Description technique

ZEISS FORUM Versions 4.2

1. Système d'exploitation

ZEISS FORUM 4.2 est compatible avec les dernières versions du système d'exploitation de Microsoft (64 bits seulement).

FORUM Server

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012
- Microsoft Windows 8/8.1
- Microsoft Windows 10

FORUM Viewer

FORUM Viewer prend en charge les dernières versions (au moment de leur sortie) des systèmes d'exploitation de Microsoft et d'Apple (64 bits seulement).

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012
- Microsoft Windows 8/8.1
- Microsoft Windows 10
- macOS 10.15 Catalina, 10.14 Mojave, 10.13 High Sierra

1.1 Support de visualisation

FORUM Server peut être installé et exploité sur VMware vSphere, Citrix Hypervisor ou HyperV.

2. Système de gestion de base de données relationnelle (SGBDR)

Le serveur FORUM dispose d'un SGBDR d'Oracle entièrement intégré. Il existe actuellement deux versions, utilisées en fonction du déploiement.

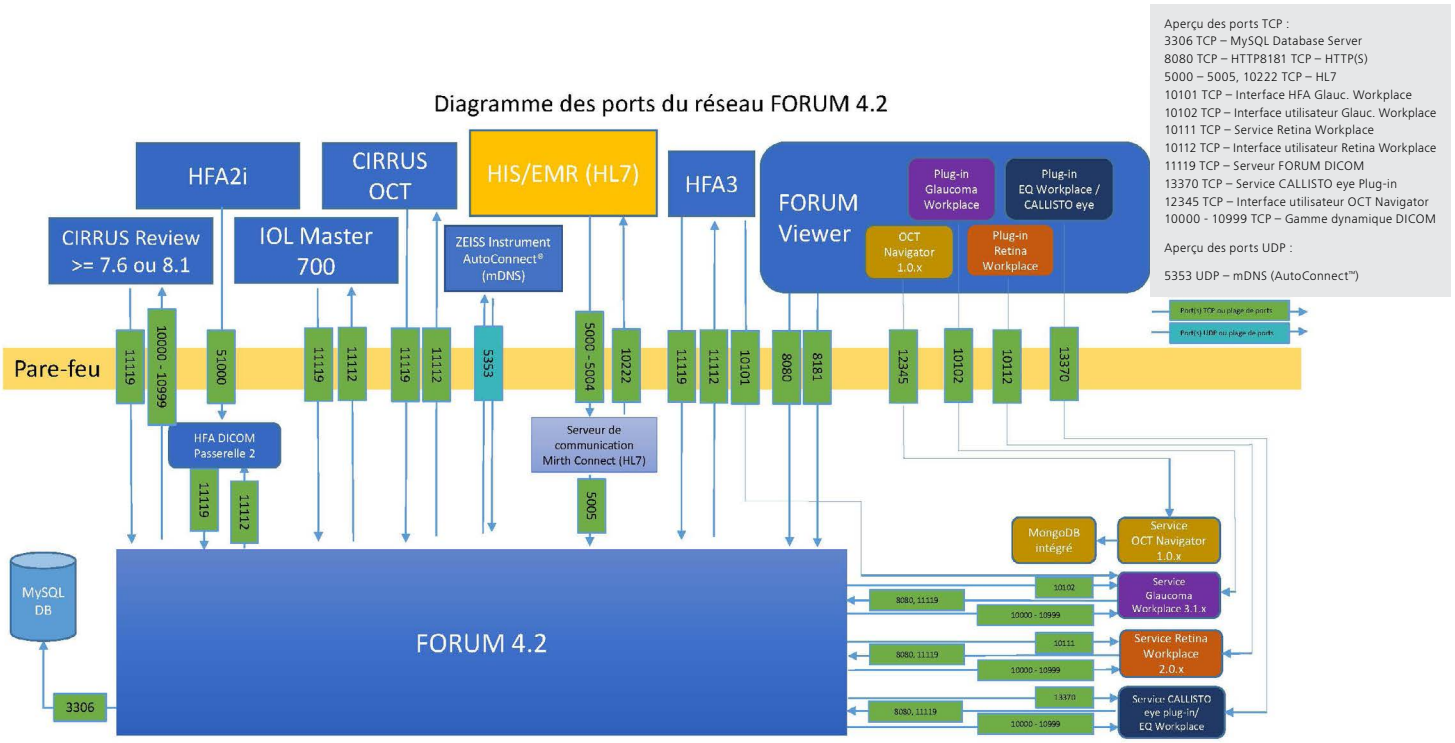
- MySQL Community Edition : 5.7
- MySQL Enterprise Edition : 5.7

3. Ports et protocoles

ZEISS FORUM 4.2 avec communication sécurisée.

Remarque : à partir de FORUM 4.2, seuls les protocoles HTTPS et mDNS sont utilisés pour la communication entre FORUM Viewer et le client.

Port	Protocole	Description	Trafic entrant/sortant
FORUM			
5353	UDP	mDNS (AutoConnect pour instruments)	Trafic entrant
8080	TCP	Port HTTP du serveur d'application	Trafic entrant
8181	TCP	Port HTTPS du serveur d'application (sécurisé)	Trafic entrant
11119	TCP	Port DICOM (forum.dicom.port)	Trafic entrant
5000	TCP	HL7	Trafic entrant
Retina Workplace			
10112	TCP	HTTPS	Trafic entrant
Glaucoma Workplace			
10102	TCP	HTTPS	Trafic entrant
EQ Workplace/CALLISTO eye plug-in			
13370	TCP	HTTPS	Trafic entrant
OCT Navigator			
12345	TCP	HTTPS	Trafic entrant



Le back office de FORUM 4.2 est à l'écoute de toute information arrivant sur les ports TCP par défaut figurant sur l'illustration. Les flèches indiquent la direction de la communication, et le numéro de port TCP est le port de destination. Dans ce diagramme, les services de plug-in MySQL DB, Mirth Connect, HFA DICOM Gateway 2, Glaucoma/Retina et le service de plug-in CALLISTO eye sont hébergés sur le même serveur (Windows) que le back office de FORUM. AutoConnect™ est une fonction utilisée par tous les instruments ZEISS de nouvelle génération tels que HFA3, IOL Master 700 et CIRRUS 500/5000 pour configurer les paramètres DICOM. Les ports TCP sur le poste de travail sont spécifiques à chaque version, veuillez vous référer au manuel de service de chaque version. Les ports Mirth Connect varient en fonction de l'accord conclu pour le projet concerné et n'ont qu'un rôle indicatif dans cette illustration.

4. Anti-malware

Tout logiciel anti-malware peut être utilisé, selon les directives informatiques du client.

5. Intégrité des données

5.1 Protection des données pendant le transit

Dernier chiffrement TLS 1.2 pour la protection contre la manipulation des données en transit ou les attaques par interception entre FORUM Archive, FORUM Viewer et les FORUM Workplaces. La modification des données dans ZEISS FORUM est protégée par un contrôle d'identité (p. ex. nom d'utilisateur et mot de passe, ou authentification par jeton pour accéder au système).

La communication d'authentification est cryptée par défaut, en particulier avec l'authentification unique basée sur Kerberos. LDAPS est pris en charge.

5.2 Protection des données au repos

La philosophie sous-jacente veut que la meilleure protection contre le vol de disque dur (protection des données au repos) soit celle protégeant l'accès au système d'exploitation. Si un assaillant parvient à accéder au système d'exploitation avec des privilèges d'administrateur, les données au repos ne peuvent pas être protégées efficacement. En outre, ZEISS recommande d'utiliser un logiciel standard de protection des données au repos par chiffrement des disques, par exemple BitLocker. Associer ces deux mécanismes de protection protège les données de manière effective et efficace.

Étape 1 : BitLocker protège le disque en entier dès que la machine est éteinte. Toutes les données sont chiffrées et ne peuvent être modifiées (p. ex. pour obtenir des privilèges d'administrateur). Le niveau d'optimisation étant élevé pour l'utilisation avec le système de fichiers MS, l'impact/la pénalité sur les performances est minime.

Étape 2 : ZEISS FORUM doit être installé par un administrateur, dans un dossier uniquement accessible par un utilisateur administrateur. Aucun autre utilisateur ne doit pouvoir lire, écrire, exécuter ou énumérer le contenu en question.

Toute protection supplémentaire des données au repos au niveau de l'application ne jouera son rôle que si l'une des deux étapes de protection susmentionnées est compromise. Avec FORUM 4.2, la protection des données démographiques des patients au niveau de la base de données a été renforcée par la possibilité de chiffrer les tables contenant les informations des patients.

6. Confidentialité

Prévention de la divulgation d'informations à des personnes et/ou systèmes non autorisés réalisée à plusieurs niveaux.

Au niveau de l'application :

- Authentification standard comparée à la base des utilisateurs déclarés dans ZEISS FORUM (nom d'utilisateur et mot de passe).
- Autorisation basée sur LDAP(S)/AD pour la gestion centralisée des utilisateurs.
- Authentification unique SSO basée sur le serveur Microsoft Active Directory utilisant Kerberos5.
- Niveaux d'autorisation dans le système (administrateur, éditeur, lecteur, lecteur d'EMR) et utilisation possible des groupes Active Directory.
- Chiffrement TLS 1.2 pour les données en transit dans le système FORUM.

Au niveau du système d'exploitation :

- Utilisation recommandée d'un logiciel de chiffrement du système de fichiers (p. ex. BitLocker) pour chiffrer les données au repos.
- Installation dans les dossiers du système, accessibles uniquement par les administrateurs du système (protection contre l'accès non autorisé aux données et le vol).

7. Protocoles d'autorisation et d'authentification pris en charge

Actuellement, les protocoles LDAP et Kerberos version 5 de Microsoft sont pris en charge.

Les versions typiques du web comme SAML 2.0, WS-federation, oAuth2 ou OpenID Connect ne sont pas encore prises en charge. Cette situation pourrait évoluer dans les versions ultérieures, en fonction du marché.

8. Support de stockage externe

ZEISS FORUM prend en charge le stockage en réseau (NAS) à l'aide du protocole SMB pour le stockage DICOM. FORUM doit être exécuté en tant qu'utilisateur ayant un accès au niveau du/des partage(s) CIFS et du système de fichiers. Le stockage SAN est recommandé dans le cadre de déploiements complexes. Les exigences minimales et les spécifications recommandées pour chaque version figurent dans des documents accessibles sur le site web de ZEISS. Les meilleures performances sont obtenues en utilisant le stockage DAS ou SAN.

9. Prise en charge de la surveillance du système

Le suivi de l'espace de stockage disponible et des services Windows peut être assuré par la plupart des outils de surveillance du système comme MS System Center Operations Manager (SCOM, SSCM ou MOM). D'autres outils peuvent offrir le même service.

10. Sauvegarde, restauration et aide à la récupération après sinistre

La sauvegarde appropriée des données relève entièrement de la responsabilité de l'opérateur du système. Plusieurs possibilités existent pour sauvegarder la base de données FORUM, la configuration, les licences et les données DICOM.

À son niveau le plus élémentaire, ZEISS FORUM dispose d'une fonction de sauvegarde et de restauration intégrée, accessible à partir de l'outil de Service ZEISS. Lorsqu'elle est activée, cette fonction permet la sauvegarde manuelle des données. Le Service ZEISS peut aider l'opérateur du système à programmer une sauvegarde automatique via le planificateur de tâches de Windows.

Une sauvegarde de ZEISS FORUM se compose essentiellement de trois parties :

- le système FORUM et la configuration
- la base de données MySQL intégrée, utilisée par FORUM
- les fichiers DICOM

Un module séparé ZEISS FORUM Enterprise Backup-Restore est disponible à titre complémentaire pour ajouter la possibilité de sauvegarder la base de données rapidement en cours de fonctionnement.

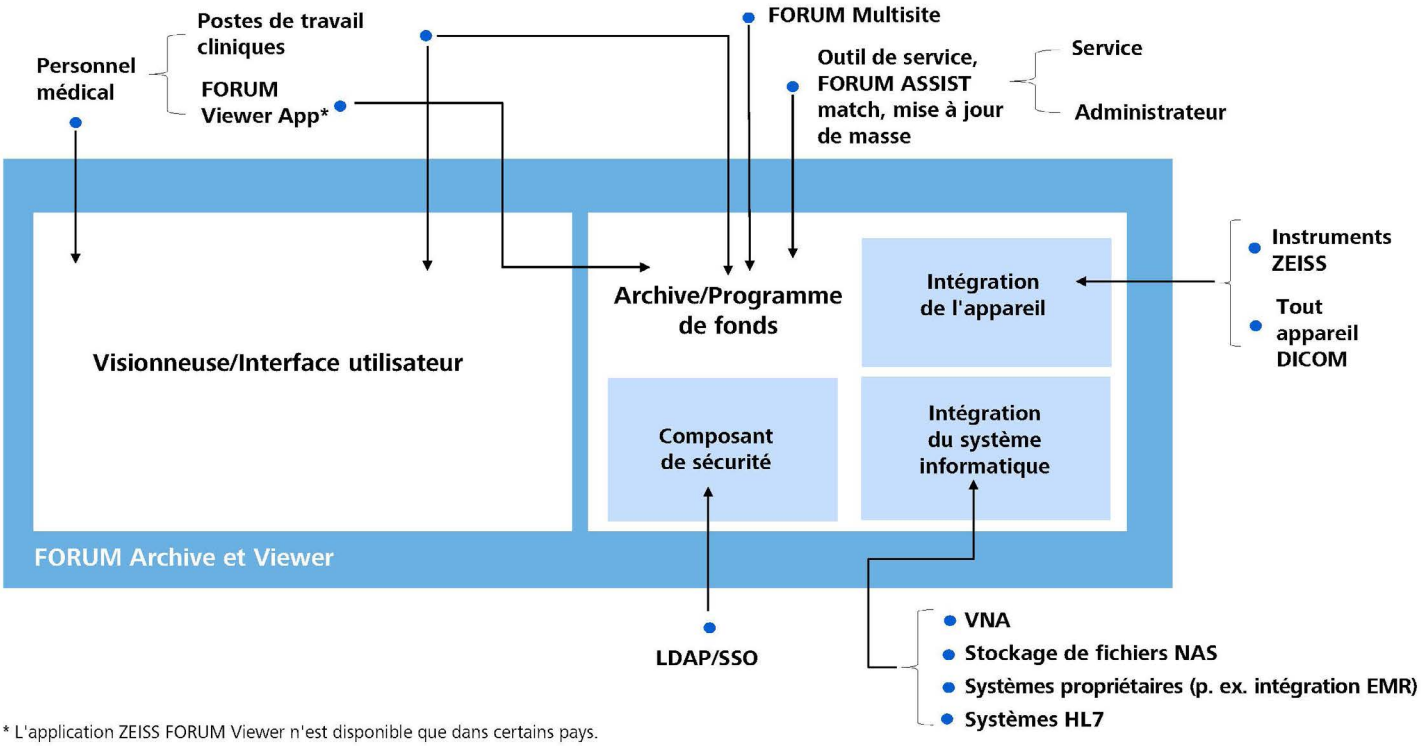
Tout outil standard de sauvegarde peut servir à sauvegarder les données du système FORUM et les données DICOM. Les sauvegardes de la base de données s'effectuent en utilisant la fonctionnalité intégrée, comme expliqué ci-dessus. Une fois qu'une sauvegarde de la base de données est disponible, cette sauvegarde est enregistrable sur des sites secondaires à l'aide d'un outil de sauvegarde du marché.

11. Schéma de l'architecture des dispositifs médicaux

Le schéma suivant montre la « Vue contextuelle » architecturale de FORUM. Cette vue présente les interfaces externes et internes entre FORUM et l'environnement informatique sur un plan conceptuel.

À l'aide de plusieurs interfaces, ZEISS FORUM échange des données avec l'infrastructure environnante.

EMR	HL7
	EMR-XML (format propriétaire ZEISS pour l'échange de données basé sur XML)
Instruments	Le standard DICOM est utilisé pour communiquer avec les appareils ZEISS et/ou des appareils tiers
	FORUM LINK net (encapsuleur DICOM) pour les autres appareils non-DICOM
Archive DICOM	DICOM/HL7
	Fournisseur d'archives neutres (VNA), basé sur DICOM : licence FORUM Hospital IT Integration
FORUM vers FORUM	Transmission DICOM
	Protocole (propriétaire) multisite
FORUM vers Active Directory	LDAP(S) (dans ce cas, la gestion des utilisateurs déléguée à AD)
	Kerberos5 (dans ce cas, la gestion des utilisateurs déléguée à AD)



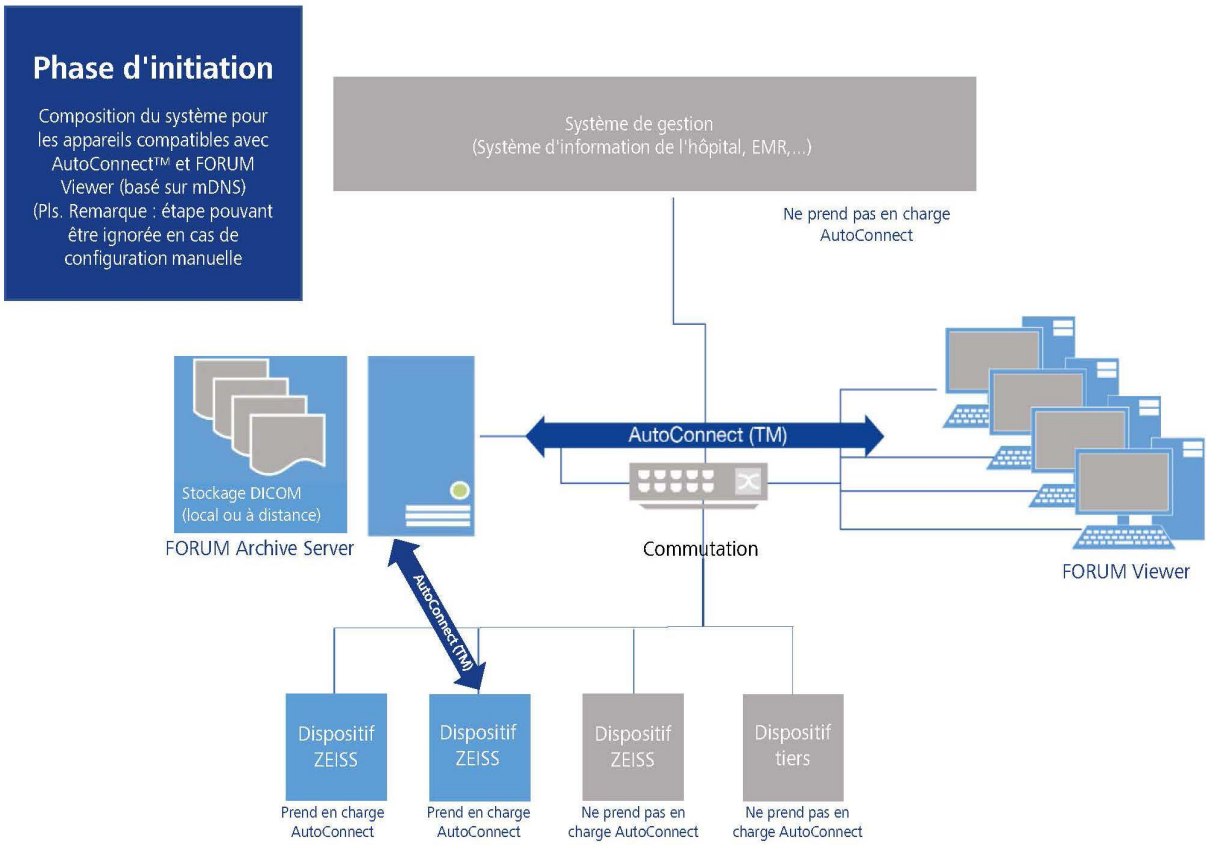
* L'application ZEISS FORUM Viewer n'est disponible que dans certains pays.

Dans un environnement informatique complexe, le déploiement peut être le suivant :

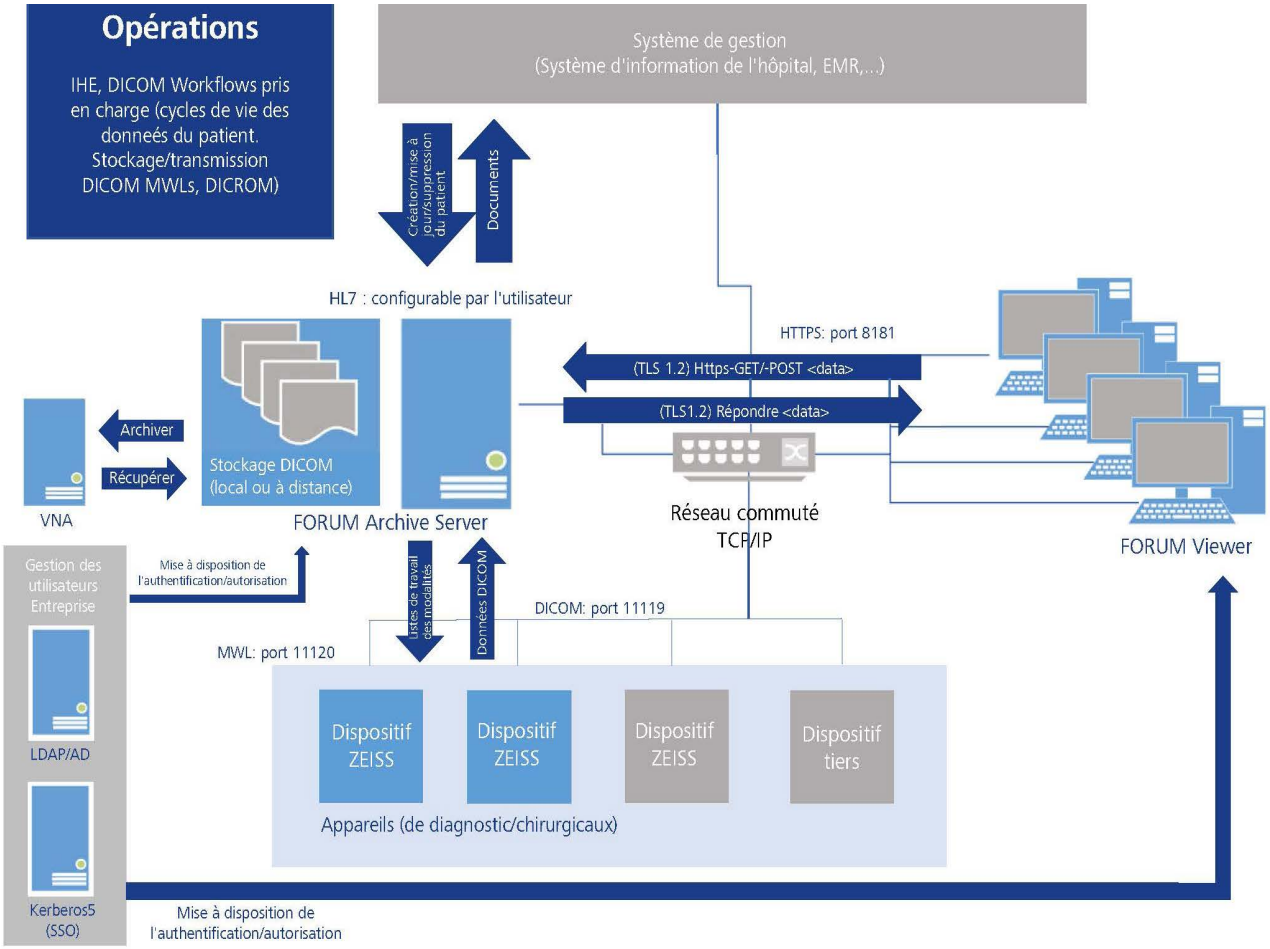
- Un ou plusieurs serveurs couvrant plusieurs sites
- Déploiement fédéré incluant un PACS/VNA
- Couverture de plusieurs réseaux physiques (y compris VPN)
- Connexions de multiples FORUM Viewer
- Multiples instruments connectés
- Intégration avec Active Directory via Kerberos5 ou LDAP(S) (dans ce cas, gestion des utilisateurs déléguée à AD) ; non représenté dans le schéma ci-dessus.

12. Diagramme de topologie physique/logique avec interfaces externes et flux de données

Flux de données pendant la phase d'initialisation du système



Vue opérationnelle :



13. Technologies essentielles

13.1 Technologies de base de FORUM 4.2

- Plate-forme Java 8, mise à jour 121, édition standard RE Binary (intégrée et fournie avec l'application).
- GlassFish 3.1.2.20 (intégré et fourni avec l'application).
- MySQL 5.7.17 Enterprise (intégré et fourni avec l'application).

13.2 Serveur web/application

Site web interne fourni par Glassfish. Utilisé pendant l'installation pour :

- Portail de téléchargement du logiciel client (https://<server-ip>:8181/, offrant des paquets de téléchargement pour le logiciel FORUM Viewer).
- Page unique affichant des informations sur l'état de l'indexation interne après l'installation de la mise à niveau.

Veuillez noter qu'en cours de déploiement, les pages nommées peuvent être bloquées contre l'accès extérieur sans effets secondaires.

13.3 Navigateur web

Aucun.

13.4 Moteur de base de données

Moteurs utilisés :

- MySQL 5.7 Community pour ZEISS FORUM standard
- MySQL 5.7 Enterprise pour FORUM Enterprise installations

La base de données (BD) relationnelle n'est pas exposée à l'utilisateur ou à l'administrateur du système. Un utilisateur spécifique MySQL est utilisé pour la communication entre FORUM Archive (application serveur) et la BD. La BD est « entièrement intégrée » dans l'application. Ainsi, il n'y a aucune relation entre un utilisateur de FORUM (authentifié via la base de données de l'utilisateur local ou Active Directory) et l'utilisateur de la base de données. Tous les audits et les journaux d'accès font partie de l'application serveur et ne sont pas exécutés au niveau de la base de données.

La base de données est intégrée dans ZEISS FORUM et fait partie de l'enregistrement des dispositifs médicaux pour FORUM. En d'autres termes, la BD ne peut être séparée de ZEISS FORUM et aucune base de données préexistante ne peut être utilisée. De plus, un espace disque suffisant doit être disponible sur le lecteur d'installation de FORUM, la BD se développant au fil du temps. Des conseils relatifs à l'espace disque nécessaire sont fournis dans la documentation recommandée sur les spécifications du matériel informatique et la gestion des projets individuels.

13.5 Intégration dans un domaine

ZEISS FORUM 4.2 peut être intégré au serveur qui héberge FORUM en utilisant Active Directory (authentifié via le domaine). Toutefois, les nœuds exécutant FORUM Viewer doivent également être reliés à un domaine si une connexion unique SSO pour les utilisateurs de Windows est souhaitée. Cette disposition peut poser problème aux clients basés sur MacOS. Lors d'une authentification LDAP, l'utilisateur devra saisir des informations d'identification qui seront ensuite vérifiées sur le serveur Active Directory (AD).

ZEISS FORUM 4.2 et les versions ultérieures peuvent être intégrés avec l'authentification unique SSO basée sur Microsoft Active Directory. Cette dernière est basée sur la norme Kerberos v5. Les autres mécanismes SSO ne sont actuellement pas pris en charge. Avec l'authentification unique SSO, l'utilisateur de FORUM Viewer utilise le contexte de session Windows pour s'authentifier aucune fenêtre de connexion n'est donc présentée.

Ces deux mécanismes rendent possible une gestion centralisée de l'administration des utilisateurs. De plus, toute politique de mots de passe peut être mise en œuvre par le biais des politiques d'AD. D'autres configurations liées à l'utilisateur sont également déléguées à l'administration centrale des utilisateurs, comme l'autorisation des utilisateurs et l'attribution des rôles pour les utilisateurs de FORUM, ainsi que les Workplaces cliniques. Les adhésions aux groupes Active Directory servent à définir et à déterminer le niveau d'accès des utilisateurs.

L'intégration LDAP prend en charge une configuration de serveur unique (URL du serveur LDAP). La mise en œuvre actuelle de LDAP ne prend en charge qu'un seul domaine. Les structures de domaines multiples et sécurisées ne sont pas prises en charge avec un seul serveur FORUM. Pour prendre en charge une telle structure de domaine, un serveur FORUM spécifique doit être associé à chaque domaine. Cependant, la solution SSO, basée sur l'implémentation de Kerberos de Microsoft, prend en charge plusieurs sous-domaines dans une seule forêt.

13.6 Autres plateformes prises en charge

Le serveur FORUM Archive est disponible pour la plupart des versions actuelles de Windows 64 bits.

L'application FORUM Viewer est disponible pour les versions MacOS et Windows 64 bits.

La plupart des solutions standard de virtualisation sont prises en charge. Les capacités et détails sont à clarifier entre le client et la gestion de projet ZEISS pendant la phase de création du projet.

13.7 Séparation entre l'application, le serveur web, la BD et le système d'exploitation

- Le système ZEISS FORUM est conçu pour être totalement autonome :
  - Serveur FORUM installé dans un seul dossier
  - Application de base du serveur FORUM
  - Fichiers de licence
  - Fichiers de configuration
  - Fichiers journaux
  - Serveur d'application autonome avec applications FORUM uniquement
  - Base de données MySQL autonome (intégrée) contenant uniquement les tables de base de données FORUM
- Emplacement des fichiers de stockage DICOM sur n'importe quel disque local ou distant. Pour une installation dans une grande structure, un dispositif de stockage dédié est recommandé, de préférence avec chiffrement intégré des données au repos.
- S'il y a lieu : plug-ins de FORUM (Workplaces) installés séparément.

14. Procédures de gestion du cycle de vie et du changement

14.1 Généralités

Le logiciel ZEISS FORUM est qualifié d'appareil de classe II (selon 21 CFR 862-892) et est soumis à diverses réglementations internationales, à des normes harmonisées par l'Union européenne, à des normes reflétant l'état de la technique ainsi qu'à des normes et directives consensuelles reconnues (p. ex. par la FDA ou le MDCG). En outre, la société Carl Zeiss Meditec est soumise à des audits annuels conformément aux normes ISO et aux normes applicables sur les dispositifs médicaux.

En particulier, ZEISS exploite un système de gestion de la qualité (QMS) certifié incluant des procédures opérationnelles standard et des instructions de travail.

Le logiciel FORUM fait par ailleurs l'objet d'audits réguliers portant sur toutes les parties du cycle de vie du produit.

14.2 Détection des vulnérabilités et des faiblesses

ZEISS vérifie périodiquement l'application FORUM à l'aide d'un vérificateur de vulnérabilité standard et fournira une nouvelle version si un nouvel évènement devient critique. Néanmoins, sur décision d'un comité de contrôle des changements, toutes les vulnérabilités potentielles ne sont pas considérées comme critiques et n'appellent donc pas forcément une nouvelle version.

Au cours de son développement, le logiciel est testé à différents niveaux et, dans le cadre du processus de construction continue, il est automatiquement testé à un degré élevé lors de chaque nouvelle version logicielle. Un processus rigoureux d'examen par les pairs garantit la qualité de la conception et de la mise en œuvre de tous les artefacts du produit.

14.3 Actions correctives et préventives (CAPA)

Conformément au règlement sur les dispositifs médicaux et à la directive sur les dispositifs médicaux, Carl Zeiss Meditec applique un processus d'actions préventives correctives (CAPA) certifiant que les problèmes et incidents liés au logiciel sont collectés, évalués et, si nécessaire, intégrés à des actions correctives et préventives. Il s'agit d'un processus à plusieurs niveaux dans lequel un conseil de contrôle des changements établit la marche à suivre.

14.4 Maintenance et correctifs du logiciel

En général, pour FORUM, le rythme annuel de mise sur le marché de nouvelles versions est d'une version principale et de deux mises à jour selon les nécessités de maintenance. En fonction des réglementations internationales, chaque nouvelle version doit être enregistrée auprès des organismes de réglementation nationaux avant d'être disponible dans les différents pays.

Chaque version mettra à jour le logiciel pour prendre en charge les dernières versions des systèmes d'exploitation importants et inclura des mises à jour des logiciels OTS/SOUP (Off-the-Shelf Software/Software of Unknown Provenance) si nécessaire ou obligatoire.

Dans les cas urgents ou critiques, un client peut recevoir un correctif individuel.

14.5 Disparition progressive des anciennes versions

Les versions plus anciennes du logiciel bénéficient d'une assistance pendant plusieurs années. Néanmoins, les clients doivent mettre leur programme à jour régulièrement avec la dernière version du logiciel.

15. Autres remarques

Lors d'une utilisation conjointe de FORUM Viewer avec le logiciel de visualisation ZEISS CIRRUS, deux URL HTTP doivent être accessibles pour permettre à CIRRUS de fonctionner : (1) interface pour la création d'un « temp AE Title » utilisé pour la configuration au niveau DICOM du logiciel de visualisation CIRRUS via FORUM. (2) interface de récupération des licences du logiciel de visualisation CIRRUS via FORUM. Ces deux interfaces ne transfèrent pas de données électroniques de santé, ni d'autres données sensibles. Elles sont utilisées uniquement pour la compatibilité et la configuration (héritée).

Les produits Glaucoma Workplace, Retina Workplace, FORUM ASSIST match, Hospital IT Integration Module et FORUM Viewer App* doivent être mis à niveau avec les dernières versions, les anciennes versions n'étant pas compatibles avec le dernier modèle de sécurité implémenté dans ZEISS FORUM 4.2 et les versions supérieures. Des versions correspondantes pour tous les Workplaces sont disponibles. Les Workplaces plus récents (EQ Mobile et EQ Workplace) ou les extensions (OCT Navigator) sont tous compatibles avec le modèle de sécurité FORUM 4.2. Toute nouvelle version d'un Workplace ou d'une extension est compatible par défaut.

Mars 2021

* L'application ZEISS FORUM Viewer n'est disponible que dans certains pays.