Hardening guidelines

Installation manual

for system providers and tenants

10/22/2021

Product line *neo*, version 6.x

The described functions can be used with the following ASC products:

EVOIP*neo*

EVOLUTION*neo* / XXL / eco

INSPIRATION*neo*

Please note that you can always find the most up-to-date technical documentation and product updates in the partner area on our website at http://www.asctechnologies.com.

ASC Technologies AG - Seibelstr. 2-4 - 63768 Hösbach - Germany

Contents

1 General information

In the context of this document ASC represents ASC Technologies AG, its subsidiaries, branch offices, and distributors. An up-to-date overview of the aforementioned entities can be found at https://www.asctechnologies.com

ASC assumes no guarantee for the actuality, correctness, integrity or quality of the information provided in the manuals.

ASC regularly checks the content of the released manuals for consistency with the described hardware and software. Nevertheless, deviations cannot be excluded. Necessary revisions are included in subsequent editions.

Some aspects of the ASC technology are described in general terms to protect the ownership and the confidential information or trade secrets of ASC.

Representative, if not defined otherwise, is the technical status at the time of the delivery of the software, the devices and the manuals of ASC. Technical changes without specified announcements are reserved. Previous manuals lose their validity.

The general conditions of sales and delivery of ASC in their latest version apply.

2 Introduction

This document gives detailed instructions on how to harden the Windows servers which are used for the ASC recording solutions.

3 Deployed software

3.1 Operating system

For the *neo* Suite, the following server operating systems are supported:

- Microsoft Windows Server 2012 R2 English - 64 Bit (only for updates)
- Microsoft Windows Server 2012 R2 German - 64 Bit (only for updates)
- Microsoft Windows Server 2016 English - 64 Bit
- Microsoft Windows Server 2016 German - 64 Bit
- Microsoft Windows Server 2019 English - 64 Bit
- Microsoft Windows Server 2019 German - 64 Bit

The *neo* Suite consists of several Windows services.

3.2 3rd-party components

The following 3rd-party components are installed:

3rd-party components	Version	Description
Glassfish	5.0	
OpenJDK	≥ 1.8.0_232-b09	
Liquibase	3.1.1	
OSCCSDK *)	V8R2_GP05	Unify OSSC
PGAdmin *)	4	PostgreSQL
PostgresJDBC *)	42.2.5	PostgreSQL
PostgreSQL *)	12.5-1-x64	PostgreSQL
TSAPIClient *)	6.4.7	Alcatel
WinPcapP *)	4.1.3	only for passive integrations - can otherwise be uninstalled

Tab. 1: Required 3rd-party components

*) optional

3.3 Update of 3rd-party components

Observe the following rules by all means when updating 3rd-party components:

- Do not update **operating systems** unless during the installation of hotfixes. New service packs and versions must have been released for installation by ASC.
- **JAVA** may be updated as long as the released basic version (e. g. JRE 1.8.0_x) remains.
- **MSSQL** may be updated as long as the released basic version remains.
- **Other 3rd-party components** (e. g. PostgreSQL, Glassfish) must **not** be updated without prior consent of ASC. Safety-relevant updates of these products are provided by ASC.

ⓘ **Before** a Windows update, all *neo* services must be stopped. Once the update has been completed, the *neo* services can be started again.

4 User accounts

If you are using a PostgreSQL database, **only** the user account *postgres* is created during the installation. All *neo* services run using the local system account.

5 Encryption of communication

neo exclusively supports the encryption protocol TLS 1.2 for secure data transmission.

To deactivate TLS < 1.1 there is a script available in the installation directory. Execute the script *DisableWeakTLS.ps1* as administrator (`\ASC\ASC Product Suite\scripts>DisableWeakTLS.ps1`).

The ASC application server supports only the following Cipher Suites for HTTPS:

- +TLS_RSA_WITH_AES_128_CBC_SHA
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- +TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- +TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- +TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- +TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- +TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- +TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- +TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- +TLS_ECDH_anon_WITH_AES_128_CBC_SHA
- +TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- +TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- +TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

ATTENTION!

It is strongly recommended to replace the self-signed ASC SSL/TLS certificate with a customer-specific SSL/TLS certificate.

For information about importing a HTTPS certificate refer to the installation manual *Installation of the recording software of ASC*.

ATTENTION!

Security scans without a customer-specific SSL/TLS certificate are useless.

5.1 SMB signing

For the purpose of secure data transmission, ASC supports SMB signing.

SMB signing can be configured by means of the registrations key *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters*:

Value name:	EnableSecuritySignature
Data type:	REG_DWORD

Value:	0 = deactivated 1 = activated

Activated SMB signing may decrease the performance of accesses to networks by 10 to 15 percent.

For PCI DSS compliance, SMB signing must have been activated.

6 Hardening the operating system

Microsoft Windows Server 2012 R2

The operating system Windows 2012 R2 may be hardened according to the CIS Microsoft Windows Server 2012 R2 Benchmark v2.2.0.

Follow this link to register and download a free manual https://learn.cisecurity.org/benchmarks.

Please be aware of the following exceptions:

- 18.3.8 (L1) - the following value must **not** be *Enabled*: *MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)*.
- 18.9.22 EMET must not have been installed.

On 31st August 2018, Microsoft announced the end of support (EOS) for EMET.

Microsoft Windows Server 2016

The operating system Windows 2016 may be hardened according to the CIS Microsoft Windows Server 2016 v1.0.0.

Follow this link to register and download a free manual https://learn.cisecurity.org/benchmarks.

Please be aware of the following exceptions:

- 18.3.8 (L1) - the following value must **not** be *Enabled*: *MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)*.
- 18.9.22 EMET must not have been installed.

On 31st August 2018, Microsoft announced the end of support (EOS) for EMET.

7 Communication

For the entire internal communication of the *neo* Suite the TLS protocol (Transport Layer Security) is used. *neo* clients connect by means of https as well as by TLS. The communication with external software runs via encrypted connection wherever possible.

The Communication Matrix lists all ports deployed by the software components of the *neo* Suite.

Please note that the majority of the port numbers are only predefined values that may be changed in the *neo* Suite or in external applications.

7.1 Communication matrix

Inforamtion about the ports used by the *neo* Suite can be found on the in the file *Communication matrix* in folder *5_Communication matrix*.

8 Digital signatur

The *neo* files and the client setup files as well as all MSI packages carry the digital signature of ASC Technologies AG.

List of figures

List of tables

Glossary

Cipher suite

A cipher suite is a standardized collection of cryptographic concept used for e. g. encryption purposes. In the Transport Layer Security (TLS) protocol, the cipher suite defines which algorithms are used to establish a secured data connection. (Source: Wikipedia 1st February 2017)

PCI DSS

Payment Card Industry Data Security Standard

SMB

Server Message Block is a network communication protocol for providing shared access to files, printers, and serial ports between nodes on a network. It also provides an authenticated inter-process communication mechanism. (Source: Wikipedia 24th October 2019)

SSL

Secure Socket Layer

TLS

Transport Layer Security, former name Secure Sockets Layer (SSL), is a hybrid encryption protocol for secure data transmission on the Internet.

Index