JiveX

VISUS

Systemvoraussetzungen

DICOM-Mail Gateway

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
- Microsoft Server 2016/ 201919

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.

Einzelplatzlösung (Minimalvoraussetzung):

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

Mehrplatzlösung (Minimalvoraussetzung):

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

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 Kommunikation zu folgenden Servern über die 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
- smtp.dicommail.com (**häufig wechselnde IP!** Versand erfolgt über alle betriebenen Server im Round-Robin-Verfahren)

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]

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

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

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