JiveX

VISUS
Systemvoraussetzungen

DICOM-Mail Gateway im Westdeutschen Teleradiologieverbund
(Stand: Mai 2021)

VISUS Health IT GmbH
Gesundheitscampus-Süd 15–17
D-44801 Bochum
www.visus.com

Inhalt

Einleitung

Dieses Dokument enthält die Systemvoraussetzungen für DICOM-Mail-Gateways im Westdeutschen Teleradiologieverbund. Die genannten Anforderungen gelten gleichermaßen für virtualisierte als auch physische Systeme.

Systemanforderungen Server

Unterstützte Betriebssysteme

Es werden folgende Betriebssysteme im jeweils aktuellsten Patchlevel unterstützt:

- Microsoft Windows 10 64bit
- Microsoft Windows Server 2016/ 2019

Die Einrichtung und Partitionierung der Systempartitionen erfolgt nach Best-Practice Vorgaben des Kunden. JiveX nutzt ausschließlich u. g. Partitionen D:\ und E:\ zur Installation und Dateiablage.

Serverausstattung (empfohlene Voraussetzungen bei intensiver Nutzung)

- 8 CPU-Kerne
- 24 GB RAM
- C: Partition für Betriebssystem nach Kundenvorgabe
- Zusätzlich min. 200 GB Speicherplatz aufgeteilt in D: 50 GB und E: 150GB

Systemsicherheit

Systembetrieb

Die insgesamt zunehmende Bedrohungslage durch Schadsoftware erfordert grundsätzlich, dass die bekannten Vorkehrungen für den sicheren Betrieb des DICOM Mail Gateways getroffen werden. Im Besonderen wird auf die nachfolgenden Maßnahmen hingewiesen:

- VISUS empfiehlt den Betrieb des Systems in einer möglichst vom übrigen Netzwerk (intern/extern) separierten Umgebung. Es sollten nur die für den Betrieb notwendigen Ports zum Betrieb geöffnet sein. Die Ports sind abhängig von ihrer individuellen Installation und müssen daher bei Einrichtung mit dem zuständigen VISUS Mitarbeiter abgesprochen werden
- Es ist davon abzusehen, dass dauerhaft Laufwerksfreigaben auf das Gateway eingerichtet werden. In der Regel ist dies für den Betrieb des Gateways nicht erforderlich
- Windows Systemupdates/-upgrades sollten bei Verfügbarkeit möglichst direkt eingespielt werden. Eine automatisierte Überwachung dieses Prozesses wird empfohlen.

Virenscanner

Zur weiteren Absicherung empfehlen wir den Einsatz eines Virenscanners. Erfahrungsgemäß läuft JiveX mit den gängigen Produkten einwandfrei. Die Verwendung eines Virenscanners kann jedoch großen Einfluss auf die Systemperformance haben.

Um einen optimalen Betrieb zu ermöglichen empfehlen wir daher folgende Ordner und Prozesse als Ausnahmen zu definieren:

1. Die Ordner in denen sich die Bild- / Dokumentendaten befinden (D:\VISUS\jivexcs\images und Unterordner bzw. angebundene Laufwerke)
2. Die Ordner D:\VISUS\jivexcs und D:\mariaDB\data
3. Die Prozesse CSNTService.exe und mysqld.exe

Sollte es nicht möglich sein, ganze Ordner als Ausnahmen zu definieren, können Sie alternativ auch die folgenden Dateitypen als Ausnahme definieren:

- .dicom
- .dicomzip
- .dcmpre
- .jp2

Firewall-Regeln

Datenversand

Der Datenversand erfolgt über Mailserver, die von VISUS betrieben werden. Sämtlicher Datenverkehr ist dabei zertifikatbasiert SSL-verschlüsselt. Die Authentifizierung an den Mailservern erfolgt ebenfalls über von VISUS herausgegebene SSL-Zertifikate.

Für den korrekten Betrieb ist daher die ausgehende Kommunikation zu folgenden Servern über die TCP Ports 25 (SMTP/TLS) und Port 995 (POP3S) sicher zu stellen. Der Einsatz von Proxyserver oder Firewalls, die eigene SSL-Zertifikate nutzen um den Datenverkehr zu scannen, ist aufgrund der eingesetzten SSL-Authentifizierung nicht möglich.

- mail1.dicommail.com
- mail2.dicommail.com
- mail3.dicommail.com
- mail4.dicommail.com
- mail5.dicommail.com
- mail6.dicommail.com

JiveX Status Monitoring

VISUS nutzt zur Überwachung des Betriebszustandes und zur Administration der JiveX-Dienste ein Monitoring auf Basis der Software *check_mk*. Die Freischaltung dieses Monitoring-Dienstes ist grundlegender Teil der getroffenen Servicevereinbarung im Rahmen der Teilnahme am Westdeutschen Teleradiologieverbund und daher essenziell. Nur durch den konsequenten Einsatz und die Überwachung von Statusinformationen kann der Betrieb der Verbundstruktur nachhaltig sichergestellt werden.

Im Rahmen des Monitorings werden weder personenbezogene Daten wie Benutzerzugänge noch Patientendaten verarbeitet oder gespeichert. Sämtliche Kommunikation erfolgt verschlüsselt und wird durch zertifikatbasierte Authentifizierungsmechanismen geschützt. Details zu dieser Lösung senden wir Ihnen gerne auf Anfrage zu.

Zur Einrichtung wird eine weitere Firewall-Freischaltung für die ausgehende Kommunikation zu dem von VISUS betriebenen Monitoring-Server benötigt:

- atlas79.mydhp.de Port 8140 [TCP]

Verwendete Clients

Als Client steht mit JiveX Web ein HTML5-basierter Zero-Footprint Webclient zur Verfügung. Dieser Client ist lauffähig und freigegeben für alle gängigen Browser unter Windows und MacOS. Detaillierte Freigabelisten stellen wir auf Anfrage gerne zur Verfügung.

Als Systemressourcen werden ca. 500 MB Arbeitsspeicher, abhängig vom anzuzeigenden Datenvolumen, am Client benötigt.

VPN-Zugang

Für Installation und Wartung ist ein Fernwartungszugang zum Mailgateway erforderlich, der durch den Kunden bereitzustellen ist. VISUS bevorzugt End2Site VPN Zugänge.

Für den Aufbau einer End2Site VPN Fernwartungsverbindung stehen folgende VPN Clients zur Verfügung:

IPSec VPN

- ShrewSoft Client
- Cisco Systems VPN Client
- WatchGuard IPsec VPN Client
- Checkpoint Endpoint Security Client

SSL VPN

- OpenVPN Client
- Cisco Systems AnyConnect VPN Client
- WatchGuard Mobile VPN with SSL Client
- diverse web-basierte Plugins (WebSSL)

Des Weiteren stehen für den VPN Fernwartungszugriff die in Microsoft Windows Betriebssystemen integrierten VPN Lösungen über die Tunnelprotokolle PPTP, L2TP/IPsec bzw. SSTP zur Verfügung.

Sollte keine der vorgenannten Zugangsoptionen realisierbar sein, kann in begründeten Ausnahmefällen nach Rücksprache auf alternative Fernwartungszugänge wie Teamviewer oder Anydesk ausgewichen werden.

Sofern der End-To-Site VPN Fernwartungszugriff auf definierte Hosts eingeschränkt werden soll, so sind folgende von VISUS verwendeten IP-Adressen zu hinterlegen:

- 87.234.208.130
- 212.23.146.170

Informationen & Checkliste

VPN-Verbindung zu Installation und Service-Zwecken:

Der Service-Bereich der Visus-Health IT-GmbH verwendet für Wartungs- und Supportfälle einen End-to-Site-VPN Zugang. Für die Koordinierung der VPN-Verbindung melden Sie sich bitte bei Hr. Vietig (support@visus.com 0234/936 93 200) Verwenden Sie im Betreff der Email bitte VPN+Ortsname. Bitte teilen Sie uns vorab die Kontaktdaten Ihres VPN-Verantwortlichen mit:

Name: _____ Telefon: _____

E-Mail: _____

PACS-Anbindung:

Für die Kommunikation Ihrem PACS-System gibt es verschiedene Konzepte. Grundvoraussetzung ist, dass Ihr PACS mit dem Mailgateway bidirektional per DICOM Send kommunizieren kann.

Zusätzlich empfehlen wir, dass das PACS per Query/Retrieve abgefragt werden kann. Dies ermöglicht es den Anwendern, den DICOM Mail Versand aus der PACS-Arbeitsliste heraus zu starten.

Sie können die DICOM Send Konfiguration in Ihrem PACS vorab schon vorbereiten:

IP-Adresse Mailgateway: _____

Port: 4499

AETitle: DICOMMAIL

Bitte füllen Sie die Informationen für das DICOM Send zu Ihrem PACS, wie auch für das (optionale)

Query/Retrieve:

DICOM-Send (C-Store)

IP: _____ Port: _____ AET: _____

Query/Retrieve

IP: _____ Port: _____ AET: _____

Ansprechpartner für Ihr PACS:

Name: Telefon:

E-Mail:

Checkliste:

- ☐ VM gemäß Anforderungen bereit. IP:
- ☐ VISUS Mailserver von der VM über Port 25 und 995 erreichbar
- ☐ Status Monitoring Server von der VM über Port 8140 erreichbar
- ☐ VPN-Verbindung vorbereitet, Ansprechpartner genannt
- ☐ PACS Anbindung vorbereitet

For more Information please visit **www.visus.com**