Release Notes

NCP VS GovNet Server

Minor-Release: 2.10 r30479
Datum: Mai 2024

Voraussetzungen

Server-Hardware
Standard-Server mit x86-64 Hardware und Kompatibilität zu Debian 11.7;

SmartCard-Leser
Zwei Omnikey 3121 (Revision A oder B) und mindestens ein weiterer, baugleicher SmartCard-Leser zum Personalisieren der SmartCards am Administrations-PC.

SmartCards
Zwei SmartCards TeleSec TCOS 3.0 Signature Card 2.0

Für den Einsatz anderer NCP-Komponenten werden folgende Versionen benötigt

- Secure Enterprise Management Server Version 7.10 oder höher
- Management Console Version 7.10 oder höher
- Management Plug-in Server Configuration Version 13.20 oder höher
- Management Plug-in PKI Version 7.0 oder höher

1. Neue Leistungsmerkmale und Erweiterungen

UEFI-Unterstützung

Während der Installation des VS GovNet Servers wird der verwendete Modus – UEFI oder BIOS bzw. Compatibilty Support Module – automatisch ausgewählt.

Eine detaillierte Beschreibung der Funktion befindet sich im beiliegenden CHANGELOG-Dokument.

2. Verbesserungen / Fehlerbehebungen

Firewall-Anpassung bei der Verwendung von Netzwerk-Bonding

Bei der Verwendung von Netzwerk-Bonding konnten keine Daten auf interne Bonding-Interfaces geroutet werden. Das Problem wurde durch das automatische Anlegen zweier Firewall-Regeln beim Start des GNS behoben.

Fehlermeldung beim Start der NCP-Dienste

Es wurde ein Problem beim Aufruf des verwendeten PKCS#11-Moduls behoben.

Sicherheits- und Serviceupdates des Basisbetriebssystems

Das Debian- Basisbetriebssystems wurde aktualisiert. Insbesondere wurden die folgenden Sicherheitslücken behoben:

- NCPVE-2024-0417: SSH Host-Keys werden nicht mehr mit ausgeliefert.
- Linux kernel local privilege escalation (GSM and XEN virtualization): Durch eine Race Condition im Modul für GSM wird eine Rechteausweitung (Privilege Escalation) ausgelöst.

Eine detaillierte Auflistung und Beschreibung aller aktualisierten Pakete befindet sich im beiliegenden CHANGELOG-Dokument.

3. Bekannte Einschränkungen

Die Bonding-Konfiguration wird erst nach einem Reboot der VS GovNet Server-Appliance vollständig angewandt

Anzeige der Bonding-Konfiguration

Wird das Netzwerk-Bonding im zentralen Management konfiguriert, so wird es im Netzwerk-Konfigurationstool des VS GovNet Servers nicht korrekt angezeigt obwohl es voll funktional ist. Es wird daher empfohlen das Netzwerk-Bonding im lokalen Netzwerk-Konfigurationstool des VS GovNet Servers zu konfigurieren.

Minor-Release: 2.01 r30478
Datum: März 2024

Voraussetzungen

Server-Hardware
Standard-Server mit x86-64 Hardware und Kompatibilität zu Debian 11.7;

UEFI/BIOS Konfiguration: Legacy BIOS Mode (UEFI im CSM-Modus)

SmartCard-Leser
Zwei Omnikey 3121 (Revision A oder B) und mindestens ein weiterer, baugleicher SmartCard-Leser zum Personalisieren der SmartCards am Administrations-PC.

SmartCards
Zwei SmartCards TeleSec TCOS 3.0 Signature Card 2.0

Für den Einsatz anderer NCP-Komponenten werden folgende Versionen benötigt

- Secure Enterprise Management Server Version 7.0 oder höher
- Management Console Version 7.0 oder höher
- Management Plug-in Server Configuration Version 13.20 oder höher
- Management Plug-in PKI Version 7.0 oder höher

1. Neue Leistungsmerkmale und Erweiterungen

Keine.

2. Verbesserungen / Fehlerbehebungen

Sicherheits- und Serviceupdates des Basisbetriebssystems

Das Debian- Basisbetriebssystems wurde aktualisiert. Insbesondere wurden die folgenden Sicherheitslücken behoben:

- glibc: Debian Security Advisories [DSA 5611-1] und [DSA-5514-1]; Buffer-Overflow in qsort() sowie CVE-2023-4911
- Intel Microcode: Debian Security Advisory [DSA 5563-1]; CVE-2023-23583
- curl; CVE-2023-46218, CVE-2023-38545 und CVE-2023-38546

Eine detaillierte Auflistung aller aktualisierten Pakete befindet sich im beiliegenden CHANGELOG-Dokument.

3. Bekannte Einschränkungen

Die Bonding-Konfiguration wird erst nach einem Reboot der VS GovNet Server-Appliance vollständig angewandt

Anzeige der Bonding-Konfiguration

Wird das Netzwerk-Bonding im zentralen Management konfiguriert, so wird es im Netzwerk-Konfigurationstool des VS GovNet Servers nicht korrekt angezeigt obwohl es voll funktional ist. Es wird daher empfohlen das Netzwerk-Bonding im lokalen Netzwerk-Konfigurationstool des VS GovNet Servers zu konfigurieren.

Major-Release: 2.00 r30467
Datum: Juni 2023

Voraussetzungen

Server-Hardware
Standard-Server mit x86-64 Hardware und Kompatibilität zu Debian 11.7;

UEFI/BIOS Konfiguration: Legacy BIOS Mode (UEFI im CSM-Modus)

SmartCard-Leser
Zwei Omnikey 3121 (Revision A oder B) und mindestens ein weiterer, baugleicher SmartCard-Leser zum Personalisieren der SmartCards am Administrations-PC.

SmartCards
Zwei SmartCards TeleSec TCOS 3.0 Signature Card 2.0

Für den Einsatz anderer NCP-Komponenten werden folgende Versionen benötigt

- Secure Enterprise Management Server Version 7.0 oder höher
- Management Console Version 7.0 oder höher
- Management Plug-in Server Configuration Version 13.20 oder höher
- Management Plug-in PKI Version 7.0 oder höher

1. Neue Leistungsmerkmale und Erweiterungen

Integration des NCP High Availability Servers

Der NCP High Availability Server ist ab dieser Version des VS GovNet Servers in der Installation enthalten. Zur Nutzung ist lediglich der Erwerb des zugehörigen Lizenzschlüssels notwendig. Damit lässt sich der Aufbau eines leistungsfähigen Verbundes mehrerer VS GovNet Server realisieren, der den ausfallsicheren und performanten Betrieb mehrerer 10.000 Anwender ermöglicht.

Implementierung von VRRP

Im Rahmen der Load Balancing-Funktionalität wurde das VRRP (Virtual Router Redundancy Protocol) implementiert. Damit wird, zur Erhöhung der Ausfallsicherheit, die Erreichbarkeit zweier Gateways unter einer einzigen IP-Adresse realisiert.

Netzwerkkonfiguration: Bonding

Mit dieser Version des VS GovNet Servers wird das Zusammenfassen mehrerer Netzwerkkarten (Bonding) unterstützt.

Self Check durch neuen Integritätsdienst

Der im VS GovNet Server vorhandene Integritätsdienst führt eine kontinuierliche Überwachung der korrekten Funktionalität durch. Eine etwaige Kompromittierung des VS GovNet Servers resultiert in der Überführung in einen sicheren Zustand, der eine weitere Kommunikation jeglicher Art unterbindet.

Zentrale Konfiguration

Die Konfiguration des VS GovNet Servers geschieht über den zentralen NCP Secure Enterprise Management Server. Über das zugehörige Server Plug-in werden Konfigurationen angelegt und auf die entsprechenden VS GovNet Server und High Availability Server verteilt. Das zentrale Management unterstützt ebenso den Mandantenbetrieb. Damit kann mit einer leistungsfähigen Remote Access-Lösung, Behörden oder Unternehmen, der sichere Zugang in ihr jeweiliges zentrales Netz ermöglicht werden.

Audit-Meldungen

Dem VS GovNet Server wurden neue Audit-Meldungen hinzugefügt. Diese enthalten Informationen zu:

- Ein- und Ausschalten sowie Neustarts des VS GovNet Servers,
- Auf- und Abbau eines VPN-Tunnels,
- Ein- und Ausschalten der Auditfunktion,
- administrative Zugriffe und durchgeführte Konfigurationsänderungen,
- Auslösen eines Alarms,
- fehlerhafte Authentisierungsversuche

Neue Option: Erlaube RSA Authentisierung mit SHA-1 Hash

Gemäß der Signature Authentication nach RFC7427 wird bei einer eingehenden IKEv2-Verbindung mit RSA-Authentisierung der SHA-1 Hash grundsätzlich erlaubt. Ist die Verwendung von SHA-1 gewünscht, so kann diese Option aktiviert werden.

2. Verbesserungen / Fehlerbehebungen

Neue OpenSSL Version 1.1.1t

Verbesserung der Kompatibilität zu Drittherstellern innerhalb der IKE-Verhandlung

Optimierung der IKEv2 Cookie Challenge

3. Bekannte Einschränkungen

Die Bonding-Konfiguration wird erst nach einem Reboot der VS GovNet Server-Appliance vollständig angewandt

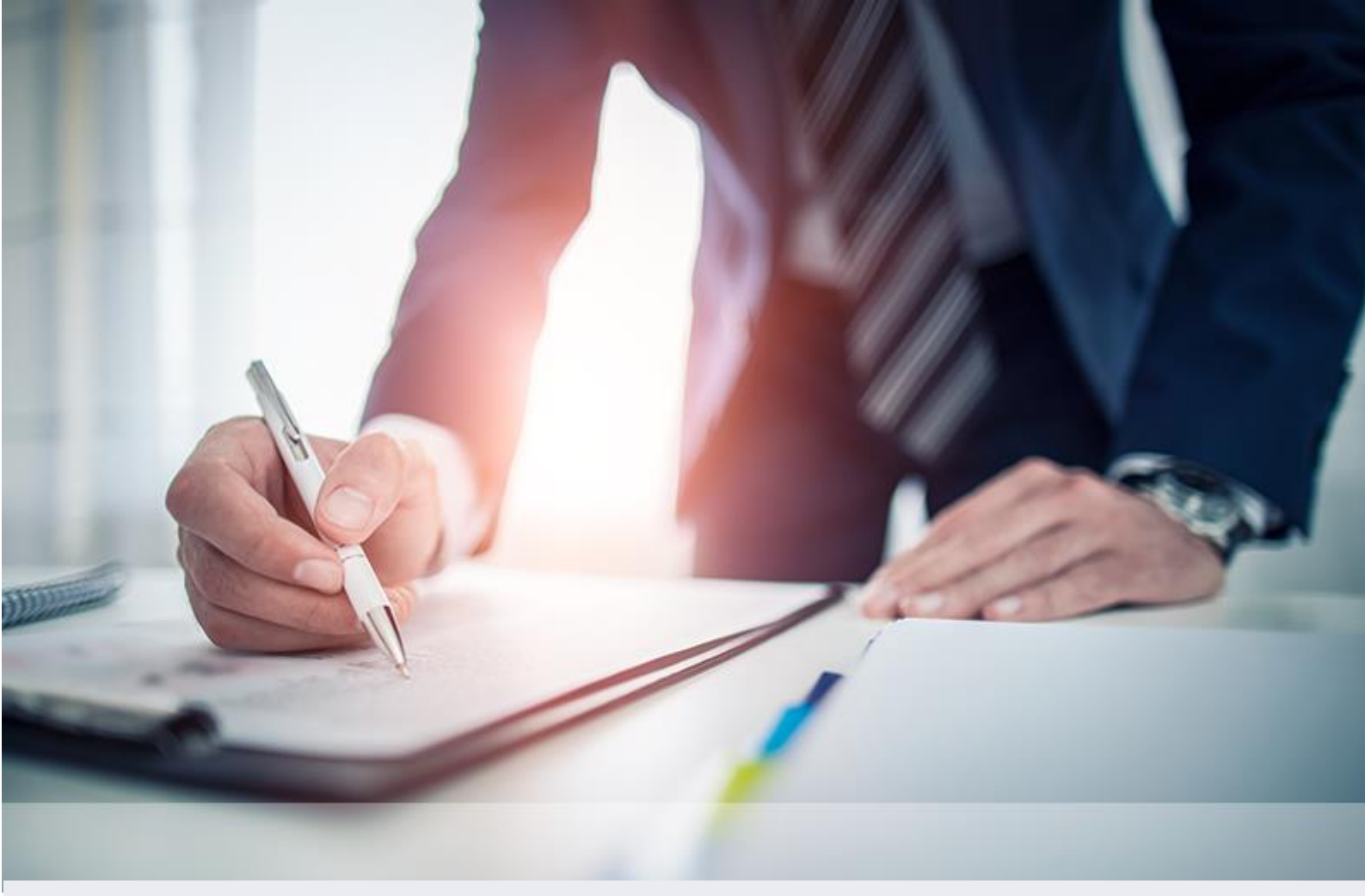
Anzeige der Bonding-Konfiguration

Wird das Netzwerk-Bonding im zentralen Management konfiguriert, so wird es im Netzwerk-Konfigurationstool des VS GovNet Servers nicht korrekt angezeigt obwohl es voll funktional ist. Es wird daher empfohlen das Netzwerk-Bonding im lokalen Netzwerk-Konfigurationstool des VS GovNet Servers zu konfigurieren.

4. Hinweise zum NCP Secure Enterprise VPN Server

Weitere Informationen zum letzten Stand der Entwicklung des NCP VS GovNet Servers erhalten Sie auf der Website:

https://www.ncp-e.com/de/produkte/vpn-fuer-vs-nfd/



NCP engineering GmbH
Dombühler Str. 2
90449 Nürnberg
Deutschland

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com