

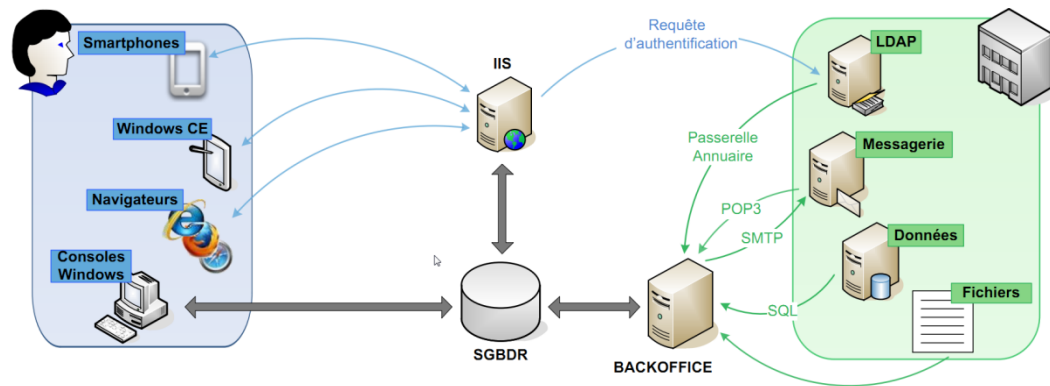
Pré-Requis Cim DataCenter



Table des matières

Serveur Web eDatacenter	2
Serveur Applicatif (Back Office)	3
Console déportée	3
Navigateur compatible Windows	4
Navigateur compatible Mac OS 10.x	4
Navigateur compatible Linux	4
Navigateur compatible iPhone, iPad	4
Navigateur compatible Android	4
Active Directory	4
LDAP	5

Architecture



Pré requis pour les serveurs

Configuration Minimale requise	
Processeur	Multi cœur
Systèmes d'exploitation	Windows 64 bit 2012 R2, 2016, 2019
Mémoire	4 Go
Application	.NET Framework 4.6 ou supérieur

Les processus Cim DataCenter sont multithreads et peuvent exploiter des architectures multiprocesseurs. Dans tous les cas si le serveur de base de données est sur le serveur Cim DataCenter, il nécessite au minimum 2 processeurs logiques, 4 sont souhaitables.

Suivant l'option choisie, la base de données peut être de type :

- SQL Server Express 2017 (elle ne requiert pas de licence).
- Microsoft SQL Server 2017 ou supérieur (une licence est requise).

Serveur Web eDatacenter

Le site web peut être installé sur une machine dédiée si le nombre de clients le nécessite. Vous devrez réinstaller IIS et notre produit dans le cas d'un renommage du serveur. Le serveur doit être dans le domaine pour l'utilisation du Login Universel Implicite.

Serveur Applicatif (Back Office)

Le Back Office est un service qui a pour rôle d'envoyer les mails liés aux alarmes et actions, de recalculer les champs formules et de déclencher les différentes passerelles (LDAP...). Il est notamment nécessaire de pouvoir communiquer avec un serveur SMTP de l'entreprise.

La supervision du backoffice nécessite que les routeurs doivent être perméables au port TCP/IP utilisé par le serveur (par défaut 4148) entre le poste de supervision et la machine hébergeant le BackOffice

Le compte « System » doit disposer des droits tels qu'ils sont positionnés par une installation de Windows par défaut.

Console principale

Il est nécessaire de partager le répertoire d'installation avec les droits de modification pour les utilisateurs des consoles Windows.

Console déportée

Configuration Minimale requise	
Processeur	I3
Systèmes d'exploitation	Windows 7 32/64 bit Windows 8 32/64 bit Windows 10 32/64 bit
Mémoire	512 Mo
Réseau	Bande passante maximale et garantie de type 100 Mbits vers la base de données ET la console principale, ainsi qu'une réponse au ping inférieure à 5 ms et stable

L'export « Excel » génère un fichier au format SLK. Il est ouvert par l'application définie dans Windows pour ouvrir ces extensions de fichiers. Si Open Office est installé sur la machine, l'export « Excel » ouvre le tableur de Open Office.

L'export « Word » génère un fichier au format RTF. Il est ouvert par l'application définie dans Windows pour ouvrir ces extensions de fichiers.

Navigateur sur les postes clients

- ✓ Les navigateurs doivent autoriser les cookies.
-

- ✓ le fonctionnement d'autres navigateurs ou d'autres versions de navigateur n'est pas garanti

Navigateur compatible Windows

- Internet Explorer 9, 10 11 et plus
- Edge
- Firefox 3.6 et +
- Chrome 9 et +

Navigateur compatible Mac OS 10.x

- Safari 4 et +
- Firefox 3.6 et +

Navigateur compatible Linux

- Firefox 3.6 et +

Navigateur compatible iPhone, iPad

- Safari

Navigateur compatible Android

- Chrome

Login Universel Implicite (LUI)

Active Directory

Lui exploité dans un contexte active directory permet d'utiliser les pièces d'identité Windows, et évitant de demander le compte et le mot de passe de l'utilisateur. Néanmoins pour que cela fonctionne correctement il est nécessaire que :

- Pour Windows : La machine ET le compte courant fassent partie du domaine AD exploité par la règle.
 - Pour le web :
 - La machine ET le compte courant fassent partie du domaine AD exploité par la règle
 - Le mode challenge/response soit activé sur le serveur Web ET les permissions correctement définie sur les composants du site Apsynet.
 - Il n'existe pas de filtrage par proxy ou firewall des échanges Windows.
-

- Sous Internet Explorer et Chrome l'authentification Windows est transmise automatiquement au serveur IIS. Les autres navigateurs ne disposent pas de cette fonction. Par conséquent ils vous demanderont l'authentification Windows à fournir à IIS à l'ouverture du site web

LDAP

Le fonctionnement LDAP ne permet pas de reprendre les pièces d'identités existantes sur le client, de même que pour des raisons de sécurité nous ne stockons pas les mots de passe saisis. L'identification fonctionne donc de la manière suivante : Le compte est demandé la première fois et stocké, mais éditable pour les connexions futures.

- Pour Windows Le mot de passe est systématiquement demandé.
 - Pour le web L'utilisateur peut choisir de mémoriser son mot de passe au niveau du navigateur, mais cela reste de sa décision.
-