolgt noch nicht.

Um die Einstellungen zu testen, wählen Sie mit der Tab-Taste die Schaltfläche *Verbindung testen* aus oder drücken Sie F8. Im Erfolgsfall sollte eine Meldung wie in Abbildung 3 gezeigt erscheinen. Im Fehlerfall zeigt die Meldung genauere Informationen zur Fehlerursache.

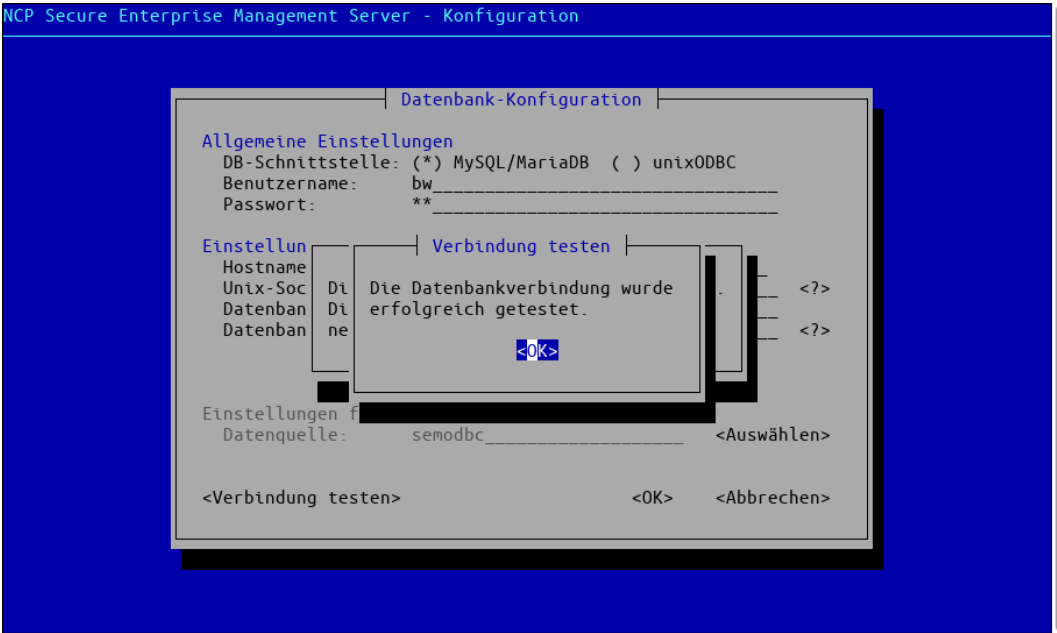


Abbildung 3: Erfolgreicher Verbindungstest

Die Konfiguration wird für den Verbindungstest noch nicht gespeichert. Dies geschieht erst, wenn Sie den Dialog mit *OK* bzw. F12 verlassen. Mit *Abbrechen* oder F11 verlassen Sie, ohne zu speichern.

Datenbankkonfiguration unter Verwendung von unixODBC

In diese Fall wird zur Datenbankanbindung die Schnittstelle *ODBC* (Open Database Connectivity) verwendet. Dies ist eine Softwareschicht, die zwischen der eigentlichen Datenbank und dem NCP Secure Enterprise Management Server vermittelt.

Um die Datenbank und die ODBC-Schnittstelle zu konfigurieren, müssen Sie einige Pakete auf Ihrer Linux-Distribution installieren und vorbereiten. Obwohl prinzipiell verschiedene Datenbankverbindungen und ODBC-Schnittstellen unterstützt werden ist die gängige Konfiguration die folgende:

- **MySQL** für die eigentliche Datenbank
- die Bibliothek **unixODBC** als ODBC-Schnittstelle
- der Treiber **myodbc**, um unixODBC mit MySQL zu verknüpfen

In diesem Handbuch nehmen wir an, dass Sie noch keines dieser Pakete bisher eingerichtet haben. Typischerweise können Sie diese Software über den Paketmanager Ihrer Linux-Distribution installieren. Die folgende Tabelle gibt einen Überblick über die Paketnamen und Kommandos, um die Pakete auf den üblichen Linux-Distributionen zu installieren:

Tabelle 7: MySQL / ODBC Paketinstallation unter Linux

Linux-Distribution	Paketnamen	Installationskommando
Debian, Ubuntu	mysql-server, unixodbc, libmyodbc	apt-get install mysql-server unixodbc libmyodbc
Red Hat, CentOS	mysql-server, unixodbc, mysql-connector-odbc	yum install mysql-server unixodbc mysql-connector-odbc
SUSE SLES	unixODBC, mysql, MyODBC-unixODBC	zypper install unixODBC mysql MyODBC-unixODBC

Anmerkung

Es kann notwendig sein, zusätzliche Repository-Quellen in SUSE zu konfigurieren, um das MyODBC-Paket zu erhalten.

Anmerkung

Sollte in Ihrer Linux-Distribution die `mysql`-Datenbank durch die alternative `mariadb`-Datenbank ersetzt worden sein, so treffen die hier aufgeführten Instruktionen weitestgehend ebenfalls zu. Sie müssen in diesem Fall lediglich anstatt der `mysql`-Pakete analog die `mariadb`-Pakete installieren. `unixodbc` und `myodbc` bleiben gleich.

Abhängig von der Linux-Distribution werden sich nach der erfolgreichen Installation aller nötigen Pakete neue Konfigurationsdateien entweder in `/etc` oder in `/etc/unixODBC` befinden. Die Namen dieser Dateien sind `odbc.ini` und `odbcinst.ini`. Diese Dateien müssen von Ihnen für Ihre Umgebung angepasst werden.

In `odbcinst.ini` wird der *ODBC*-Treiber bekannt gemacht. Ein Name für die Treiberkonfiguration muss gewählt werden und der Pfad zu der Treiberbibliothek muss angegeben werden. Im folgenden Beispiel benutzen wir den Namen *myodbc*. Der Pfad zu der Treiberbibliothek kann sich zwischen Linux-Distributionen unterscheiden:

Beispielinhalt von `odbcinst.ini`

```
[myodbc]
Driver=/usr/lib/libmyodbc5.so
UsageCount=1
```

Danach wird in `odbc.ini` die Datenbankverbindung unter Verwendung des zuvor bekannt gemachten *ODBC*-Treiber konfiguriert. Wieder müssen Sie einen Namen für diese Datenbankverbindung wählen. Zusätzlich muss die Verbindung zu der *MySQL*-Datenbank angegeben werden. Die Verbindung wird über das Netzwerk hergestellt. In unserem Fall, da *MySQL* auf derselben Maschine läuft wie *ODBC* und NCP Secure Enterprise Management Server, ist die *MySQL* Serveradresse `localhost`. Sie können jedoch auch komplexere Konstellationen erreichen, in denen die *MySQL*-Datenbank auf einer separaten Maschine läuft.

Weiterhin müssen der Name der *MySQL*-Datenbank zu der verbunden wird und ein gültiger Benutzername und Passwort angegeben werden. Nachfolgend eine Beispielfunktion:

Beispielinhalt von `odbc.ini`

```
[semodbc]
Driver = myodbc
Description = MySQL connection for NCP-SEM
Server = localhost
Port = 3306
Database = semdb
```

- ❶, ❶ Dies ist der Name der Treiberkonfiguration wie angegeben in [odbcinst.ini](#)
- ❷, ❷ Dies sind der Standardserver und -port für den lokal laufenden *MySQL*-Server.
- ❸ Dies ist der Name der Datenbank innerhalb *MySQL*, die von NCP Secure Enterprise Management Server verwendet werden wird.

Starten Sie nun `sem-config`, wählen Sie *Datenbank-Konfiguration*. Ändern Sie den Verbindungstyp in *unixODBC*, indem Sie das entsprechende Auswahlfeld mit der Tab-Taste auswählen und mit der Leertaste aktivieren.

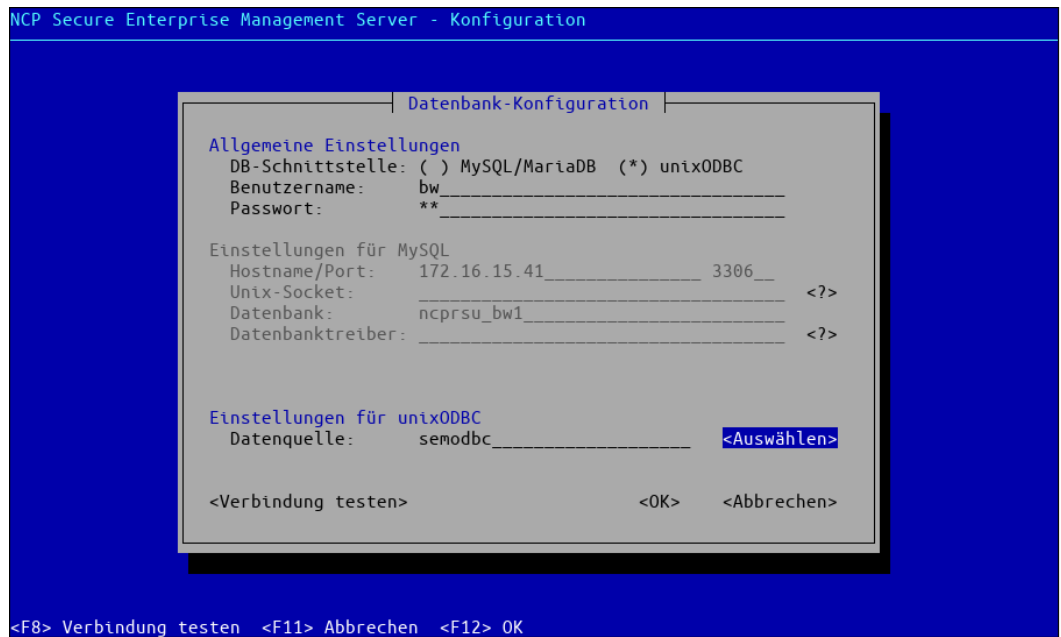


Abbildung 4: Datenbankkonfiguration einer unixODBC-Verbindung

Nun werden die meisten Felder ausgegraut, da sie ja bereits in der ODBC-Konfiguration festgelegt wurden. Sie müssen nur noch den *Benutzernamen*, das *Passwort* und die *Datenquelle* aus der `odbc.ini` eintragen. Mit Hilfe des Buttons *Auswählen* werden alle Datenquellen gelesen und Sie müssen sie nur noch auswählen.

Um die Einstellungen zu testen, wählen Sie mit der Tab-Taste die Schaltfläche *Verbindung testen* aus oder drücken Sie F8. Im Erfolgsfall sollte eine Meldung wie in Abbildung 3 gezeigt erscheinen. Im Fehlerfall zeigt die Meldung genauere Informationen zur Fehlerursache. Die Konfiguration wird für den Verbindungstest noch nicht gespeichert. Dies geschieht erst, wenn Sie den Dialog mit *OK* bzw. F12 verlassen. Mit *Abbrechen* oder F11 verlassen Sie, ohne zu speichern.

Verbindungstest über die Kommandozeile

Ein Verbindungstest kann nicht nur über das Konfigurationswerkzeug erfolgen sondern auch über die Kommandozeile durch den Parameter `-testDB` des `ncprsud`:

Erfolgreiche Verbindung von `ncprsud` mit einer Datenbank

```
$ ncprsud -testDB
Init Database Connection
Database Connection ok
Begin Test Database Access and Types
[...]
```

Verwenden Sie diese Art des Verbindungstests, um eventuelle Fehlermeldungen vollständig angezeigt zu bekommen und ggf. in eine Datei umleiten zu können.

6.4.2 Dienste-Konfiguration

Der NCP Secure Enterprise Management Server besteht aus mehreren Diensten, die miteinander interagieren. Welche Dienste für den Betrieb notwendig sind, hängt im Wesentlichen von der *Betriebsart* ab. Die Dienste werden vom *Sentinel-Programm* gestartet und gestoppt, sind dem Init-System also nur indirekt bekannt.

Der einzige Dienst, der normalerweise manuell aktiviert oder deaktiviert werden soll, ist der Webserver `sem-nginx`, der die Webseite bereitstellt, welche die Anwender direkt aufrufen, um ihre TOTP-Zugangsdaten abzurufen. Wenn diese Funktionalität nicht benötigt wird, muss der Webserver nicht laufen. Da dies für die Mehrzahl der Installationen zutrifft, ist er auch im Auslieferungsumfang deaktiviert.

Die Dienste-Konfiguration stellt sich wie in Abbildung 5 gezeigt dar.

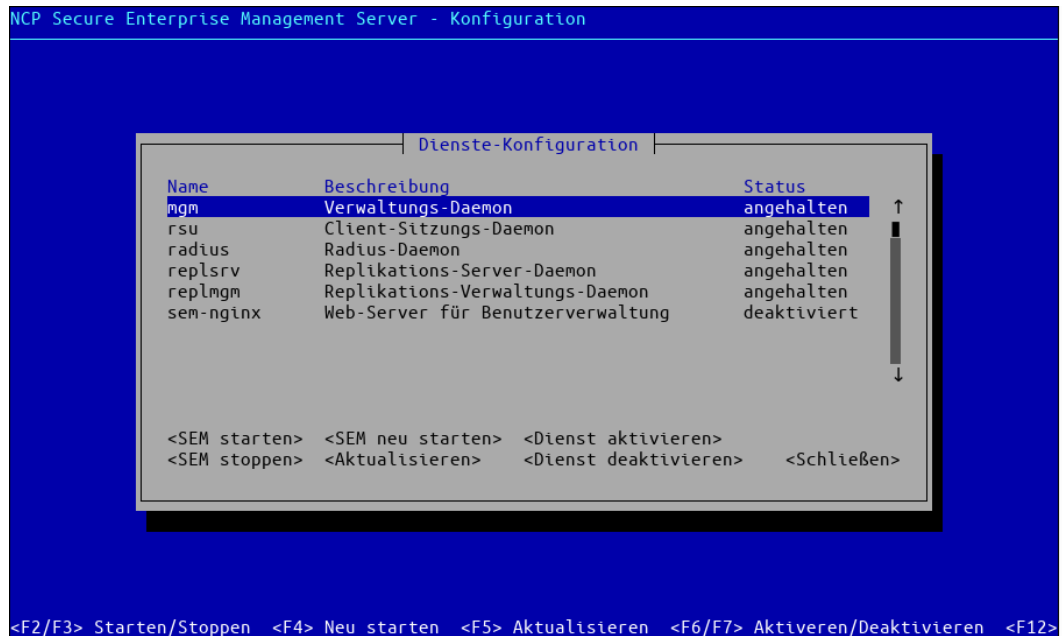


Abbildung 5: Dienste-Konfiguration

Im oberen Bereich des Dialogs wird der Zustand des Dienstes angezeigt. Neben *angehalten* und *läuft* gibt es auch den zusätzlichen Zustand *deaktiviert*, was bedeutet, dass er nicht läuft und auch nicht gestartet wird, wenn der Master-Daemon *Sentinel* gestartet wird.

Folgende Funktionen stehen über die entsprechenden Auswahlfelder bzw. Funktionstasten zur Verfügung:

- **SEM starten (F2):** Der NCP Secure Enterprise Management Server wird über das Init-System gestartet, falls er noch nicht läuft. Diese Funktion ist äquivalent zu `sem-initconfig --start`.
- **SEM stoppen (F3):** Der Management-Server wird über das Init-System beendet, falls er läuft. Diese Funktion ist äquivalent zu `sem-initconfig --stop`.
- **SEM neu starten (F4):** Der Management-Server wird neu gestartet, falls er läuft. Der Master-Dienst *Sentinel* wird nicht neu gestartet. Diese Funktion ist äquivalent zu `sem-control --reload --restart`.
- **Aktualisieren (F5):** Der Status der Dienste in der Anzeige wird aktualisiert. Dies ist vor allem dann erforderlich, wenn sich der Zustand geändert hat ohne dass Änderung durch dieses Werkzeug veranlasst wurde.
- **Aktivieren (F6):** Ein deaktivierter Dienst wird aktiviert und gleich gestartet. Diese Funktion ist äquivalent zu `sem-sentinel --enable <service>` (aktiviert den Dienst) gefolgt von `sem-control --enable <service>` (startet den Dienst sofort und nicht erst beim nächsten Start).
- **Deaktivieren (F7):** Ein aktivierter Dienst wird deaktiviert und gleich beendet. Diese Funktion ist äquivalent zu `sem-sentinel --disable <service>` (deaktiviert den Dienst) gefolgt von `sem-control --disable <service>` (beendet den Dienst sofort und nicht erst beim nächsten Beenden).

6.4.3 Konfiguration der Betriebsart

Wie Sie der allgemeinen Produktdokumentation entnehmen gibt es drei Betriebsarten des Management-Servers:

- *Primary Server* (Primärmodus): Der primäre NCP Secure Enterprise Management Server verwaltet die Hauptkopie aller Daten.
- *Backup Server* (Backupmodus): Kann verwendet werden, um einen nur-lesenden Spiegel des Primärservers zu betreiben.
- *Failsafe Server* (Notfallmodus): Ein Server, der im Backupmodus läuft kann in diesen Modus versetzt werden, um einen ausgefallenen NCP Secure Enterprise Management Server im Primärmodus zu ersetzen. Er übernimmt dann die Rolle des Primärservers bis der ursprüngliche Server wieder zur Verfügung steht.

`sem-config` ermöglicht sowohl das Umschalten der Betriebsart als auch die initiale Konfiguration. Abbildung 6 zeigt die Konfiguration des Primärmodus, Abbildung 7 im Backupmodus. Die Änderungen werden erst nach einem Neustart angewandt. Wenn der Management-Server läuft, während Sie den Dialog mit *OK* verlassen, wird automatisch angeboten, den Server neu zu starten.

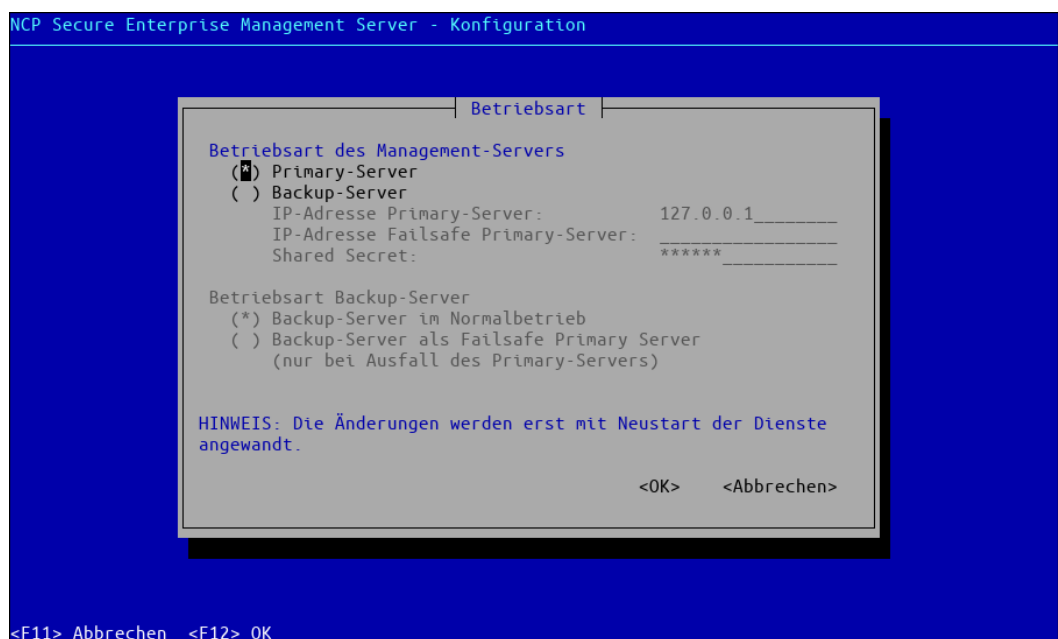


Abbildung 6: Konfiguration der Dienste — Ansicht im Primärmodus

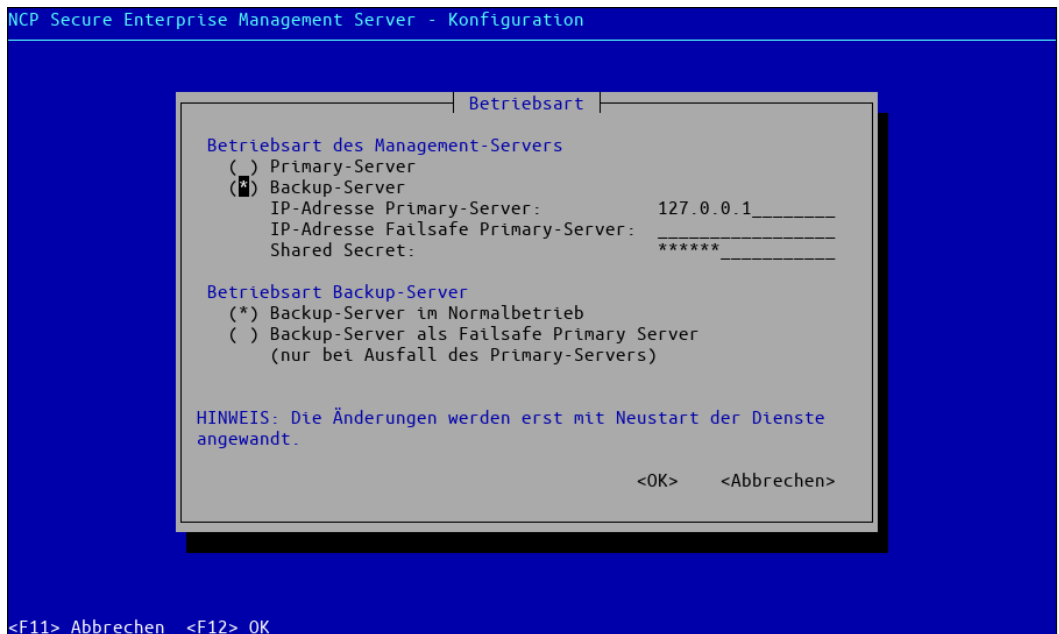


Abbildung 7: Konfiguration der Dienste — Ansicht im Backup-Modus

Umschalten zwischen Backup- und Failsafe-Modus im Batchmodus

Mit Hilfe des Schalters `--mode <BACKUP|FAILSAFE>` kann zwischen den Betriebsarten Backup und Failsafe gewechselt werden, ohne dass hierfür die Textoberfläche gestartet werden muss.

Umschalten der Betriebsart auf „Failsafe“

```
$ sem-config --mode=FAILSAFE
```

Die Änderungen werden erst nach einem Neustart wirksam, welcher manuell durchgeführt werden muss, entweder über das Init-System oder mit `sem-control --reload --restart`. Der Schalter `--reload` bewirkt, dass der Sentinel-Dienst seine Konfiguration – und damit auch die SEM-Betriebsart – neu liest, bevor er die Programme neu startet. Beim Wechsel der Betriebsart sind nämlich ggf. andere Dienste zu starten.