

Cloud Computing et SaaS

On a vu fleurir ces derniers temps un grand nombre de sigles.

L'un des premiers est SaaS, Software as a Service, sur lequel nous aurons l'occasion de revenir.

Mais il y en a beaucoup d'autres...

- SaaS : *Software* as a Service
- VaaS : *Video* as a Service
- IaaS : *Infrastructure* as a Service
- PaaS : *Platform* as a Service
- CaaS : *Communication* as a Service
- ...

Finalement, quelqu'un a « frappé » (comme dirait les anglais) le terme XaaS, pour [Quelque chose] as a Service

Evidemment, tout le monde a envie de le comprendre comme [Mes problèmes] as a Service. Mais peut-on penser les choses de cette façon ?

Les technologies à la base du Cloud Computing et du SaaS

Par essence, le terme de *service* désigne quelque chose d'immatériel.

Pour toutes les fonctions liées au matériel, il faut donc les rendre indépendantes d'un matériel spécifique. En d'autres termes, il faut donc les « virtualiser »

La virtualisation va donc consister à s'abstraire d'un matériel spécifique, pour pouvoir, en théorie tout au moins, exécuter la fonction sur n'importe quelle machine.

La virtualisation est donc un préalable pour toutes les fonctions serveur liées au matériel.

Par ailleurs s'il y a, bien sûr un sens usuel (et relativement ancien) au terme de

« service », les expressions comme « On Demand » ou « as a Service » sont très liées à la

diffusion de l'Internet. De manière implicite, l'accès au « service » va se faire pour les utilisateurs au travers d'un *navigateur Internet*, c'est-à-dire un *client web*. En

conséquence, les fonctions d'accès client doivent reposer sur des technologies web. Les technologies web sont donc nécessaires pour toutes les fonctions d'accès client au système.

Nous avons donc les deux prérequis. Mais ce que nous allons voir, c'est que loin de n'être que des prérequis, ces capacités apportent *en elles-mêmes* les plus grands bénéfices pour le contrôle industriel.

Des gains immédiats pour le contrôle industriel grâce aux technologies Web

Pour l'illustrer, commençons par un exemple plutôt agréable...

Pour la préparation du champagne, il y a deux fermentations : la fermentation alcoolique, classique pour tous les vins, et une deuxième fermentation ou prise de mousse, où agissent les levures. Cette seconde fermentation se déroule lentement, durant plusieurs semaines, voire plusieurs mois, à basse température (10 à 12°C). Elle est particulièrement critique et quelques degrés en plus ou en moins peuvent altérer irrémédiablement la qualité du Champagne...

Durant ces phases critiques, des exigences sont prévues pour les responsables qualité du champagne.



Figure 1 : Le contrôle à distance grâce aux technologies web

L'accessibilité Web permet le contrôle à distance, en temps réel, de la température de chaque cuve de l'installation. Elle évite au personnel de se déplacer et permet une plus grande réactivité en cas de problème, puisqu'on peut agir immédiatement sur l'installation.

Les bénéfices de la virtualisation

Voyons maintenant les bénéfices de la virtualisation...

Plaçons-nous dans le cadre d'une usine, comprenant par exemple cinq ateliers.

L'approche la plus courante (que vous voyez ici) est souvent dictée par l'histoire (on équipe les ateliers les uns après les autres) et par la volonté de préserver l'autonomie de fonctionnement de chacun des ateliers. On a donc un serveur par atelier et plusieurs clients qui y sont reliés (les connexions entre les clients et le serveur ne sont pas représentées pour simplifier le schéma).

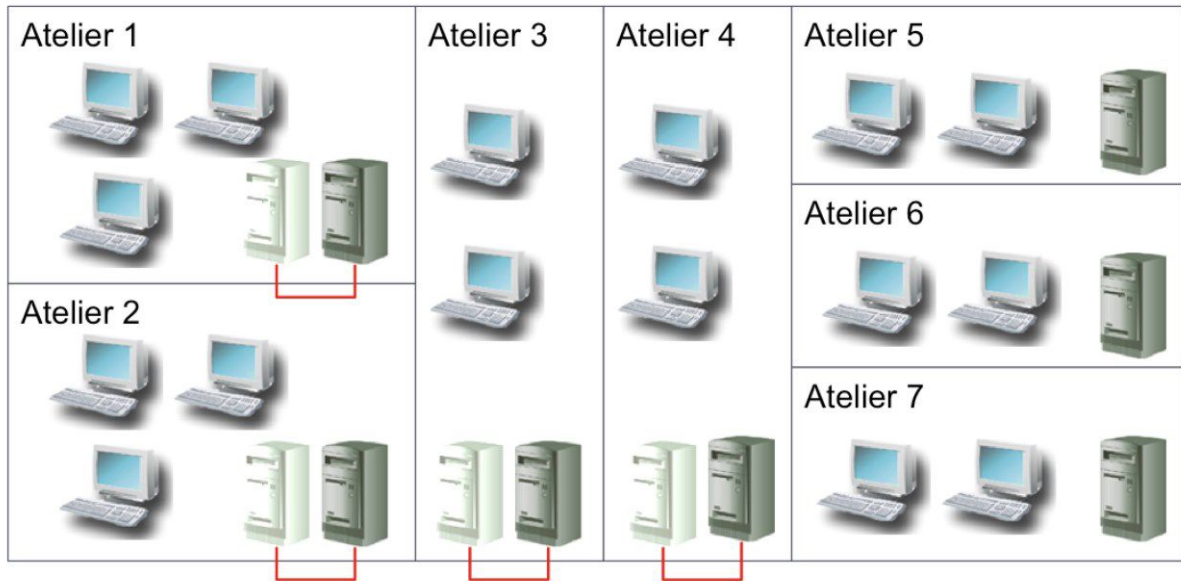


Figure 2a : Architecture classique de contrôle de plusieurs ateliers

Beaucoup de sites produisent en 24/24, voire 7/7 et la disponibilité du système de production est essentielle. Il est donc courant que l'on adjoigne des serveurs redondants pour les ateliers critiques.

Dans une telle installation, les ateliers sont indépendants, un peu trop d'ailleurs :

- Les postes d'un atelier ne permettent pas d'être informé de ce qui se passe dans les autres
- Le process de production englobe généralement plusieurs ateliers, la continuité du process repose sur des procédures organisationnelles manuelles
- La traçabilité d'ensemble ne peut pas être automatisée et nécessite dans le meilleur des cas une consolidation a posteriori

En mettant en œuvre une architecture dite « multi-tiers », avec un serveur d'application et une plateforme logicielle commune, on fournit une bonne solution à ce problème :

- Pas d'installation spécifique sur chaque poste
- La plateforme et les services déployés autorisent l'accès aux autres ateliers
- Un process d'ensemble est envisageable
- Une traçabilité automatisée de bout en bout devient possible

Mais l'architecture, très déployée, est plus complexe en termes d'administration.

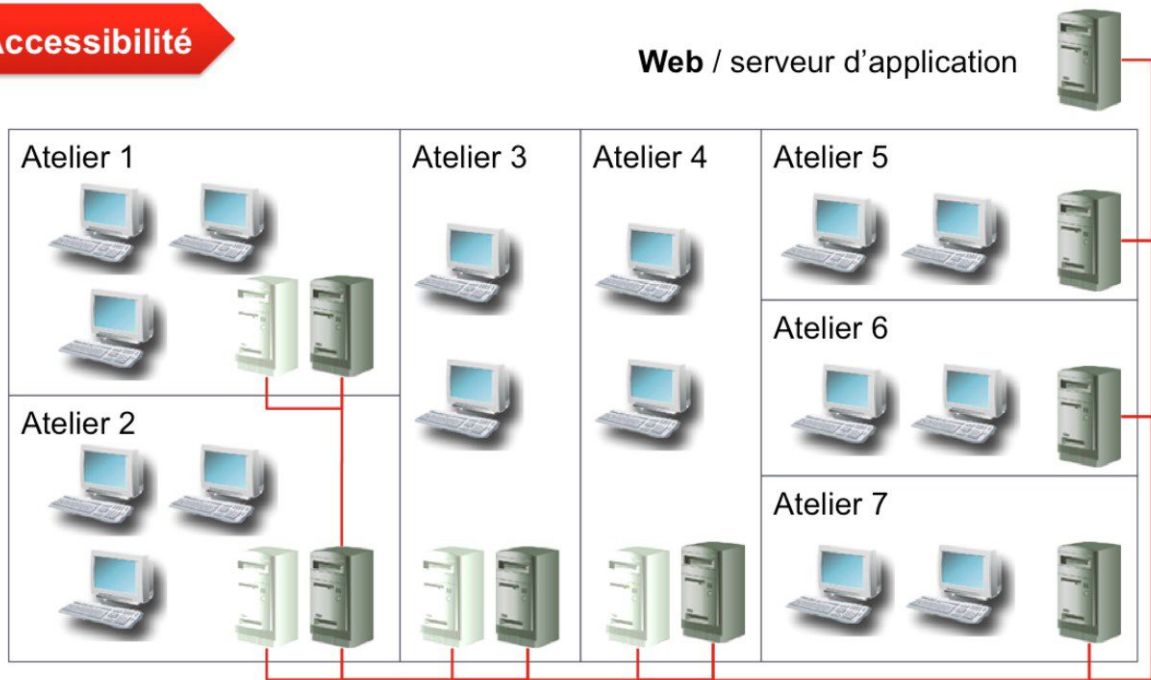


Figure 2b : Architecture multi-tiers de contrôle de plusieurs ateliers

La virtualisation permet de ramener une architecture déployée à une architecture centralisée

- Meilleure maîtrise de la granularité (celle-ci n'est plus liée à la géographie du site, mais plutôt au découpage logique du process)
- Préservation de l'étanchéité entre les blocs
- Rapidité et robustesse des communications
- MTFB accru

Dans le milieu industriel, une production 24/24 7/7 est courante. Si le système pilote effectivement l'installation en temps réel, ce qui est encore plus vrai si la solution inclut la supervision, la disponibilité du système est essentielle.

En plus de la maîtrise de la complexité, l'architecture virtualisée présentée permet d'augmenter la disponibilité. En milieu industriel, on met peu en œuvre des techniques comme le *load balancing*, mais plutôt la redondance et la réplication. Comme il est clair qu'il est beaucoup plus facile dans ce type d'architecture de prévoir la redondance d'un service, on la mettra plus souvent en œuvre, augmentant ainsi la disponibilité.

Accessibilité

Maîtrise de la complexité

Disponibilité

Evolutivité

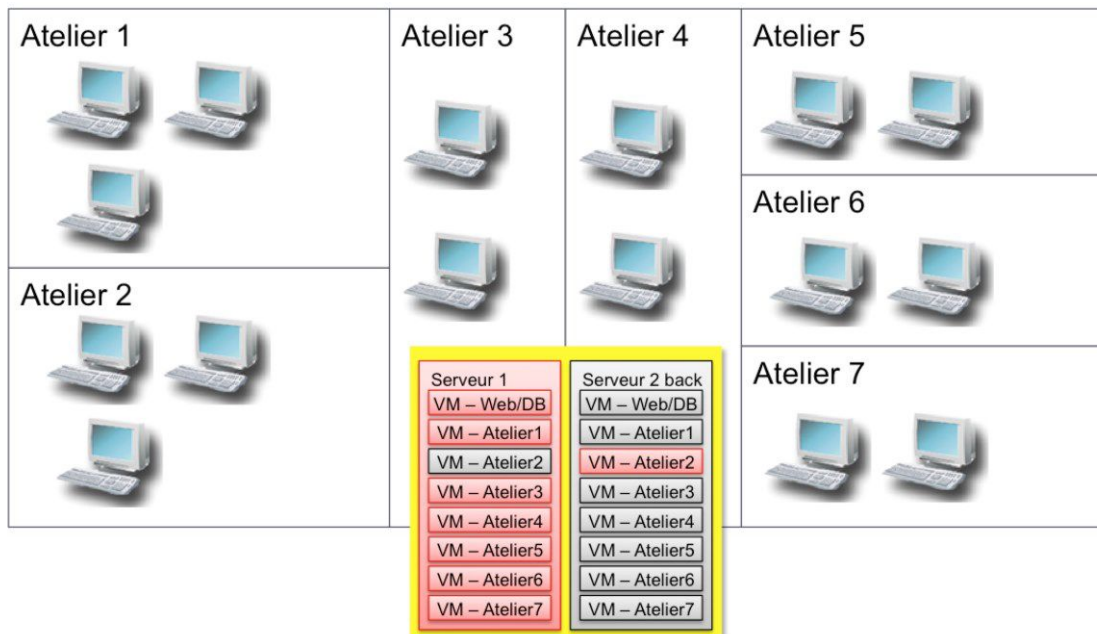


Figure 2c : Architecture multi-tiers virtualisée de contrôle de plusieurs ateliers

L'informatique évolue en permanence, et les systèmes d'exploitation, les bases de données, les protocoles réseau, évoluent régulièrement.

Les industriels ne sont généralement pas friands de la dernière version en date mais sont parfois confrontés à la nécessité d'évoluer sous la contrainte.

En fait, la virtualisation, en diminuant le temps d'installation d'un nouvel environnement, va faciliter cette évolution, mais elle permettra aussi dans certains cas de continuer à faire fonctionner dans une machine virtuelle une version particulière de système d'exploitation, quand celui-ci est requis.

Il ne faut pas négliger non plus l'aspect coût. Pour les grandes infrastructures informatiques, les économies au niveau du matériel, en particulier des serveurs, sont la raison principale du passage à la virtualisation. La raison en est simple : chaque serveur est en moyenne exploité à 5% de ses capacités. En virtualisant les serveurs, on peut regrouper une dizaine de serveurs sur un seul tout en conservant une réserve de puissance suffisante.

Même si ces chiffres sont à modifier dans le cas du contrôle industriel, où il n'est pas rare que les serveurs soient utilisés entre 30% et 50% de leur capacité le gain est indéniable.

Et si l'on décide de ne pas réduire les budgets matériels, on peut mieux les utiliser, par exemple en dotant le serveur de disques RAID à 10000 ou 15000 tours, qui accroissent la performance et la disponibilité matérielle.

Mettre l'usine dans les nuages ?

Alors, pourquoi ne pas aller plus loin et ☐ mettre l'usine dans les nuages ☐ ?

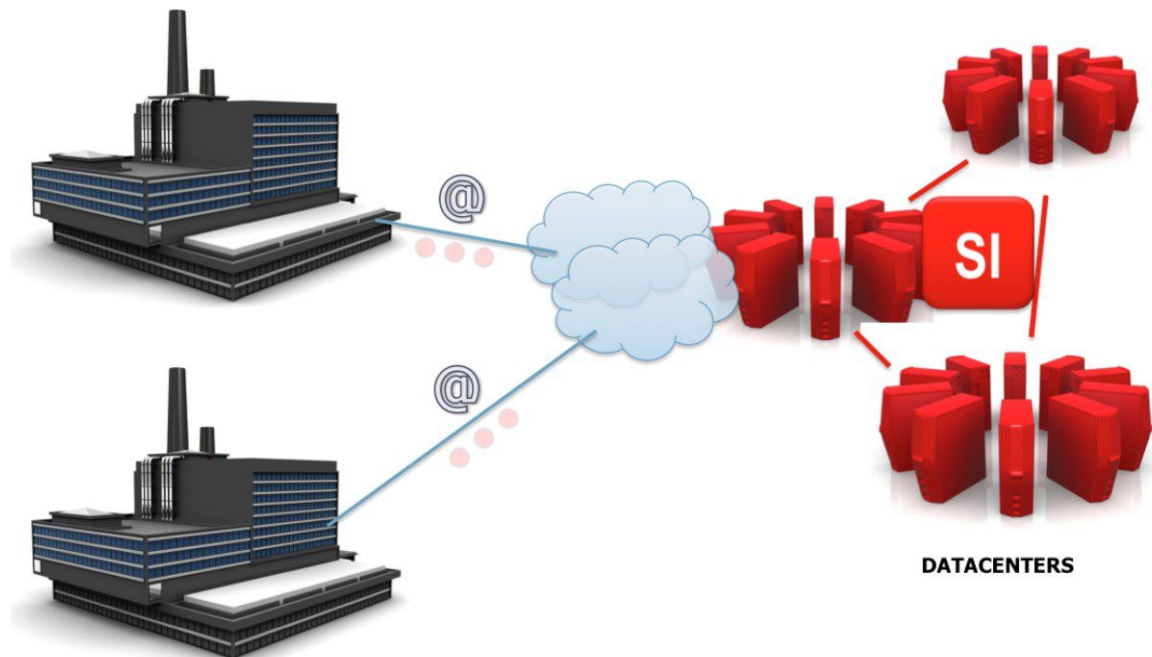


Figure 3 : Schéma de principe d'une application industrielle en « cloud »

La première difficulté est la collecte des informations des capteurs. Disons-le tout net, les technologies dont nous parlons ont été conçues pour les applications de gestion, où l'entrée d'informations s'effectue essentiellement par saisie manuelle. Cela peut être le cas dans l'industrie, mais une bonne partie des informations, et en particulier les informations de supervision, est collectée de manière automatique, sur les automates programmables qui pilotent les installations ou sur des capteurs intelligents. Les uns comme les autres n'ont pas encore de « prises web » qui leur permettrait de nourrir directement une application distante, même si le protocole TCP/IP s'est imposé de plus en plus.

La seconde difficulté est de disposer d'une installation homologuée par les différents fournisseurs

Le fonctionnement dans un environnement virtualisé est *théoriquement* identique à celui de l'environnement matériel et logiciel (système d'exploitation) équivalent. C'est évidemment le *théoriquement* qui est important. Cela nécessite une validation ou une homologation par le fournisseur des logiciels concernés. C'est le cas par exemple de notre logiciel de Supervision/MES COOX (validé sur VMware et VirtualBox), mais tous les éditeurs, et surtout les constructeurs d'automates n'assurent pas le fonctionnement de leur logiciel sur plateforme virtualisée.

Le troisième point tient aux performances.

Les systèmes virtualisés accordent des bandes passantes limitées (partiellement paramétrables) pour les connexions entre les serveurs virtuels. Le fait que ces échanges s'effectuent au sein du même serveur physique semble a priori un avantage pour les débits, mais cet avantage est contrebalancé par l'absence d'un hardware « intelligent »

depuis pour chaque connexion, prenant en charge la gestion du protocole. Dans un système virtualisé les connexions entre serveurs internes sont gérées par le logiciel. Dans le milieu industriel, l'interface logicielle la plus courante avec les automatismes est OPC. Lancé par Microsoft en 1995, ce standard s'est rapidement diffusé dans le monde industriel en même temps que Windows. Aujourd'hui, la plupart des constructeurs d'automatismes privilégient cette interface pour les logiciels de supervision et de MES. Prenons l'exemple d'un serveur d'atelier qui doit historiser des informations sur un serveur de base de données : les informations collectées par l'atelier sont disponibles au niveau du serveur OPC du serveur d'atelier.

OPC s'appuie sur l'interface Microsoft de communication COM/DCOM. Entre deux serveurs, la liaison la plus « naturelle » est la connexion d'un client OPC au serveur OPC distant au travers du protocole DCOM. Conçu à l'origine pour des objets complexes, et des flux d'échanges limités, le protocole DCOM n'est pas particulièrement adapté à des flux de notifications importants. Il constitue souvent un goulot d'étranglement dans les architectures distribuées.

Solution classique

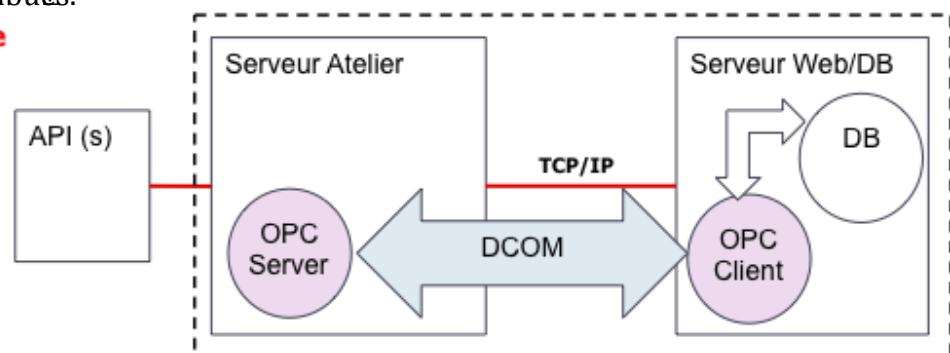


Figure 4a : Dialogue OPC interserveur classique

On peut améliorer considérablement les performances en effectuant plutôt la connexion inter-serveur avec une encapsulation réduite du protocole TCP/IP : COOX utilise par exemple une sérialisation d'un événement standard du Java. Le dialogue OPC s'effectue sur base COM, beaucoup moins gourmande que l'échange DCOM, car elle s'effectue au sein d'un même serveur virtuel.

Solution hautes performances

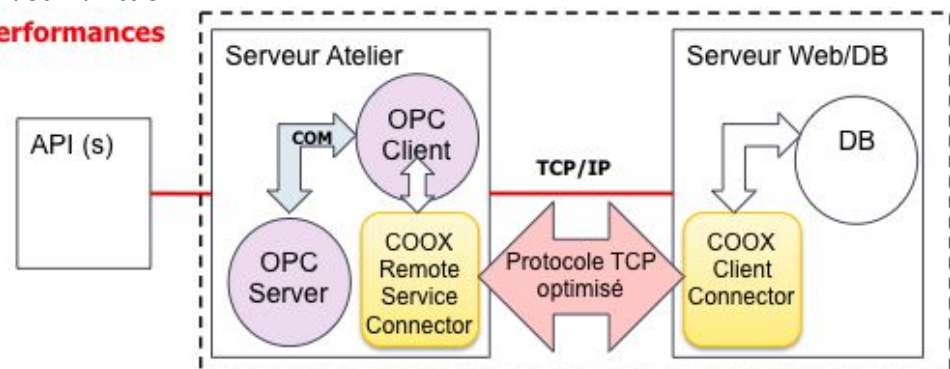


Figure 4b : Dialogue OPC interserveur optimisé

Si on s'intéresse cette fois aux clients, c'est-à-dire à l'accès web, il faut s'intéresser aux performances temps réel de ces technologies. C'est particulièrement vrai pour la supervision.

- Les pages HTML 1.0 d'origine sont statiques, et exigent un rafraichissement de la page qui n'est pas compatible avec le temps réel

- Les technologies AJAX, ou web 2.0 utilisant souvent le JavaScript comme langage sur le client permettent une animation temps réel avec un nombre d'objets raisonnable à l'écran.
- Le langage Java, et les clients riches en applet ou Java Web Start autorisent un très haut niveau de performance avec un grand nombre d'objets (c'est souvent le cas dans des synoptiques de supervision), en même temps qu'un fonctionnement très similaire à des clients Windows classiques.

Une dernière difficulté, et non des moindres, est la protection de l'installation dans l'hypothèse d'une externalisation des données.

A plusieurs reprises, des intrusions malveillantes sur des installations industrielles telles que des centrales nucléaires ont montré la fragilité des systèmes vis-à-vis d'une attaque terroriste. L'industriel doit aussi protéger son savoir faire. Comment bâtir et assurer la confiance avec un prestataire qui sera amené à le détenir ? Des contrats de confidentialité suffisent-ils ?

On peut aussi se poser la question de l'intérêt que doit y trouver le prestataire. Or pour qu'il y ait un intérêt pour lui à prendre à sa charge le fonctionnement tendu des applications, il faut qu'il y ait une mutualisation importante de celles-ci. Pour des besoins un peu tendus dans le domaine du contrôle industriel (supervision et MES), cela ne paraît pas particulièrement simple.

Il est probable que se développe en fait une approche fonction par fonction, les fonctions les plus universelles (on peut penser à l'archivage par exemple) étant par exemple transférées au niveau du Cloud, avec des avantages significatifs au niveau du coût et de la disponibilité.

Conclusion

Les technologies informatiques sont prêtes et même matures, pour la virtualisation et le SaaS. Sans qu'il soit nécessaire d'aller d'emblée vers la mise « sur le cloud » de l'ensemble des applications de supervision et de MES, le contrôle industriel peut tirer de larges bénéfices de la virtualisation et des technologies web, et tant les constructeurs d'automatismes que les éditeurs de logiciels se doivent de prendre en compte ces technologies.