Release Notes

NCP VS GovNet Server

Minor release: 2.01 r30478
Date: March 2024

Prerequisites

Server hardware
Standard server with x86-64 hardware and compatibility with Debian 11.7;

UEFI/BIOS configuration: Legacy BIOS Mode (UEFI in CSM mode)

SmartCard reader
Two Omnikey 3121 (revision A or B) and at least one additional, identical SmartCard reader for personalizing the SmartCards at the administration PC.

SmartCards
Two smart cards TeleSec TCOS 3.0 Signature Card 2.0

The following versions are required for the use of other NCP components

- Secure Enterprise Management Server version 7.0 or higher
- Management Console version 7.0 or higher
- Management Plug-in Server Configuration Version 13.20 or higher
- Management Plug-in PKI Version 7.0 or higher

1. New features and enhancements

None.

2. Improvements / Problems Resolved

Security and service updates of the base operating system

The Debian base operating system has been updated. In particular, the following security vulnerabilities have been fixed:

- glibc: Debian Security Advisories [DSA 5611-1] and [DSA-5514-1]; Buffer overflow in qsort() and 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

A detailed list of all updated packages can be found in the attached CHANGELOG document.

3. Known Issues

The bonding configuration is only fully applied after a reboot of the VS GovNet server appliance

Display of the bonding configuration

If the network bonding is configured in the central management, it will not be displayed correctly in the VS GovNet Server network configuration tool although it is fully functional. It is therefore recommended to configure the network bonding in the local network configuration tool of the VS GovNet Server.

Major release: 2.00 r30467
Date: June 2023

Prerequisites

Server hardware
Standard server with x86-64 hardware and compatibility with Debian 11.7;

UEFI/BIOS configuration: Legacy BIOS Mode (UEFI in CSM mode)

SmartCard reader
Two Omnikey 3121 (revision A or B) and at least one additional, identical SmartCard reader for personalizing the SmartCards at the administration PC.

SmartCards
Two smart cards TeleSec TCOS 3.0 Signature Card 2.0

The following versions are required for the use of other NCP components

- Secure Enterprise Management Server version 7.0 or higher
- Management Console version 7.0 or higher
- Management Plug-in Server Configuration Version 13.20 or higher
- Management Plug-in PKI Version 7.0 or higher

1. New features and enhancements

Integration of the NCP High Availability Server
The NCP High Availability Server is included in the installation starting with this version of the VS GovNet Server. To use it, only the purchase of the corresponding license key is necessary. This makes it possible to set up a high-performance network of several VS GovNet Servers, which enables the fail-safe and high-performance operation of several 10,000 users.

Implementation of VRRP
VRRP (Virtual Router Redundancy Protocol) was implemented as part of the load balancing functionality. This allows two gateways to be reached from a single IP address, thus increasing reliability.

Network configuration: Bonding
This version of the VS GovNet Server supports the combination of several network cards (bonding).

Self Check through new integrity service

The integrity service available in VS GovNet Server performs continuous monitoring of correct functionality. Any compromise of the VS GovNet Server results in the transfer to a secure state, which prevents further communication of any kind.

Central configuration

The VS GovNet Server is configured via the central NCP Secure Enterprise Management Server. Configurations are created via the associated server plug-in and distributed to the corresponding VS GovNet Server and High Availability Server. The central management also supports multi-client operation. Thus, with a powerful remote access solution, authorities or companies can be provided with secure access to their respective central network.

Audit messages

New audit messages have been added to the VS GovNet Server. These contain information on:

- Switching on and off as well as restarts of the VS GovNet Server,
- VPN tunnel setup and teardown,
- switching on and off of the audit function,
- administrative accesses and performed configuration changes,
- triggering of an alarm,
- incorrect authentication attempts

New option: Allow RSA authentication with SHA-1 hash

According to Signature Authentication as defined in RFC7427, the SHA-1 hash is generally allowed for an incoming IKEv2 connection with RSA authentication. If the use of SHA-1 is desired, this option can be enabled.

2. Improvements / Problems Resolved

New OpenSSL version 1.1.1t

Improvement of compatibility to third party vendors within IKE negotiation

Optimization of the IKEv2 Cookie Challenge

3. Known Issues

The bonding configuration is only fully applied after a reboot of the VS GovNet server appliance

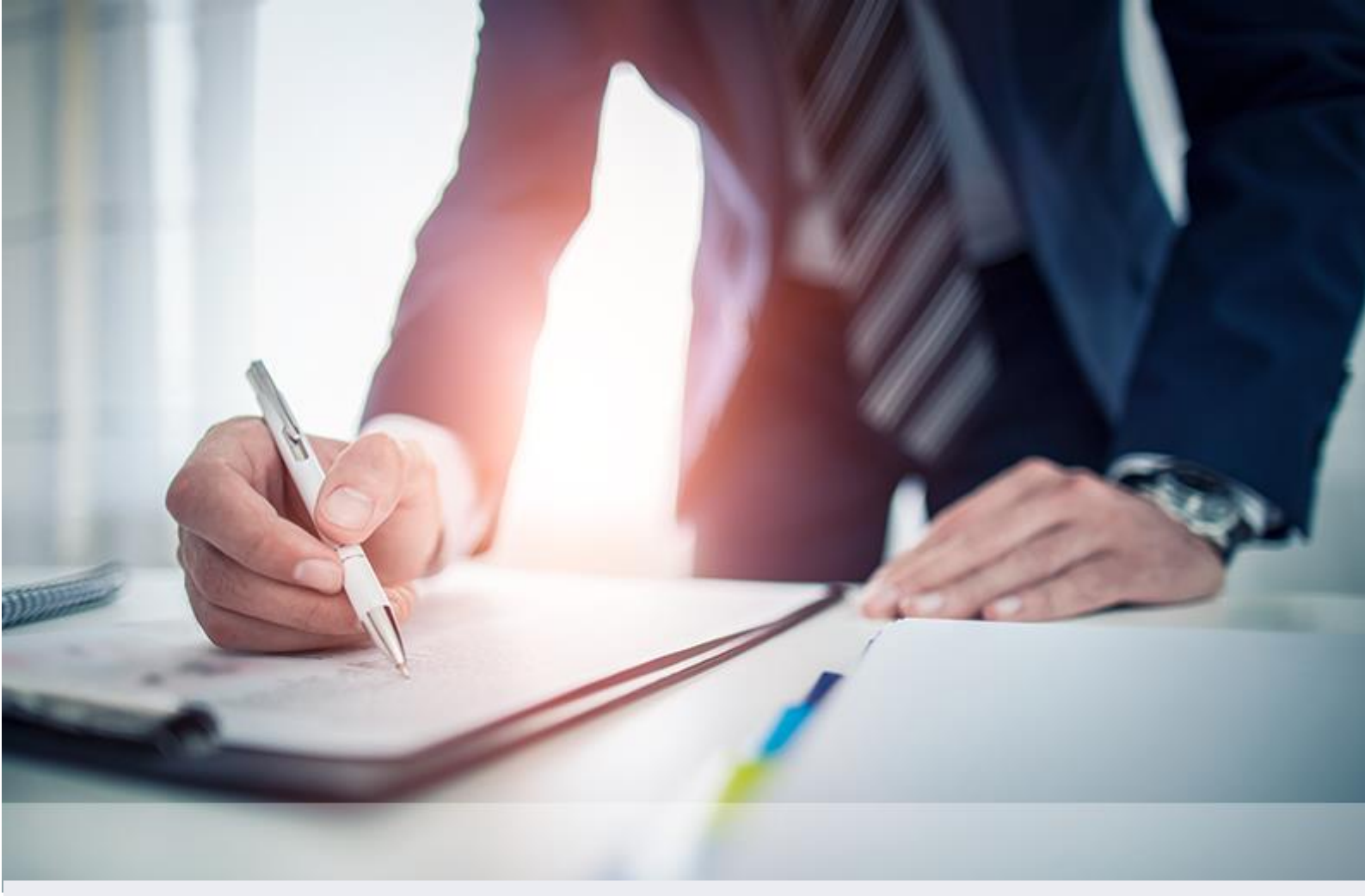
Display of the bonding configuration

If the network bonding is configured in the central management, it will not be displayed correctly in the VS GovNet Server network configuration tool although it is fully functional. It is therefore recommended to configure the network bonding in the local network configuration tool of the VS GovNet Server.

4. Getting Help for the NCP VS GovNet Server

To ensure that you always have the latest information about the NCP VS GovNet Server, always check the NCP website at:

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



NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg
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