Benutzerhandbuch für Linux-Produkte

Administrationshandbuch

Next Generation Network
Access Technology

www.ncp-e.com

Kontakt

Wenn Sie weitere Informationen wünschen oder Fragen zu NCP-Produkten und Service-Leistungen haben:

Deutschland
NCP engineering GmbH
Dombühlerstraße 2
D-90449 Nürnberg
Tel.: +49 (911) 9968 0
Homepage: http://www.ncp-e.com
Mail: info@ncp-e.com

USA, North America
NCP engineering, Inc.
601 Cleveland Street
Suite 501-25
Clearwater, FL 33755
Phone: +1 (650) 316-6273

Support per E-Mail:

support@ncp-e.com (deutsch)
helpdesk@ncp-e.com (englisch)

Support Hotline:

0900 / 1 99 68 00
(nur aus Deutschland erreichbar, 80 Cent / Minute)
Unsere Supportzeiten sind von Mo - Fr von 08:00 - 17:00 Uhr.

Bei einer Support-Anfrage benötigen wir folgende Informationen:
- Genauer Produktname
- Seriennummer
- Versionsnummer
- Genaue Problembeschreibung
- Fehlermeldung

Benutzerhandbuch für Linux-Produkte

Inhaltsverzeichnis

1. Einleitung

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

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 Funktionen hinzugefügt oder Fehler behoben werden.

Um vollen Nutzen aus diesem Dokument zu ziehen, sind Grundlagenwissen über das Linux-Betriebsystem und die Linux-Kommandozeile erforderlich.

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 für die individuelle Abkürzung, die für jedes NCP-Produkt zum Einsatz kommt, verwendet. 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

Produkt	Wert für `<prod>`
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 werden, sind dafür vorgesehen, von einer Linux-Konsole aus ausgeführt zu werden. Andere Begriffe für *Konsole* in diesem Dokument sind *Terminal* oder *Kommandozeile*. Sie erhalten für jedes Konsolenkommando `<cmd>` eine kurze Hilfe, indem Sie `<cmd> --help` oder `<cmd> -h` eingeben.

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

1.3. Unterstützte Linux-Distributionen

NCP-Produkte laufen auf folgenden Linux-Distributionen:

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

1.4. Firewall

Beachten Sie, dass alle Produkte außer dem NCP Secure Client für einen einwandfreien Gebrauch eingehende Netzwerkverbindungen benötigen. Daher ist es notwendig, bestehende Firewall-Konfigurationen 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 folgendes zu beachten: Sämtliche Hinweise in diesem Dokument, welche die Systemumgebung betreffen (beispielsweise die unterstützten Linux-Distributionen), haben keine

Gültigkeit, da es sich um eine virtuelle Appliance handelt. Diese bringt 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 via speziell dafür zur Verfügung gestellte Paketquellen. Ziehen Sie deshalb die entsprechende Installationshilfe zurate.

Beide Produkte basieren auf den gleichen Mechanismen und bringen die gleichen Kommandozeilenwerkzeuge mit. Sämtliche Funktionen erreichen Sie über die Weboberfläche bzw. den Management-Server.

2. Umstellung von älteren Versionen von NCP-Software

Falls Sie ein NCP-Produkt aktualisieren, das älter ist als hier 1 aufgelistet, dann ergeben sich einige wesentliche Änderungen:

- Eine neue Installationsroutine wird verwendet und die Ablageorte von Dateien haben sich verändert. Sie finden allgemeine Informationen über den Installationsvorgang 3 und Informationen spezifisch für Aktualisierungen alter Versionen 7 in diesem Dokument.
- Die Art wie NCP-Programme gestartet und in das Linux-*Init*-System integriert werden, hat sich verbessert. Sie finden weitere Informationen in Starten und Stoppen 12 des Produkts.
- Eine Reihe neuer und standardisierter Kommandozeilenprogramme sind nun Teil jedes NCP-Produktes. Informationen darüber finden Sie in dem Abschnitt über Kommandozeilenwerkzeuge 15.

Hinweis

Die Änderungen zu vorherigen Versionen der NCP-Software sind stellenweise beträchtlich. Die Aktualisierungen werden automatisch vorgenommen. Aufgrund der Komplexität des Vorgangs und der individuellen Umgebung können jedoch Fehler auftreten. Lesen Sie sich die Unterschiede zu älteren Versionen aufmerksam durch, um etwaige Fehler zu vermeiden.

3. Installation unter Linux

3.1. Das Installationsprogramm

Jedes NCP-Linux-Produkt wird als binäres Installationsprogramm ausgeliefert, das auf die Dateiendung `.bin` endet.

Kopieren Sie das Installationsprogramm auf die Zielmaschine, um die Installation auszuführen.

Falls das `executable bit` für die Installationsdatei nicht gesetzt ist, müssen Sie dies vorher tun. Die folgende Auflistung zeigt, wie man das Installationsprogramm auf ein `executable bit` überprüft, und wie man es hinzufügt.

Hinweis

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

Hinzufügen des executable bit zum Installationsprogramm

```
$ ls -l fnd_linux_x86-64_200_rev16909.bin
-rw-rw-r-- ① 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 ② 1 user user 27887112 30. Apr 13:50 fnd_linux_x86-64_200_rev16909.bin
```

① Falls hier `x` steht, ist das `executable bit` bereits gesetzt (ist in diesem Beispiel nicht der Fall).

② Hier ist das Bit gesetzt, nachdem es mittels `chmod` hinzugefügt wurde.

Führen Sie das `executable bit` aus, sobald Sie sichergestellt haben, dass es für das Installationsprogramm gesetzt ist.

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. Darin werden die Parameter erklärt, die an das Installationsprogramm übergeben werden können. Diese Parameter beeinflussen die Details der Installation. Sie können das Installationsprogramm ohne zusätzliche Parameter ausführen.

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

Informationen zur 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-Betriebsystem: 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 sowie über das Linux-System, das es erkannt hat. Danach beendet sich das Programm von selbst.

Startet die Installation, benötigen Sie ausreichende Berechtigungen (*root*-Rechte), um diese durchzuführen.

Um *root*-Rechte zu erhalten, wird das Installationsprogramm das Programm `su` oder `sudo` aufrufen, welches Sie nach dem *root*- oder Benutzerpasswort fragt, abhängig von der Systemkonfiguration. Nach Eingabe wird sich das Installationsprogramm selbst erneut mit *root*-Rechten aufrufen.

Um mit den Programmen `su` und `sudo` arbeiten zu können, müssen diese konfiguriert sein. Jede Linux-Distribution benutzt eine andere Voreinstellung. Für die typischen Linux-Distributionen und in den meisten Fällen wählt der NCP-Installer das korrekte Programm. Manchmal ist es nötig, das Werkzeug explizit zu wählen, welches für diesen Zweck verwendet werden soll. Tun Sie dies, indem Sie den Schalter `--su` oder `--sudo` als Parameter an das Installationsprogramm übergeben.

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

```
                    ------------------------------------
                    > 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 ===
[...]
```

① Hier wird das Werkzeug angezeigt, das zur Erlangung von *root*-Rechten verwendet wird.

3.2. Installation

Lesen Sie vor Beginn der Installation das Kapitel Das Installationsprogramm 3.

Um die Installation auszuführen, rufen Sie 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 Kompatibilitätsüberprüfungen durchgeführt. Diese stellen sicher, dass das Linux-System kompatibel mit der enthaltenen Software ist. Sind beide kompatibel, gibt der Installer Informationen über die Software aus, die installiert werden soll. Nach Bestätigung fährt die Installation fort.

Hinweis

Standardmäßig wird die Software im Verzeichnis `/opt/ncp/<prod>` installiert. Während der Installation können Sie ein anderes Verzeichnis angegeben. Um Datenverlust zu verhindern, muss das Zielverzeichnis jedoch leer sein. Beachten Sie, dass eine Änderung des Verzeichnisses nach der Installation mit größerem Aufwand verbunden ist.

Folgen Sie den Anweisungen des Installationsassistenten und lesen Sie die Lizenzbedingungen.

Unter Fehlerbehandlung 11 finden Sie Informationen, falls bei der Installation Fehlermeldungen erscheinen.

3.3. Versionsupdate

Um eine Update eines NCP-Produkts durchzuführen, starten Sie die Installation der neuen Version.

Rufen Sie 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.

Beim Installationsschritt *Prüfe Kompatibilität* prüft der Installationsassistent, ob die bereits installierte Version aktualisiert werden kann.

Hinweis

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.

Anschließend werden vom Installationsassistenten Informationen zur installierenden Version angezeigt. Folgen Sie den Anweisungen des Installationsassistenten. Beachten Sie, dass sich bei der Installation einer neuen Version Verzeichnisse und Speicherorte ändern sowie bereits vorhandene Dateien überspeichert werden können.

Achtung!

Eine Zurückstufung einer NCP-Installation auf eine vorherige Version oder Revision wird möglicherweise nicht vollständig unterstützt. In solchen Fällen gibt der Installationsassistent eine Warnung aus. Wenden Sie sich bei Fragen an den NCP-Support.

Beachten Sie gegebenenfalls auch Versionsupdate mit inkompatibler Dateistruktur 7.

3.3.1. Versionsupdate mit inkompatibler Dateistruktur

Vorherige Versionen von NCP-Produkten verwendeten eine andere Installationsroutine und unterschiedliche Dateistruktur. Während in aktuellen Versionen die meisten Daten in einem Installationsverzeichnis gespeichert werden, waren die Daten in vorherigen Versionen über mehrere Pfade verteilt. Diese vormaligen Versionen von NCP-Produkten können auf die neue Dateistruktur aktualisiert werden. Die Aktualisierung der vorherigen auf die aktuelle Struktur kann nur von folgenden Versionen aus ausgeführt werden:

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

Sollte die Version Ihres NCP-Produkts älter sein als hier gezeigt, ist es notwendig, dass Sie erst auf eine der hier gelisteten Versionen aktualisieren und dann die Aktualisierung auf die Installation der neuen Version vornehmen.

Die aktuelle Installationsroutine wird diese Bedingungen überprüfen und nur Aktualisierungen von den oben genannten Versionen erlauben. Falls die Aktualisierung möglich ist, zeigt der Installationsassistent Versionsinformationen der neuen Version an.

Bei der Installation haben Sie die einmalige Möglichkeit, das Installationsverzeichnis der Software zu bestimmen. In vorherigen Installationen von NCP-Produkten (außer NCP Secure Enterprise Management Server) war das Installationsverzeichnis auf den Pfad */usr/local/ncp/<prod>* festgelegt. Falls Sie sich entscheiden, das Installationsverzeichnis zu wechseln, ist es unter Umständen notwendig, dass Sie die Konfigurationsdateien des NCP-Produkts entsprechend der Installationspfade anpassen.

Auswahl eines neuen Installationsverzeichnisses während der Aktualisierung vorheriger Installationen

Im vorherigen Installationskonzept wurden Dateien in das übergeordnete Installationsverzeichnis gelegt. In der aktuellen Installation sind die Dateien in Unterverzeichnisse des Installationsverzeichnisses strukturiert wie `bin`, `sbin` und `etc`. Der Installer entscheidet während der Aktualisierung, welche existierenden Dateien in welche Unterverzeichnisse gehören. Alle Dateien, die der Installer kennt, werden automatisch an die richtige Stelle verschoben.

Wenn der Benutzer benutzerdefinierte Dateien zur Installation hinzugefügt hat, erkennt der Installer diese Dateien nicht. In diesem Fall legt die Installationsroutine diese an einem sicheren Ort unterhalb des Unterverzeichnisses `old` ab. Der Installer gibt zudem eine Warnmeldung während der Aktualisierung aus. Die entsprechenden Dateien müssen Sie selbstständig im gewünschten Verzeichnis ablegen.

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

Wenn Sie den NCP Secure Enterprise Server und NCP Secure Enterprise HA Server bereits installiert haben und beide aktualisieren wollen, müssen Sie folgendes Vorgehen beachten. NCP Secure Enterprise HA Server kann nur installiert werden, wenn NCP Secure Enterprise Server bereits installiert ist. Zur Aktualisierung auf die neue Installationsroutine ist es notwendig, erst NCP Secure Enterprise HA Server auf die aktuelle Version zu aktualisieren. Erst danach aktualisieren Sie NCP Secure Enterprise Server. Es ist nicht möglich, nur NCP Secure Enterprise HA Server auf die aktuelle Version zu aktualisieren. Die Installationsroutine wird Sie informieren, falls die vorgesehene Aktualisierungs-Reihenfolge nicht eingehalten wird und eine Aktualisierung in diesem Fall ablehnen.

3.4. Produktspezifische Intallationen

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

3.4.1. NCP Secure Enterprise Manager

Im Falle des NCP Secure Enterprise Management Server wird Sie der Installer während der Installation nicht fragen, ob Sie die Software direkt starten möchten. Hierfür muss eine Datenbankverbindung 28 konfiguriert sein, bevor erfolgreich gestartet werden kann.

3.4.2. NCP Secure Client

Für den NCP Secure Client wird während der Installation ein Gruppenkonto standardmäßig mit dem Namen `ncp-` 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 nachlesen. Das Programm `clnt-monitor` wird verwendet, um die grafische 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 zur Rechteverwaltung. Diese ermöglicht einigen Diensten als gewöhnlichen Benutzer ohne *root*-Rechte zu agieren. Das reduziert die Auswirkungen möglicher Sicherheitslücken.

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. Nur der Standardbenutzer und die -gruppe *ncp* werden automatisch durch den Installer angelegt. Um ein Benutzer- oder Gruppenkonto anzulegen, benutzen Sie die üblichen Linux-Administrationswerkzeuge. 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 zugreifen wie zum Beispiel auf die Datei `/etc/ncp.db`.

3.6. Deinstallation

Achtung!

Nach der Deinstallation bleibt keine Sicherungskopie zurück. Sichern Sie Ihre Daten daher rechtzeitig.

Für jedes NCP-Produkt existiert ein separates Programm `<prod>-uninstall` zur Deinstallation. Das Deinstallations-Programm wird Sie über das Produkt, das Sie deinstallieren wollen, sowie die betroffenen Pfade informieren. Bestätigen Sie abschließend, ob Sie wirklich mit dem Deinstallationsvorgang fortfahren möchten.

Das Deinstallations-Programm wird alle produktspezifischen Dateien entfernen. Verschiedene Systemeinstellungen, die für die Software angepasst wurden, wie zum Beispiel das Linux-*Init*-System, Gruppenkonten usw. werden ebenfalls zurückgesetzt. Die einzige Datei, die nicht entfernt wird, ist `/etc/ncp.db`. Diese wird mit anderen möglichen Installationen von NCP-Produkten geteilt und enthält NCP-Lizenzdaten, die Sie möglicherweise 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.

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-Betriebsystem: 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
```

3.7. Liste der Dateipfade

Abgesehen vom Haupt-Installationsverzeichnis benutzt NCP-Software einige andere Pfade im Linux-Dateisystem, um Daten abzulegen:

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 sowie Lizenz- und Versionsdaten für jedes installierte Produkt.
`/etc/ncp.info`	Eine Konfigurationsdatei, in der alle Installationen von NCP-Produkten, deren Installationsverzeichnisse und Versionen verzeichnet werden.

`/var/log/ncp/<prod>`	Logdateien, die NCP-Programme erzeugen, werden je Produkt in einem gesonderten Verzeichnis an diesem Ort abgelegt.
`/var/adm/ncp/<prod>/crashes`	Informationen über Programmabstürze

3.8. Automatische Installation

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

Um den *automatischen Installationsmodus* einzuschalten, fügen Sie den grundlegenden Parameter `--batch` der Installationsroutine hinzu. In diesem Modus werden jegliche interaktive Fragen als positiv beantwortet angenommen. Für etwaige Konfigurationswerte, die der Benutzer eingeben muss, werden Standardwerte ausgewählt. Übergeben Sie den Parameter `--dir` und den gewünschten Installationspfad, um das Installationsverzeichnis zu wählen.

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

Beim Versuch, ein NCP-Produkt zu installieren oder zu aktualisieren, können Probleme entstehen. Es gibt eine Reihe von Dingen, die Sie ausprobieren können, bevor Sie den NCP-Support kontaktieren. Das Installationsprogramm bietet einige Schalter, die helfen, Installationsfehler zu untersuchen oder zu beheben.

Überprüfen Sie zunächst die Integrität der im Installationsarchiv enthaltenen Daten. Das machen Sie, indem die Option *--verify* übergeben. Dies veranlasst den Installer dazu, sich selbst zu verifizieren; keine Installationsschritte werden ausgeführt. Falls die Verifikation fehlschlägt, dann ist das Installationsprogramm fehlerhaft. In diesem Fall beziehen Sie eine korrekte Version des Installationsprogramms und versuchen Sie es erneut.

Einige kleinere Probleme vermeiden Sie, indem Sie den Schalter `--compatibility` an den Installer übergeben. Dies ändert das Verhalten des Installers an einigen Stellen, um mit unerwarteten Linux-Umgebungen kompatibler zu sein.

Falls die Integration des NCP-Produkts in das Linux-*Init*-System fehlschlägt, wird dies durch den Schalter `--relaxed` ignoriert und die Installation fortgesetzt. Dies gilt nur für Installationsschritte, die nicht elementar für die Grundfunktion der Software sind. Bestehende Probleme beheben Sie daraufhin manuell.

Der Schalter `--verbose` veranlasst den Installer dazu, mehr Hintergrund-Informationen auszugeben. Wenn Sie den *verbose*-Modus einschalten, wird jede Datei, die der Installer installiert, sowie ihr Zieltort angezeigt. Diese Informationen geben einen Hinweis darauf, warum die Installation nicht funktioniert. Die umfangreiche Ausgabe ist zudem für den NCP-Support wertvoll, um Ihr Problem zu untersuchen und zu beheben.

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 zu gewährleisten. Solche Hintergrundprozesse werden in Linux *Daemon* genannt.

Das Programm `<prod>-sentinel` ist dafür zuständig alle *Daemons*, die zu einem NCP-Produkt gehören, zu starten. Verwenden Sie das Programm, um die Software manuell zu starten. Somit können Sie etwa überprüfen, ob alles korrekt funktioniert, bevor die Software automatisch während des Systemstarts hochgefahren wird.

Als ersten Test rufen Sie das Programm *sentinel* mit dem Schalter `-f` auf, sodass dieses im Vordergrund bleibt und Informationen auf die Konsole ausgibt. Das *sentinel*-Programm beginnt damit, das komplette NCP-Produkt hochzufahren. Sollte ein Fehler auftreten, wird das *sentinel*-Programm das NCP-Produkt wieder herunterfahren und einen Fehler ausgeben. Andernfalls läuft das Programm weiter, bis eine Aufforderung zum Herunterfahren auftritt.

Ein Beispielaufruf 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
```

① Beim Drücken von *Strg + C* wird das *sentinel*-Programm das Produkt wieder herunterfahren und zurückkehren, nachdem einige Aufräumarbeiten durchgeführt wurden.

Hinweis

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.

Weitere Informationen über das *sentinel*-Programm finden Sie hier 16.

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

In Linux ist ein *Init*-System dafür zuständig, Dienste während des Startvorgangs in Betrieb zu nehmen, so auch NCP-Software. Derzeit gibt es eine Reihe unterschiedlicher *Init*-Systeme, die in den verbreiteten Linux-Distributionen zum Einsatz kommen.

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

Name	Beschreibung	Verwendet in
SystemV	Dies ist das klassische UNIX-artige *Init*-System, das Shell-Skripten und Abhängigkeiten zwischen ihnen verwendet.	Debian bis zu Version 7, openSUSEvor Version 12.3, SLES vor Version 12, Rückwärtskompatibiltät in CentOS 6 and RHEL 6
Upstart	Ein fortgeschrittenes, ereignis-orientiertes *Init*-System, das für Ubuntu-Linux entwickelt wurde.	Ubuntu-Versionen bis zu Version 14, grundlegende Unterstützung in CentOS 6 und RHEL 6
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. Sie können NCP-Programme so einrichten, dass diese während des Systemstarts hochgefahren werden. Während der Installation von NCP-Software wird diese Integration standardmäßig durchgeführt, wenn nicht anders angewählt. Um die Autostart-Einstellung später zu ändern, benutzen Sie das Programm <prod>-initconfig 21.

Da unterschiedliche *Init*-Systeme in Linux verwendet werden, unterscheiden sich die Kommandos, um ein NCP-Produkt zu starten oder zu stoppen. Wenn Sie sich nicht sicher sind, 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
```

① Dies ermittelt das Kommando, um NCP Friendly Net Detection Server über das Debian-*Init*-System zu starten.

② Unter Verwendung des Startkommandos fahren Sie NCP Friendly Net Detection Server hoch

③ Gibt den aktuellen Betriebszustand von NCP Friendly Net Detection Server aus. **Achtung: Das entsprechende Kommando ist unterschiedlich je nach *Init*-System.**

Möchten Sie nachträglich das Autostart-Verhalten der NCP-Software ändern, verwenden Sie `<prod>-initconfig -a 1` zum Einschalten, bzw. `<prod>-initconfig -a 0` zum Ausschalten. Wenn Autostart aktiviert ist, wird die NCP-Software während des Systemstarts Ihres Linux-Systems hochgefahren.

Hinweis

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

Wenn Sie NCP Secure Enterprise HA Server installiert haben, der von NCP Secure Enterprise Server abhängt, dann werden 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 manchen Fällen müssen Sie sicherstellen, dass beide Softwares zum Autostart hinzugefügt sind, um eine 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 die Orte der jeweiligen 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>` (unterscheidet sich zwischen Linux-Distributionen)
OpenRC	`/etc/conf.d/ncp-<prod>`

Im Falle des NCP Friendly Net Detection Server kann ein solche Konfigurationsdatei folgendermaßen aussehen:

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. Die Variablen `SENTINEL_OPTS` und `CONTROL_OPTS` erlauben, 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 21 finden.

5. Kommandozeilenwerkzeuge

Hier finden Sie Dokumentation über Kommandozeilenwerkzeuge, die zusammen mit NCP-Produkten unter Linux installiert werden:

Tabelle 5: Überblick über Kommandozeilenwerkzeuge

Programm	**Beschreibung**
`<prod>-config`	Ein Konfigurations-Werkzeug, das nur für manche NCP-Produkte installiert wird. Es ermöglicht, interaktive und nicht-interaktive Konfiguration diverser Software-

	Einstellungen vorzunehmen. Siehe produktspezifische Konfiguration 25 für weitere Informationen.
`<prod>-control`	Ermöglicht es, 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`	Entwicklungswerkzeug zum Abrufen von Analyse-Informationen von NCP-Software zur Laufzeit.
`<prod>-license`	Anzeige und Verwaltung aktiver Softwarelizenzen
`<prod>-sentinel`	Verwaltungsprozess für alle *Daemon*-Prozesse eines NCP- Produktes.
`<prod>-uninstall`	Deinstallations-Programm

5.1. Die Programme sentinel und control

`sentinel` ist das Hauptprogramm, das dafür zuständig ist, alle Hintergrundprozesse (*Daemons*) die zu einer NCP-Software-Lösung gehören, zu starten und zu beenden. NCP-Produkte wie NCP Friendly Net Detection Server bestehen lediglich aus einem einzelnen *Daemon*-Prozess. Der Großteil jedoch besteht aus einer Gruppe von mehreren *Daemon*-Prozessen. Diese gewähren die volle Funktionalität der Software. 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. Indem Sie `<prod>-control -s` aufrufen, wie im Beispiel für NCP Friendly Net Detection Server gezeigt, erhalten Sie Informationen über den aktuellen Betriebszustand des NCP-Produkts. Die Ausgabe zeigt Informationen über jeden derzeit laufenden *Daemon*-Prozess, etwa seit wann er läuft, welche Parameter 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 von *sentinel* ausgeführt werden, zu stoppen oder neuzustarten. Dazu übergeben Sie die Schalter `--shutdown` bzw. `--restart`.

Hinweis

Wenn Sie ein NCP-Produkt über das Linux-*Init*-System oder das `<prod>-initconfig`-Werkzeug gestartet haben, fahren sie dieses nicht auf demselben Weg herunter. Das kann zu Komplikationen führen, da das *Init*-System das NCP-Programm nicht dazu aufgefordert hat und deshalb annimmt, dass er abgestürzt sei.

5.1.1. Konfiguration der gestarteten Dienste

Über die Konfigurationsdatei `sentinel.conf` können die vom s*entinel* 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 Einsatz. Sie dient zum Einschalten des standardmäßig deaktivierten Webservers für das Ausrollen der TOTP-Zugangsdaten.

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. Informationen dazu werden im nächsten Abschnitt beschrieben.

5.1.2. Operationen auf individuellen Daemon-Prozessen

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

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. Im Fall von NCP Friendly Net Detection Server ist das, wie oben gezeigt, *ncpfndd.* Das 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*: `--restart-daemon <Basisname>`
- Ausschalten des angegebenen *Daemons*: `--disable <Basisname>`
- Einschalten eines zuvor ausgeschaltenen *Daemons*: `--enable <Basisname>`
- Überprüfung, ob der angegebene *Daemon* gerade läuft: `--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 das Programm vorzeitig und ohne Ergebnis zurückkehren zu lassen. Möchten Sie eine Obergrenze für die Zeit zu festlegen, die darauf gewartet wird, dass ein *Daemon* zurückkehrt (in der Regel 60 Sekunden), verwenden Sie den Parameter `--timeout <Sekunden>`. Sollte die angegebene Zeit überschritten werden, wird der betroffene *Daemon*-Prozess zwangsweise beendet. Möchten Sie das Programm *sentinel* so konfigurieren, dass bestimmte *Daemon*-Prozesse vom Starten ausgenommen sind, übergeben Sie `-x <Basisname>` oder `-o <Basisname>` an den *sentinel* . `-x` schließt den angegebenen *Daemon* vom Start aus während `-o` ausschließlich den angegebenen *Daemon* startet.

Hinweis

Die Operationen auf einzelnen *Daemon*-Prozessen sind nur für die fortgeschrittene Verwendung oder zur Fehlersuche notwendig.

Manche *Daemon*-Prozesse werden in mehreren verschiedenen Konfigurationen gleichzeitig gestartet wie etwa bei *ncprsud* in NCP Secure Enterprise Management Server. In diesem Fall reicht die Angabe des `<Basisnamen>` nicht aus, um eine bestimmte Instanz eines *Daemon* zu identifizieren. Es wird dem *Daemon* eine Persönlichkeit hinzugefügt. Durch `<prod>-sentinel -l` Können Sie die Liste von Persönlichkeiten einsehen. Die Identifikation auf der Kommandozeile erfolgt dann über `<Basisname>:<Persönlichkeit>`. Geben Sie zum Beispiel `ncprsud:radius` an, um die radius-Persönlichkeit des *Daemon ncprsud* von NCP Secure Enterprise Management Server auszuwählen.

5.1.3. Einfluss darauf nehmen, wie sentinel mit Abstürzen umgeht

Wenn sich einer der Dienste, die vom Programm *sentinel* gestartet wurden, unerwartet beendet (etwa, weil er abgestürzt ist), wird der *sentinel* standardmäßig alle verbleibenden *Daemon*-Prozesse herunterfahren und sich beenden. Dies verhindert einen unvollständigen Satz an Diensten und gewährleistet einen sauberen Betriebszustand.

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

Für den Fall, dass ein Daemon ständig Fehler verursacht (zum Beispiel, weil eine Konfigurationsdatei fehlerhaft ist), können zusätzlich die Schalter `--max-crashes-per-time` und `--crash-timebase` verwendet werden. Diese Schalter erlauben Ihnen, 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 Einfluss darauf nehmen wollen, was in Fehlerfällen geschieht, konfigurieren Sie ein benutzerdefiniertes Skript, das entscheidet, wie mit der jeweiligen Situation umgegangen werden soll. Hierfür übergeben Sie den Parameter `--script <Programmpfad>`, wobei `<Programmpfad>` der Pfad zum ausführbaren Skript ist, das gerufen werden soll, wenn ein *Daemon* sich fehlverhält. Dem Skript geben Sie eine Reihe von Umgebungsvariablen mit, welche die gegebene Situation beschreiben.

Tabelle 6: Umgebungsvariablen für Absturz-Skripte

Variable	Beschreibung	Beispielwert
`ncp_service`	Der NCP-*Daemon* der abgestürzt ist	`ncpfndd`
`ncp_crash_code`	Der Rückgabewert des abgestürzten *Daemons*	`1`
`ncp_crash_signal_nr`	Falls der *Daemon* sich beendet hat, weil er ein Signal empfangen hat, wird dessen Nummer in dieser Variable zur Verfügung gestellt.	`9`
`ncp_crash_signal_name`	Selbe Funktion wie `ncp_crash_signal_nr`, enthält jedoch eine lesbare Bezeichnung für das Signal.	`SIGKILL`
`ncp_exit_restart`	Der Rückgabewert, den das Skript zurückgeben sollte, um den abgestürzten *Daemon* neu starten zu lassen.	`n.A.`
`ncp_exit_restart_product`	Der Rückgabewert, den das Skript zurückgeben sollte, um das komplette Produkt geordnet neu zu starten.	`n.A.`

`ncp_exit_shutdown`	Der Rückgabewert, den das Skript zurückgeben sollte, um den *sentinel* zu veranlassen, alle verbleibenden Prozesse zu beenden und zurückzukehren.	`n.A.`
`ncp_exit_disable`	Der Rückgabewert, den das Skript zurückgeben sollte, um den *sentinel* 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 *sentinel* zu veranlassen, den Absturz gemäß der internen Logik zur Behandlung von Abstürzen gemäß den Schaltern `--max-rashes, --max-crashes-per-time` und `--crash-timebase` zu behandeln.	`n.A.`

Auf diesem Weg ist es möglich, eine E-Mail verschicken, um über den aufgetretenen Fehler zu informieren oder das Linux-System neuzustarten. Beachten Sie jedoch, dass das Programm *sentinel* keine weiteren Operationen ausführen kann, bis das Absturzbehandlungs-Skript zurückgekehrt ist. Es folgt ein Beispiel eines *bash*-Skripts, das 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*, 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. Sollten solche Daten zurückbleiben, könnte das Starten des NCP-Produkts das nächste Mal fehlschlagen, da unerwartete globale Daten gefunden wurden. 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 Parameteren an Daemons

Sie können *sentinel* zusätzliche Parameter an die einzelnen *Daemon*-Prozesse übergeben lassen. Dies kann zu Zwecken der Fehlersuche nützlich sein. Die meisten NCP-*Daemon*-Prozesse unterstützen die Option `--verbose`, wodurch diese detailliertere Ausgaben auf die Kommandozeile machen lassen. Um solche zusätzlichen Parameter zu übergeben, setzen Sie Umgebungsvariablen nach dem Muster `ncp_args_<Basisname>`, wobei `<Basisname>` der Basisname des *Daemons* ist, welcher zusätzliche Parameter erhalten sollte. Nachstehend 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 finden Sie bereits einen Eintrag, um zusätzliche Parameter an *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 der entsprechenden Stelle hinzufügen, wenn die NCP-Software über das *Init*-System gestartet wird.

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* auf die Konsole schreiben würde, landen in dieser Logdatei. Die Logausgaben werden zu dieser Datei nur hinzugefügt, sodass 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. Die Ausgabe aller *Daemon*-Prozesse wird stattdessen 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 Funktion, die dieses Werkzeug zur Verfügung stellt.

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 des *Init*-Systems. Diese umfasst:

- ob das Produkt 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 ebenfalls hilfreich, um den Ort der *Init*-Konfigurations-Datei festzustellen.

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
```

Möchten Sie 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-command` und `<prod>-initconfig --show-stop-command` angezeigt werden, können Sie auch `<prod>-initconfig` aufrufen. Um die NCP-Software über das *Init*-System zu starten, geben Sie den Parameter `--start` und um es zu stoppen den Parameter `--stop` ein.

Wie Sie die Auto-Einstellungen ändern, erfahren Sie hier.

Möchten Sie die Integration der NCP-Software in das *Init*-System komplett entfernen, verwenden Sie den Schalter `--remove`. Um selbiges wieder zu integrieren, verwenden Sie den Schalter `--integrate`. Diese Befehle kommen jedoch nur in Ausnahmefällen zum Einsatz, etwa um 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

Im Falle eines Programmabsturzes ist es wichtig, für den NCP-Support alle verfügbaren Informationen 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 registriert sich zum einen im Linux-System, sodass es im Falle von Programmabstürzen aufgerufen wird und alle notwendigen Informationen einsammelt, falls es sich um den Absturz eines NCP-Prozesses gehandelt hat. Zum anderen vereinfacht es dem Endbenutzer 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` auf. Wenn mindestens 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 liegt ein Absturz für einen *Daemon*-Prozess von NCP Friendly Net Detection Server vor. Das Basisverzeichnis für Absturzinformationen ist `/var/adm/ncp/<prod>/crashes`. Für jeden Absturz wird ein separates Verzeichnis erstellt, in welchem Absturzinformationen vom Linux-Betriebsystem 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. Dazu übergeben Sie den Schalter `--report` sowie den Pfad, wohin das Archiv geschrieben werden soll:

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 an den NCP-Support senden, wenn eine Fehlersituation vorliegt.

Absturzberichte können sensible Informationen wie Benutzernamen, E-Mail-Adressen oder gar Teile von geheimem Schlüsselmaterial beinhalten. Zu Ihrer Sicherheit werden diese Absturzberichte in der aktuellen Version von NCP-Produkten verschlüsselt abgelegt, sodass nur autorisierte NCP-Mitarbeiter diese Daten einsehen können.

Möchten Sie diese Verschlüsselung abschalten, übergeben Sie den Parameter `--no-encryption`.

Das Programm `<prod>-crash` ermöglicht auch die Ausgabe von Daten über das laufende System. Diese können 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 vergangene Berichte automatisch gelöscht. Möchten Sie die Bericht manuell löschen, nutzen Sie `<product>-crash --delete-old`. 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, in welchem Sie das Produkt ausprobieren können. Danach ist es notwendig, dass Sie eine gültige Lizenz für das Produkt registrieren.

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 sowie weitere Informationen, die von der aktiven Lizenz und dem Produkt abhängen. Es 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)
  Lizensierte 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 (NCP Secure Enterprise Server und NCP Secure Enterprise HA Server) oder über die Monitoranwendung (NCP Secure Client) aktiviert.

Für NCP Secure Enterprise Management Server wird die Lizenz über das Programm `sem-license` aktiviert und aktualisiert. Sie rufen dieses mit dem Parameter `--activate` auf. Das veranlasst das Programm Sie aktiv nach den Lizenzdaten zu fragen. Alternativ können Sie die Lizenzdaten über den Parameter `--license` angeben, welcher die Lizenz in der Form `<schlüssel>:<seriennummer>` entgegennimmt, wobei `<schlüssel>` ein zwanzigstelliger Schüssel ist, der durch Minuszeichen getrennt wird, und `<seriennummer>` eine achtstellige 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.

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 vom 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. Voraussetzung ist, dass der Benutzer ein Mitglied der Installationsgruppe von NCP Secure Client ist (standardmäßig *ncp*). 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 Benutzers entfernen bzw. ausführen.

Hinweis

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

6.2. NCP Secure 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 dient zur Überwachung.

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 1 -c public localhost iso.3.6.1.4.1.1213.8
```

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 26. 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 macht eine Datenbankverbindung zwingend erforderlich, damit der Server startet. Deshalb muss die Konfiguration 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. NCP hat sich bewusst für ein semi-grafisches Werkzeug statt einer grafischen Benutzeroberfläche entschieden. Somit wird gewährleistet, dass eine SSH-Verbindung möglich ist oder das Programm direkt auf der Linux-Konsole funktioniert und somit auch auf Servern nutzbar ist, welche gar keine grafische Oberfläche eingerichtet haben.

Hinweis zur Aktualisierung von vorherigen Versionen

Das hier beschriebene semigrafische Konfigurationstool `sem-config` wurde in Version 5.30 des NCP Secure Enterprise Management Server neu eingeführt.

Für ältere Versionen konsultieren Sie bitte die Dokumentation, welche mit der jeweiligen Version ausgeliefert wurde. Die Beschreibung der Konfigurationsdatei wurde in dieser Version der Dokumentation entfernt. Natürlich ist es nach wie vor möglich, die Datei von Hand zu editieren. Der Batch-Modus des Tools zum Umschalten der Betriebsart funktioniert wie gewohnt, sodass Skripte nicht angepasst werden müssen.

Das Programm orientiert sich an der Management-Konfiguration unter Windows. Nach dem Start erscheint zunächst das Hauptmenü. Dieses Menü entspricht den Tabs der Windows-Oberfläche.

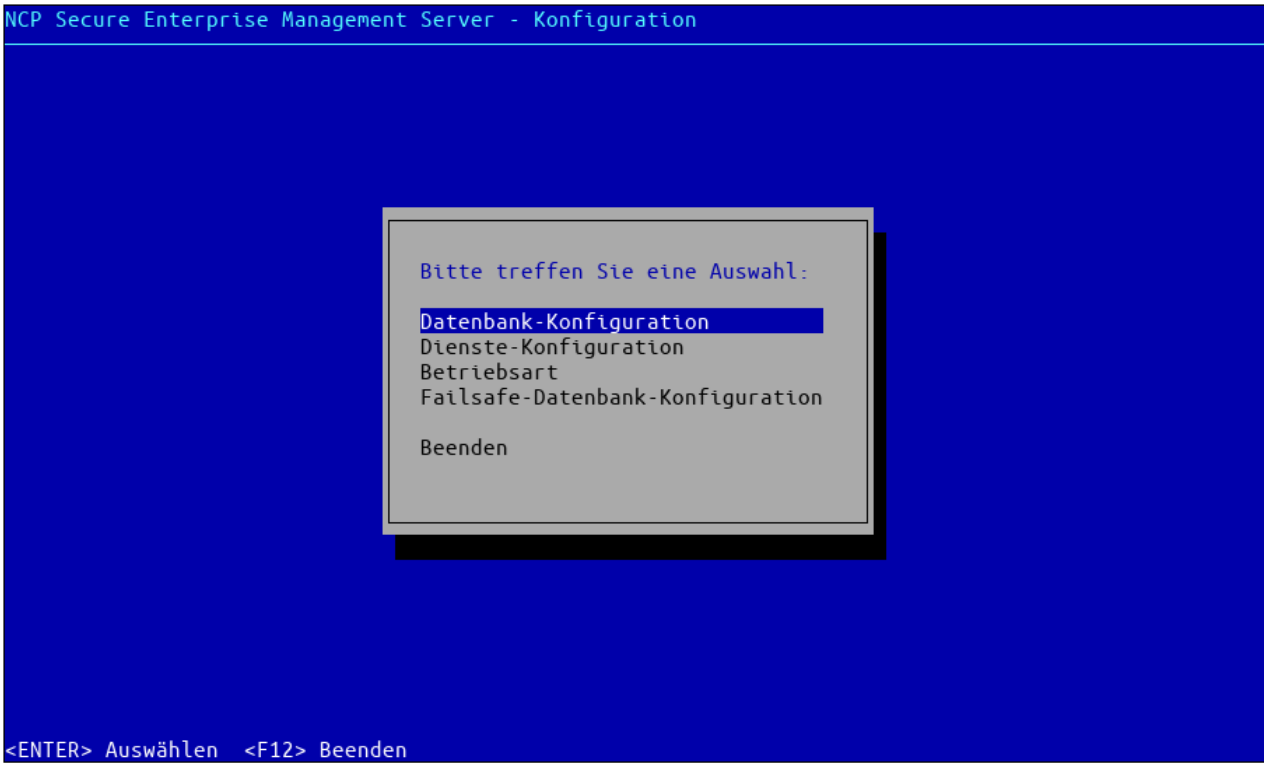

Abbildung 1: Hauptmenü

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

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. Alle Funktionen sind zusätzlich über Schaltflächen verfügbar, falls die Funktionstasten (zum Beispiel über SSH) wider Erwarten nicht funktionieren sollten.

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, die 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 zuerst eine Datenbank erstellt werden. Dies wird im nächsten Abschnitt beschrieben. Falls die Datenbank schon existiert, können Sie den Abschnitt überspringen.

Einrichten der Datenbank

Egal ob der Zugriff über den nativen Connector oder über ODBC konfiguriert wurde, muss eine Datenbank eingerichtet werden. Bitte nutzen Sie die Dokumentation Ihrer Linux-Distribution für den MySQL-Server für weitere Informationen zum Einrichten eines MySQL-Servers.

Hinweis

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

Vorausgesetzt, Ihr MySQL-Server ist korrekt eingerichtet, 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 folgt dar:

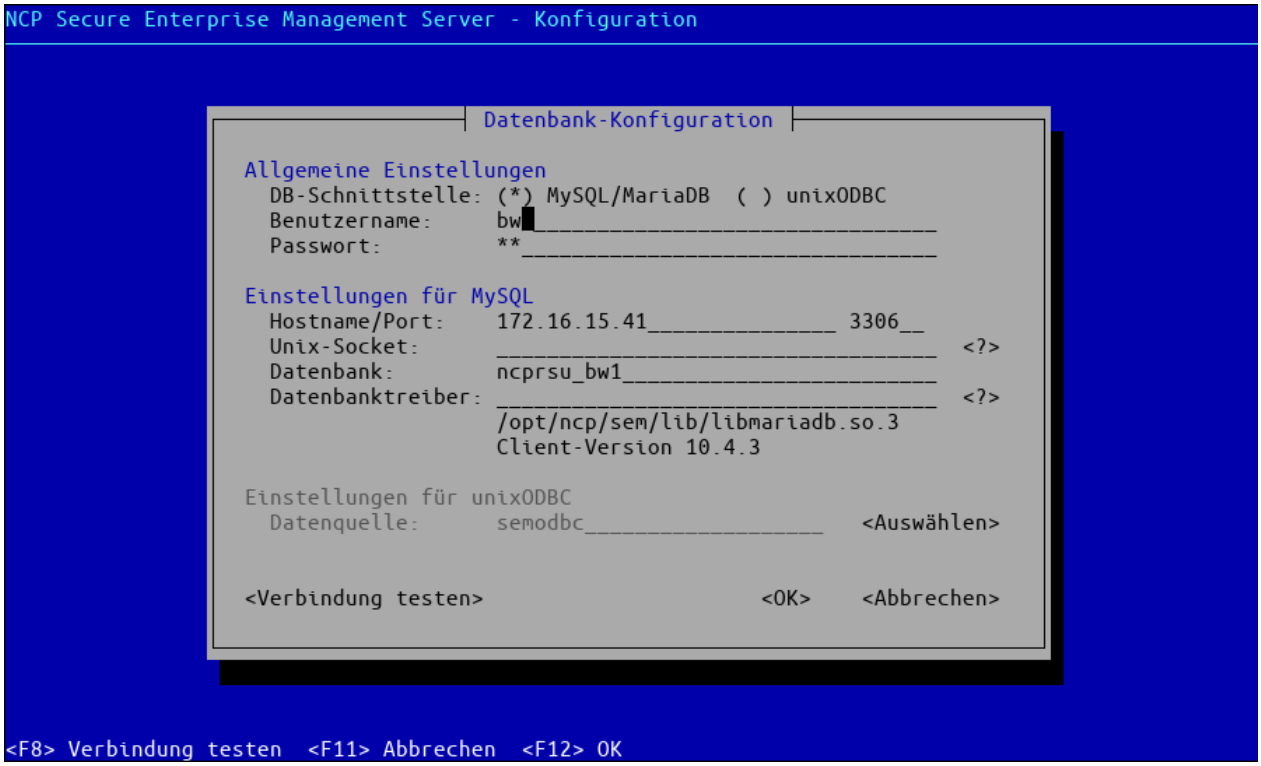

Abbildung 2: Konfiguration einer MariaDB-Datenbank

Wählen Sie die MariaDB-Schnittstelle, indem Sie das Optionsfeld *(*) MySQL/MariaDB* mit der Tab-Taste ansteuern und mit der Leertaste aktivieren.

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), welche 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 ausgelieferten Treiber verwendet. Wenn Sie einen Treiber manuell oder über die Linux-Distribution konfigurieren wollen, tragen Sie in besagtes Feld den absoluten Pfad oder den Dateinamen (dann wird in den System-Bibliotheksverzeichnissen gesucht) zum Datenbanktreiber mit ein. Wenn Sie dieses Feld verlassen wird geprüft, ob es sich um einen gültigen Datenbanktreiber handelt. 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.

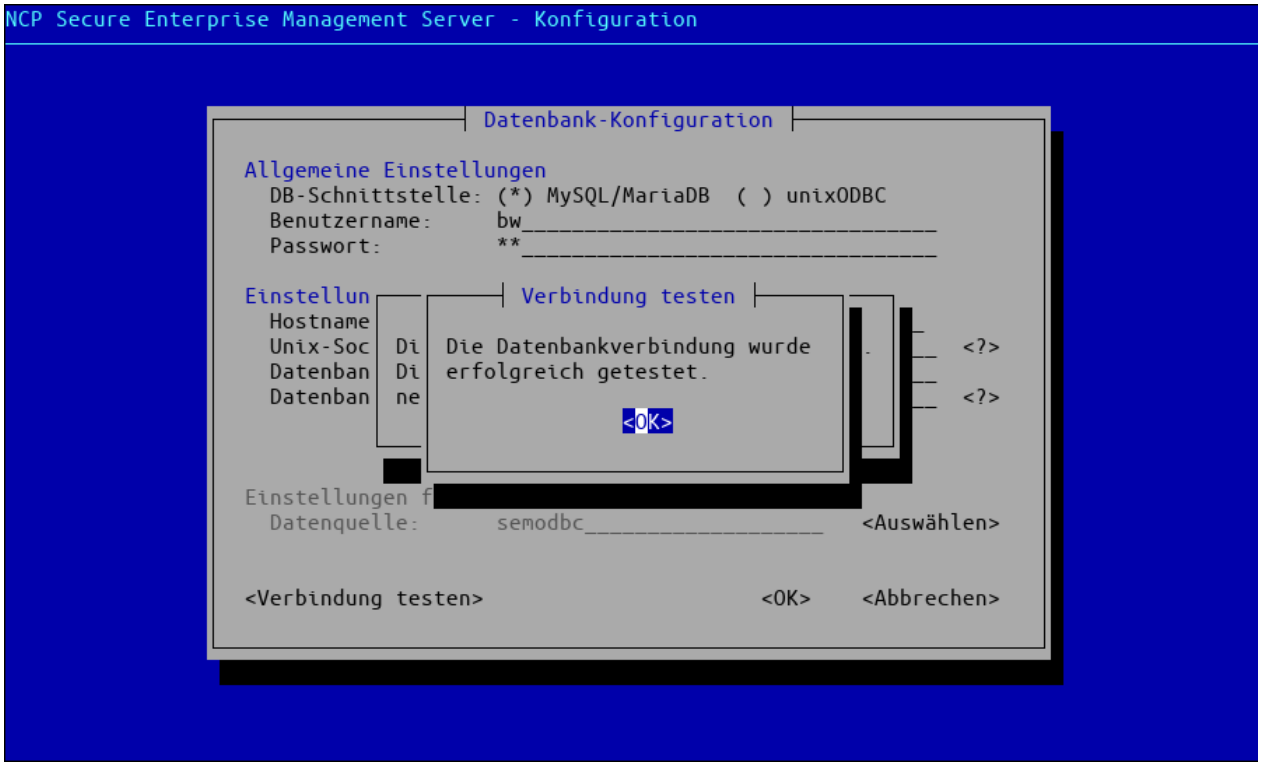

Abbildung 3: Erfolgreicher Verbindungstest

Die Konfiguration wird für den Verbindungtest 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 Software, 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 verschiedene Datenbankanbindungen 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 eingerichtet haben. Sie können 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	Paktenamen	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`

Hinweis

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

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. *unixodb* 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. Wählen Sie einen Name für die Treiberkonfiguration sowie den Pfad zur Treiberbibliothek. Im folgenden Beispiel benutzen wir den Namen `myodbc`. Der Pfad zu der Treiberbibliothek kann sich zwischen Linux-Distributionen unterscheiden:

Beispielinhalt von odbc.ini

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

① Name der Treiberkonfiguration wie angegeben in odbcinst.ini

② Standardserver und -port für den lokal laufenden MySQL-Server

③ Name der Datenbank innerhalb MySQL, die von NCP Secure Enterprise Management Server verwendet werden wird

Starten Sie nun `sem-config` und 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.

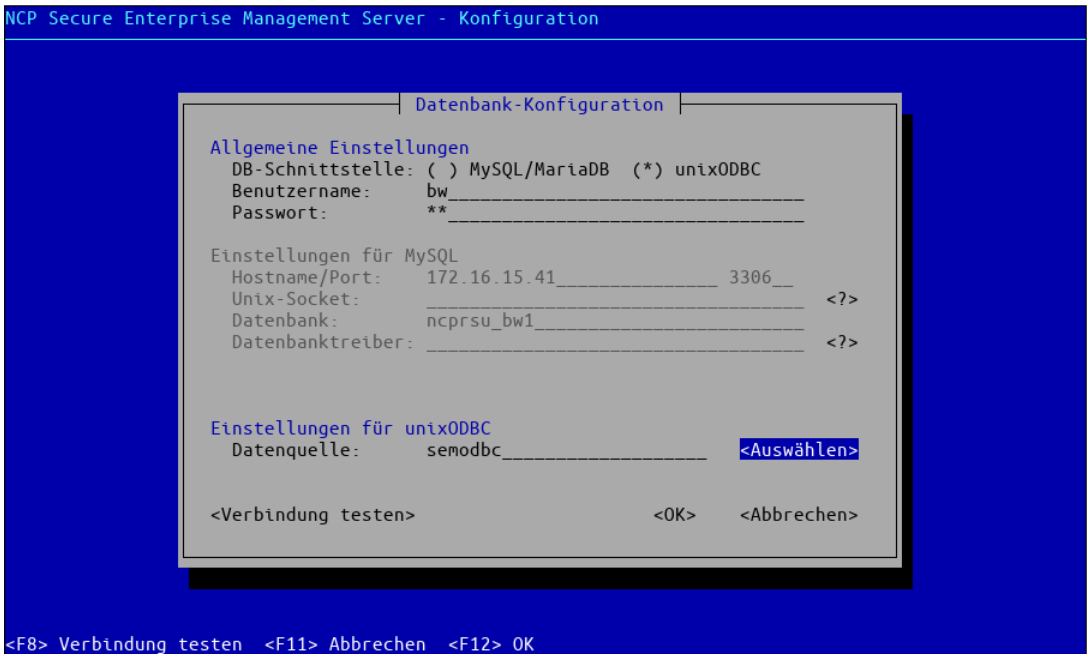

Abbildung 4: Datenbankkonfiguration einer unixODBC-Verbindung

Nun werden die meisten Felder ausgegraut, da diese 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 diese 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 manuell aktiviert oder deaktiviert wird, ist der Webserver *sem-nginx*. Dieser stellt die Webseite bereit, auf welcher die Anwender ihre TOTP- Zugangsdaten abrufen. Wird diese Funktion nicht benötigt, muss der Webserver nicht laufen. Da dies für die Mehrzahl der Installationen zutrifft, ist er im Auslieferungsumfang deaktiviert.

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

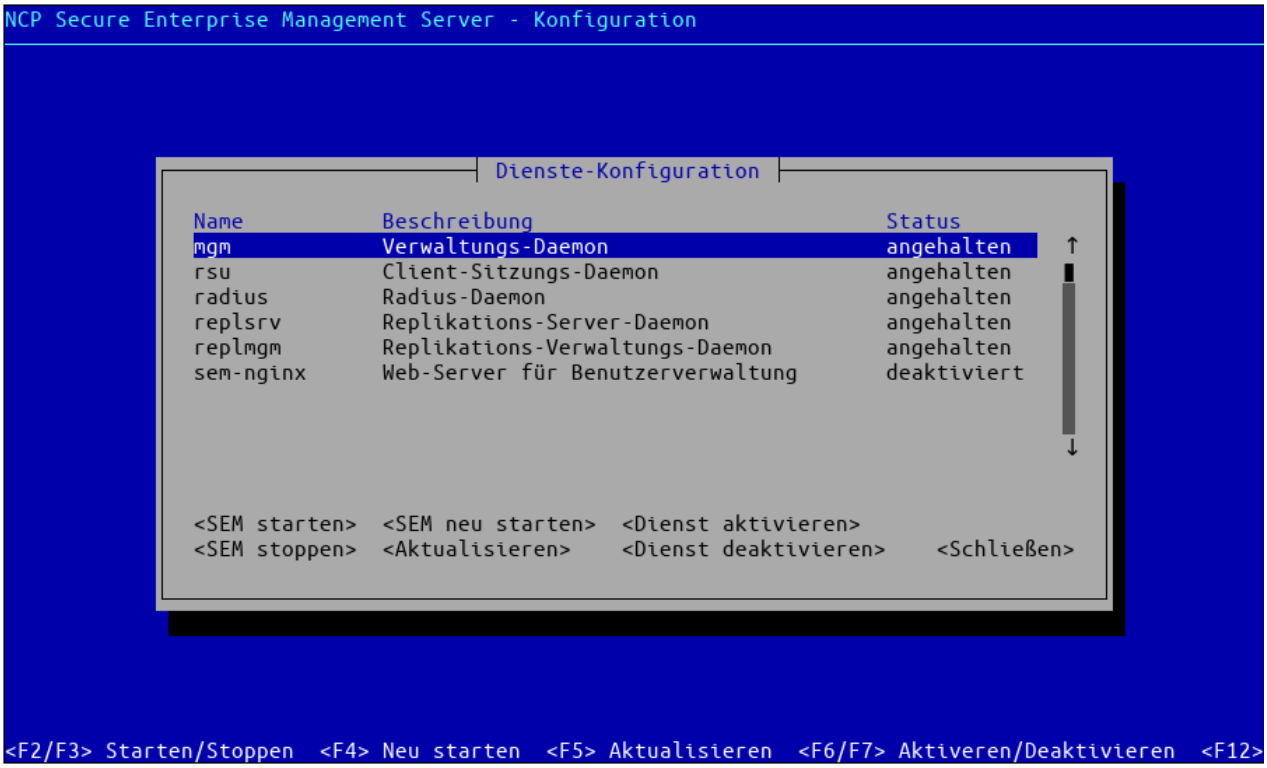

Abbildung 5: Dienste-Konfiguration

Im oberen Bereich des Dialogs wird der Zustand des Dienstes angezeigt. Neben *angehalten* und *läuft* wird hier der Zustand *deaktiviert* angezeigt. Das bedeutet, dass der Dienst nicht läuft und auch nicht aktiviert wird, wenn der Master-Daemon *sentinel* startet. 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 dieser läuft. Diese Funktion ist äquivalent zu `sem-initconfig --stop`.

- SEM neu starten (F4): Der Management-Server wird neu gestartet, falls dieser läuft. Der Master-Dienst *sentinel* wird nicht neugestartet. 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

Es gibt 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 angewendet. Wenn der Management-Server läuft, während Sie den Dialog mit *OK* verlassen, wird automatisch angeboten, den Server neu zu starten.

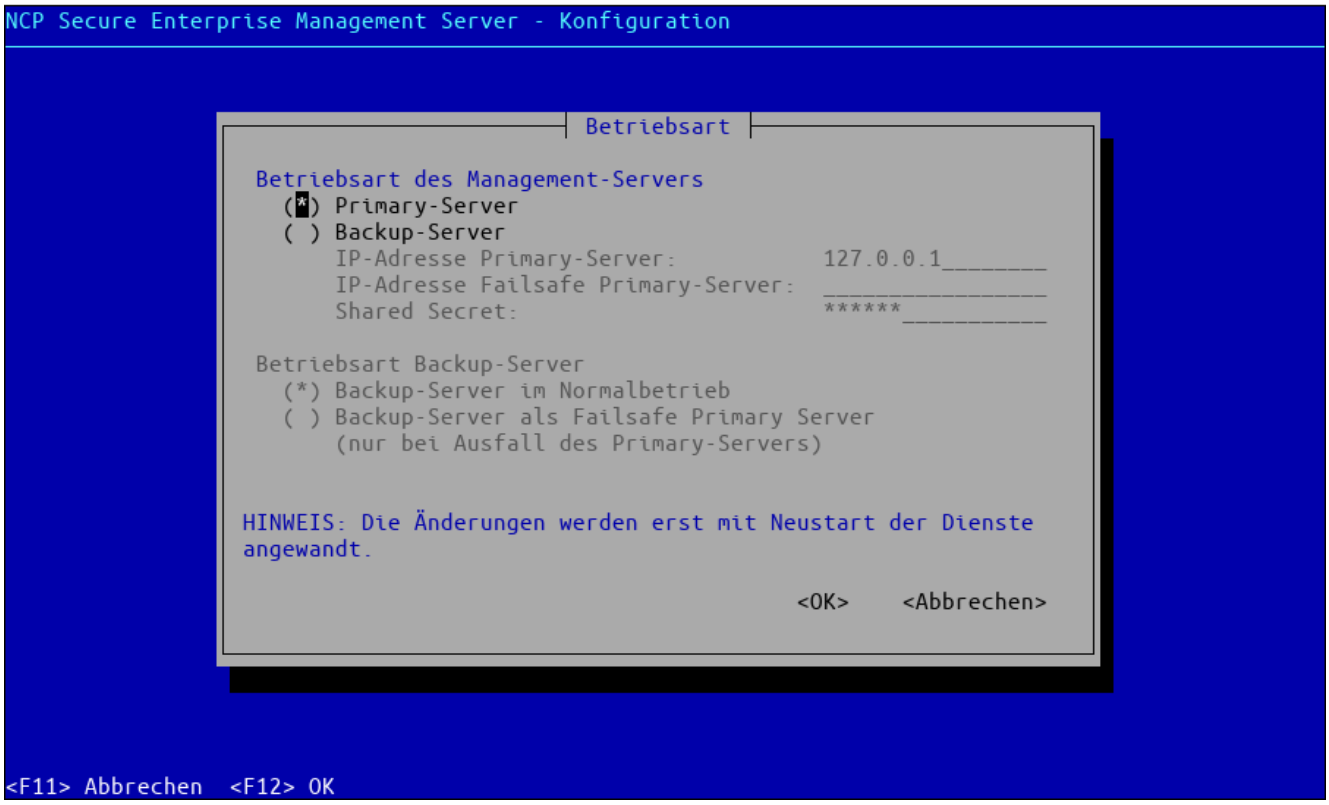

Abbildung 6: Konfiguration der Dienste – Ansicht im Primärmodus

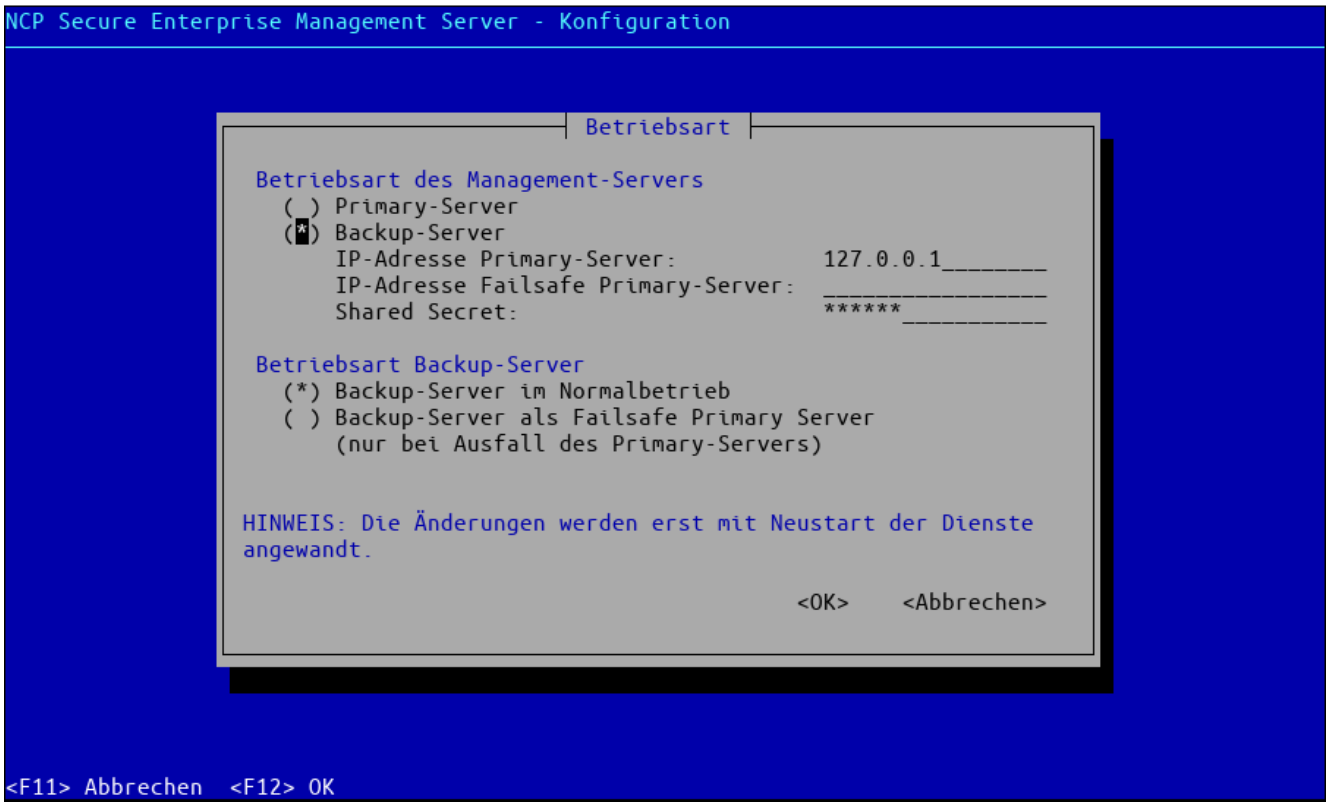

Abbildung 7: Konfiguration der Dienste – Ansicht im Backup-Modus

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.

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

Die Änderungen werden erst nach einem Neustart wirksam, welcher manuell durchgeführt werden muss. Das geschieht 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 ggf. andere Dienste zu starten.