NCP Secure Enterprise Management

Linux

Release Notes

Service Release: **5.20 r44377**
Datum: **Juni 2019**

Voraussetzungen

Das NCP Secure Enterprise Management (SEM) ist nur in der 64 Bit Variante verfügbar. Folgende Distributionen und Datenbanken mit zugehörigen Connector/C Treibern wurden mit dieser Freigabe getestet und freigegeben:

Linux Distribution	Datenbank	Treiber
Red Hat Enterprise Linux Server 7.5 64 Bit	MariaDB 5.5.56	MySQL libmysqlclient.so.18
Debian GNU/Linux 9.9 64 Bit	MariaDB 10.1.38	MariaDB libmariadbclient.so.18

MySQL 8.x wird nicht unterstützt.

Der MariaDB ODBC Treiber kann nicht im SOCKET-Modus Verbindung zur MySQL-Datenbank aufnehmen. Es wird empfohlen die Version 5.3.6 des MySQL-ODBC-Treibers zu verwenden.

Im Allgemeinen wird der Einsatz eines Connector/C-Treibers statt eines ODBC-Treibers empfohlen.

Voraussetzung für den Betrieb des NCP Secure Enterprise Management (SEM)

Um diese Management Version nutzen zu können bedarf es der folgenden Komponenten:

- NCP Management Console: Version 5.20
- Client Configuration Plug-in: Version 11.21 oder neuer (bei Bedarf)
- Server Configuration Plug-in: Version 12.00 oder neuer (bei Bedarf)
- License Plug-in: Version 11.30 oder neuer (bei Bedarf)

1. Neue Leistungsmerkmale und Erweiterungen

Neue 2-Faktor-Authentisierung gemäß Time-based One-time Password Verfahren

Integration der Time-based One-time Password Authentisierung für eine 2-Faktor-Authentisierung des VPN Clients. Zur Erzeugung des Einmalpasswortes nach dem TOTP-Verfahren ist ein Software-Token wie beispielsweise Google Authenticator notwendig.
Voraussetzung: Client Configuration Plug-in 11.21 oder neuer

Pay-per-Use Lizenzierung

Unterstützung einer Pay-per-Use Lizenzierung für NCP Secure Enterprise Clients und Secure Enterprise VPN Server.
Voraussetzung: Client Configuration Plug-in 11.21 oder neuer

Unterstützung des NCP Virtual Secure Enterprise VPN Servers

Mit dieser Version des Managements wird das neue Produkt NCP Virtual Secure Enterprise VPN Server (NCP vSES) und dessen Subscription-Lizenzierung unterstützt. Im Falle mehrerer verwalteter NCP vSES kann die Kommunikation mit dem NCP Lizenzierungsserver über den NCP SEM erfolgen. Hierzu ist in einer vorhandenen Firewall HTTPS (Port 443) zwischen dem einzelnen NCP vSES und `licensing.ncp-e.com` freizuschalten.

Konfiguration der Passwortkomplexität bei SEM-Anmeldung

Im SEM ist es jetzt möglich die Passwortkomplexität für die Anmeldung über die NCP Management Console festzulegen.

2. Verbesserungen / Fehlerbehebungen

Fehler beim Upload von SEM-Upload-Paketen mit Unterverzeichnissen

Enthält ein Upload-Paket welches auf dem SEM hochgeladen werden soll Unterverzeichnisse, so bricht der Upload des Pakets mit einer Fehlermeldung ab. Dieses Problem wurde behoben.

Maximale Laufzeit von Scripten

Die maximale Laufzeit eines Scriptes hängt von der Länge des Aufruf-Intervalls ab. Für eine Wiederholung des Scriptes bis zu einer Stunde Aufruf-Intervall beträgt die maximale Laufzeit des Scriptes eine Stunde. Bei längeren Aufruf-Intervallen darf ein Script maximal 23 Stunden und 59 Minuten Laufzeit haben.

Maximale Anzahl fehlerhafter RADIUS-Anmeldungen

Der Eintrag der maximal fehlerhaften RADIUS Anmeldungen innerhalb der RADIUS Gruppen-Einstellungen war nicht wirksam. Ein Benutzer wurde immer nach fünf falschen Eingaben gesperrt. Dieses Problem wurde behoben.

`localhost` funktioniert für eine MySQL-Konfiguration nicht

Bei der Konfiguration der Datenbankanbindung musste bisher der lokale Hostname oder die lokale IP-Adresse `127.0.0.1` konfiguriert werden. Die Auflösung von `localhost` funktionierte nicht. Dieses Problem wurde behoben.

Replikationsdienst muss nach Änderungen in der Backup-Server-Konfiguration neu gestartet werden

Bei Anlage oder Änderungen der Backup-Server-Konfiguration musste der Replikationsdienst neu gestartet werden. Dieses Problem wurde behoben. Die Konfigurationsänderungen werden sofort übernommen.

Absturz des RADIUS-Dienstes

Unter bestimmten Umständen konnte der RADIUS-Dienst abstürzen. Dieser Fehler wurde behoben.

Problem beim Anlegen von Filtern im NCP Gateway

Unter bestimmten Umständen konnten nach einem Update des Management Servers in der Konfiguration des VPN Gateways keine neuen Filter angelegt werden. Dieses Problem wurde behoben.

Falsche Darstellung von Umlauten nach Update des Management Servers

Bei der Verwendung des Connector/C wurden in der Management Konsole Umlaute falsch dargestellt. Dieses Problem wurde durch die Konfiguration der Codepage in der Datei *ncprsu.conf* innerhalb der Gruppe „DB“ oder „DB-MgmBackup“ mit „CharSet=…“ behoben.

Problem bei Datenbankanbindung im Failsafe-Mode

Die Verwendung des Konfigurationstools (ncprsucfg.exe) lieferte im Falle der nativen Datenbankanbindung via Connector/C und des Failsafe-Modes eine Fehlermeldung. Dieses Problem wurde behoben.

SQL-Fehler beim Betrieb mit einer Oracle Datenbank

Wurde der Backup Management Server mit einer Oracle-Datenbank betrieben, so kam es beim Start des Backup Management Servers zu einem SQL-Fehler. Dieser Fehler wurde behoben.

Status-Benachrichtigung kann nicht gelöscht werden

Wurde ein zentral verwalteter NCP Secure Enterprise VPN Server heruntergefahren, so wurde dies durch eine Benachrichtigung in der Management Konsole angezeigt. Wurde daraufhin der VPN Server aus dem Management entfernt, lies sich die Benachrichtigung nicht löschen. Dieser Fehler wurde behoben.

Absturz des Client Session Dienstes

Bei der Verlängerung bzw. dem Versenden einen erneuerten Hardware-Zertifikates an den Client stürzte der Client Session Dienst ab. Dieser Fehler wurde behoben.

Administrator-Passwort zurücksetzen

Der Aufruf `ncprsud -clearadminpw` zum Zurücksetzen des Administrator-Passwortes zeigte keine Wirkung, wenn gleichzeitig der Management Server gestartet war. Dieser Fehler wurde behoben.

Absturz der Management Konsole

War eine große Anzahl von Benutzer mit RADIUS-Authentisierung via VPN verbunden, so stürzte die Management Konsole beim Aufruf der zugehörigen Link Profile in Statistik ab. Dieser Fehler wurde behoben.

Anzeigefehler beim Ablaufdatum des CA-Zertifikats

Die Warnmeldung zum Ablauf eines CA-Zertifikates zeigte ein falsches Datum an. Dieser Fehler wurde behoben.

„Invalid incoming Attribute“-Fehler bei RADIUS-Anmeldung

Wurde mit einem Script eine RADIUS Gruppen Konfiguration geändert, so konnte dies einen „Invalid incoming Attribute“-Fehler bei RADIUS-Anmeldung hervorrufen. Dieses Problem wurde behoben.

Fehler bei externer RADIUS-Authentisierung

Bei der Authentisierung über einen externen RADIUS-Server wurde aufgrund vom Benutzer unterschiedlich eingegebener Groß-/Kleinschreibung beim Suffix des Benutzernamens, der Suffix nicht immer korrekt entfernt. Dieses Problem wurde behoben.

Fehlerbehebung innerhalb der Konfiguration "Failsave-Datenbank-Verbindung"

Fehlerbehebung innerhalb Administrator Anmeldung

Sofern ein neuer SEM-Administrator innerhalb des Active Directory in einer OU mit Umlauten angelegt wurde, konnte sich dieser Administrator nicht korrekt am SEM anmelden. Dieses Problem wurde behoben.

In Dialogen der SEM-Einstellungen lassen sich nun die Parameter nach den Namen der Spalten sortieren.

Änderung des Standart-Ports in der NCP SEM Script-IDE auf 12504

Viele Log-Meldungen nach fehlerhafter RADIUS-Anmeldung

Erfolgte die Anmeldung am RADIUS-Server des Backup-SEM mit einem falschen Passwort, so wurde eine große Anzahl an Log-Meldungen erzeugt. Dieser Fehler wurde behoben.

3. Bekannte Einschränkungen

Keine.

Servicerelease: **5.01 r40724**
Datum: **August 2018**

Voraussetzungen

Folgende Distributionen und Datenbanken mit zugehörigen Connector-C Treibern werden mit dieser Freigabe unterstützt:

Linux Distribution	Datenbank	Treiber
CentOS 7.4 64 Bit	MariaDB 5.5.56	MySQL libmysqlclient.so.18 Version: 5.5.56-MariaDB
Ubuntu Server 16.04.4 LTS 64 Bit	MySQL 5.7.22	MySQL libmysqlclient.so.18 Version: 5.6.25-MySQL

Das NCP Secure Enterprise Management (SEM) ist nur in der 64 Bit Variante verfügbar.

Soll die Datenbank-Kommunikation via ODBC erfolgen so wird der MariaDB ODBC Treiber 3.0.3 oder neuer empfohlen. In Verbindung mit einer MySQL-Datenbank kann die Kommunikation mit der Datenbank nicht via SOCKET erfolgen.
Grundsätzlich sollte der Connector-C Treiber verwendet werden.

NCP Management Console 5.0 zur Konfiguration.

1. Neue Leistungsmerkmale und Erweiterungen

Keine.

2. Verbesserungen / Fehlerbehebungen

Problembehebung beim Einspielen von Lizenzen

Lizenzen mit weniger als 100 Managed Units konnten nicht korrekt im SEM eingespielt werden. Ebenso konnten Update-Lizenzen der gleichen Seriennummer in unterschiedlichen Gruppen importiert werden. Diese Fehler wurden behoben.

Problembehebung beim Erstellen eines Backup-SEM

Wurden am primären SEM Plug-ins gelöscht, z.B. nach dem Einspielen einer aktuelleren Version des Plug-ins, so konnte ein Backup-SEM nicht fehlerfrei installiert werden. Dieser Fehler wurde behoben.

„Hängen“ des Management Dienstes

Sofern mehrere Skripte gleichzeitig in der selben Tabelle Einträge angelegt bzw. gelöscht haben konnte dies zu einer Blockierung der Kommunikation des *ncprsumain* Prozesses führen. Dieser Fehler wurde behoben.

Fehlerhafte Konsolenanmeldung

Bei der Verwendung der nativen Datenbankanbindung (C-Connector) von MySQL/MariaDB konnte es bei der Konsolenanmeldung zu dem Fehler *„Fehlerhafte Anmeldung“* kommen. Die darauffolgende Anmeldung verlief korrekt. Dieser Fehler wurde behoben.

Fehler bei der Erstellung von Vorlagen mit dem Verbindungsmedium ISDN

Die Erzeugung eines Vorlagenprofils mit dem Verbindungsmedium ISDN erzeugt eine Fehlermeldung. Dieser Fehler wurde behoben.

Unerwartetes Beenden des RADIUS-Dienstes

Ist der externe Authentisierungsserver (MS Active Directory) während der Anmeldephase eines Benutzers nicht erreichbar (z.B. via MC CHAPv2), so führte dies zum Beenden des RADIUS-Dienstes. Dieser Fehler wurde behoben.

Fehler beim Zuweisen einer MAC-Adresse auf den NCP Secure Enterprise VPN Server (SES)

Bei bestimmten Codepage-Einstellungen der Datenbank konnte dem SES keine MAC-Adresse durch den SEM zugewiesen werden. Die Fehlermeldung lautete: *„Eintrag konnte nicht geändert werden" (en: "Entry cannot be modified")*. Dieser Fehler wurde behoben.

Löschen von statischen Routen funktioniert nicht

Bei der Verwendung von MariaDB mit dem MariaDB C-Connector 3.0.5 konnten statische Routen im SES nicht gelöscht werden. Dieser Fehler wurde behoben.

Keine Fehlermeldung, wenn DB nicht verbunden ist

Ist beim Start des SEM die Datenbank nicht erreichbar, so wurde der Verbindungsversuch der Konsole abgelehnt aber die entsprechende Fehlermeldung nicht angezeigt. Dieser Fehler ist behoben

RADIUS MSCHAPv2: Die Fehlermeldung "Password expired" wurde nicht weitergeleitet

Gibt der externe Authentisierungsserver (MS Active Directory) während der Anmeldephase eines Benutzers die Fehlermeldung *„Password expired“* aus, so wurde diese Meldung nicht an den Client weitergeleitet. Dieser Fehler wurde behoben.

Falsche SEM Benachrichtigung "Zertifikat abgelaufen"

Die SEM Benachrichtigung "Zertifikat abgelaufen" wurde weiterhin angezeigt, obwohl das abgelaufene Zertifikat bereits gelöscht wurde

Fehler bei Verwendung von „rsurestore“

Unter bestimmten Umständen wurde die Funktion „rsurestore“ beim Aufruf an einem Primary-SEM nicht korrekt ausgeführt. Dieser Fehler wurde behoben.

3. Bekannte Einschränkungen

Keine.

Major Release: **5.00 r39572**
Datum: **Mai 2018**

Voraussetzungen

Folgende Distributionen und Datenbanken mit zugehörigen Connector/C Treibern werden mit dieser Freigabe unterstützt:

Linux Distribution	Datenbank	Treiber
CentOS 7.4 64 Bit	MariaDB 5.5.56	MySQL libmysqlclient.so.18 Version: 5.5.56-MariaDB
Ubuntu Server 16.04.4 LTS 64 Bit	MySQL 5.7.22	MySQL libmysqlclient.so.18 Version: 5.6.25-MySQL

NCP empfiehlt die Verwendung der getesteten Connector/C-Treiber.

Soll die Datenbank-Kommunikation via ODBC erfolgen so wird der MariaDB ODBC Treiber 3.0.3 oder neuer empfohlen. In Verwendung mit einer MySQL-Datenbank kann die Kommunikation mit der Datenbank nicht via SOCKET erfolgen.

NCP Management Console 5.0 zur Konfiguration.

1. Neue Leistungsmerkmale und Erweiterungen

Interner Umbau der Datenbank-Schnittstelle

Ab dem SEM 5.0 ist es möglich mehrere Datenbank-Sessions gleichzeitig zu nutzen. Die maximale Anzahl kann in der Konfigurationsdatei ncprsu.conf angegeben werden. Als Standardwert werden 10 Sessions verwendet.
Des Weiteren können die MySQL- oder MariaDB-Datenbank nun neben ODBC auch nativ über den Connector/C angesteuert werden. Ein ODBC-Treiber wird in diesem Falle nicht benötigt.

Optimierung des integrierten RADIUS-Servers

Im integrierten RADIUS-Server wurde ein Thread Pool implementiert. Wird eine RADIUS Message über einen der RADIUS Ports empfangen, so wird diese in der Queue des Thread Pools zwischengespeichert. Ein freier Thread bearbeitet anschließend die RADIUS Message und sendet die Antwort zum RADIUS Client. Die Anzahl der Threads im Pool kann über einen Konfigurationsparameter geändert werden. Als Standardwert werden 8 Threads verwendet.

RADIUS Secret für externe Authentisierung
Für die externe Authentisierung über RADIUS/OTP kann jetzt ein eigenes RADIUS Secret konfiguriert werden. Ist dieses Secret leer, wird das Secret des RADIUS Clients verwendet. Diese Funktionalität erfordert ein RADIUS-Plug-in der Version 5.0 oder neuer.

EAP allgemein
Der zu verwendende Typ der EAP-Verhandlung wird immer durch den Server bestimmt. In diesem Fall durch den RADIUS Server im SEM. Hierzu können im RADIUS Client und in den RADIUS Gruppen-Einstellungen die gewünschten EAP-Protokollvarianten freigeschaltet werden. Sind sowohl im RADIUS Client als auch in den RADIUS Gruppen-Einstellungen mehrere EAP-Protokolle gleichzeitig aktiviert, so wird der EAP-Typ durch folgende Reihenfolge bestimmt.

- EAP-TLS
- EAP-MSCHAPv2
- EAP-OTP(NCP)
- EAP-MD5

EAP-OTP (NCP)
Hierbei werden Benutzername und Passwort (im Klartext) nach NCP proprietärem Protokoll zwischen Secure Enterprise VPN Server und SEM übertragen. Es wird aber der EAP Type "OTP" verwendet. Es ist geplant, dies mit EAP-PEAP oder EAP-TTLS zukünftig verschlüsselt zu übertragen. Externe Authentisierung ist mit allen Protokollen möglich (OTP/RADIUS, LDAP, Kerberos). Ebenfalls kann zusätzlich die "NCP Advanced Authentication" verwendet werden.

EAP-MSCHAPv2
EAP-MSCHAPv2 ist RFC konform implementiert. Externe Authentisierung bzw. "NCP Advanced Authentication" kann nicht verwendet werden.

Optimierte EAP-TLS Kommunikation

Installation der Plug-ins während der SEM Installation

Sofern noch keine Plug-ins im SEM installiert sind, wird nach dem Login mit der SEM Konsole die Installation der SEM-Plug-ins angeboten.

Benachrichtigungen

Aktuell anliegende Ereignisse z.B. Fehler, Warnungen oder Infos werden über ein Icon im Menü der Konsole angezeigt. Ein Klick auf dieses Icon zeigt weitere Details. Die Farbe des Icons gibt Auskunft darüber, welche Ereigniskategorie mindestens einmal vorhanden ist,

- rot: Error
- gelb: Warnung
- blau: Info
- schwarz: es liegen keine Benachrichtigungen vor

Eingabe des Lizenzschlüssels

Die Eingabe des Lizenzschlüssels erfolgt ab SEM 5.0 über die Konsole unter "Management Server" → "Lizenz". Wenngleich der SEM jetzt auch ohne gültige Lizenz läuft, so sind folgende Funktionen abgeschaltet:

- Software Download der Update Clients
- RADIUS Server (Antwortet nicht)
- SES und HA Server Verwaltung (Verbindung zum SEM wird nicht mehr zugelassen)

Der oben genannte Menüpunkt wird nur angezeigt, wenn ein Admin mit dem Benutzernamen "Administrator" in der Root Gruppe anmeldet ist. Nach Eingabe der Lizenzdaten muss der SEM nicht mehr neu gestartet werden.

Administrativer Zugriff nur aus vordefinierten IP-Netzen

Administratoren können sich nur aus definierten IP-Netzen am SEM anmelden.

2. Verbesserungen / Fehlerbehebungen

SEM Konsole und SEM Konsolen Plug-in

Der NCP Secure Enterprise Management 5.0 (SEM) benötigt zur Konfiguration die NCP Management Console 5.0. Diese Konsole kann sich mit einem SEM der Version 5.x oder 4.05 verbinden. Ältere SEM Versionen – vor 4.05 – benötigen ältere, zugehörige Konsolen. Das SEM Console Plug-in ist ab der Version 5.0 nicht mehr verfügbar.

Allgemeine Verbesserungen beim Logging

Die Scopes der einzelnen Logging-Agenten können über die Management Konsole 5.0 zur Laufzeit geändert werden.
Menü: "Management Konsole" → "Scopes".

Überprüfung des SEM-Zertifikates

Ab der Version 5.0 überprüft die Konsole das SEM-Zertifikat. Liefert die Zertifikatsüberprüfung einen Fehler zurück, wird der Administrator darauf hingewiesen und kann den Verbindungsaufbau ggf. zulassen oder stoppen.

Start-Information

Ab dem SEM 5.0 und der Konsole 5.0 wird während des Startvorgangs des SEM der Status in der Konsole angezeigt.

Scripting mit Passwörtern

Passwörter können in der Datei ncprsu.conf mit dem Präfix "crypt:" verschlüsselt gespeichert werden. Die verschlüsselten Passwörter können in der NCP Script IDE unter Edit / Crypt Password erzeugt werden. Diese verschlüsselten Passwörter können in einem Skript mit dem Präfix "crypt:" entsprechend verwendet werden.

SEM Einstellungen Dialog – suche nach Parameter

Der Dialog wurde mit einer Suchfunktion erweitert (Menü "Management Server" → "Einstellungen").

Anzeige ODBC / MySQL Treiber Version

Im Info Dialog (Menü "Management Server" → "Info") wird unter Details die Version des ODBC/MySQL-Treibers angezeigt.

Anzeige der Warnungen im System Monitor Plug-in anpassen

Der Schwellwert zur Anzeige einer Warnung betreffend der genutzten Management Units kann innerhalb der Management Server-Einstellungen in der Gruppe SystemMonitor mit dem Parameter MaxMUsWarnValue eingestellt werden (Wertebereich: 0 – 100).

Neuer Button zur Ansicht der „Start-Seite“

Durch Klick auf diesen Button bekommt der Administrator die Ansicht wie unmittelbar nach der Anmeldung der Konsole angezeigt.

3. Bekannte Einschränkungen

Um einen stabilen Betrieb zur gewährleisten sollte die MariaDB/MySQL-Datenbankanbindung via Connector/C-Treiber erfolgen. Eine Anbindung via ODBC funktioniert derzeit nur mit der MariaDB ODBC-Treiberversion 3.0.3 fehlerfrei. Bei der Verwendung anderer ODBC-Treiberversionen kann es zu Instabilitäten kommen.

4. Hinweise zum NCP Secure Enterprise Management

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
https://www.ncp-e.com/de/service/
Weitere Unterstützung bei Fragen zum NCP Secure Enterprise Management, erhalten Sie über die Mail-Adressen auf folgender Seite:
https://www.ncp-e.com/en/support/

E-Mail: support@ncp-e.com

5. Leistungsmerkmale

Zentrale Verwaltung

Das NCP Secure Enterprise Management (SEM) ist der zentrale Bestandteil der NCP Next Generation Network Access Technology. Als **Single Point of Administration** schafft es die erforderliche Transparenz für Netzwerkadministratoren, um mobile und stationäre Telearbeitsplätze sowie remote VPN-Gateways in Filialnetzen zentral zu verwalten. Das NCP Software-Tool bietet alle Funktionalitäten und Automatismen, die für die Inbetriebnahme und den Betrieb eines Remote Access-Projektes erforderlich sind.
Mit dem Secure Enterprise Management werden Konfigurationen, Zertifikate und Software Updates zentral erzeugt und gespeichert bzw. verteilt und aktualisiert oder ausgerollt.
Die Richtlinien für eine Endpoint Security (Network Access Control) werden am Secure Enterprise Management (SEM) zentral erstellt. Entsprechend der erstellten Regeln erhält der Enterprise Client Zugang zum Firmennetz.

Lizenzierung der Managed Units

Die Gesamtzahl der zu lizenzierenden Managed Units (MU) für ein Secure Enterprise Management-System setzt sich aus der Anzahl der Client-Einträge (Benutzer) plus der Anzahl der Einträge für Remote Server zusammen. Die Einheiten der zentralen Server (Server Configuration Plug-ins mit Secure Server und HA Server) werden den Lizenzbestimmungen entsprechend nicht zu den Managed

Units gezählt.

Komponenten des Secure Enterprise Managements

Das NCP Secure Enterprise Management (SEM) besteht aus dem Management Server und der Management Console. Das Datenbank-System ist nicht im Lieferumfang enthalten.

Voraussetzungen für die Server-Komponente

64 bit operating systems / Linux distributions / Database / ODBC

Siehe Voraussetzungen auf Seite 1

Rechner

CPU mind. Pentium III-800 MHz (abhängig von der Anzahl der Managed Units)
Mit RADIUS Plug-in: Pentium IV-1,5 GHz
Festplatte: min. 50 MB freier Speicher zzgl. Speicherplatz für Log-Dateien und ca. 20 MB pro Software-Paket

Unterstützte Datenbanken

Der Management Server ist ein datenbankbasiertes System und korrespondiert mit nahezu jeder Datenbank. Unterstützte Datenbanken siehe Seite 1.
Alle systemrelevanten Informationen werden in der Datenbank abgelegt und sind üblicherweise in den Backup-Prozess eingebunden. Dazu gehören unter anderem: Benutzer-Profile (Konfigurationen der Managed Units), Lizenz-Keys und Authentisierungsdaten, Zertifikate, Providerkennungen etc.

Backup-System

Optional steht ein Backup-System mit integriertem Replikationsdienst für den Management Server zur Verfügung.

Unterstützte Certification Authorities

Microsoft Certificate Services als integrierte und stand alone CA.

Voraussetzungen für die Console

Über die Management Console werden die VPN-Benutzerdaten zentral verwaltet.

Betriebssysteme

Windows Desktop Betriebssysteme 32-Bit und 64-Bit

Management Server-Module

Die Management Server-Module werden als Plug-ins von jedem Rechner im lokalen Netzwerk unter Angabe der IP-Adresse des Management Servers auf diesem installiert. Dies gilt auch für die Management Console, die ebenfalls als Plug-in installiert werden kann. (Das Datenbank-System ist nicht im Produktumfang enthalten.)

Verfügbare Plug-ins

- Client Configuration Plug-in

- Firewall Plug-in
- Server Configuration Plug-in (HA Server und Secure Server)
- License Management Plug-in
- PKI Management Plug-in
- Endpoint Policy Plug-in
- Script Plug-in
- RADIUS Plug-in
- System Monitor Plug-in (experimental)

Unterstützte RFCs und Drafts

- RFC 2138 Remote Authentication Dial In User Service (RADIUS)
- RFC 2139 RADIUS Accounting
- RFC 2433 Microsoft CHAP
- RFC 2759 Microsoft CHAP V2
- RFC 2548 Microsoft Vendor-specific RADIUS Attributes
- RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)
- RFC 2716 PPP EAP TLS Authentication Protocol
- RFC 2246 The TLS Protocol
- RFC 2284 PPP Extensible Authentication Protocol (EAP)
- RFC 2716 Certificate Management Protocol
- RFC 2511 Certificate Request Message Format
- Draft-ietf-pkix-cmp-transport-protocols-04.txt, Transport Protocols for CMP
- Draft-ietf-pkix-rfc2511bis-05.txt, Certificate Request Message Format (CRMF)

Zentrale Funktionalitäten

Administratoren-Management und Mandantenfähigkeit (Multi-Company Support)
Die Mandantenfähigkeit prädestiniert das Secure Enterprise Management für den Einsatz bei Managed Security Service Providern (MSSP) in sog. „Managed VPNs“ oder Remote Access-Strukturen, in denen mehrere Firmen gemeinsam eine VPN-Plattform nutzen (VPN Sharing).
Über die zentrale Administratoren-Verwaltung werden die Zugriffsrechte für die jeweiligen Administratoren auf die jeweiligen selbständigen Firmen mit angeschlossenen VPN-Benutzern definiert. Durch Gruppenzuordnung werden die Rechte der Administratoren so angelegt, dass jeder ausschließlich Zugriff auf seinen zu verwaltenden Mandantenkreis (Organisationsgruppe) hat. Ein Übergriff auf Daten anderer Mandanten ist ausgeschlossen.
Als VPN-Gateway kann der NCP Secure Enterprise Server aber auch das eines Fremdherstellers eingesetzt werden (siehe Kompatibilitätsliste unter www.ncp-e.com). Damit ist das Secure Enterprise Management auch in jede vorhandene IT-Infrastruktur integrierbar und ermöglicht den Betrieb auch in komplexen VPN-Umgebungen.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

Lizenz-Management (License Management Plug-in)
Mit der Lizenzierung steht die Gesamtzahl der Managed Units für den Management Server zur freien Verfügung. Die Managed Units können entweder als Benutzer- oder Remote Server-Lizenzen eingesetzt werden. Alle Lizenzen werden in einen Pool übernommen und nach festgelegten Richtlinien automatisiert verwaltet:

- Lizenzübernahme kann automatisiert erfolgen oder manuell vorgenommen werden
- Lizenz wird nach Ausscheiden eines Mitarbeiters in den Pool zurück gestellt
- Meldung wird ausgegeben wenn keine Lizenz mehr verfügbar ist

Erzeugung der Konfigurationen für die Managed Units
Mit der Management Console werden User-Daten abgerufen oder Konfigurationen und Zertifikate gespeichert. Alle relevanten Informationen werden in der Datenbank abgelegt und sind üblicherweise in den Backup-Prozess des VPN-Betreibers eingebunden.
Die Eingabe aller relevanten Daten kann an der Management Console interaktiv durch den Administrator vorgenommen oder skriptgesteuert über das Script Plug-in erfolgen.

Automatic Update (über LAN und VPN)
Der Update Service des Secure Enterprise Managements gestattet alle für das Remote Access-Umfeld relevanten Software-Komponenten zentral verfügbar zu halten. Sobald eine Verbindung zwischen Client und Corporate Network besteht, werden diese Komponenten automatisch auf der Client-Seite eingespielt. Sollte es während der Übertragung zu Störungen kommen, bleiben der bereits vorhandene Softwarestand sowie die Konfiguration unberührt. Erst nach einem komplettem, fehlerfreiem Transfer aller vordefinierten Daten findet das Update statt.

- Steuerung der Update-Pakete
  Mittels Update-Liste, die der Administrator nach den jeweiligen Erfordernissen zusammenstellt, erfolgt die Verteilung der Software-Komponenten. Dabei kann pro Komponente nach Verbindungsmedium, Häufigkeit der Ablehnungen eines Updates und Art des Updates differenziert werden.
- Update-Komponenten
  Folgende Software-Komponenten können für das automatische Update bereitgestellt werden:
  - Konfigurationen (Profile und Monitor-Einstellungen des Enterprise Clients)
  - Benutzer-Zertifikate (Soft-Zertifikate, p12-Format)
  - Aussteller-Zertifikate (Soft-Zertifikate, cer- und pem-Formate)
  - Update Client
  - Software-Versionen (Software Updates / Upgrades sind für Clients nur unter Windows Desktop-Betriebssystemen möglich)

- Verbindungsmedium
  Alle Verbindungsmedien, die die Remote-Seite unterstützt, können einer der Update-Komponenten zugeordnet werden. So lässt sich zum Beispiel steuern, dass für große Datenmengen schnelle Verbindungsmedien genutzt werden.
- Update-Verfahren
  Alternativ zu einem Update über VPN, kann die Option des LAN Updates genutzt werden. (Eine NCP Dynamic Personal Firewall kann nur über LAN aktualisiert werden.) Bei einem Update über VPN werden alle Daten durch den Tunnel verschlüsselt übertragen. Bei einem LAN Update, wenn sich der Client PC im heimischen Firmennetz befindet, wird die SSL-Verschlüsselung eingesetzt.

Beschreibung der Plug-ins

System Monitor Plug-in (Test-Software)

Dieses Plug-in dient der schnellen Information über alle wichtigen Ereignisse innerhalb einer VPN-Installation als Balken- oder Linien-Diagramme. Der Administrator kann über den System Monitor je nach Bedarf aktuelle Status-Informationen in Echtzeit abrufen bzw. auf bereits gespeicherte Datenbestände der Remote Access-Umgebung zugreifen. Im jeweiligen Diagramm kann im Zeitraum beliebig zurück bzw. vorwärts geblättert werden. Die grafische Darstellung der Diagramme ist frei wählbar.

Client Configuration Plug-in

Hiermit werden die Profile der Secure Enterprise Clients erstellt, konfiguriert und verwaltet. Folgende Einstellungen sind damit möglich:

- alle gruppenspezifischen und verbindungstechnischen Parameter können mithilfe von Vorlagen (Templates) automatisiert generiert werden
- nur personenbezogene Daten werden manuell eingegeben (Authentisierungsdaten für Erstverbindung bei Rollout)
- Parametersperren, die der entfernte Benutzer nicht verändern kann, können definiert werden
- automatische Konfiguration der Benutzer-Profile für Zentralkomponenten (RADIUS, LDAP, SNMP)
- umfassendes Logging (Versionsstände, Zeitstempel für Konfigurationsänderungen, automatischer Upload von Client-Logdateien)
- Erzeugung eines generalisierten Init-Benutzers für Rollout
- automatisierte Erzeugung und Bereitstellung von Konfigurations-Updates

Firewall Plug-in

Zur Konfiguration der Personal Firewall in den Secure Enterprise Clients und der Dynamic Personal Firewall der Client Suite. Folgende Einstellungen können vorgenommen werden:

- applikations- und verbindungsabhängige Filterregeln
- protokoll-, port- und adressbezogene Filterregeln
- Vorgaben für die Erkennung von „friendly networks“ (IP-Adresse Netzwerk, Netzwerkmaske, IP-Adresse des DHCP-Server, MAC-Adresse)
- Logging-Einstellungen
- FND-Serverkonfiguration (Friendly Net Detection)
- Firewall-Einstellungen, die der entfernte Benutzer nicht verändern kann, können definiert werden

Server Configuration Plug-in

Das Server Configuration Plug-in dient der Konfiguration und Verwaltung von Secure Servern (Secure Enterprise Server und Secure High Availability Server) im zentralen Netz. Die Lizenzierung der Server-Komponenten erfolgt dezentral an der jeweiligen Maschine über deren Web-Interface.
An der Management Console werden die Zugriffsrechte für den jeweiligen Server verwaltet und die komplette Konfiguration des Servers erstellt.
Die Konfigurations- und Statistik-Oberfläche des Web-Interfaces der Server-Komponente wird an der Management Console eins zu eins abgebildet. Darüber hinaus kann von der zentralen Management Console die Konfiguration über das Web-Interface vor Ort temporär gestattet werden. Konkurrierende Konfigurationsänderungen sind ausgeschlossen.
Zur Konfiguration einer Gruppe von Servern (Server Farm) können Vorlagen genutzt werden, ebenso wie für Client-Benutzergruppen.

PKI Enrollment Plug-in

Das Plug-in fungiert als Registration Authority (RA). Im Zusammenwirken mit unterschiedlichen Certification Authorities (CA) werden elektronische Zertifikate (X.509 v3) erstellt und verwaltet. Ein erzeugtes Zertifikat kann wahlweise zur Verwendung als Soft-Zertifikat (PKCS#12) oder für den Einsatz auf Smart Card oder USB-Token (PKCS#11) abgelegt werden. Die im Lieferumfang enthaltene NCP Demo-CA kann während der Testphase für die Abbildung einer PKI genutzt werden, ist jedoch nicht für den produktiven Einsatz vorgesehen. Die Umstellung auf eine externe CA ist problemlos möglich. Die wichtigsten Funktionalitäten des PKI Plug-ins sind:

- Erstellen von Benutzer- und Hardware-Zertifikaten (auch Bulk Mode)
- Verlängern der Zertifikatsgültigkeit (PKCS#7)
- Sperren von Zertifikaten
- Verteilung der Zertifikate (auch Multi-Client-Zertifikate)
- Anlegen der Benutzerkonfiguration über LDAP im Verzeichnisdienst
- Erstellen eines PAC-Briefes (Personal Authentication Code) für Erstverbindung und Lizenzierung
- Generieren und Verteilen von Server-Zertifikaten

Endpoint Policy Plug-in

Mit Hilfe dieses Plug-ins werden alle sicherheitsrelevanten Parameter definiert, die vor einem Zugriff auf das Firmennetz überprüft werden sollen (Network Access Control). Die Einhaltung der vorgegebenen Sicherheitsrichtlinien ist zwingend und vom Anwender nicht umgehbar oder manipulierbar. Folgende Einstellungen am entfernten Rechner des Benutzers können überprüft werden:

- Software-Stand des Secure Enterprise Clients
- Betriebssystem-Informationen, z. B. Version oder Hotfixstand
- Dienste-Informationen
- Datei-Informationen
- Status des Virenscanners
- Registry-Werte
- Inhalte von Benutzer- und Hardware-Zertifikaten

Abweichungen von den Sollvorgaben werden protokolliert und können unterschiedliche Meldungen bzw. Aktionen auslösen. Z. B.:

- Anzeige einer Meldung am Client
- Ausgabe einer Meldung im Log-Buch des Clients
- Senden einer Meldung zum Management Server
- Senden einer Meldung zu einem Syslog Server
- Freischalten der relevanten Firewall-Regeln
- Weiterleitung in eine Quarantänezone
- Trennung der VPN-Verbindung

RADIUS Plug-in

Für die Konfiguration der Managed Units (Benutzern) in den zentralen VPN-Gateways steht optional die RADIUS-Schnittstelle zur Verfügung. Das RADIUS Plug-in dient der Verwaltung des integrierten RADIUS Servers und deckt folgende Funktionen ab:

- Automatische Anlage von RADIUS-Accounts über die Client- und Remote Server Configuration Plug-ins
- Unterstützung von PAP/CHAP-Requests
- Erfassung von Accounting-Daten
- Sperren von Benutzern bei wiederholten fehlerhaften Anmeldungen
- Verwaltung von mehreren RADIUS-Konfigurationen unterschiedlicher Gateways
- RSA Authentication Manager Proxy-Funktionalität

Optional steht ein Backup RADIUS-Server zur Verfügung. Dies gestattet vorhandene RADIUS Server durch den integrierten RADIUS Server des Management-Systems zu ersetzen.