

NCP Secure Enterprise VPN Server (Linux)

Release Notes



Service Release: 11.01 r38204
Datum: Dezember 2017

Voraussetzungen

Linux Distributionen:

Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.4
- Debian GNU/Linux 9.2.1
- SUSE Linux Enterprise Server 12 SP3
- Ubuntu Server 16.04.3 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Für den Einsatz anderer NCP-Komponenten werden folgende Versionen benötigt

- Secure Enterprise Management Server Version 4.05 oder höher
- Management Console Version 4.05 oder höher
- Management Plug-in Server Configuration Version 11.00 oder höher
- Secure Enterprise HA Server Version 10.01 oder höher

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server produktiv nutzen zu können.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Die Ausführung des VRRP-Scripts funktioniert nun auch unter CentOS 7.4.

Bei der Installation unter Debian ab 9.0 wird der Fall berücksichtigt, dass bei der Betriebssystem-Installation dem Root-Benutzer kein Passwort zugewiesen wurde.

Nach einem Update auf Version 11.0 oder deren Neu-Installation musste ein Reboot des Systems durchgeführt werden, bevor der Server gestartet werden konnte. Dieser Fehler ist behoben. Nach einem Neustart des SNMP-Dienstes sind auch SNMP-Abfragen möglich.

Next Generation Network Access Technology



Beim Download der CRL-Liste konnte ein Absturz des Dienstes ncpsrvmgm erfolgen. Dieser Fehler ist behoben.

SEM-Anfragen für Software Update über LAN werden nicht mehr weitergeleitet.

Mit dem RADIUS-Attribut "NCPS-PCCertCN" = "*" wird die Verwendung eines Hardware-Zertifikats erzwungen.

Weiterleitung von "nicht an den Secure Server Adapter gebundenen VPN IP-Adressen" funktioniert wieder.

Die Auswahl des Server-Zertifikates erfolgt so wie sie eingestellt wurden, entweder „automatisch“ vom Server oder „manuell konfiguriert“.

Der Server änderte beim Start die Reihenfolge in der Konfigurationsdatei ncpwsupd.conf. Dieser Fehler wurde behoben.

Wenn keine Daten über die VPN-Verbindung mehr geschickt werden, bleiben die Path Finder Sessions nicht länger geöffnet, sondern werden automatisch abgebaut.

Der Secure Enterprise Server unterstützt nun auch Pathfinder 2 und SSL-VPN, wenn ECC-Zertifikate konfiguriert werden.

In der Konfigurations-Webseite des SES erschien sporadisch fälschlicherweise die Meldung: „Änderungen erfordern einen Neustart des NCP Secure Enterprise Servers!“

Bei konfigurierter „ARRE-Option“ konnte es vorkommen, dass der Server keine VPN-Verbindungen mehr akzeptierte. Dieser Fehler ist behoben.

Wurden Filter für den VPN-Datenstrom gesetzt, so wurden äußerst sporadisch Datenpakete dennoch weitergeleitet. Dieser Fehler ist behoben.

3. Bekannte Einschränkungen

Keine

NCP Secure Enterprise VPN Server (Linux)

Release Notes



Major Release: 11.0 r36600
Datum: August 2017

Voraussetzungen

Linux Distributionen:

Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.3
- Debian GNU/Linux 8.7
- SUSE Linux Enterprise Server 12 SP2
- Ubuntu Server 16.04.2 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Voraussetzung für Server-Konfiguration mit dem Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 oder höher
- Management Plugin - Server Configuration: Version 11.00 oder höher

Voraussetzungen für die High Availability Funktionalität

Bei Einsatz des Secure Enterprise VPN Servers 11.00 im High Availability-Verbund, ist darauf zu achten, dass der High Availability Server (HA Server) mindestens die Version 10.01 besitzen muss.

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server produktiv nutzen zu können.



1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Gelöschte Domaingruppen nach Update auf Version 11.0

Ist innerhalb der Domain-Gruppen-Konfiguration im NCP Secure Enterprise VPN Server die Option „Erlaube nur die ausgewählten CA-Zertifikate“ ausgewählt, werden mit dem Update des NCP Secure Enterprise VPN Servers auf die Version 11.0 die Domain-Gruppen, einschließlich der Standard-Domain-Gruppe, gelöscht. Dieser Fehler ist behoben.

3. Bekannte Einschränkungen

Keine

NCP Secure Enterprise VPN Server (Linux)

Release Notes



Major Release: 11.00 r36322
Datum: Juli 2017

Voraussetzungen

Linux Distributionen:

Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.3
- Debian GNU/Linux 8.7
- SUSE Linux Enterprise Server 12 SP2
- Ubuntu Server 16.04.2 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Voraussetzung für Server-Konfiguration mit dem Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 oder höher
- Management Plugin - Server Configuration: Version 11.00 oder höher

Voraussetzungen für die High Availability Funktionalität

Bei Einsatz des Secure Enterprise VPN Servers 11.00 im High Availability-Verbund, ist darauf zu achten, dass der High Availability Server (HA Server) mindestens die Version 10.01 besitzen muss.

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server produktiv nutzen zu können.



1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

IKEv2-Verbindung mit Computer- und Benutzerzertifikat

War für eine VPN-Verbindung über IKEv2 die Authentisierung des Gerätes über Computerzertifikat **und gleichzeitig** die Authentisierung des Benutzers über Benutzerzertifikat erforderlich, schlug der Verbindungsaufbau fehl. Dieser Fehler ist nun behoben.

Anzeige von Benutzern, die über LDAP authentisiert werden

VPN-Benutzer, die über LDAP authentisiert werden, wurden fälschlicherweise in der Statistik unter „Link-Profile (lokal)“ aufgelistet. Dieser Fehler ist behoben, sodass sie nun korrekt unter „Link-Profile (RADIUS/LDAP)“ angezeigt werden.

Die maximale Anzahl der gleichzeitig möglichen LDAP-Benutzer wurde von 10000 auf 40000 erhöht.

3. Bekannte Einschränkungen

Keine

4. Hinweise zum NCP Secure Enterprise VPN Server

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:

<https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/gateway/>

NCP Secure Enterprise VPN Server (Linux)

Release Notes



Major Release: 11.00 r36173
Datum: Juli 2017

Voraussetzungen

Linux Distributionen:

Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.3
- Debian GNU/Linux 8.7
- SUSE Linux Enterprise Server 12 SP2
- Ubuntu Server 16.04.2 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Voraussetzung für Server-Konfiguration mit dem Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 oder höher
- Management Plugin - Server Configuration: Version 11.00 oder höher

Voraussetzungen für die High Availability Funktionalität

Bei Einsatz des Secure Enterprise VPN Servers 11.00 im High Availability-Verbund, ist darauf zu achten, dass der High Availability Server (HA Server) mindestens die Version 10.01 besitzen muss.

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server mit dem Secure Enterprise HA Server produktiv nutzen zu können.



1. Neue Leistungsmerkmale und Erweiterungen

Erweitertes Lizenzmanagement für iOS Clients

Ab dieser Version des NCP Secure Enterprise VPN Servers wird das Lizenzmanagement des NCP Secure Enterprise iOS Clients unterstützt.

Deutliche Performanceverbesserungen

Erhöhung möglicher ausgehender Verbindungen

Die maximale Anzahl von ausgehenden VPN-Verbindungen wurde von 750 auf 10000 erhöht.

IKEv2 Signature Authentication nach RFC 7427 mit RSA-PSS-Padding

Im Client und Server wurde eine neue Zertifikats-Authentisierungsmethode nach RFC7427 implementiert.

Für Benutzer- und Hardware-Zertifikate werden folgende Schlüsseltypen unterstützt: RSA, ECC NIST, ECC BP in verschiedenen Schlüssellängen.

In der „Zertifikatsüberprüfung“ einer Domain-Gruppe ist der Schalter „Erlaube RSA Authentisierung mit PKCS#1 V1.5 Padding“ standardmäßig aktiv. Nur wenn dieser Schalter deaktiviert wird, kann die bisherige IKEv2 RSA-Zertifikatsauthentisierung noch genutzt werden.

Client VPN-IP-Adresszuweisung für getaktete Verbindung

Diese Funktionalität findet Verwendung in Home Office-Umgebungen, bei denen die Internetanbindung des Routers über ein Medium mit volumenabhängiger Abrechnung erfolgt, vorzugsweise Mobilfunk. Der Anwenderarbeitsplatz ist dabei über WLAN an den Internet-Router angebunden. In diesem Fall kann das zugehörige WLAN-Profil des NCP Secure Clients in den Profileinstellungen als „getaktete Verbindung“ („metered connection“) konfiguriert werden. Dieses Merkmal wird zur weiteren Verarbeitung an den NCP Secure Enterprise VPN Server gesendet.

Zur Kostenersparnis bei Volumentarifen, erhält der Client beim Tunnelaufbau vom Server eine IP-Adresse aus einem dafür angelegten Pool für Clients mit Mobilfunkanbindung. Zentralseitige Anwendungen, die den Client mit Updates versorgen, können nur Datenpakete an den Client übertragen, die auf das Nötigste reduziert sind.

Am Server werden unter „Adressvergabe“ die Pool-Bereiche für getaktete Verbindungen definiert und erhalten eine Ordnungsnummer. Mit dem Eintragen dieser Nummer im Link-Profil unter „Routing“ wird dem Client eine IP-Adresse aus dem entsprechenden Pool zugewiesen. Werden an dieser Stelle die Pool-Nummern auf null gesetzt und ist keine feste IP-Adresse vergeben, so wird der IP-Adressbereich des konfigurierten DHCP-Servers genutzt.

Unterstützung mehrerer Server-Zertifikate

Pro Domain-Gruppe können nun verschiedene Standard-Zertifikate eingestellt werden. Der Secure Enterprise VPN Server kann daraus für die jeweilige Domain-Gruppe dasjenige selektieren, welches am besten zur Anfrage des Clients passt (z.B. längste Laufzeit).

Zusätzliche Sicherheitsbarriere

Die sicherheitskritischen Server-Dienste ncpwsupd und ncpsrvmgmd werden mit eingeschränkten Rechten betrieben, um potentielle Systemangriffe zu erschweren.



Anzeige zusätzlicher Verbindungsinformationen

Folgende Informationen werden in der Statistik unter „Link-Profile“ angezeigt:

- NCP VPN Path Finder Version
- Seamless Roaming

Im Account Log wird angezeigt, auf welche lokale Endpunkt-IP-Adresse sich der Client einwählt.

2. Verbesserungen / Fehlerbehebungen

Beim Verbindungsaufbau der Clients wurde die Netzmaske nicht korrekt übertragen.
Dieser Fehler ist behoben.

Neues Tool zur Erstellung der Scripte für dve_up und dve_down unter
[SES-INSTALL-DIR]/sbin/ses-vrrp-setup.

3. Bekannte Einschränkungen

Keine

4. Hinweise zum NCP Secure Enterprise VPN Server

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:

<https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/gateway/>