Recommandations Techniques WEB

Complément pour l'hébergement d'applications ISA utilisables à distance via Internet

Le présent document a été mis à jour en date du lundi 9 juillet 2018

Ce document indique les prérequis et contextes d'installation de nos progiciels utilisables à travers Internet pour la grande majorité des cas d'installation actuellement rencontrés.

Ce document complète le document de référence « **Recommandations Techniques »** uniquement pour les extensions de nos applications utilisables via un navigateur internet. Pour les applications utilisables en monoposte ou en réseau, même quand ces applications sont indispensables au fonctionnement de leur extension WEB, il est nécessaire de se référer au document « Recommandations Techniques».

Les cas non mentionnés dans ce document sont considérés exclus de nos prestations.

Merci de nous consulter pour toute précision ou complément.

Avenue des Censives - BP 50333 - 60026 BEAUVAIS Cedex - SAS au capital de 5 100 000 € - 327 733 432 RCS Beauvais

SOMMAIRE

1. PRÉ-REQUIS

Ce document regroupe les pré-requis techniques pour l'utilisation des extensions WEB des logiciels ISA édités par ISAGRI et AGIRIS. Ces pré-requis sont complémentaires à ceux décrits dans le document principal « **Recommandations techniques** » qui intègre également des recommandations générales concernant la sécurité des systèmes et des données. Il est donc important de prendre connaissance de l'ensemble des deux documents qui forment l'ensemble de nos recommandations techniques pour les progiciels.

Ce document ne prend pas en compte les contraintes des autres logiciels ou systèmes pouvant cohabiter avec les logiciels ISA dans une même installation.

L'assistance technique est assurée pour la version actuellement diffusée ainsi que le millésime précédent.

1.1 Configuration logicielle

Les logiciels ISA sont développés exclusivement pour les systèmes d'exploitation de la gamme Microsoft.
L'assistance technique est assurée par nos équipes sur la version actuelle et la version précédente.

1.1.1 Pour le serveur supportant les applications

Le serveur hébergeant les applications doit intégrer les éléments suivants :

- un serveur de fichier sous Microsoft Windows Server 2008 R2 ou plus récent
- le framework Microsoft .NET® version 4.5 ou plus récent
- le logiciel de gestion de base de données Microsoft SQL Server *(la version minimale peut varier selon les logiciels à installer)*, avec un nombre de licences adapté au contexte d'utilisation *(licence non fournie, à acquérir séparément)*
- le service internet IIS v6.0 ou plus récent *(composant Microsoft)*

1.1.2 Pour les postes de travail des utilisateurs finaux

Nos applications web font l'objet de tests, et donc d'une garantie de fonctionnement et d'assistance, uniquement avec les navigateurs internet suivants dans leurs versions les plus récentes :

- Google Chrome®
- Mozilla Firefox®

Pour certaines applications, le navigateur doit être compatible avec l'extension **Silverlight** (Microsoft), qui est proposé en téléchargement gratuit (installation automatique) lors de la première utilisation nécessitant sa présence.

1.2 Configuration Matérielle

1.2.1 Pour les utilisateurs finaux accédant aux applications

Les prérequis matériels sont principalement ceux permettant le bon fonctionnement de la connexion internet et le fonctionnement du navigateur internet. Il est cependant recommandé une résolution écran de 1440x900 pixels ou supérieure.
Le poste utilisateur doit permettre l'installation de Microsoft Silverlight®, nécessaire à la plupart de nos applications Web

1.2.2 Pour les serveurs hébergeant les applications

Disques durs

Il est conseillé de préserver un espace disque disponible supérieur à 10 Go et à 25% de la taille totale du disque (car sur les disques mécaniques on constate une dégradation progressive des performances du disque quand il approche de la saturation)

Pour plus de sécurité, nous conseillons d'utiliser des disques en RAID5. Plus globalement, la redondance des éléments du serveur est conseillée quand la criticité des applications est élevée.

SQL Server

Si Microsoft SQL Server est utilisé par le logiciel, et au-delà de 15 utilisateurs sur un même serveur, un serveur dédié pour Microsoft SQL Server est nécessaire.

Connexion internet

La bande passante disponible doit prendre en compte l'ensemble des applications hébergées, le nombre d'utilisateurs simultanés et les potentielles crêtes d'utilisation. Aucune préconisation de débit ne peut être réalisée sans une étude spécifique.

2. INSTALLATION

La base SQL server peut être installée sur un serveur distinct, accessible depuis le serveur sur lequel sera installée l'application ISA.

Il est préférable d'installer le Microsoft .Net Framework **après** Microsoft IIS pour assurer sa bonne configuration.

Cependant, si IIS a été installé après le .Net Framework, il est nécessaire d'effectuer les manipulations suivantes pour que IIS soit correctement configuré pour comprendre les pages aspx et les services WCF svc.

ÉTAPE 1 : ouvrir une fenêtre de commande (Accessoires)

ÉTAPE 2 : aller dans le dossier « C:\WINDOWS\Microsoft.NET\Framework*version_xxxx* »

ÉTAPE 3 : exécuter la commande « aspnet_regiis.exe –i »

3. SÉCURITÉ ET DISPONIBILITÉ

La sécurité des serveurs proposant des applications via internet doit être mûrement organisée en fonction de la sensibilité des applications et données hébergées, ainsi que du nombre d'utilisateurs potentiels et de la criticité éventuelle des applications.

Une attention particulière sera portée aux plans de maintenance de la base de données et aux sauvegardes, ainsi qu'à l'étendue des horaires d'utilisations. Si ces horaires dépassent les horaires de travail courants, une stratégie (de communication ou de traitement) devra être mise en place pour couvrir les incidents pouvant survenir dans ces plages élargies.

Il est particulièrement recommandé de veiller aux éléments suivants :

- Disponibilité et sécurisation de la ligne internet et des serveurs (sécurité logique, physique et électrique)
- Si les accès aux applicatifs peuvent être externes au VPN de l'entreprise utilisatrice, l'installation du serveur IIS dans une DMZ est indispensable. Dans ce cas, un certificat officiel validé par un organisme reconnu (VeriSign, RSA…) est indispensable pour travailler en mode HTTP**S** et garantir la sécurité du système d'informations