PcVue - Architectures & déploiement

Dernière mise à jour :	Sept. 2022
Révision :	11
Contenu :	Contient les différentes architectures et solutions de déploiement PcVue
Confidentialité :	Publique

Les informations contenues dans ce document sont susceptibles d'être modifiées sans préavis et ne représentent pas un engagement de la part de l'éditeur. Le logiciel décrit dans ce manuel est fourni en vertu d'un accord de licence et ne peut être utilisé ou copié conformément aux termes de cet accord. Il est illégal de copier le logiciel sur tout support, sauf autorisation spécifique dans le contrat de licence. Aucune partie de ce manuel ne peut être reproduite ou transmise sous quelque forme ou par tout moyen, sans l'autorisation expresse de l'éditeur. L'auteur et l'éditeur ne garantissent en aucun cas l'exhaustivité ou l'exactitude du contenu de ce document et n'acceptent aucune responsabilité de quelque nature, y compris mais sans s'y limiter à la performance, la qualité marchande, ou l'adéquation à un usage particulier, ou des pertes ou dommages de toute nature causés ou prétendument causés directement ou indirectement par ce document. En particulier, les informations contenues dans ce document ne se substituent pas aux instructions de l'éditeur des produits. Ce document peut contenir des informations appartenant à des tiers. Ces informations sont à usage exclusivement interne et ne visent pas à être divulgués.
En outre, cet avis ne constitue pas une demande de propriété sur les informations appartenant à des tiers. Tous les noms de produits et marques mentionnés dans ce document appartiennent à leurs propriétaires respectifs.

PcVue Solutions

Sommaire

1. GENERALITES 2

1.1 ARCHITECTURES 3
1.2 ROLES 3
1.3 BRIQUES D'ARCHITECTURE 5
1.3.1 Légende 5

2. EXEMPLES D'ARCHITECTURES 8

2.1 POSTE AUTONOME 9
2.2 MULTI-POSTES 11
2.3 MULTI-POSTES AVEC UN SERVEUR DE SESSIONS BUREAU A DISTANCE POUR LES POSTES CLIENTS 12
2.4 HAUTE DISPONIBILITE 13
2.4.1 Redondance temps réel 14
2.4.2 Mode Serveur d'Acquisition Actif Unique 14
2.4.3 Redondance d'archives. 16
2.4.4 Redondance de serveurs d'accès à distance 18
2.5 SERVEUR MUTUALISE 19
2.6 MULTI-NIVEAUX 20
2.6.1 Multi-niveaux: implémentation #1 21
2.6.2 Multi-niveaux: implémentation #2 23
2.7 ARCHITECTURES CLOUD 25
2.7.1 Architecture #1: Interopérabilité Cloud 25
2.7.2 Architecture #2: Hypervision CLOUD 27
2.7.3 Architecture #3: CLOUD hybride 29
2.8 POSTE DE DEVELOPPEMENT ET GESTION CENTRALE DE VERSION 31
2.9 ARCHITECTURES D'ACCES A DISTANCE 32
2.9.1 EasyMobileTechnology 33
2.9.2 Console de déploiement Web 33
2.9.3 Clients Web & mobile 35
2.9.4 Bureau d'accès à distance 39
2.9.5 Architecture #1: Déploiement "tout-en-un" 40
2.9.6 Architecture #2: Ségrégation réseau et DMZ 43
2.9.7 Architecture #3: Scénario NAT simplifié pour l'accès à distance 47
2.10 ARCHITECTURE MIXTE 50
2.11 VIRTUALISATION 52
2.11.1 Virtualisation d'application 52
2.11.2 Virtualisation de ressources 53
2.11.3 Example d'implementation 53

3. GLOSSAIRE 54

Arc Informatique - © Copyright 2022. Tous droits réservés.

1. Généralités

Cette section contient des explications sur les options qui s'offrent à vous pour déployer le Superviseur.
Le déploiement consiste à allouer des rôles aux postes de travail et aux serveurs, dans une architecture réseau physique donnée, afin de satisfaire les besoins.
Dans le cadre de cette section, il est considéré que le Superviseur assure les fonctions principales suivantes:

• **Acquisition de données** - Collecte des données temps-réel, représentant des valeurs physiques ou calculées, en utilisant un protocole de communication tel que Modbus, OPC...
• **Archivage de données** - L'enregistrement des données temps-réel afin de pouvoir les mettre à disposition ensuite du Superviseur lui-même ou d'applications tierces.
• **Alarmes** - Déclenchement et gestion des alarmes.
• **IHM** - Interface Homme Machine. L'interface graphique de présentation des données qui permet aux opérateurs d'interagir avec le système supervisé.
• **Multiposte**. L'ensemble des mécanismes par lesquels le Superviseur échange des données temps réel et historiques entre les postes d'un système en réseau.
• **Web Server extensions**. Un ensemble de composants utilisés pour interfacer le Coeur de l'architecture du Superviseur avec les clients web.
• **Interfaces avec les systèmes tiers** - Tels que GMAO, SIG, ERP, MES...

L'allocation des fonctions et des rôles ne peut pas être faite indépendamment des choix de licences. Pour plus d'informations sur les licences, contactez votre interlocuteur commercial.

Arc Informatique - © Copyright 2022. Tous droits réservés.

1.1 Architectures

Les architectures typiques sont les suivantes:
• **Poste autonome** - Toutes les fonctions SCADA sont assurées par un seul poste.
• **Architecture multiposte** - Les fonctions SCADA sont partagées entre 2 postes ou plus, dans une architecture client/serveur.
• **Architecture haute disponibilité** - Les fonctions et les rôles sont distribuées pour offrir une meilleure résilience et une capacité à monter en charge. De tels déploiements multipostes peuvent inclure:

- La redondance de l'acquisition de données - 2 serveurs ou plus sont configurés en redondance (hot standby).
- La redondance de l'archivage - 2 serveurs ou plus sont configurés en redondance (hot standby).
- Serveurs mutualisés.

• **Architecture 3 niveaux** - En utilisant un ou plusieurs postes comme passerelle.
• **Station d'ingénierie** avec gestion de version.
• **Web & mobile** - Serveur Web et Clients Web & mobiles.

1.2 Rôles

Les architectures ci-dessus requièrent l'allocation des rôles suivants:

Acquisition de données
• Communication avec les équipements de terrain,
• Production des données temps-réel et des alarmes,
• Fourniture des données temps réel et les alarmes aux autres postes.

Archivage
• Consommation des données temps-réel et des alarmes produites par d'autres postes,
• Gestion du stockage, de l'enregistrement et du replay des données archivées,
• Gestion des connexions aux SGBD,
• Fourniture des données historiques aux autres postes.

Serveur Web
• Consommation des données temps-réel et des alarmes produites par d'autres postes,
• Consommation des données historiques produites par d'autres postes,
• Gestion de l'interface avec IIS,
• Fourniture des données au clients Web, notamment les clients WebVue, les clients TouchVue, le WebScheduler et les clients du Web Services Toolkit.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Passerelle

• Pour le transfert de données sécurisé entre 2 réseaux,
• Consommation des données temps-réel, des alarmes et des historiques produits par d'autres postes sur un réseau,
• Fourniture des données temps-réel, des alarmes et des historiques à des postes sur un autre réseau.

IHM

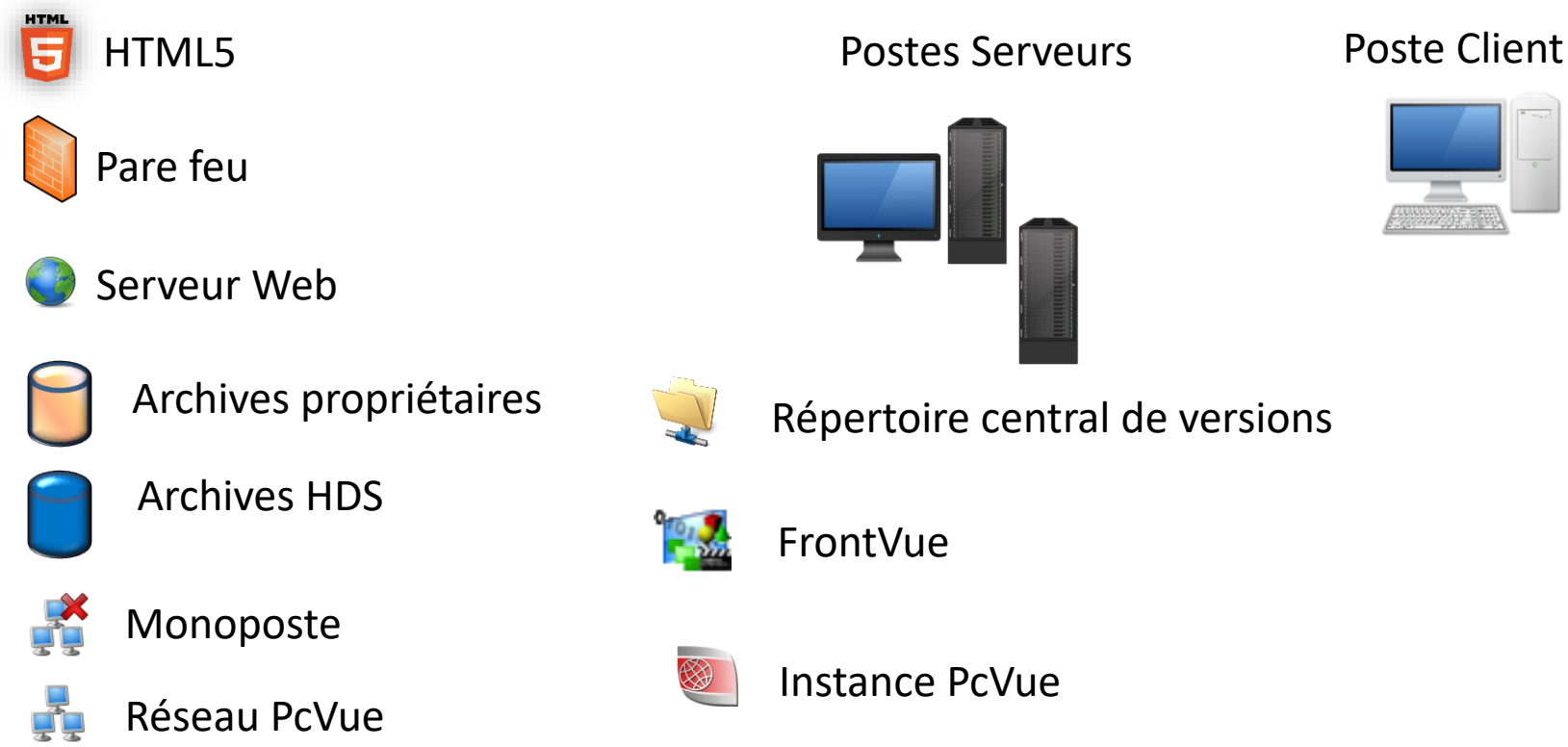
• Affichage de synoptiques, d'objets graphiques, de fenêtres d'alarmes, de fenêtres de consignation, de fenêtres de tendance... aux opérateurs

En fonction des combinaisons de rôles, les postes du Superviseur ont vocation à être déployés sur un système d'exploitation desktop ou serveur.
Voir le tableau ci-dessous pour plus d'informations.

Arc Informatique - © Copyright 2022. Tous droits réservés.

1.3 Briques d'architecture

1.3.1 Légende



Arc Informatique - © Copyright 2022. All rights reserved.

Brique	Rôles typiques	Mode de déploiement typique
Mono-poste	• Acquisition de données • Archivage • IHM • Ne peut pas échanger des données avec d'autres postes	• En tant qu'application interactive • Sur un système d'exploitation desktop
SCADA station	• Acquisition de données • Historical data • IHM	• En tant qu'application interactive si elle nécessite un IHM • Sur un système d'exploitation desktop Ou • Comme un Service Windows si un IHM n'est pas nécessaire • Sur un système d'exploitation Serveur
Data acquisition server	• Acquisition de données	• Comme un Service Windows • Sur un système d'exploitation Serveur
Client station	• IHM	• En tant qu'application interactive • Sur un système d'exploitation desktop Ou • Sur un système d'exploitation serveur hébergeant les Services Bureau à distance combiné avec des terminaux légers utilisés comme postes opérateur
Historical data server	• Données d'historiques	• Comme un Service Windows • Sur un système d'exploitation Serveur
Web server	• Serveur Web	• Comme un Service Windows • Sur un système d'exploitation Serveur
Web clients	• Surveillance déportée et contrôle par Internet ou Intranet • Clients WebVue et Clients TouchVue	• Utilisation d'un navigateur Web ou d'une application Web • Sur un PC en session Bureau à distance ou un équipement mobile

Arc Informatique - © Copyright 2022. Tous droits réservés.

Station d'ingénierie

- Selon l'architecture et la conception du projet car un poste Engineering peut avoir différents rôles, allant de celui de Serveur d'acquisition de données (pour tester une communication avec des champs équipement) au Serveur d'archives ou juste un poste de travail IHM (pour la conception de synoptiques)
- Projet de développement et de maintenance
- Gestion de versions de projets et de bibliothèques
- Interopérabilité avec des outils tiers.
- En tant qu'application interactive
- Sur un système d'exploitation desktop

Arc Informatique - © Copyright 2022. Tous droits réservés.

2. Exemples d'Architectures

Ce chapitre décrit les architectures de base les plus communes. Il existe de nombreuses variantes pour s'adapter aux exigences du système en terme de :

- Nombre d'utilisateurs
- Type et nombre de postes opérateur (IHM)
- Disponibilité
- Flexibilité
- Evolutivité
- Résilience
- Maintenance et gestion du cycle de vie des applications

Pour plus d'informations, vous pouvez contacter votre support technique.

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.1 Poste autonome

- ✓ L'architecture la plus simple
- ✓ Pour exploiter votre procédé depuis un poste unique « tout-en-un »
- ✓ Toutes les performances d'un poste PcVue pour une architecture mono-poste

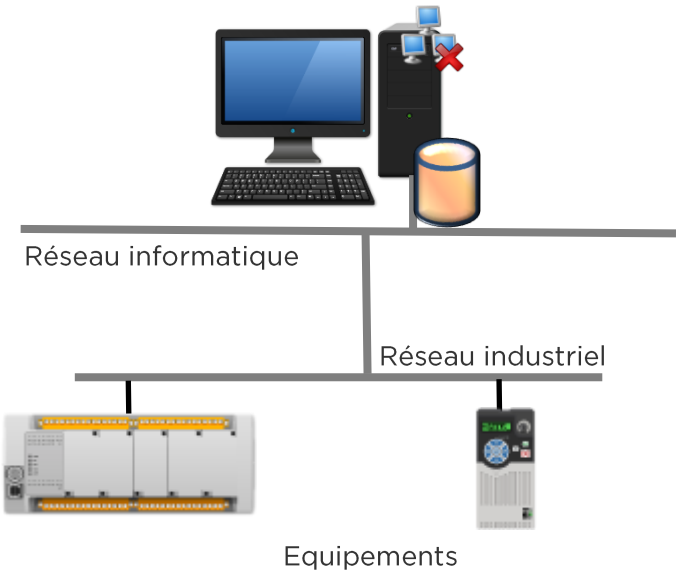


Figure 1 - Poste autonome

Les postes autonomes sont généralement des panels opérateur, c'est l'architecture la plus simple avec tous les rôles et fonctions intégrés dans un seul poste.
Dans une configuration traditionnelle monoposte, le superviseur gère l'ensemble des données automates ainsi que les opérations de contrôle-commande opérateur. PcVue supporte une base de données de plusieurs dizaines de milliers de variables sur un seul poste.
Le poste PcVue HMI est un poste unique qui inclut toutes les fonctionnalités de la supervision :

- ✓ Acquisition des données,
- ✓ Base de données,
- ✓ IHM,
- ✓ Archivage,
- ✓ Alarmes et historiques,
- ✓ Tendances,

Arc Informatique - © Copyright 2022. Tous droits réservés.

- ✓ Traitement des données, rapports
- ✓ Gestion utilisateurs

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.2 Multi-postes

- ✓ L'architecture multiposte la plus simple
- ✓ Votre procédé peut être exploité depuis plusieurs postes opérateurs distants
- ✓ La charge sur le réseau informatique est optimisée

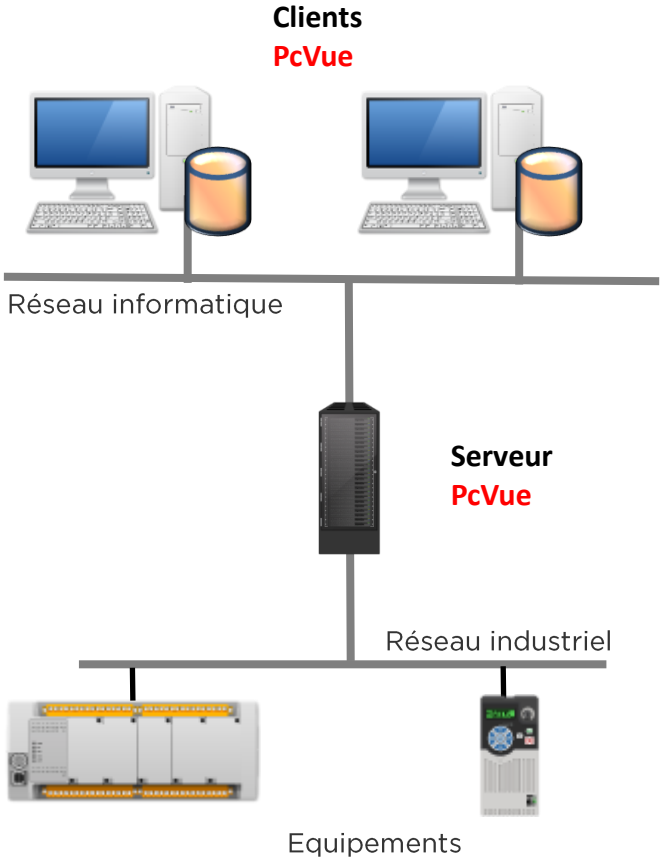


Figure 2 - Multi-postes

L'architecture Client-Serveur est la solution la plus simple pour les applications nécessitant plusieurs postes opérateurs, mais avec une seule connexion aux réseaux industriels.
Le serveur est une source de données (producteur) qui communique avec les automates et diffuse les informations vers les postes clients (consommateurs). La communication inter postes TCP/IP native de PcVue fonctionne en mode événementiel et transmet par paquets les informations significatives.
Le poste Serveur peut être un poste d'exploitation ou un simple Frontal de communication. Il exécute tous les traitements communs à l'application. Les données historisées peuvent être centralisées sur le serveur seulement, ou être locales à chaque client.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Un Client peut se connecter via un service accès distant à un Serveur situé dans un autre lieu géographique. Une liaison par ligne téléphonique spécialisée, RTC,3G/4G,ADSL, ou même satellite est possible.
Une variante usuelle est de séparer l'Acquisition de données et la production des données historiques sur deux serveurs différents ou que les clients produisent les données historiques localement.

2.3 Multi-postes avec un Serveur de sessions Bureau à distance pour les postes clients

- ✓ Pour réduire les efforts d'administration
- ✓ Faible coût des postes clients banalisés
- ✓ Pas d'installation sur les postes banalisés

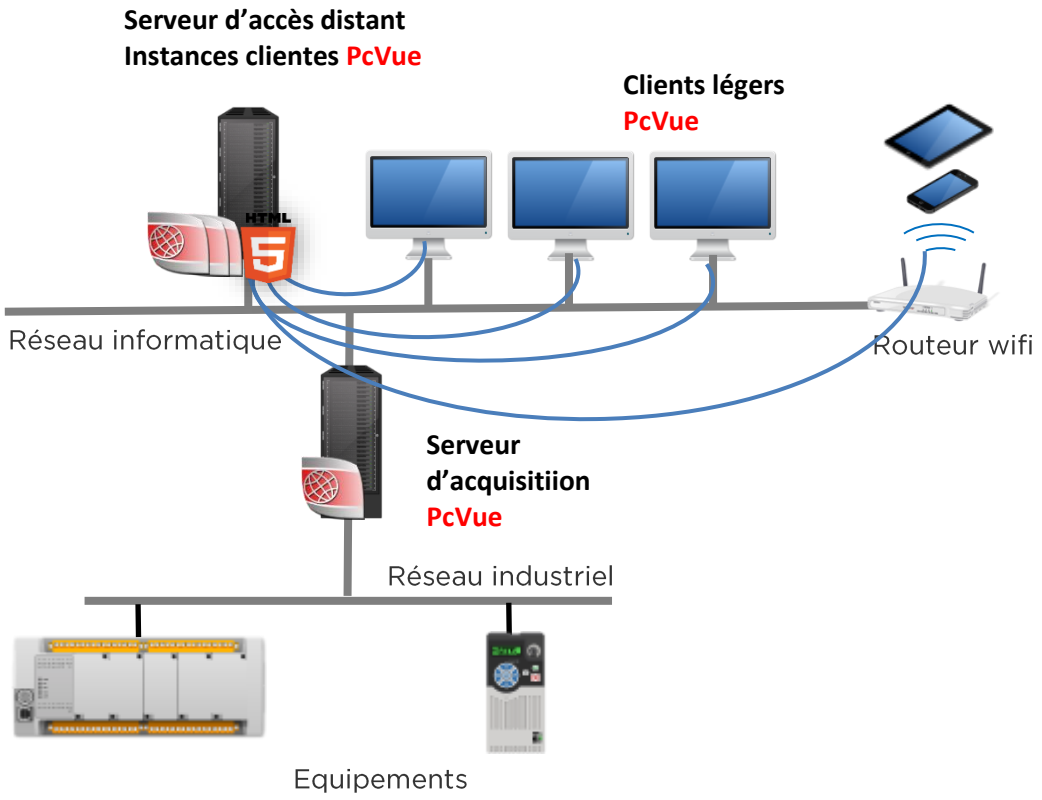


Figure 3 - Bureau à distance

Cette architecture, est la même que la précédente d'un point de vue réseau du Superviseur, excepté l'usage de sessions Bureau à distance et de terminaux légers qui permettent de rationaliser le déploiement des postes clients.
Afin de faciliter l'administration des postes clients PcVue, un client PcVue est hébergé sur un poste Windows Server, configuré pour servir de serveur de bureau à distance

Arc Informatique - © Copyright 2022. Tous droits réservés.

(aussi appelé Remote Desktop Server – RDS). Depuis un terminal banalisé, incluant tablettes et smartphone, il est possible d'ouvrir une session sur ce poste RDS et de lancer une instance du Client PcVue. Une interface installée sur le serveur permet l'usage de terminaux supportant HTML5.
Les terminaux banalisés ne nécessitent aucune installation particulière, ce qui facilite le déploiement de l'application sur site.
Des logiciels gérant le protocole de bureau à distance (aussi appelé Remote Desktop Protocol – RDP) sont disponibles pour des terminaux type Wyse sous Linux ou Unix.

2.4 Haute disponibilité

- ✓ Très haut niveau de sécurisation et de disponibilité du système et des données
- ✓ Architecture Client-Serveur sécurisée avec réseaux dupliqués

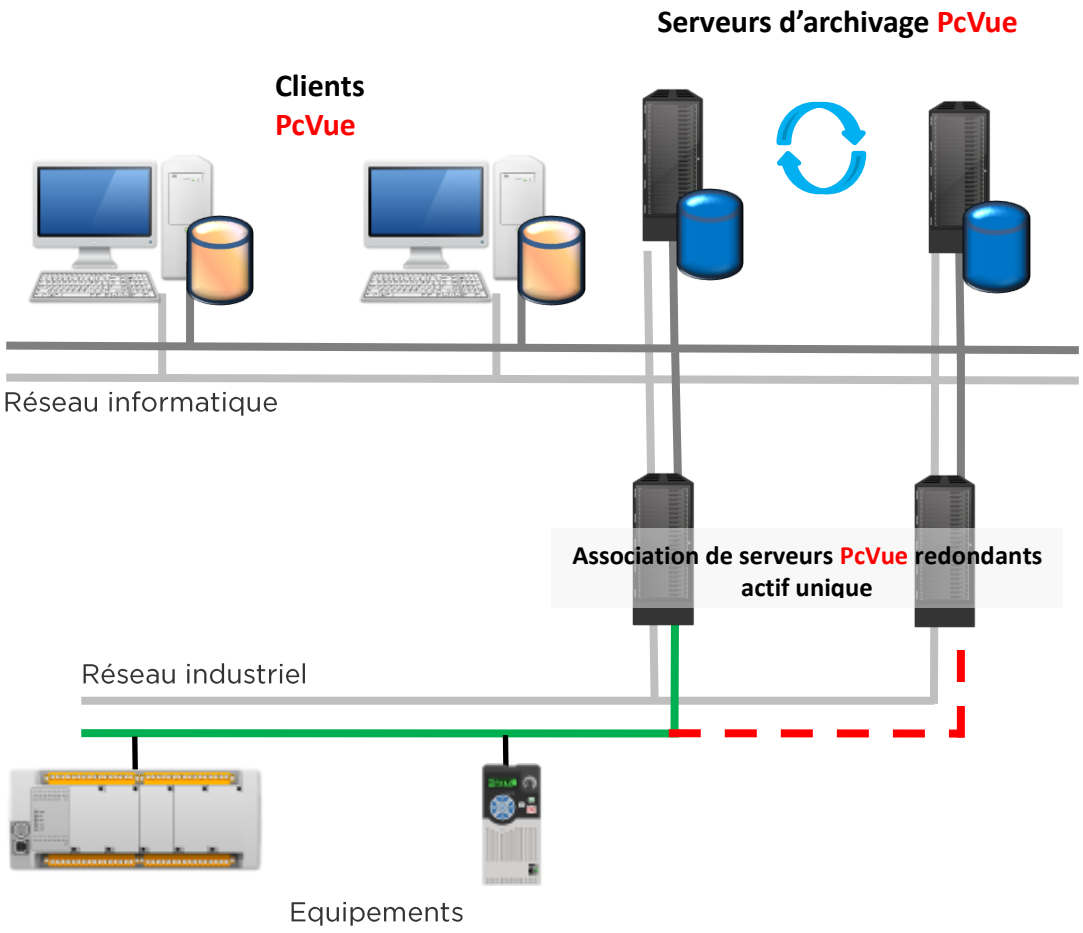


Figure 4 - Haute disponibilité

Arc Informatique - © Copyright 2022. Tous droits réservés.

Lorsqu'une plus grande disponibilité et de la résilience sont nécessaires, cette architecture, plus distribuée, apporte la redondance et la séparation des rôles.
Elle est similaire à l'architecture multi-postes mais avec des serveurs d'acquisition de données et des serveurs de données historiques séparés et redondants.
Il est ainsi possible de doubler le réseau local informatique et/ou le réseau industriel (bi médium) afin d'accéder depuis un poste client, aux informations des automates via deux réseaux entièrement indépendants.
Chaque poste client PcVue maintient 2 connexions avec chaque poste serveur et n'essaiera de changer de serveur que lorsque ces 2 connexions seront mauvaises.
Sur réseau industriel Ethernet, PcVue gère également la redondance de médium et la redondance d'automate.
Chaque poste peut archiver les données localement dans différents formats assurant ainsi une grande disponibilité des données archivées.
Une variation usuelle est d'inclure également un Serveur et des clients Web, combinant ainsi des postes opérateur permanents et des accès utilisateurs ponctuels.

2.4.1 Redondance temps réel

Les serveurs sont dédiés à l'acquisition sur les automates et mettent à jour en temps réel les informations (base de données) des postes clients. Les postes clients disposent des interfaces graphiques pour la conduite de l'installation.
Les 2 serveurs sont redondants entre eux et alimentent les postes client du site.

2.4.2 Mode Serveur d'Acquisition Actif Unique

Les serveurs fonctionnent en mode **Serveur d'Acquisition Actif Unique**. Le serveur qui communique avec le réseau industriel est appelé « actif ». L'autre serveur est appelé « passif ». Seul le serveur actif gère les communications sur les systèmes automates, alimente les postes clients et synchronise le serveur passif.
En cas de défaillance du serveur actif, le serveur passif active ses communications avec les systèmes d'acquisition et alimente les postes clients. Le basculement se fait à chaud et de façon totalement transparente pour les opérateurs.
Lors du démarrage d'un serveur, il y a deux scénarios possibles :

- L'autre serveur ne fonctionne pas. Le nouveau serveur amorce la communication sur le réseau industriel afin de rafraîchir ses variables Équipement et il devient le serveur actif. Tous les Clients du réseau y sont automatiquement abonnés.
- L'autre serveur est déjà en fonctionnement et actif. Le nouveau serveur devient automatiquement passif et il se synchronise à son tour sur le serveur actif.

Lorsqu'un serveur passif devient actif, la reprise de communication sur le réseau industriel est immédiate, ce qui rend instantanément opérationnel le nouveau serveur actif.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Les postes clients sont alimentés de manière événementielle et automatique par le serveur actif à l'instant T. Pour l'opérateur l'accès aux informations (contrôle/commande/acquittement/archive...) est identique depuis n'importe quel poste; il y a une totale transparence sur l'origine des données quel que soit l'état du réseau. Suivant les profils utilisateur, il est possible depuis n'importe quel poste client d'accéder à tout ou partie des informations du site.
Depuis n'importe quel poste, il est possible de connaître l'état de l'ensemble des postes du réseau et des communications sur les systèmes d'acquisition. Le système fournit un schéma complet de l'architecture avec une visualisation en temps réel des automates et superviseurs qui y sont raccordés.
Le système permet pour des questions de maintenance, et suivant autorisation, d'agir sur l'état du réseau (par exemple : forcer un serveur passif à devenir actif).

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.4.3 Redondance d'archives.

2.4.3.1 Mode avec 2 bases de données d'archives synchronisées

Les 2 serveurs sont également serveurs d'historiques de façon à historiser les informations en parallèle sur 2 Bases de Données Relationnelles SQLServer distinctes.
Les deux serveurs enregistrent simultanément les mêmes informations.
Les informations antérieures plage de dates configurable sont automatiquement purgées . De cette manière la taille de la base de données est maîtrisée, ce qui garantit les meilleurs temps d'accès possible en regard de la « profondeur » d'historique souhaitée.
Les enregistrements purgés peuvent-être récupérés dans des fichiers ASCII pour être « backupés » si nécessaire.
Périodiquement une consolidation automatique des informations manquantes est faite pour gérer les cas d'arrêts (panne ou maintenance). Cette consolidation est faite de manière croisée : le 1er serveur récupère ses historiques manquants sur le 2ème serveur et inversement. À la fin de la consolidation les Bases de Données Relationnelles sont identiques.
La consolidation s'exécute en parallèle des accès standard sur la Base (lecture ou écriture) et des communications.
Chaque Client de supervision accède de manière transparente aux historiques du serveur actif et dispose ainsi en permanence depuis n'importe quel poste client à un archivage continu.

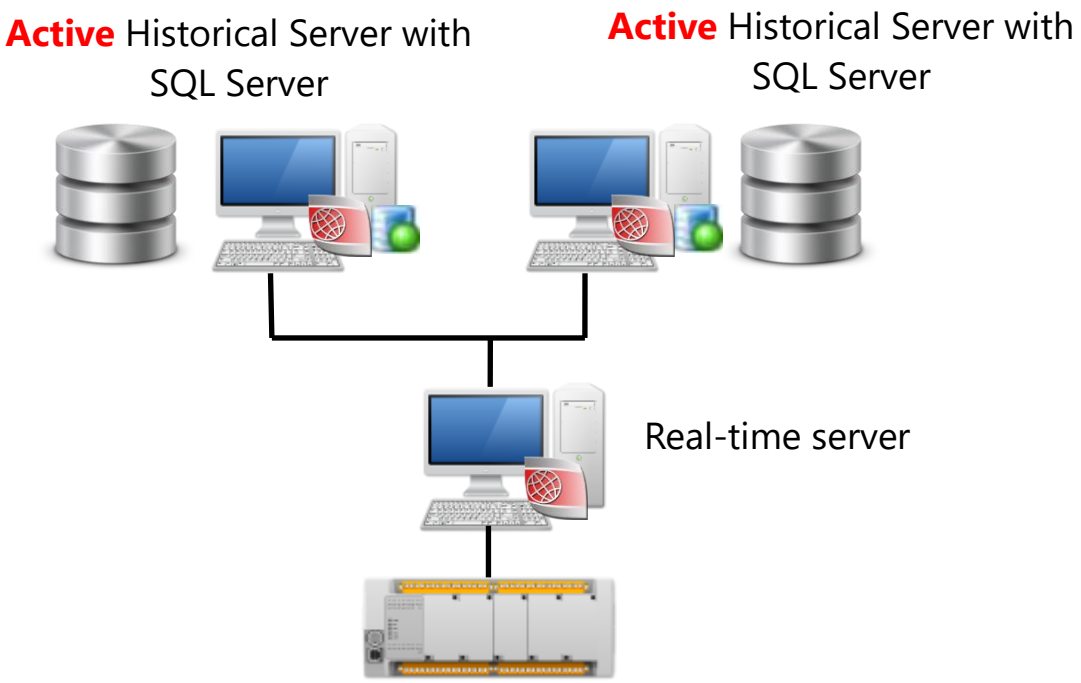


Figure 5 – Redondance

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.4.3.2 Mode avec 1 seule base de données d'archives

Le principe consiste à disposer d'une machine (de type Windows Server de préférence) qui héberge la base de données et le moteur SQL Server et qui est différente des 2 serveurs temps réel PcVue.
Suivant le principe de serveur actif unique décrit précédemment, seul le serveur actif PcVue enregistre les informations dans la base de données. Ainsi dans tous les cas il y a toujours au moins un serveur qui archive les informations.
Si le serveur qui héberge la base de données est défaillant, le serveur actif PcVue enregistre les informations en local. Au retour de la connexion avec la base de données SQL Server, le serveur actif transfère les archives générées en local dans la base de données centrale.
L'ensemble de ses fonctions intégrée permet de garantir une continuité d'archivage à partir du moment ou au moins un des serveurs PcVue est disponible.

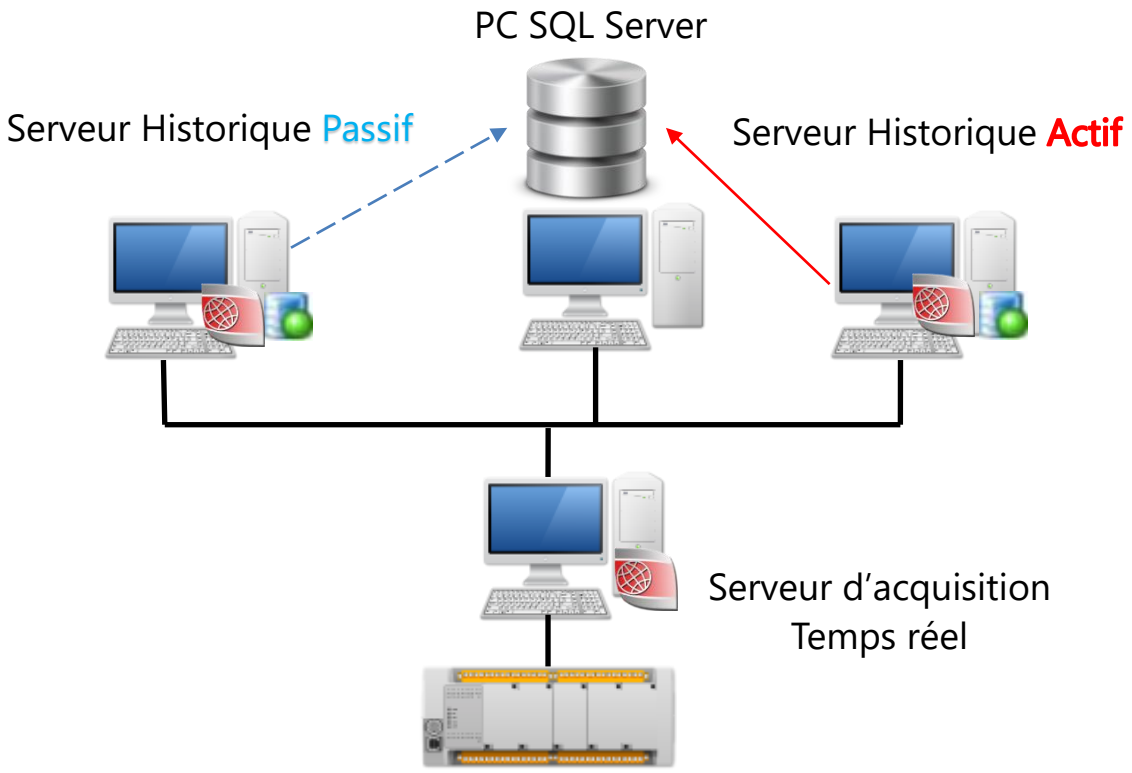


Figure 6 – Redondance

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.4.4 Redondance de serveurs d'accès à distance

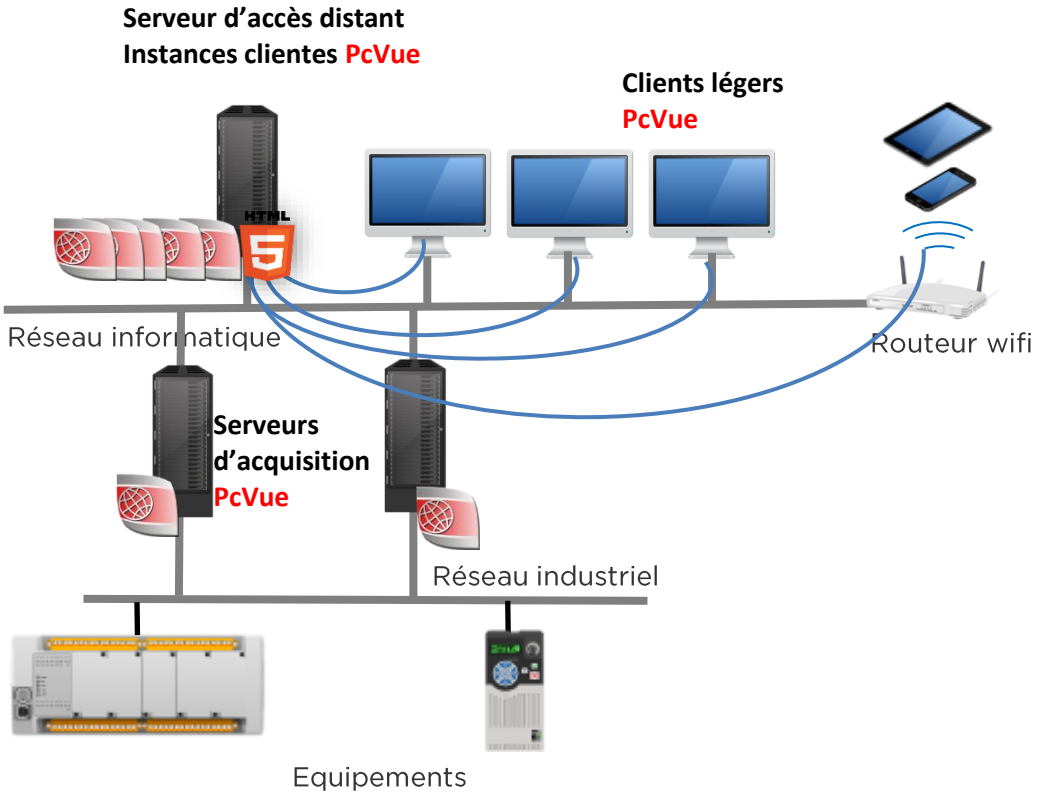


Figure 7 – Redondance RDS

Dans cette architecture la redondance est assurée par les 2 postes serveurs d'acquisition.
L'accès à distance est assuré par un poste serveur Windows avec le rôle.
Le basculement est géré automatiquement par PcVue au niveau des serveurs d'acquisition.

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.5 Serveur mutualisé

- ✓ Architecture redondante optimisée pour la supervision de plusieurs procédés
- ✓ Réduit l'effort de déploiement et de maintenance

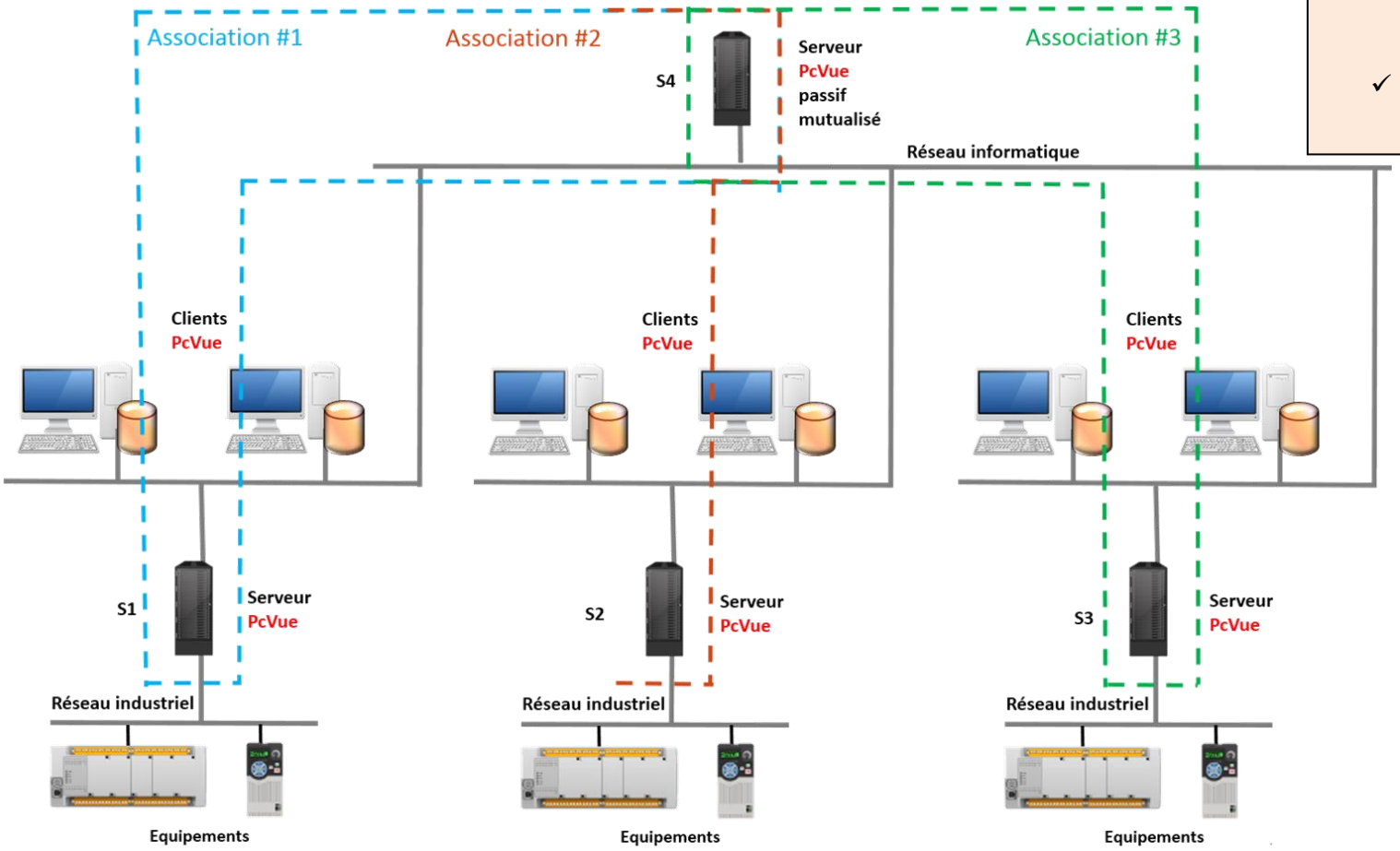


Figure 8 - Serveur mutualisé

Arc Informatique - © Copyright 2022. Tous droits réservés.

L'architecture mutualisée est une variante intéressante de la haute disponibilité. Lorsque vous surveillez et contrôlez plusieurs processus, lignes de production, usines, bâtiments, sites ... et pouvez bénéficier d'un réseau WAN fiable, vous pouvez mettre en place un serveur performant qui sera utilisé comme serveur de secours pour plusieurs ilots. En mutualisant le serveur de secours, vous obtenez la redondance et la disponibilité tout en réduisant les coûts de déploiement et de maintenance d'un ensemble de serveurs redondants dans chaque ilot.

Ce type d'architecture n'est pas compatible avec tous les protocoles de communication. Veuillez consulter le support technique pour plus d'informations.

2.6 Multi-niveaux

Lorsque vous êtes préoccupés par la segmentation de réseau, une passerelle peut être ajoutée à l'architecture.
Une telle architecture est utile lorsque, par exemple, le système est distribué sur un réseau étendu ou lorsque les consommateurs de données (postes client ou dépôt de données) sont localisés sur un réseau de moindre confiance.
Une telle passerelle peut être déployée dans une DMZ et, si nécessaire, les passerelles peuvent être redondantes.
Dans une architecture multi-niveau chaque poste peut être source de données (producteur) pour certaines variables et consommateur pour d'autres. En outre, certains postes peuvent servir de concentrateur de données pour un centre de contrôle situé dans une autre zone géographique.
PcVue permet le développement et le déploiement d'applications multi serveurs/multi clients dans lesquelles les diverses associations de serveurs sont configurées pour permettre à certaines d'entre elles d'être le point d'acquisition primaire des données issues des équipements terrain, et à d'autres d'acquérir les données depuis d'autres serveurs, comme le font les postes clients.
De plus, les serveurs centraux ne collectent qu'une partie des données, permettant la supervision optimisée des équipements terrain depuis le centre de contrôle.

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.6.1 Multi-niveaux: implémentation #1

- ✓ Pour les applications de grande ampleur et les systèmes répartis sur de vastes zones géographiques
- ✓ Différents niveaux d'exploitation
- ✓ Architecture très flexible

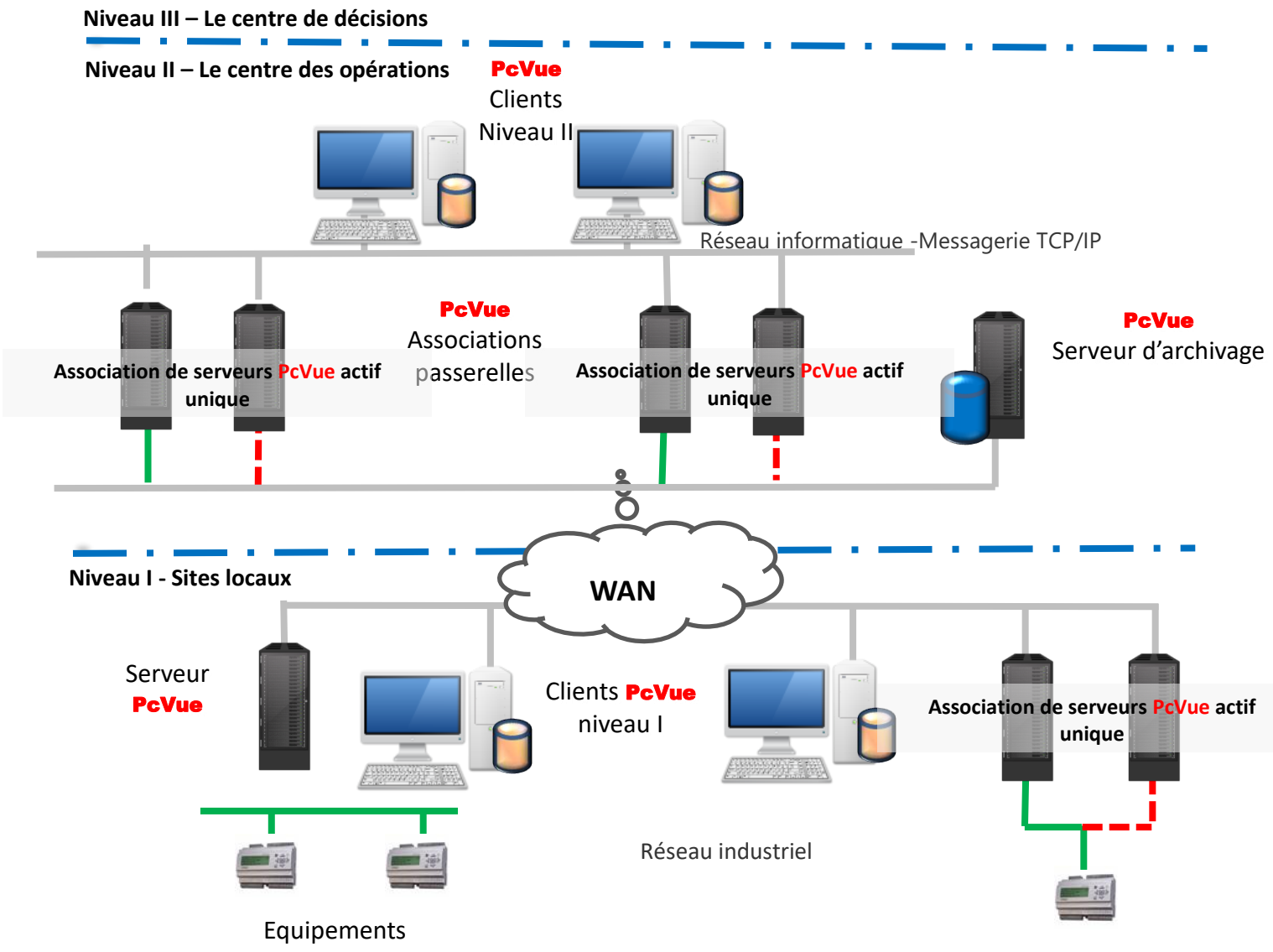


Figure 9 - Multi-niveau implémentation 1

Arc Informatique - © Copyright 2022. Tous droits réservés.

Le **Niveau I** est composé de postes PcVue répartis sur une vaste zone géographique qui acquièrent les données des équipements et les mettent à disposition du niveau II à travers un réseau WAN utilisant une liaison satellite par exemple.
Le **Niveau II** est le cœur de l'architecture avec des associations de serveurs PcVue redondants pour centraliser les données issues des différents postes du niveau I.
Chaque association de serveur gère des milliers de variables et archive les variables les plus critiques localement.
Une association de serveur d'historique peut aussi être dédiée à l'archivage des variables peu critiques dans une base de données
Les postes clients sont connectés aux postes serveurs et sont utilisés comme consoles d'exploitation et de développement et aide les opérateurs à contrôler et commander les variables des divers sites (temps réel,alarmes,…).
Le **Niveau III** est le niveau le plus élevé de l'architecture. Il reçoit les données principales agrégées issues du niveau II via OPC par exemple.

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.6.2 Multi-niveaux: implémentation #2

- ✓ Pour les applications de très grande envergure réparties sur de vastes zones géographiques
- ✓ Différents niveaux d'exploitation
- ✓ Nombre important de variables et fortes évolutivités potentielles
- ✓ Architecture très flexible

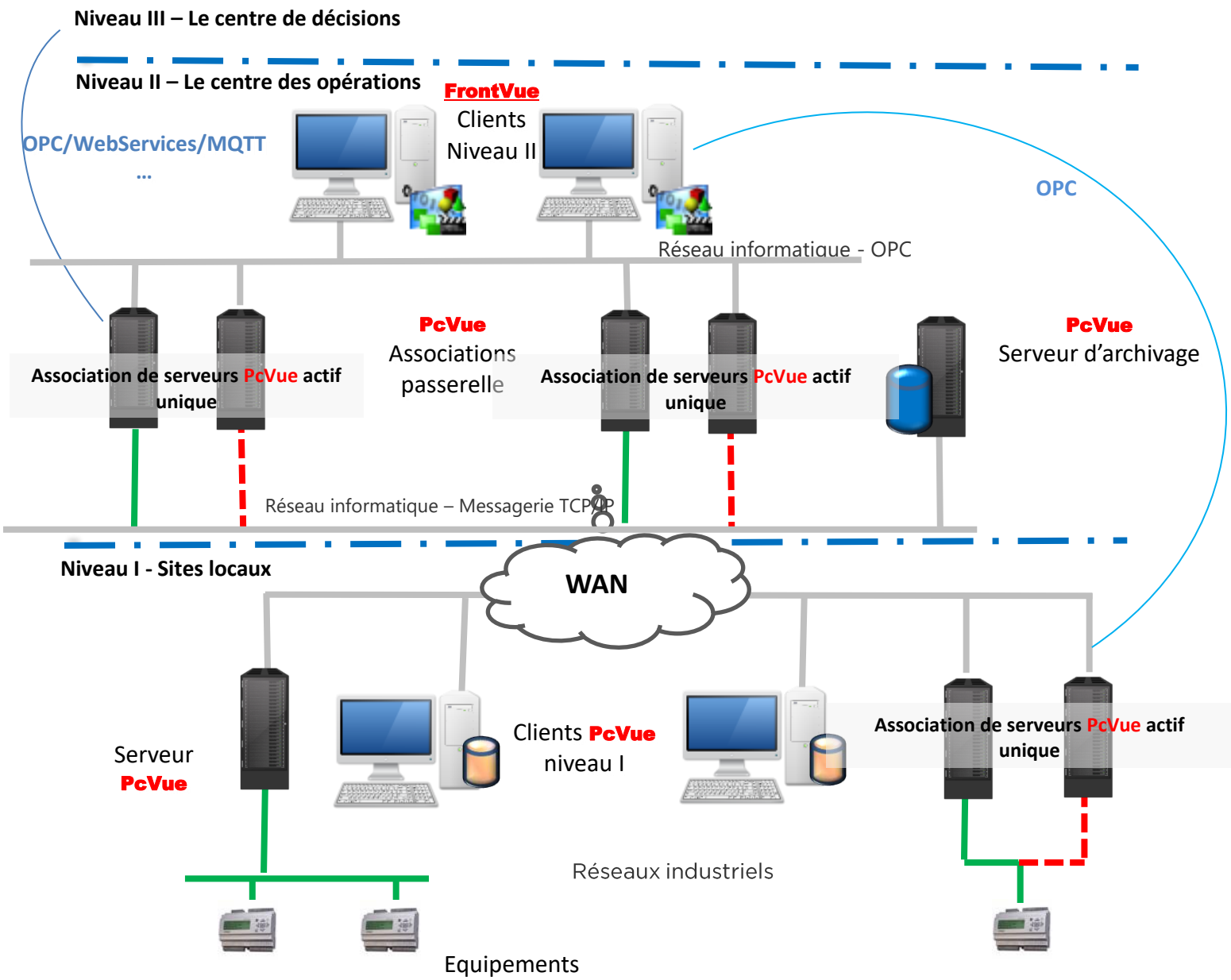


Figure 10 - Multi-niveau implémentation 2

Arc Informatique - © Copyright 2022. Tous droits réservés.

Lorsque une application devient conséquente (plus de 300 0000 variables), il est possible d'optimiser l'architecture en remplaçant les postes PcVue clients lourds, par des clients graphiques légers FrontVue et assurer ainsi l'évolutivité du système.
FrontVue est un client IHM OPC léger sans moteur de traitement ou d'archives.
Connecté à PcVue comme client OPC, il récupère les données et permet le contrôle commande de celles-ci, et peut afficher les alarmes et évènements historisés gérés au niveau de PcVue.

FrontVue ne rafraichit que les données affichées ce qui permet :

- de minimiser le temps de démarrage du projet sur les postes clients
- de réduire considérablement la charge sur le réseau

FrontVue peut être connecté à plusieurs serveurs OPC, ce qui permet :

- de se connecter à un serveur distant pour récupérer les informations détaillées de tout équipement de terrain.
- D'afficher des données concaténées issues de plusieurs serveurs et de présenter une liste unique à l'opérateur dans les fenêtres d'alarmes ou de consignation.

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.7 Architectures CLOUD

2.7.1 Architecture #1: Interopérabilité Cloud

- ✓ Connection transparente avec une base de données CLOUD
- ✓ Pour partager les données de PcVue vers des systèmes tiers tels que ERP, SCADA,…
- ✓ Pour obtenir des données d'appareils existants comme des objetsIoT vers PcVue

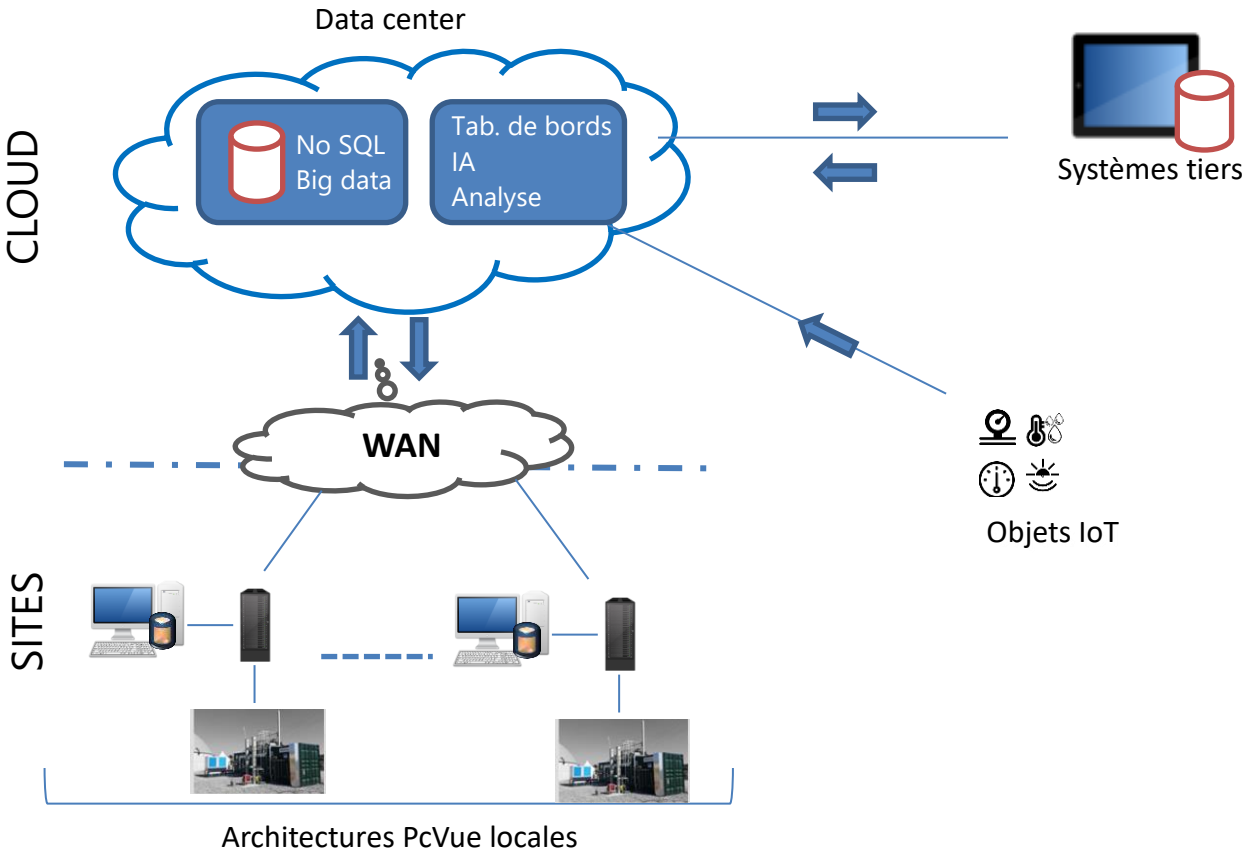


Figure 11 – Architecture base de données Cloud

Dans cette architecture un ou plusieurs postes PcVue sont déployés sur des sites locaux surveillant et pilolant les données des équipements locaux. L'architecture locale peut varier d'une station unique à plusieurs postes et peut inclure une base de données locale.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Chaque site PcVue peut se connecter à une base de données cloud via plusieurs types de connexion :

- Universal Data Connector qui fournit une gamme de connecteurs ADO.net

=> Dédié au partage et à l'obtention de données à partir de systèmes tiers

=> Non dédié aux gros volumes de données en temps réel

- Driver MQTT

=> Pour l'échange de données en temps réel d'une grande quantité de données

Cette architecture permet à PcVue de profiter d'une base de données cloud pour :

- partager toutes les données nécessaires à un système tiers tel qu'un ERP, un autre SCADA, ou autres

- obtenir des données de tous les appareils IoT qui ne font pas partie de l'architecture locale

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.7.2 Architecture #2: Hypervision CLOUD

- ✓ Délégation de l'infrastructure et de la gestion des données
- ✓ Evolutivité des ressources
- ✓ Déploiement de clients web & mobile depuis le CLOUD

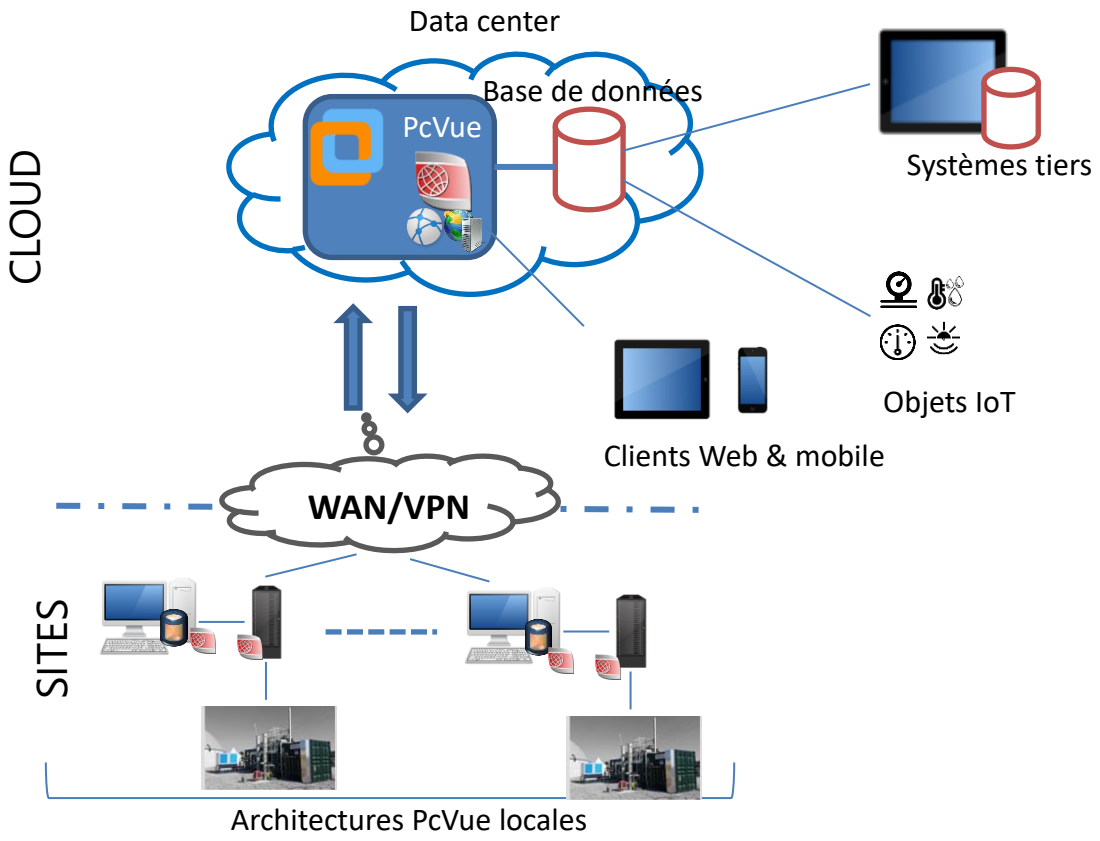


Figure 12 : Hypervision Cloud

Au niveaux des sites, un ou plusieurs postes PcVue sont déployés pour surveiller et piloter les données des équipements locaux. L'architecture locale peut varier d'une station unique à plusieurs stations et peut inclure une base de données locale.

Au niveau du cloud, PcVue est hébergé dans une machine virtuelle. Une architecture multi-stations peut être utilisée avec plusieurs VM si besoin.

PcVue collecte les données des sites PcVue locaux via un réseau WAN sécurisé utilisant la messagerie TCP/IP multiposte ou d'autres protocoles.

Les clients Web et mobiles peuvent être déployés à partir de la machine virtuelle.

Les données provenant de systèmes tiers ainsi que d'appareils IoT peuvent être collectées à partir d'une base de données à l'aide du connecteur de données universel ou MQTT.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Cette architecture permet de :

- Déléguer la gestion et la maintenance de l'infrastructure et des données à un tiers
- Une grande évolutivité des ressources avec un minimum d'effort
- Le déploiement de clients Web et mobiles depuis le CLOUD pour accéder à toutes les données

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.7.3 Architecture #3: CLOUD hybride

- ✓ Hébergement de données cloud
  - Entretien
  - Sécurité
- ✓ Hypervision depuis un centre de contrôle physique
- ✓ Intégration dans une infrastructure existante

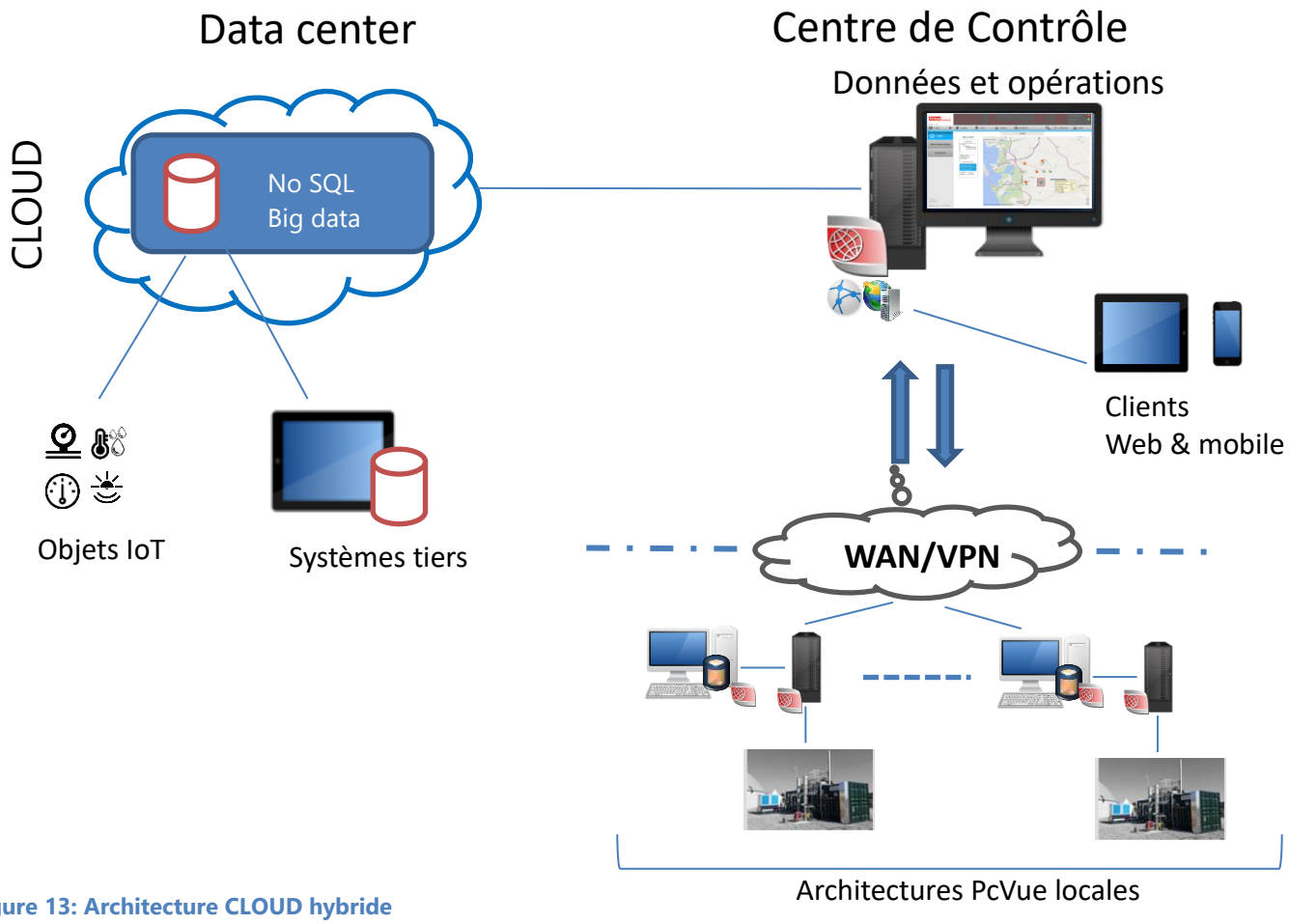


Figure 13: Architecture CLOUD hybride

Dans cette architecture, PcVue est hébergé sur site dans un centre de contrôle au sein d'une architecture pouvant inclure plusieurs serveurs d'acquisition de données et clients.

Les données sont hébergées dans une base de données cloud. PcVue obtient des données de systèmes tiers ou d'objets IoT connectés à la base de données à l'aide d'UDC ou de MQTT. Il peut également enregistrer des données dans la base de données.

PcVue collecte les données des sites PcVue locaux via un réseau WAN/VPN sécurisé utilisant la messagerie TCP/IP ou d'autres protocoles et agit comme un serveur pour les clients Web et mobiles.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Cette architecture permet de :

- L'hébergement des données dans le cloud et la délégation de la maintenance et de la sécurité des données
- L'intégration d'une infrastructure cloud dans une architecture existante

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.8 Poste de développement et gestion centrale de version

- ✓ Maintenance et déploiement facile de projet et/ou de bibliothèques
- ✓ Nombre de versions illimité
- ✓ Suivi des modifications
- ✓ Réduction des risques d'erreur et de perte

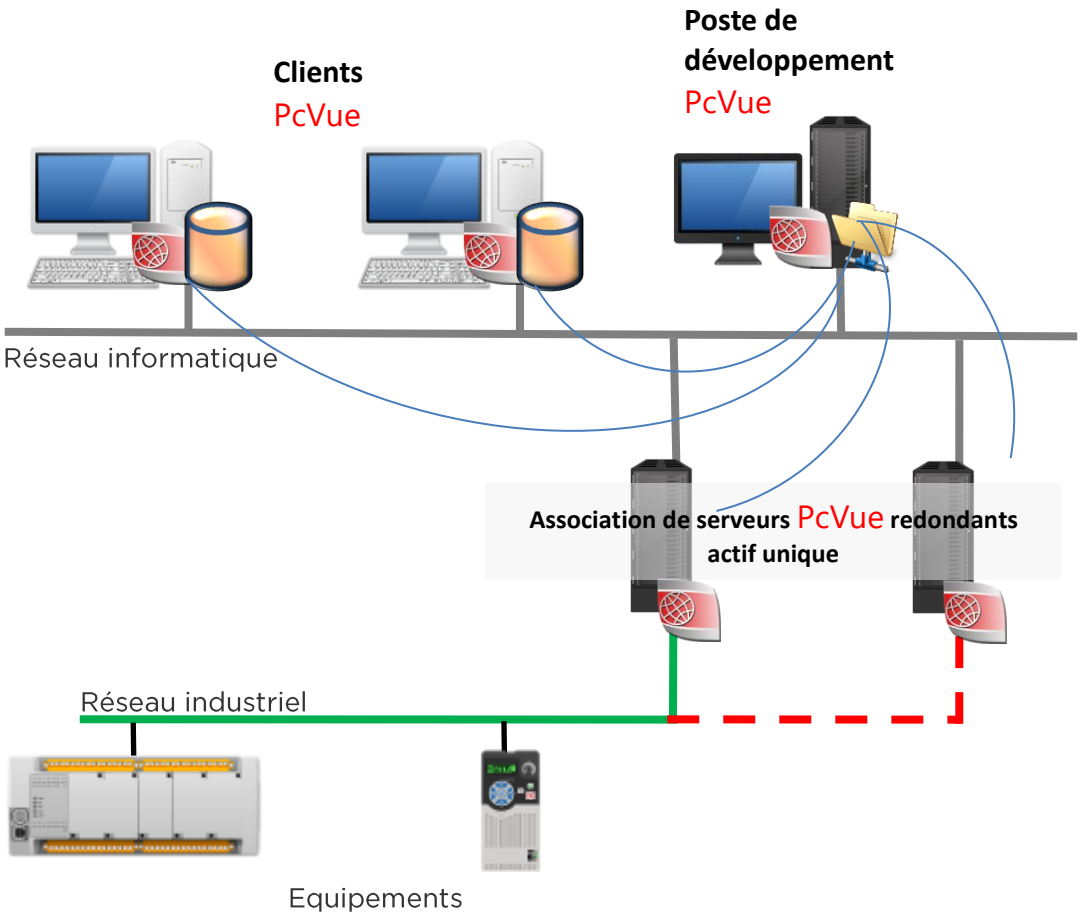


Figure 14 - Poste de développement

Pour faciliter le déploiement et la maintenance d'un projet, PcVue intègre un **gestionnaire de versions de projets natif**.
Différentes versions de projets et/ou de bibliothèques sont centralisées dans un répertoire partagé sur le réseau. Elles peuvent être chargées et modifiées depuis n'importe quel poste de l'architecture.
Habituellement un poste PcVue dédié est utilisé pour héberger le répertoire central de versions et faire les modifications.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Tout poste peut charger et exécuter manuellement tout type de version ou automatiquement une version de référence d'un projet et /ou d'une bibliothèque depuis le répertoire central de versions.
Différentes fonctionnalités sont disponibles :

- 3 types de versions : développement, opérationnelle, référence
- Configuration du contenu d'une version
- Suivi de modification pour chaque version
- Système de numérotation automatique de version
- Nombre illimité de versions possible (selon l'espace mémoire disponible)

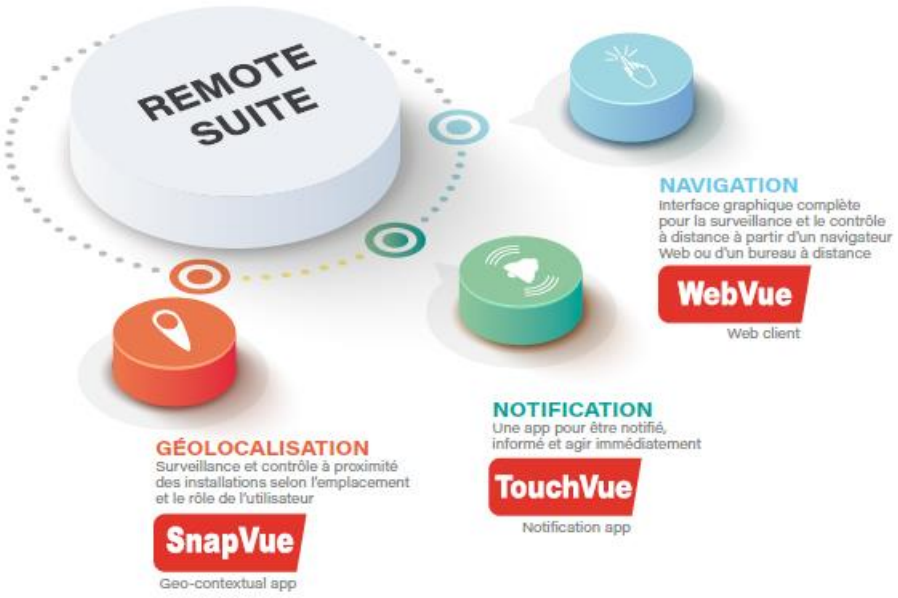
2.9 Architectures d'accès à distance

Cette section décrit les bonnes pratiques et les modèles courants de déploiement d'architectures d'accès à distance compatibles Web et mobiles pour PcVue.

PcVue permet le déploiement de composants Web et mobiles et l'intégration dans les environnements informatiques au sens large.
En particulier, il est possible de séparer la couche de serveur Web du réseau industriel.

Toutefois, cela peut ne pas être pratique dans tous les scénarios de déploiement, en particulier dans les systèmes à petite échelle. C'est pourquoi ce document met l'accent sur différents scénarios de déploiement :
- Approche simplifiée pour les configurations autonomes tout-en-un,
- Systèmes SCADA / IHM d'entreprise à grande échelle,
- Accès à distance à des systèmes à petite échelle

Plusieurs solutions montrées ci-dessous sont possibles pour l'exploitation à distance :



Arc Informatique - © Copyright 2022. Tous droits réservés.

2.9.1 EasyMobileTechnology

Les solutions Web et mobiles de PcVue s'appuient sur une technologie propriétaire exclusive EasyMobileTechnology permettant de mettre en place une architecture web et mobile sans passerelle / plug-in, intégrant toutes les fonctionnalités de sécurité nécessaires (https, Oauth, certificats) et la technologie HTML5 ainsi que des outils de maintenance.

Cette technologie répond aux critères suivants:
• Pas de passerelle ni plugin supplémentaire
• Aucune installation côté client
• Configuration par simple paramétrage - pas de scripts - Assistant seulement
• Ouvert aux applications tierces
• Adapté à tous type d'utilisateur : utilisateur final, SI, IT
• Architectures et communication sécurisées et évolutives
• Diagnostic facile

2.9.2 Console de déploiement Web

La console de déploiement Web est un composant permettant de définir, déployer et gérer une architecture Web ou mobile.
Il supporte les fonctionnalités suivantes:
- Déploiement de services Web et d'applications Web sur IIS
- Gestion des points finaux Web PcVue Web
- Gestion de la protection des données
- Gestion des certificats
- Enregistrement des accès utilisateur et gestion du serveur OAuth
- Audit / diagnostic IIS
La console de déploiement Web s'exécute sur un serveur hébergeant un serveur Web IIS.

Arc Informatique - © Copyright 2022. Tous droits réservés.

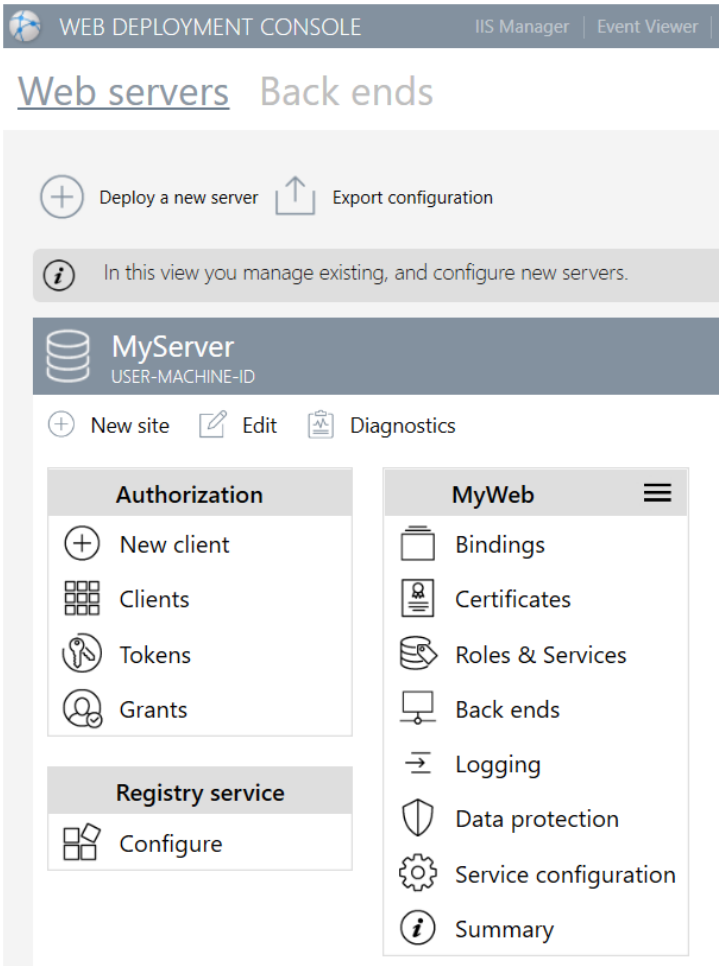


Figure 15 - Console de déploiement web et mobile

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.9.3 Clients Web & mobile

2.9.3.1 Client Web HTML5

WebVue permet à des terminaux disposant d'un simple navigateur internet, l'accès au projet PcVue via les services Web privés du serveur Web PcVue. L'utilisateur distant qui s'identifie accède alors aux synoptiques, aux courbes historiques, aux listes d'alarmes,… et peut visualiser et contrôler les données. Les terminaux banalisés ne nécessitent aucune installation particulière, ce qui facilite le déploiement de l'application sur site et à distance.

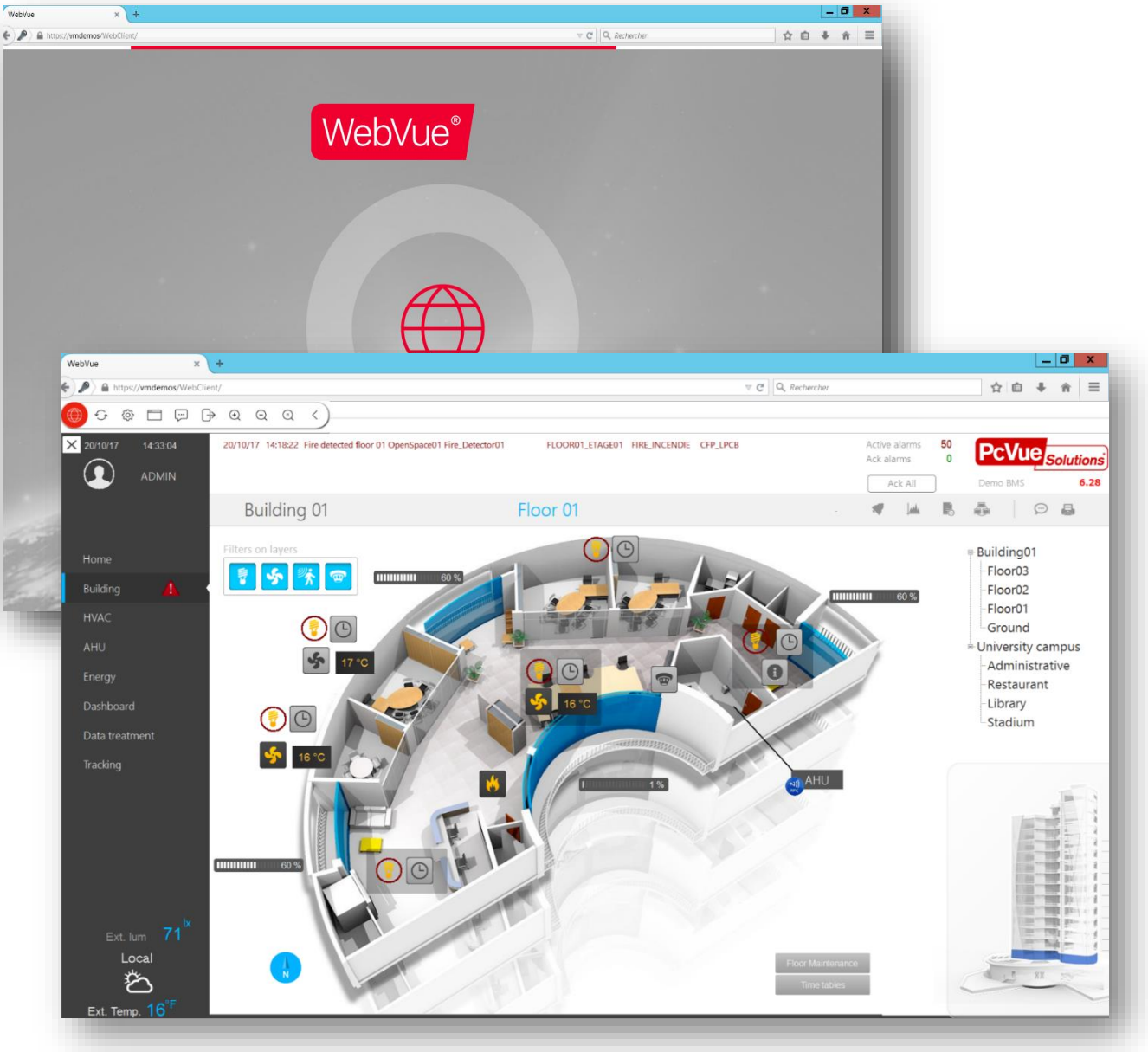


Figure 16 – Vue d'écran - Client web HTML5

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.9.3.2 TouchVue – Application mobile de notifications et de pilotage

L'application mobile TouchVue permet aux terminaux mobiles (tablettes, smartphones,…) d'accéder aux valeurs temps réel des variables d'un projet PcVue et aux différentes listes d'alarmes et d'historiques ainsi qu'aux courbes de tendances. L'opérateur peut ainsi acquitter une alarme, ou forcer une valeur de consigne par exemple.

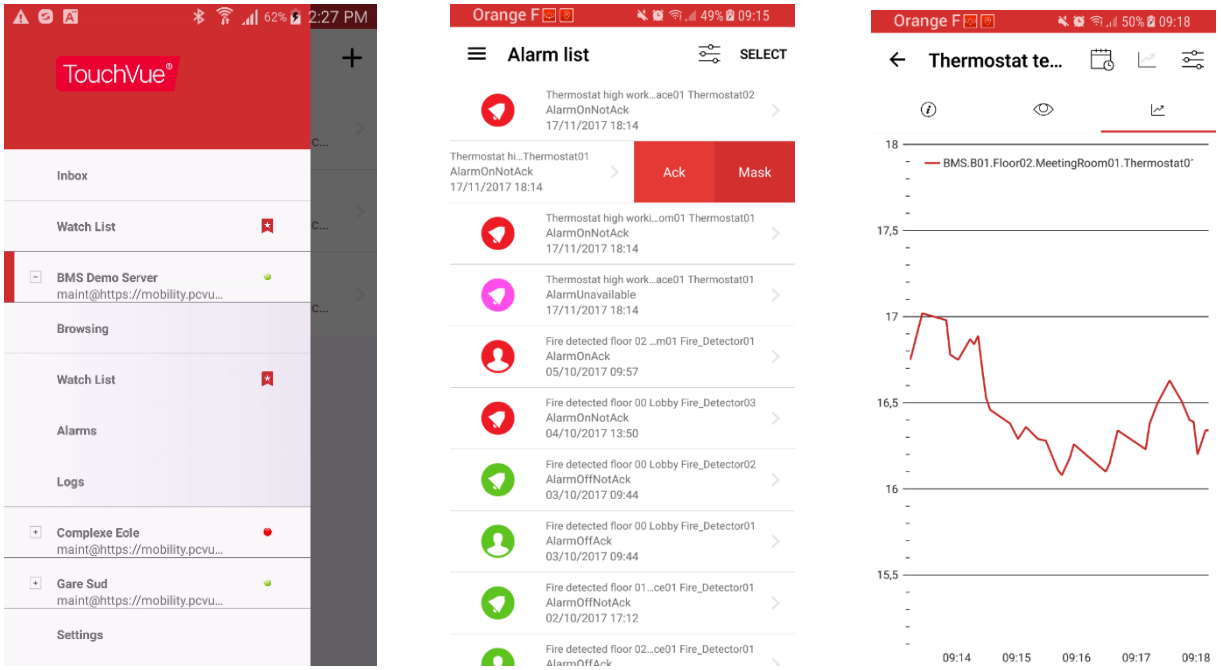


Figure 17 – TouchVue : vues d'écran

2.9.3.3 SnapVue – Application mobile basée sur la localisation

SnapVue est une application mobile qui, associée au serveur contextuel d'un projet PcVue, permet à l'utilisateur mobile d'accéder sans avoir besoin de naviguer aux informations qui le concerne en fonction de sa localisation et de son rôle. Il est alors en mesure de visualiser et/ou de piloter les équipements qui l'entourent au travers d'une interface qu'il est possible de personnaliser en phase de conception.
Différents services facilitent l'exploitation comme un système de messagerie pour échanger des messages (vocaux, vidéos, textes, images) avec les autres utilisateurs et/ou avec le serveur PcVue. Un système de bot peut également d'assister l'utilisateur en répondant à des scénarios prédéfinis.

Arc Informatique - © Copyright 2022. Tous droits réservés.

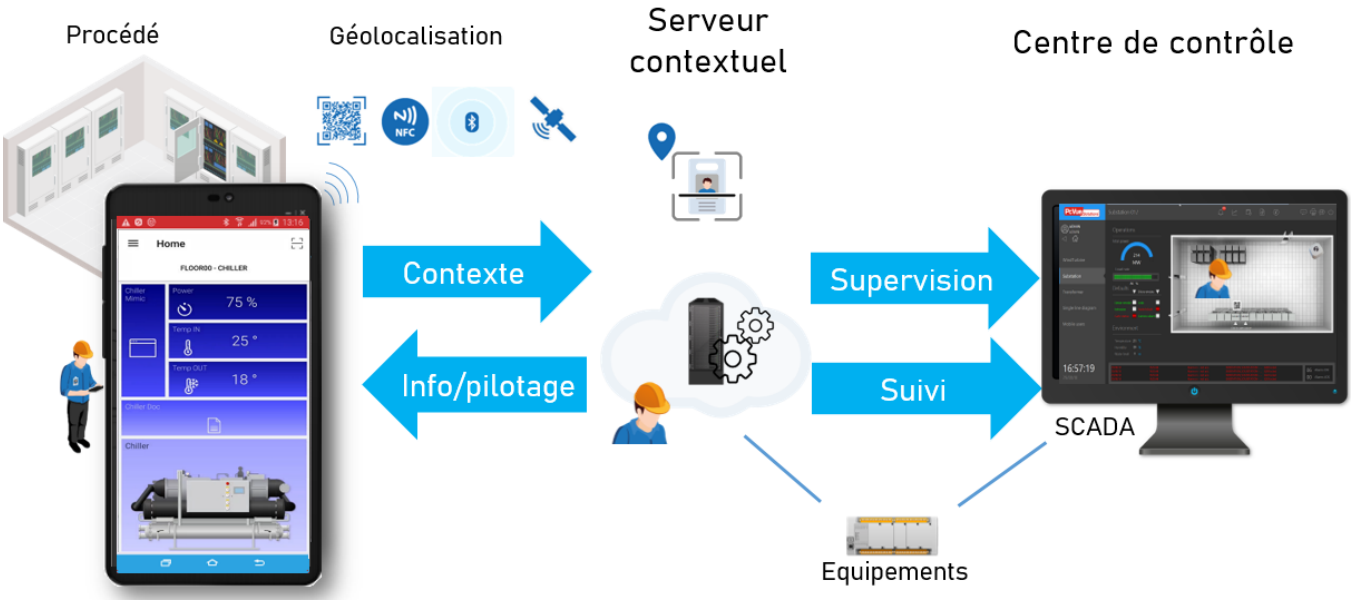


Figure 18 – SnapVue : principe de fonctionnement

SnapVue utilise les technologies et services de géolocalisation comme montré ci-dessous :

Figure 19 – SnapVue : technologies utilisées

Arc Informatique - © Copyright 2022. Tous droits réservés.

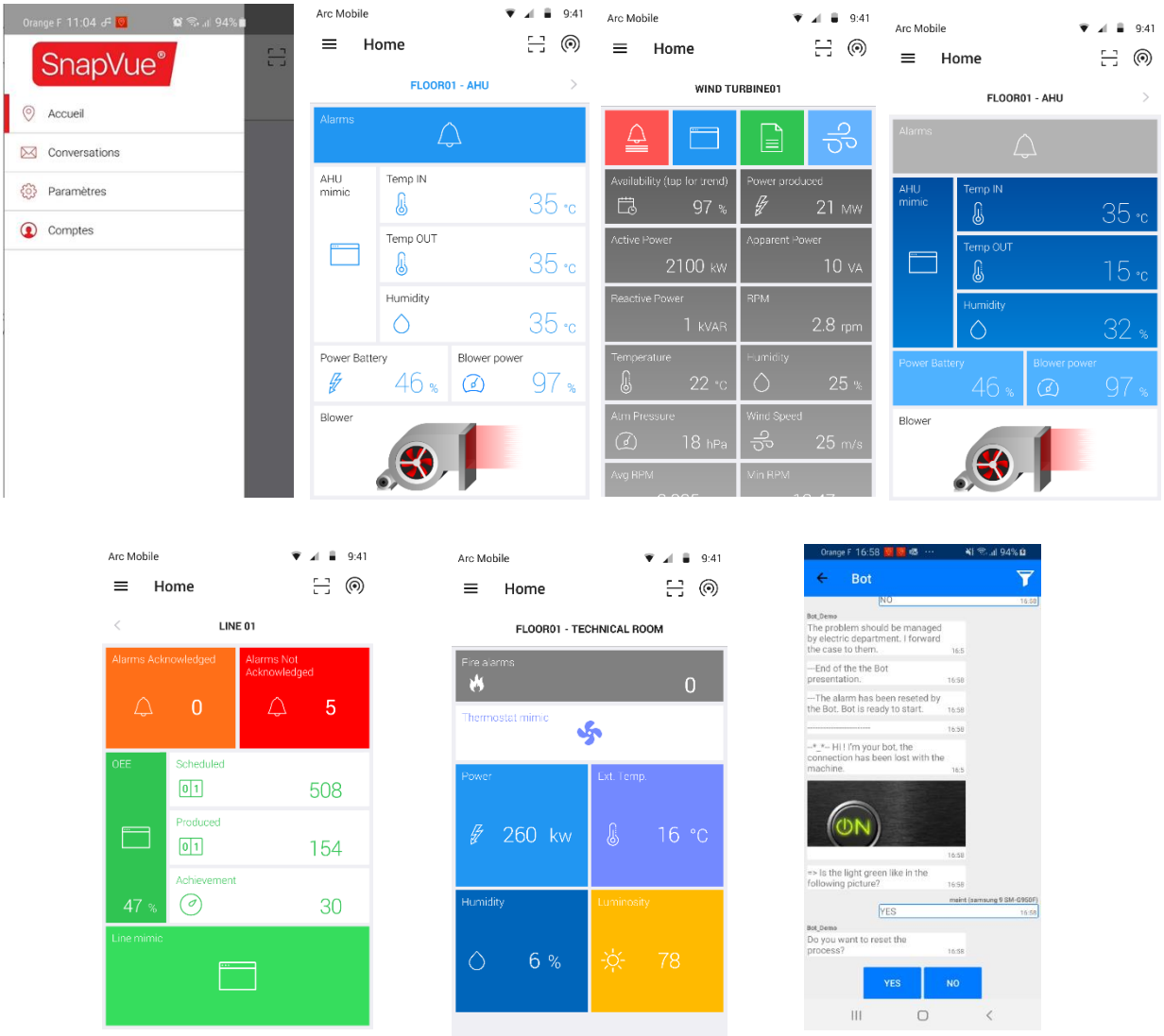


Figure 20 – SnapVue : vues d'écran

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.9.4 Bureau d'accès à distance

PcVue peut être exécuté à distance en utilisant la fonctionnalité Windows de bureau à distance depuis un PC ou tout autre terminal.
La technologie HTML5 permettra également de profiter de cette fonctionnalité depuis tout navigateur internet.

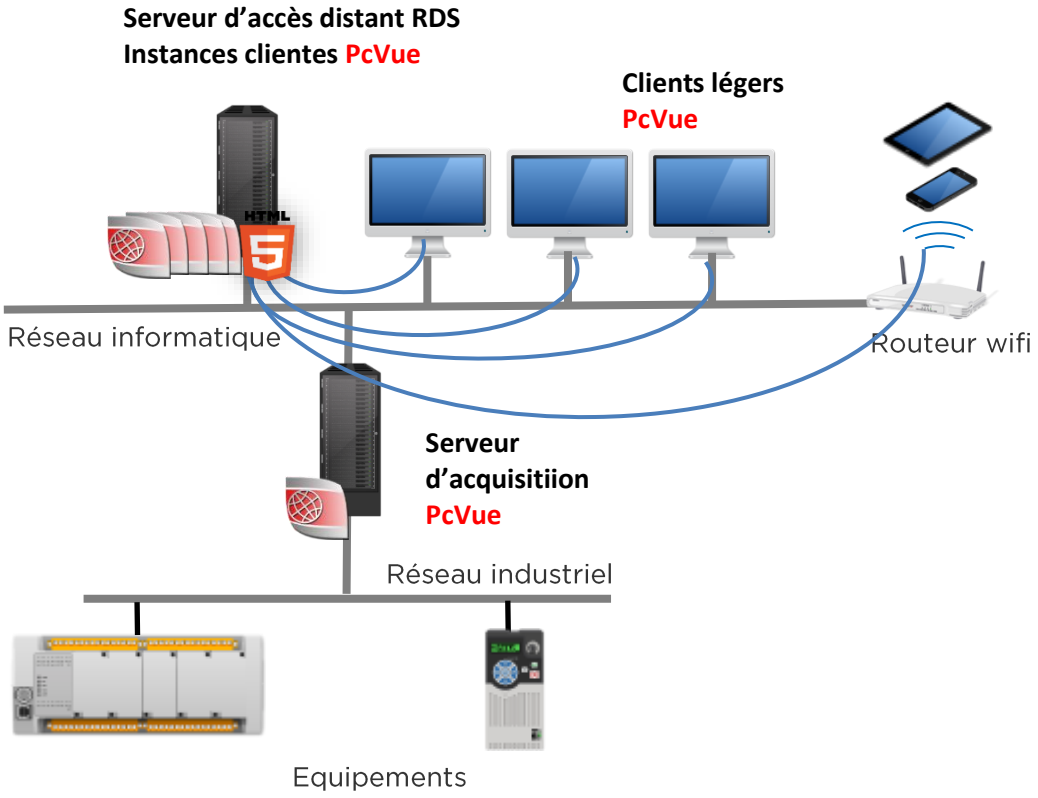


Figure 21 – Bureau d'accès à distance

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.9.5 Architecture #1: Déploiement “tout-en-un”

- ✓ Approche simple pour un déploiement mono poste “tout-en-un”
- ✓ Niveau de sécurité faible
- ✓ Adapté lorsque le réseau est privé et complétement isolé des accès extérieurs

2.9.5.1 Description

Dans ce scénario de déploiement, le poste PcVue Web backend et les composants du serveur Web ne sont pas séparés. Ils sont hébergés et exécutés sur le même ordinateur.

Les clients Web et mobiles, y compris WebVue et TouchVue, sont connectés au même réseau que le serveur Web.

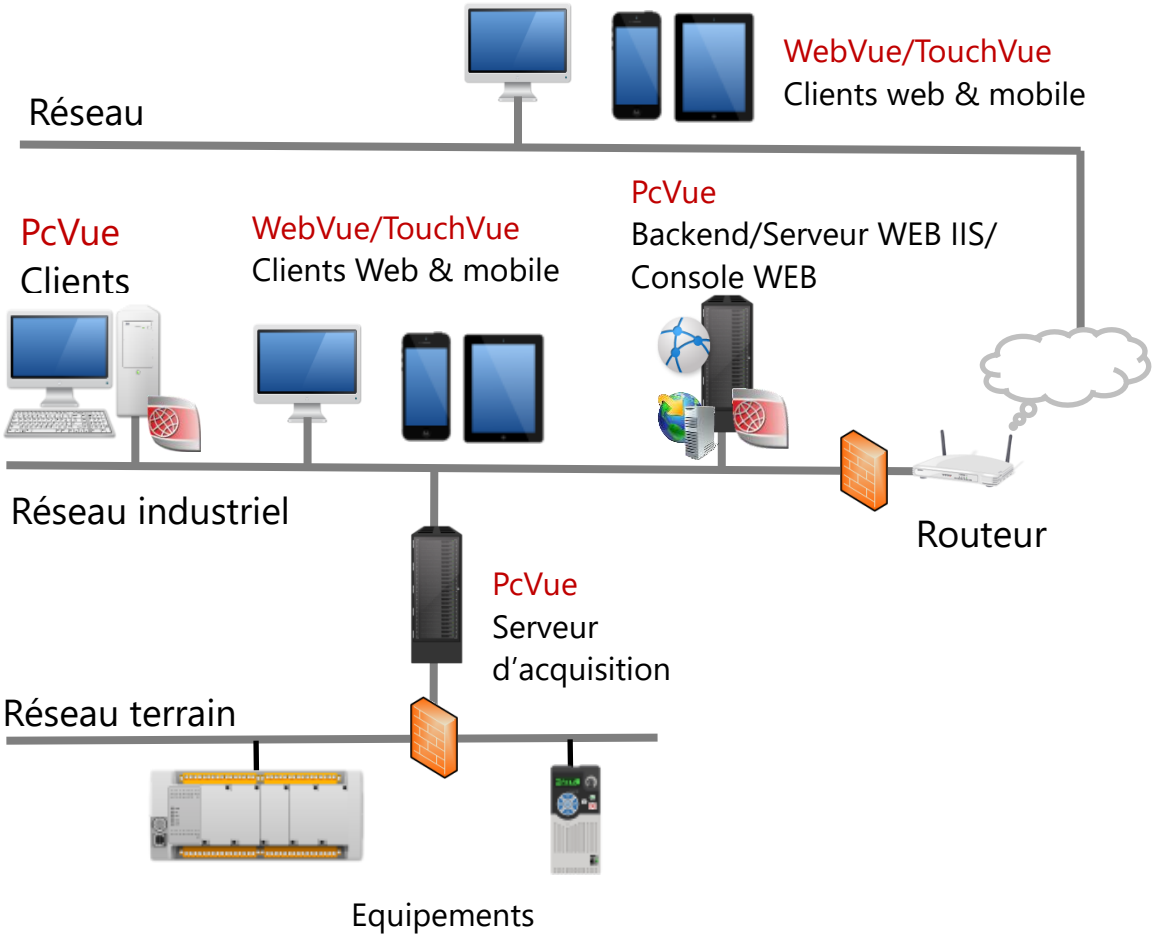


Figure 22 – Architecture #1 – Déploiement “tout-en-un”

Note:

- Les plages et les adresses IP sont purement indicatives, conformément aux modèles d'utilisation typiques décrits dans la RFC 6890. Toute autre plage ou ensemble d'adresses de sous-réseaux peut également être utilisée.

Arc Informatique - © Copyright 2022. Tous droits réservés.

-L'architecture du système SCADA PcVue est purement indicative.

- La séparation du réseau industriel du réseau d'automatisation, bien que recommandée, est purement indicative.

2.9.5.2 Contexte d'utilisation recommandée

Cette architecture est adaptée lorsque les clients Web et mobiles se trouvent sur le même sous-réseau que la station d'extrémité Web PcVue Web.
Elle est à considérer lorsque le réseau (le sous-réseau) est privé et totalement isolé des accès extérieurs. En particulier, les ordinateurs et les appareils utilisés par les opérateurs ne doivent pas non plus avoir accès au monde extérieur, afin d'éviter le risque d'être utilisés comme une porte d'accès au réseau industriel.

2.9.5.3 Contexte d'utilisation non recommandé

Ce type de déploiement ne doit pas être utilisé lorsque le réseau est ouvert aux demandes entrantes de réseaux extérieurs ou ouvert à un accès non protégé à partir de périphériques inconnus.
En particulier, lorsque l'accès à partir de systèmes clients Web et mobiles sur Internet est requis et qu'aucun autre moyen de sécurité réseau (tel que le tunneling VPN, par exemple) n'est disponible.

2.9.5.4 Pré requis

1. Le déploiement de cette architecture nécessite un minimum d'expertise réseau.

2. Nécessite que tous les ordinateurs et périphériques mobiles se trouvent sur le même sous-réseau, généralement le réseau industriel, y compris les clients Web et mobiles, le serveur Web et la station d'extrémité dorsale PcVue Web.

3. Les clients de ce réseau sont censés faire confiance à la machine du serveur Web sans réserve, car ils se trouvent sur le même réseau et, par définition, sur un réseau privé.

4. Cette architecture fonctionne avec des exigences minimales pour la fiabilité du certificat de serveur Web.Un certificat émanant d'une autorité de certification n'est pas obligatoire pour établir une confiance avec le serveur Web.

2.9.5.5 Avantages

1. Un seul ordinateur suffit pour héberger à la fois le back-office PcVue Web et le serveur Web.

2. Cet ordinateur ne nécessite pas plus d'une carte d'interface réseau.

3. Fonctionne directement lorsque vous utilisez l'adresse IP de l'ordinateur Web Server pour connecter des clients Web et mobiles.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Un DNS n'est pas requis pour la résolution de noms sur les plates-formes Windows. L'ordinateur du serveur Web peut être adressé par son nom d'hôte à partir de tout client Web basé sur Windows.

Peut fonctionner avec un système d'exploitation Windows tel que Windows 10 sur l'ordinateur PcVue Web Server s'il dessert un nombre limité d'utilisateurs. Dans tous les cas, l'utilisation d'un système d'exploitation serveur est fortement recommandée.
Lors de l'utilisation de périphériques clients non Windows (Android, iOS, Linux), la présence d'un serveur DNS est indispensable pour la résolution de noms. Cela peut être réalisé en utilisant un système d'exploitation Windows Server pour le poste de base PcVue Web et en activant le rôle de serveur DNS.

4. L'utilisation d'un certificat auto-signé fonctionne immédiatement, avec la nécessité d'ajouter une exception de sécurité sur l'agent utilisateur du client Web ou d'activer l'option «Ignorer les erreurs de certificat» sur les applications client mobiles.

S'il existe un serveur Active Directory accessible depuis le réseau, un certificat de domaine peut être émis à partir du serveur Active Directory et approuvé par tous les clients du domaine (par stratégie de domaine ou via un système MDM d'entreprise).

2.9.5.6 Limites

1. Certaines limitations peuvent s'appliquer lorsque le serveur Web est hébergé sur un système d'exploitation Windows. En particulier, le nombre maximal de connexions client que IIS peut gérer.

2. Microsoft® Edge n'autorise pas le stockage de cookies si le nom d'hôte n'est pas un nom de domaine complet. Cela provoque des problèmes avec les composants Web. L'URL https: // <nom d'hôte> .local permet d'y remédier.

3. Des performances limitées peuvent être rencontrées, notamment lors du chargement du client WebVue, lors de l'utilisation de certificats non valides (partiellement ou totalement fiables) car, dans ce cas, les fichiers ne sont pas mis en cache par les navigateurs Web.

2.9.5.7 Console de déploiement Web

Cette architecture peut être facilement déployée à l'aide de l'assistant «Quick Setup» du WDC, en laissant tous les paramètres à leur valeur par défaut.

Par conséquent, le WDC doit être installé sur le même ordinateur que le serveur principal Web de PcVue et le serveur Web.

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.9.6 Architecture #2: Ségrégation réseau et DMZ

- ✓ Architecture SCADA / IHM à grande échelle
- ✓ Haut niveau de sécurité
- ✓ Destiné aux clients Web / mobiles en dehors du réseau industriel

2.9.6.1 Description

Dans ce scénario de déploiement, le poste PcVue Web back end et les clients Web & Mobile se trouvent sur des réseaux physiques ou logiques différents, dans des périmètres de sécurité différents, nécessitant une séparation avec une zone démilitarisée. Le réseau interne (côté LAN du routeur DMZ) est un réseau sécurisé privé. Le réseau externe (côté WAN du routeur DMZ) est un réseau moins fiable, généralement un réseau d'entreprise ou Internet.
Les composants du serveur Web sont hébergés sur un ordinateur à l'intérieur de la zone démilitarisée et le back-end de PcVue est hébergé sur le réseau sécurisé.
Cette architecture offre la meilleure intégration dans les réseaux informatiques et permet une conformité maximale aux directives et pratiques informatiques.

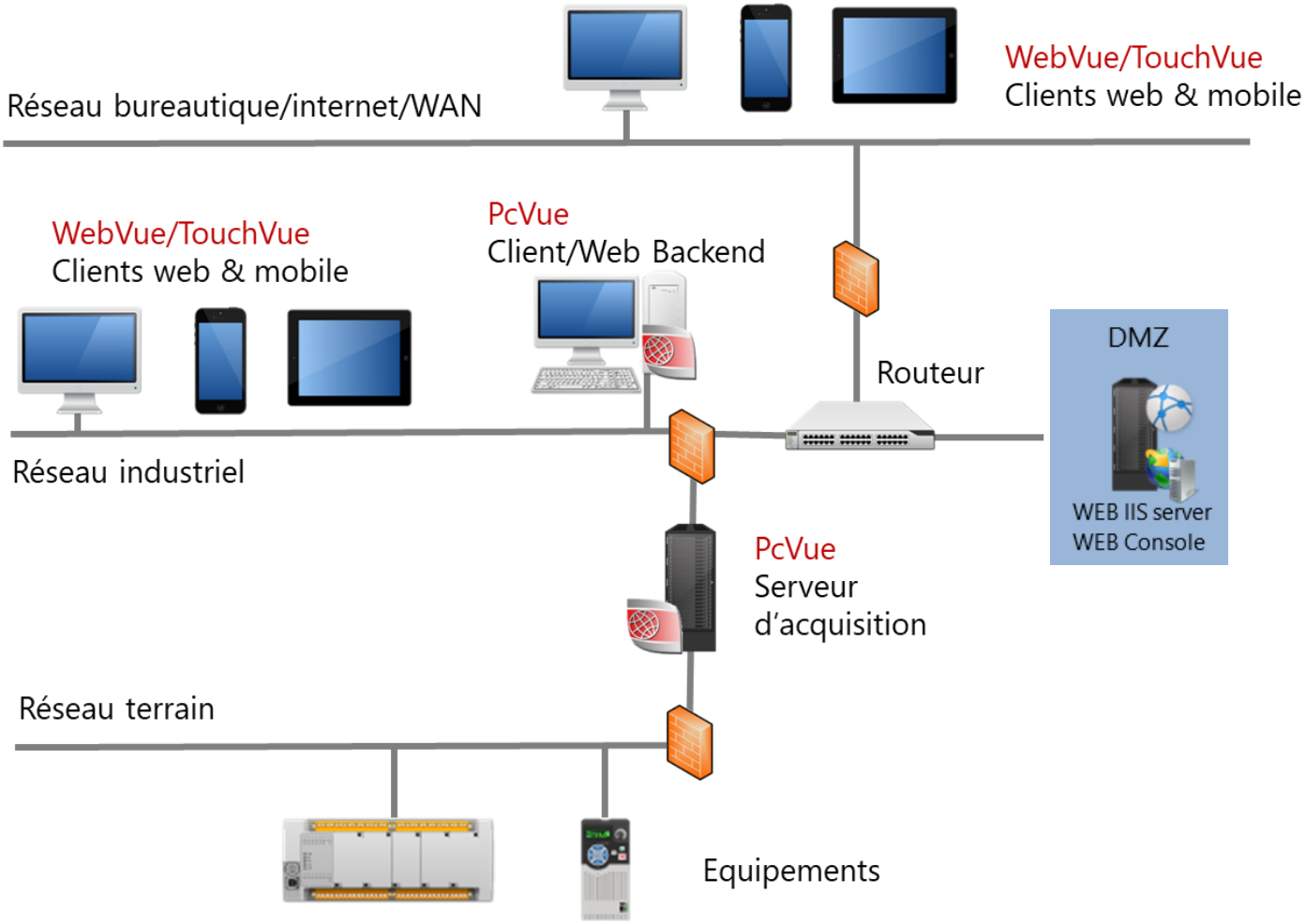


Figure 23 – Architecture #2 – Network isolation and DMZ

Arc Informatique - © Copyright 2022. Tous droits réservés.

Note:
- Les plages et les adresses IP sont purement indicatives, conformément aux modèles d'utilisation typiques décrits dans la RFC 6890. Toute autre plage ou ensemble d'adresses de sous-réseaux peut également être utilisée.
- L'architecture du système SCADA PcVue est purement indicatif.
- La séparation du réseau industriel du réseau d'automatisation, bien que recommandée, est purement indicative.

2.9.6.2 Contexte d'utilisation recommandé

Il est recommandé d'utiliser cette architecture de déploiement lorsque les clients Web et Mobile ne se trouvent pas sur le réseau industriel sécurisé.

2.9.6.3 Pré-requis

1. Le niveau d'expertise réseau et informatique nécessaire pour déployer cette architecture est intermédiaire à élevé.

2. Nécessite une infrastructure de réseau appropriée pour séparer le réseau privé du réseau moins protégé. Cela inclut un routeur (et une configuration adéquate du routage) et au moins un pare-feu.

Les architectures DMZ courantes sont prises en charge, notamment la configuration avec un seul pare-feu et la configuration avec double pare-feu:

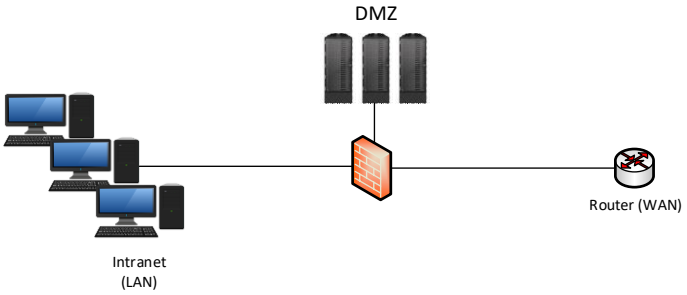


Figure 24 - DMZ – Single firewall setup

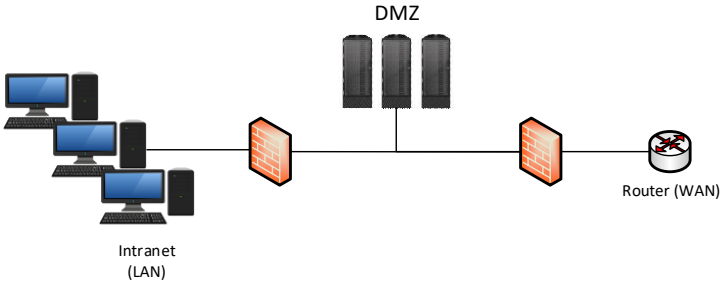


Figure 25 - DMZ – Dual firewall setup

Arc Informatique - © Copyright 2022. Tous droits réservés.

3. L’assistance du service informatique de l’utilisateur final sera probablement nécessaire pour configurer correctement la séparation du réseau, la résolution de noms et les certificats.

Cela inclut la configuration appropriée de:
- DNS
- routage
- Traduction d'adresse réseau (ou redirection de port)
- Certificats

Une infrastructure Active Directory sera probablement requise en tant qu'infrastructure PKI d'entreprise pour émettre des certificats et pour garantir des relations de confiance dans le cadre d'une stratégie globale.

4. Afin de valider l'identité de l'ordinateur Web Server sur le réseau de confiance le plus faible et d'éviter les attaques de type Man-in-the-Middle, l'utilisation d'un certificat entièrement sécurisé est indispensable.

- Ce certificat peut être délivré par le service informatique (serveur Active Directory du réseau d'entreprise). Il suffit que tous les clients Web et mobiles entretiennent une relation de confiance avec l’infrastructure réseau de l’entreprise.

- Ce certificat peut être délivré par le service informatique via une autorité de certification approuvée. Nécessaire si le client Web est accédé par des clients Web et mobiles externes (accès standard à partir d'Internet par des ordinateurs / périphériques clients ne disposant pas d'une relation de confiance avec l'infrastructure de réseau de l'entreprise).

- Ce certificat peut être émis via l’assistant Let’s Encrypt® du WDC s’il existe un accès Internet et si la stratégie d’organisation des utilisateurs autorise le service Let’s Encrypt®.

5. Un serveur DNS capable de résoudre le nom du serveur Web est requis sur le réseau de confiance inférieur.

6. Un système d'exploitation Windows Server sur l'ordinateur Web Server et, idéalement, également sur la station de base PcVue Web.
7. La station d'extrémité arrière Web PcVue doit être accessible à partir de l'ordinateur Web Server au moins par son adresse IP. L'accès via nom d'hôte est également possible, étant donné qu'un moyen de résolution de nom est présent à l'intérieur de la zone démilitarisée:
- Une entrée dédiée dans le fichier hosts de l'ordinateur Web Server.
- Un serveur DNS au sein du réseau industriel accessible depuis la zone démilitarisée.
S'il n'est pas déjà disponible, l'activation du rôle Serveur DNS sur le système d'exploitation Windows Server de la station de base PcVue Web peut être une solution.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Remarque: autoriser l'accès depuis un ordinateur d'une zone démilitarisée au réseau privé est en contradiction avec les schémas et pratiques courants de la zone démilitarisée. Pour des raisons techniques, le port TCP 8090 doit être ouvert dans cette direction.

2.9.6.4 Avantages

1. Cette architecture permet un accès pratique à partir de réseaux moins fiables, généralement Internet ou Intranet, en exposant les services Web et mobiles et les applications du serveur Web sous un nom de domaine complet.
2. Il permet un contrôle maximal du trafic réseau, conformément aux pratiques de séparation du réseau informatique, en s'assurant qu'il n'y a pas de demandes de connexion entrantes indésirables provenant de réseaux externes dans le réseau industriel, y compris le contrôle et la surveillance du trafic aux périmètres du réseau.

2.9.6.5 Console de déploiement Web

Cette architecture peut être déployée à l'aide de n'importe lequel des assistants de configuration WDC. Les paramètres par défaut de l'assistant «Installation rapide» ne conviendront pas dans toutes les situations. Le WDC doit être installé sur le serveur Web.

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.9.7 Architecture #3: Scénario NAT simplifié pour l'accès à distance

- ✓ Accès à distance pour des systèmes à petite échelle
- ✓ Adapté lorsqu'aucune infrastructure informatique gérée n'est disponible.

2.9.7.1 Description

Ce scénario de déploiement correspond à un seul réseau local privé, le réseau industriel, où résident à la fois le serveur Web, le poste PcVue Web backend et la plupart des clients Web et mobiles. Un accès Internet dédié est utilisé pour les connexions à distance.
Dans ce scénario de déploiement, les clients Web et mobiles sont répartis de chaque côté du NAT (clients Web locaux et distants).
Bien qu'il soit techniquement possible de déployer cette architecture en l'état, il n'est pas recommandé de le faire sans déploiement de mesures de sécurité supplémentaires.

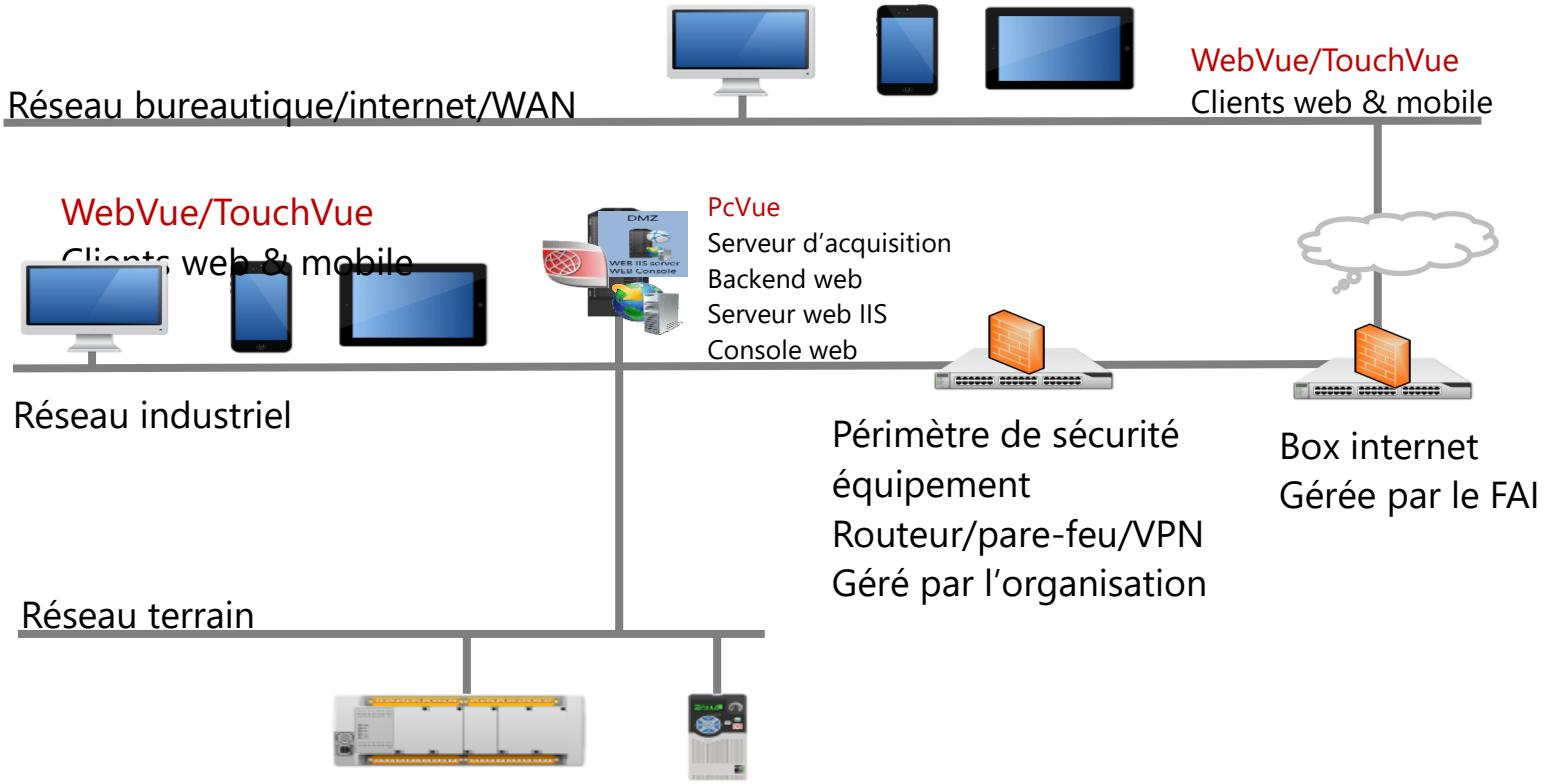


Figure 26 - Architecture #3 – Scénario NAT simplifié pour l'accès à distance

Note:
- Les plages et les adresses IP sont purement indicatives, conformément aux modèles d'utilisation typiques décrits dans la RFC 6890. Toute autre plage ou ensemble d'adresses de sous-réseaux peut également être utilisée.

Arc Informatique - © Copyright 2022. Tous droits réservés.

- L'architecture du système SCADA PcVue est purement illustrative et peut différer de votre configuration actuelle.
- L'adresse IP sous laquelle le routeur est exposé au réseau étendu peut dépendre de votre fournisseur d'accès à Internet.

2.9.7.2 Contexte d'utilisation recommandé

Ce scénario de déploiement peut être requis pour un accès distant simple lorsqu'aucune infrastructure informatique gérée n'est disponible.

2.9.7.3 Contexte d'utilisation non recommandée

Cette architecture n'est pas adaptée dans les environnements de production ou les systèmes réels sans comprendre les risques associés à une mauvaise ségrégation du réseau et à un contrôle de trafic réseau faible.

2.9.7.4 Pré requis

1. Le niveau d'expertise réseau et informatique requis pour déployer cette architecture est faible à intermédiaire.

2. L'infrastructure de réseau pour établir une connexion entre le réseau privé et le réseau moins protégé. L'infrastructure de réseau pour connecter les clients Web / Mobile de chaque côté du routeur.

3. La traduction d'adresses réseau (ou la redirection de port en particulier) est configurée sur la limite du réseau.

4. Afin de valider l'identité de l'ordinateur Web Server sur le réseau de confiance inférieur et d'éviter les attaques de type Man-in-the-Middle, l'utilisation d'un certificat entièrement sécurisé est indispensable.

- Ce certificat peut être délivré par le service informatique via une autorité de certification approuvée. Nécessaire si le client Web est accédé par des clients Web et mobiles externes (accès standard à partir d'Internet par des ordinateurs / périphériques clients ne disposant pas d'une relation de confiance avec l'infrastructure de réseau de l'entreprise).

- Ce certificat peut être émis via l'assistant Let's Encrypt® du WDC s'il existe un accès Internet et si la stratégie d'organisation des utilisateurs autorise le service Let'Encrypt®.

5. L'ordinateur du serveur Web doit être accessible aux clients Web et Mobile à partir des deux segments de réseau. Cela peut être réalisé si le serveur Web est bien connu sur les deux segments de réseau sous le même nom de domaine complet. Si ce n'est pas le

Arc Informatique - © Copyright 2022. Tous droits réservés.

cas, les clients Web et Mobile ont la possibilité de se connecter directement à l'ordinateur Web Server à l'aide de son nom de domaine complet (FQDN) sans que la messagerie ait à quitter le réseau privé. L'utilisation de NAT Loopback / Hairpinning est suggérée dans ce cas. Si aucune de ces options n'est possible, il est recommandé de créer deux sites différents via le WDC, qui se connectent tous les deux au même PcVue Web backend.

2.9.7.5 Avantages

1. Cette architecture permet un accès pratique aux clients Web et mobiles situés sur le réseau industriel et à partir d'Internet.

2. Cette architecture est la première étape d'un processus de migration de systèmes WebVue hérités offrant un accès Web à distance.

2.9.7.6 Limites

Ce scénario de déploiement offre une sécurité réseau limitée si aucun appareil spécifique n'est ajouté pour contrôler le périmètre du réseau, car:
- on s'appuie sur un décodeur appartenant à un fournisseur de services Internet pour contrôler le périmètre du réseau et la connexion à distance,
- Par conséquent, un ordinateur faisant partie du système de contrôle industriel doit être considéré comme directement exposé à Internet.

Dans le pire des cas, un attaquant pourrait exploiter les failles de sécurité potentielles à plusieurs niveaux afin d'accéder au système de contrôle industriel.

2.9.7.7 Console de déploiement Web

Cette architecture peut être déployée à l'aide de n'importe lequel des assistants de configuration WDC.
Le WDC doit être installé sur le serveur Web.

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.10 Architecture mixte

Cet exemple d'architecture s'articule autour des éléments suivants:

- L'acquisition des données est réalisée par des serveurs d'acquisition redondants sur le réseau industriel.
- Un poste de développement est utilisé pour la gestion centralisé du projet.

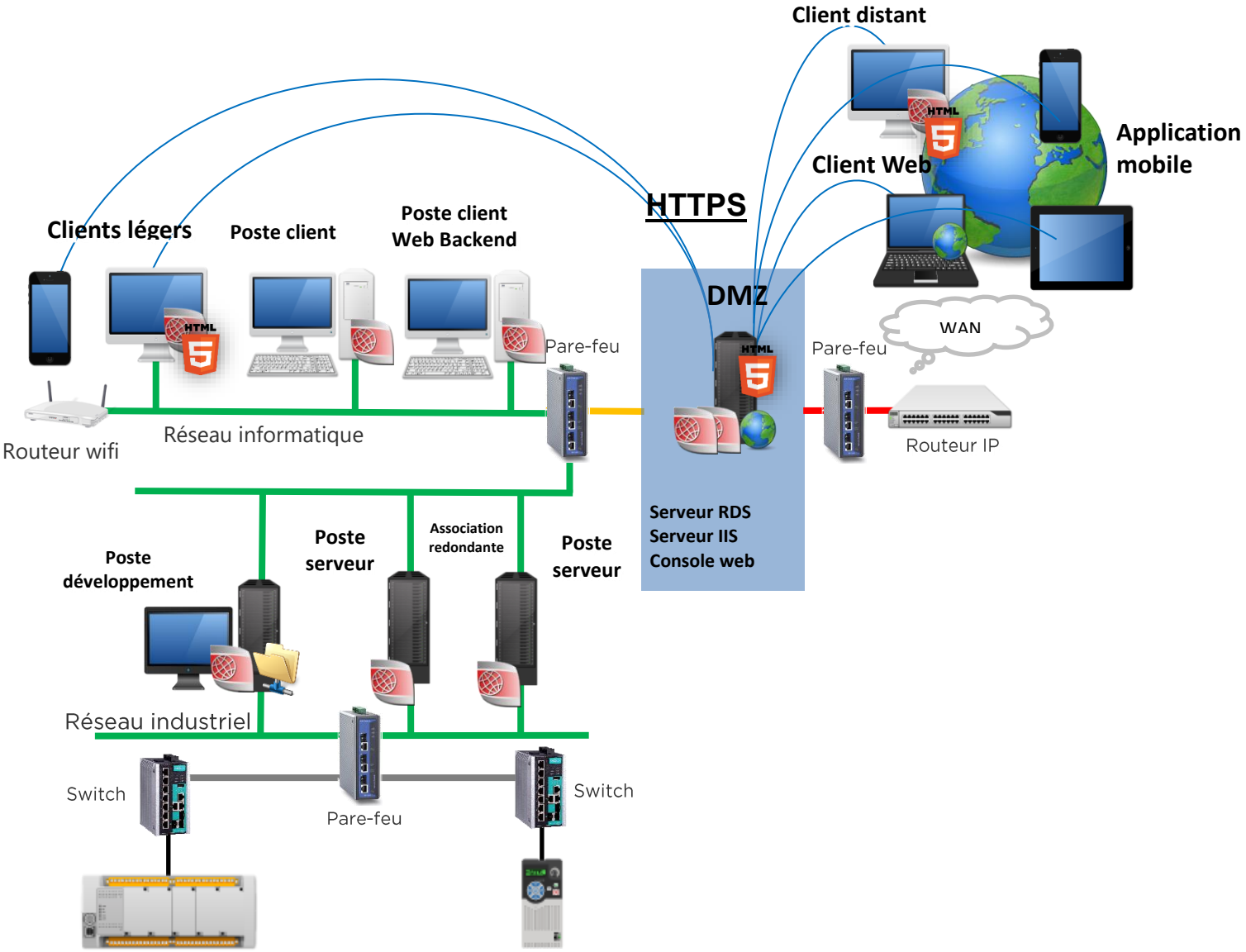


Figure 27 - Architecture mixte

- L'exploitation est réalisée par des postes clients sur le réseau informatique isolé par un pare-feu.
- Un poste client est serveur Web Backend

Arc Informatique - © Copyright 2022. Tous droits réservés.

- Un poste installé sur un serveur Windows situé dans une zone démilitarisée (DMZ[1]) isolée par des pare-feu, héberge un serveur web, un serveur mobile et un serveur d'accès distant Windows (RDS[2]).
- Les clients peuvent être exécutés à distance au travers d'instances RDS en utilisant le bureau d'accès distant de Windows.
- Une interface installée sur le serveur permet l'affichage des instances clientes sur tous les terminaux supportant HTML5.
- Des clients web permettent l'exploitation depuis un navigateur web standard.
- Une application mobile connectée au serveur mobile est utilisée pour la notification et l'acquittement d'alarmes et le contrôle depuis un smartphone ou une tablette.
- Les échanges entre le serveur Web et les terminaux utilisent des sockets sécurisées sous HTTPS[3].
- Les accès utilisateurs de l'ensemble du système sont gérés par Windows Active Directory permettant l'authentification unique (SSO[4])

Un certain nombre de précautions doivent être prises pour protéger les différents composants d'une architecture multipostes PcVue.
Ainsi, il convient :

- de segmenter les différents réseaux (informatique et industriel par exemple) par la mise en œuvre de réseaux physiques séparés et/ou la création de zones logiques séparées (VLAN[5]) qui requièrent un niveau de sécurité identique
- de filtrer les données par l'utilisation de pare-feu.

L'utilisation d'une DMZ et de routeurs permet également d'isoler les réseaux de l'extérieur et éviter les intrusions indésirables.
La mise en place de solutions de tunneling VPN[6] peut aussi s'avérer nécessaire pour protéger le trafic entre 2 composants du réseau. Typiquement, un VPN pourra être mis en place entre un poste d'acquisition PcVue et un automate communiquant via un protocole TCP/IP, ou entre plusieurs sites de supervision distants communiquant avec la messagerie inter-poste TCP/IP.

---

[1] Demilitarized Zone
[2] Remote Desktop Services
[3] HTTPS : HyperText Transfer Protocol Secure
[4] Single Sign-On
[5] VLAN : Virtual LAN
[6] VPN : Virtual Private Network

Arc Informatique - © Copyright 2022. Tous droits réservés.

2.11 Virtualisation

- ✓ Pour réduire le nombre de postes physiques
- ✓ Pour réduire les efforts d'administration
- ✓ Faible coût des postes banalisés
- ✓ Pas d'installation sur les postes banalisés

La **virtualisation** consiste à faire fonctionner un ou plusieurs systèmes d'exploitations / applications comme un simple logiciel, sur un ou plusieurs ordinateurs - serveurs / système d'exploitation, au lieu de ne pouvoir en installer qu'un seul par machine. Ces ordinateurs virtuels sont appelés serveur privé virtuel (Virtual Private Server ou VPS) ou encore environnement virtuel (Virtual Environment ou VE).

La virtualisation matériel ou de plate-forme se réfère à la création d'un ordinateur virtuel qui agit comme un véritable ordinateur avec un système d'exploitation.
Dans la virtualisation matériel, la machine hôte est la machine réelle sur laquelle la virtualisation a lieu, et l'ordinateur invité est la machine virtuelle. Les termes hôte et invité servent à distinguer les applications qui s'exécutent sur la machine physique des applications qui s'exécutent sur la machine virtuelle.
La virtualisation d'applications industrielles peut bénéficier à de nombreux services : Informatique, ingénierie et opérations.

L'utilisation d'une plateforme de machines virtuelles permet de réaliser le déploiement des architectures décrites précédemment en réduisant le nombre de postes physiques, permettant ainsi de réduire les coûts d'administration.[7]

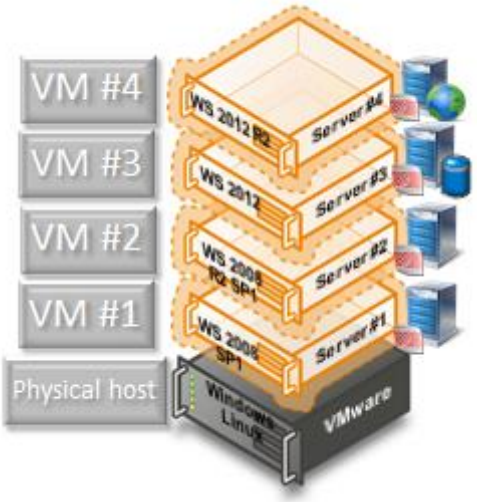
2.11.1 Virtualisation d'application

✓La machine hôte peut exécuter des versions différentes de PcVue ou de FrontVue dans un environnement séparé
✓La mise en place d'environnements de travails dédiés à des opérations ponctuelles est facilitée
✓La mise en place d'un OS ancien est possible
OS supportés: Windows 7, Windows 8, Windows 8.1, Windows 2008 SP2 et 2008 R2 SP1,2012 et 2012 R2 Server et VMWare

[7] Source : Wikipédia

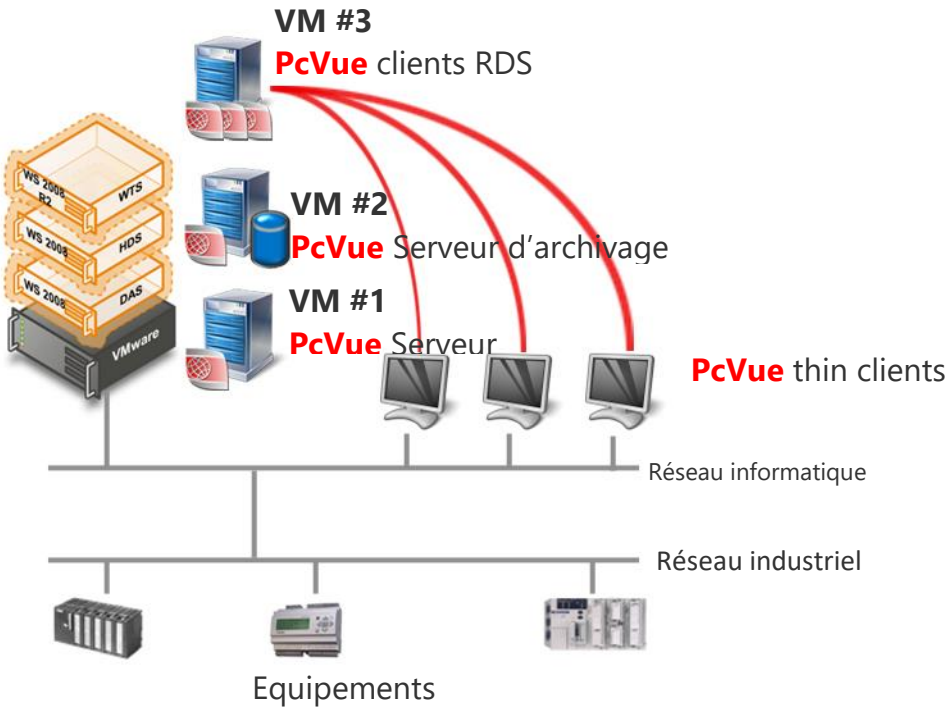
Arc Informatique - © Copyright 2022. Tous droits réservés.

2.11.2 Virtualisation de ressources



✓Les environnements virtuels peuvent exécuter plusieurs serveurs PcVue sous différents OS sur une seule machine physique
✓Les licenses PcVue peuvent de diffèrent type
✓Affectation dynamique de machines virtuelles à l'hôte physique en fonction des règles d'optimisation de ressources

2.11.3 Example d'implementation



Dans cette architecture, l'application de supervision s'exécute sur des machines administrées par un service informatique. Une machine physique unique avec un environnement virtuel VMware ou équivalent, héberge tous les postes dans des machines virtuelles indépendantes, l'une d'elles étant configurée pour servir de serveur de bureau à distance (RDS) permettant à plusieurs clients banalisés de se connecter.
La grande majorité des architectures décrites dans ce document peuvent être envisagées dans un environnement virtuel.

Arc Informatique - © Copyright 2022. Tous droits réservés.

3. Glossaire

Nom	Abbr.	Description
Microsoft® Internet Information Services	IIS	Internet Information Services (IIS) est un serveur Web créé par Microsoft® et livré avec les systèmes d'exploitation Windows. IIS est le serveur Web intégré sur les systèmes d'exploitation Microsoft® Windows.
Poste PcVue Web back end		La station PcVue du réseau industriel sert de passerelle entre le système multiposte PcVue et le serveur Web (IIS). Le serveur Web exécute Sv32.exe, le processus principal de PcVue.
Web Server		L'ordinateur qui exécute le serveur Web IIS, qui héberge à son tour les composants du serveur Web PcVue. Le serveur Web n'exécute pas Sv32.exe (processus principal de PcVue lui-même).
Composants PcVue Web Server		Ensemble de services et d'applications installés sur un serveur Web pour connecter les clients Web et mobiles PcVue.
Clients Web & Mobile		Ordinateurs et périphériques exécutant un client Web WebVue dans un navigateur Web ou une application mobile native telle que TouchVue, sur un périphérique mobile intelligent.
Console de déploiement Web	WDC	L'application de bureau installée sur la machine Web Server, qui permet à l'administrateur système de configurer, déployer et surveiller IIS et les composants du serveur Web PcVue.
Réseau industriel		Les segments de réseau qui incluent le réseau SCADA PcVue. Désigné en tant que réseau industriel de niveau 2 dans le modèle d'information ANSI / ISA-95 (également appelé niveau SCADA).
Zone démilitarisée	DMZ	Une DMZ ou zone démilitarisée - parfois appelée réseau de périmètre - est un réseau physique ou logique qui contient et expose les services externes d'une organisation à un réseau non approuvé, généralement un réseau plus étendu tel qu'Internet. Le but d'une zone démilitarisée est d'ajouter une couche de sécurité supplémentaire au réseau local (LAN) d'une organisation.
Fully Qualified Domain Name	FQDN	Un nom de domaine qui spécifie son emplacement exact dans la hiérarchie de l'arborescence du système de noms de domaine (DNS). Il spécifie tous les niveaux de domaine, y compris au moins un domaine de second niveau et un domaine de premier niveau.
Domain Name System	DNS	Le DNS est un système de nommage hiérarchisé décentralisé pour les ordinateurs, les services ou d'autres ressources connectées à Internet ou à un réseau privé.
Windows Internet Name Service	WINS	WINS est la mise en œuvre par Microsoft® du service NBNS (NetBIOS Name Service), un serveur de noms et un service pour les noms d'ordinateur NetBIOS.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Nom	Abbr.	Description
Sous réseau	Subnet	Un sous-réseau est une subdivision logique d'un réseau IP. Les ordinateurs appartenant à un sous-réseau sont adressés avec un groupe de bits commun, identique et significatif dans leur adresse IP. Le trafic est échangé entre sous-réseaux via des routeurs lorsque les préfixes de routage de l'adresse source et de l'adresse de destination diffèrent. Un routeur sert de limite logique ou physique entre les sous-réseaux.
Virtual Private Network	VPN	Un réseau privé virtuel (VPN) étend un réseau privé sur un réseau public et permet aux utilisateurs d'envoyer et de recevoir des données sur des réseaux partagés ou publics comme si leurs périphériques informatiques étaient directement connectés au réseau privé.
Pare feu		C'est un système de sécurité réseau qui surveille et contrôle le trafic réseau entrant et sortant en fonction de règles de sécurité prédéterminées.
Network Address Translation	NAT	NAT est une méthode pour remapper un espace d'adresses IP en un autre en modifiant les informations d'adresse réseau dans l'en-tête IP des paquets lorsqu'ils sont en transit sur un périphérique de routage de trafic. Une adresse IP routable Internet d'une passerelle NAT peut être utilisée pour un réseau privé entier.
Port Forwarding	PAT	Le transfert de port ou le mappage de port est une application de traduction d'adresse réseau (NAT) qui redirige une demande de communication d'une combinaison adresse / numéro de port à une autre lorsque les paquets traversent une passerelle réseau, telle qu'un routeur ou un pare-feu. Cette technique est le plus souvent utilisée pour rendre des services sur un hôte résidant sur un réseau protégé ou masqué (interne) disponible pour les hôtes situés de l'autre côté de la passerelle (réseau externe), en remappant l'adresse IP de destination et le numéro de port de la communication sur un hôte interne.
Internet Service Provider	ISP	Un fournisseur de services Internet (ISP) est une organisation qui fournit des services pour accéder à, utiliser ou participer à Internet.
Private Key Infrastructure	PKI	Une infrastructure à clé publique (PKI) est un ensemble de rôles, de stratégies et de procédures nécessaires pour créer, gérer, distribuer, utiliser, stocker et révoquer des certificats numériques et gérer le chiffrement à clé publique.
Certificate Authority	CA	Une autorité de certification est une entité qui émet des certificats numériques. L'autorité de certification peut être une tierce partie de confiance ou faire partie d'une infrastructure à clé publique.
Mobile Device Management	MDM	La gestion des appareils mobiles est un terme utilisé dans l'industrie pour l'administration des appareils mobiles, tels que les smartphones, les tablettes, les ordinateurs portables et les ordinateurs de bureau. MDM traite principalement de la ségrégation des données d'entreprise, de la sécurisation des courriers électroniques, de la sécurisation des documents d'entreprise sur les appareils, de l'application des stratégies d'entreprise, de l'intégration et de la gestion des appareils mobiles.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Nom	Abbr.	Description
Hypertext Transfer Protocol Secure Hypertext Transfer Protocol	HTTP / HTTPS	Le protocole HTTP (Hypertext Transfer Protocol) est un protocole d'application destiné aux systèmes d'information distribués, collaboratifs et hypermédia. HTTP est la base de la communication de données pour le World Wide Web. HTTPS (HTTP Secure) est une extension du protocole HTTP (Hypertext Transfer Protocol) pour une communication sécurisée. Le protocole est souvent appelé HTTP sur TLS ou HTTP sur SSL.
Hairpinning		Hairpinning (également appelé "NAT loopback") décrit une communication entre deux hôtes situés derrière le même périphérique NAT à l'aide de leur point d'extrémité mappé. En épingle à cheveux, une machine du réseau local peut accéder à une autre machine du réseau local via l'adresse IP externe du réseau local / routeur (avec la redirection de port configurée sur le routeur pour diriger les demandes vers la machine appropriée du réseau local).
WebSocket(s)		WebSocket (RFC 6455) est un protocole de communication informatique fournissant des canaux de communication en duplex intégral via une seule connexion TCP. WebSocket est conçu pour fonctionner sur les ports HTTP 80 et 443 ainsi que pour prendre en charge les proxy HTTP et les intermédiaires. Analog to HTTP WebSocket prend en charge le cryptage via sa liaison wss (Web Socket Secure).
HTTP/2 - SPDY protocol		HTTP / 2 est une révision majeure du protocole de réseau HTTP. Il a été dérivé du protocole expérimental SPDY antérieur. Les principales améliorations apportées par l'évolution du protocole concernent la réactivité des sites Web en introduisant une latence réduite, la compression d'en-tête, le multiplexage TCP et le traitement en pipeline des demandes.

Arc Informatique - © Copyright 2022. Tous droits réservés.

Table des illustrations

Figure 1 - Poste autonome 9
Figure 2 - Multi-postes 11
Figure 3 - Bureau à distance 12
Figure 4 - Haute disponibilité 13
Figure 5 – Redondance 16
Figure 6 – Redondance 17
Figure 7 – Redondance RDS 18
Figure 8 - Serveur mutualisé 19
Figure 9 - Multi-niveau implémentation 1 21
Figure 10 - Multi-niveau implémentation 2 23
Figure 11 - Poste de développement 31
Figure 12 - Console de déploiement web et mobile 34
Figure 13 – Vue d'écran - Client web HTML5 35
Figure 14 – TouchVue : vues d'écran 36
Figure 15 – SnapVue : principe de fonctionnement 37
Figure 16 – SnapVue : technologies utilisées 37
Figure 17 – SnapVue : vues d'écran 38
Figure 18 – Bureau d'accès à distance 39
Figure 19 – Architecture #1 – Déploiement "tout-en-un" 40
Figure 20 – Architecture #2 – Network isolation and DMZ 43
Figure 21 - DMZ – Single firewall setup 44
Figure 22 - DMZ – Dual firewall setup 44
Figure 23 - Architecture #3 – Scénario NAT simplifié pour l'accès à distance 47
Figure 24 - Architecture mixte 50

Arc Informatique - © Copyright 2022. Tous droits réservés.

ARC Informatique
S.A.S au capital de 1 250 000 €
RCS Nanterre B 320 695 356
APE 5829C
SIREN 320 695 356
VAT N°FR 19320695 356

PcVue - Architectures & déploiement

© Copyright 2022. Tous droits réservés.
Toute reproduction intégrale ou partielle de ce document sans autorisation écrite est strictement interdite. Les noms et marques déposées mentionnés appartiennent à leurs propriétaires respectifs.

ARC Informatique

Siège social
2 avenue de la Cristallerie
92310 Sèvres - France

tel + 33 1 41 14 36 00
fax + 33 1 46 23 86 02
hotline +33 1 41 14 36 25
arcnews@arcinfo.com
www.pcvuesolutions.com

Aix-en-provence
Le Galice Mirabeau - Bât C
11, rue Louise Colet
13090 AIX-EN-PROVENCE

Tel: + 33 4 42 52 36 83
Fax: + 33 4 42 29 74 55
email: arcaix@arcinfo.com

Grenoble
120, chemin de l'étoile
38330 MONTBONNOT-SAINT-MARTIN – France

Tel: + 33 4 76 1873 01
Fax: + 33 4 76 41 06 71
email: arcgrenoble@arcinfo.com

Lyon
Les Jardins d'Eole
1, allée des Séquoias «Le Shamal»
69760 LIMONEST - France

Tel: + 33 4 78 35 93 93
Fax: + 33 4 78 35 35 92
email: arclyon@arcinfo.com

Douai
ZI La Renaissance
59490 SOMAIN - France

Tel: + 33 3 27 80 86 80
Fax: + 33 3 27 80 86 87
email: arcdouai@arcinfo.com

Strasbourg
Immeuble le Véga
5 rue de Dublin
67300 SCHILTIGHEIM - France

Tel: +33 3 88 210 210
Fax: +33 3 88 210 211
email: arcstrasbourg@arcinfo.com