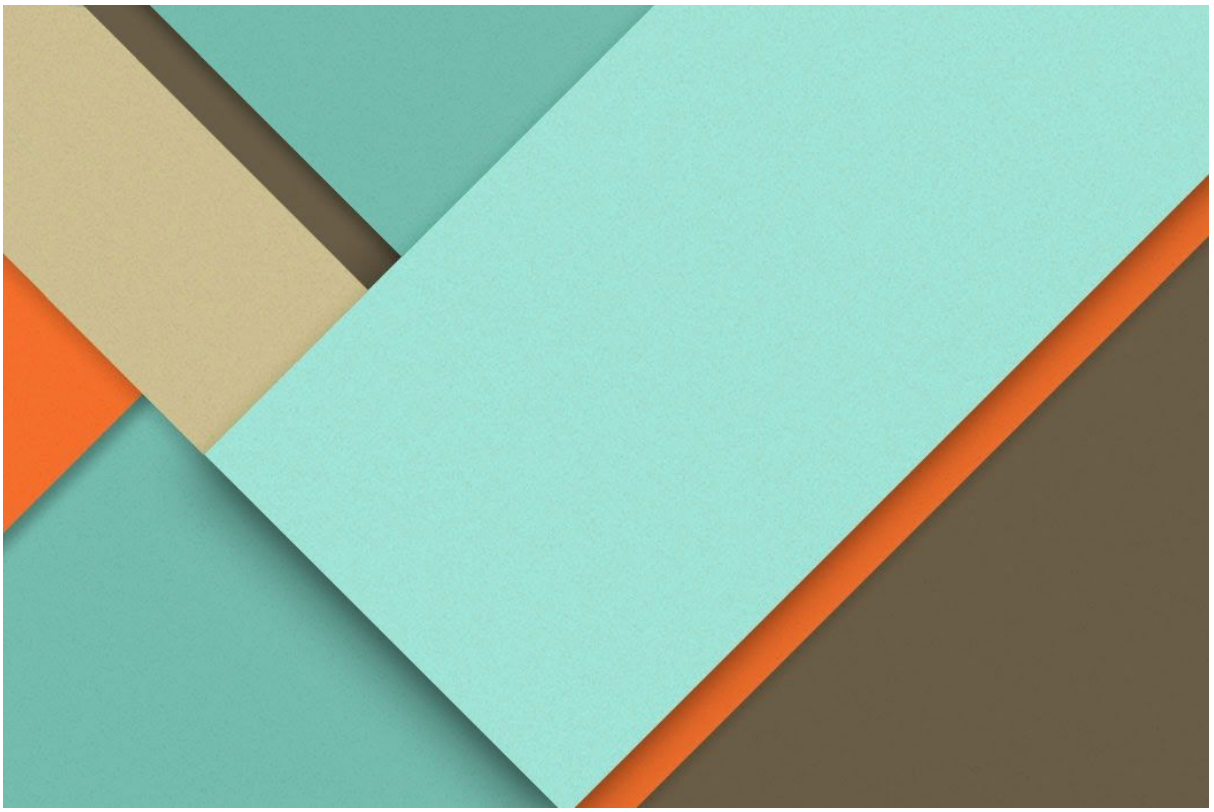


Les Artisans Réunis

Règles d'architecture et de sécurité V36.0

19.11.2019

Les Artisans Réunis
123 Votre rue
00000 Votre ville

Gestion documentaire

Versioning

Version	Date	Modifications	Rédacteur	Correcteur	Statut
1.0	19/09/2009	Initialisation	ADI	Aimée Nervgrave	Corrigé
...	...	...	...	...	...
32	27/04/2018	Version Ubuntu Server à utiliser : 18.04 LTS	ADI	Aimée Nervgrave	Corrigé
33	20/10/2018	- Visual Basic.NET désormais proscrit - WinDev et WinDev Mobile : Framework préconisé	OGU	Aimée Nervgrave	En cours
34	15/08/2019	Version Apache à utiliser : 2.4.41	ADI	Aimée Nervgrave	Corrigé
35	15/10/2019	Création du Trigramme DTE	ADI	Aimée Nervgrave	Corrigé

Liste de diffusion

Nom et prénom	Rôle	Actions
Aimée Nervgrave	Architecte	Rédacteur
Cécile Hontoussa	Architecte	Correcteur
Ella Lapêche	DSI	Approbateur

Table des matières

Règles d'architecture

Nomenclature

Dans un souci de normalisation, la société "Les Artisans Réunis" a défini une nomenclature générale à appliquer à l'ensemble des composants de l'architecture.

Codes site de l'entreprise

Le code site est l'identifiant d'un établissement de l'entreprise. Il doit être utilisé afin de rattacher chaque objet du SI à son établissement.

Sièges sociaux :

- Préfixe = SOC
- Suffixe = 999 => Numérique chronologique sur 3 caractères

Directions régionales :

- Préfixe = DIR
- Suffixe = 999 => Numérique chronologique sur 3 caractères

Agences :

- Préfixe = AGE
- Suffixe = 999 => Numérique chronologique sur 3 caractères

Trigrammes application

Depuis le 01/01/2010, chaque application utilisée par la société "Les Artisan Réunis" est identifiée par un trigramme unique communiqué par l'équipe Architecture en début de projet. Les applications antérieures au 01/01/2010 seront revues dans le cadre d'un plan de migration sur 2 ans.

Liste des applications par trigramme

Trigramme	Criticité	Application	Chef de SQUAD	Équipe Support
DEV	C2	MonBonDevis	Georgette Tousskjebouf	Front-Office
ERP	C1	ODOO	Adam Troijours	Back-Office
MSG	C3	Messagerie	Édith Orial	End User
DTE	C2	Devis To ERP	Adam Troijours	Back-Office
LDP	C1	LDAP	Édith Orial	End User
DCP	C1	Active Directory	Édith Orial	End User
DVF	C3	Devis Vers Facture	Camille Onette	Front-Office

				Back-Office

Serveurs

Nom DNS - 999888777XXX6666
999 = Code société
888 = Code direction régionale
777 = Code agence
XXX = OS (Windows = WIN - Linux = LNX)
6666 = Numéro chronologique

Criticité des applications

Le niveau de criticité des applications est dicté par le besoin fonctionnel. Il est relatif au niveau de SLA.

C1

Application critiques nécessitant une disponibilité de 99.9 %, 24 heures sur 24 et 7 jours sur 7.
Les applications C1 doivent être totalement redondées et scalables.
=> Serveurs d'application loadbalancés derrière une VIP.
=> Base de données : Oracle RAC.

C2

Application critiques nécessitant une disponibilité de 99.5 %, 10 heures sur 24 et 5 jours sur 7.
Les applications C2 peuvent être arrêtées en semaine entre 19:00 et 8:00 ainsi que les samedis et dimanches.
Les applications C2 doivent être totalement redondées et scalables.
=> Serveurs d'application loadbalancés derrière une VIP.
=> Base de données : Cluster Oracle, SQL Server ou PostgreSQL.

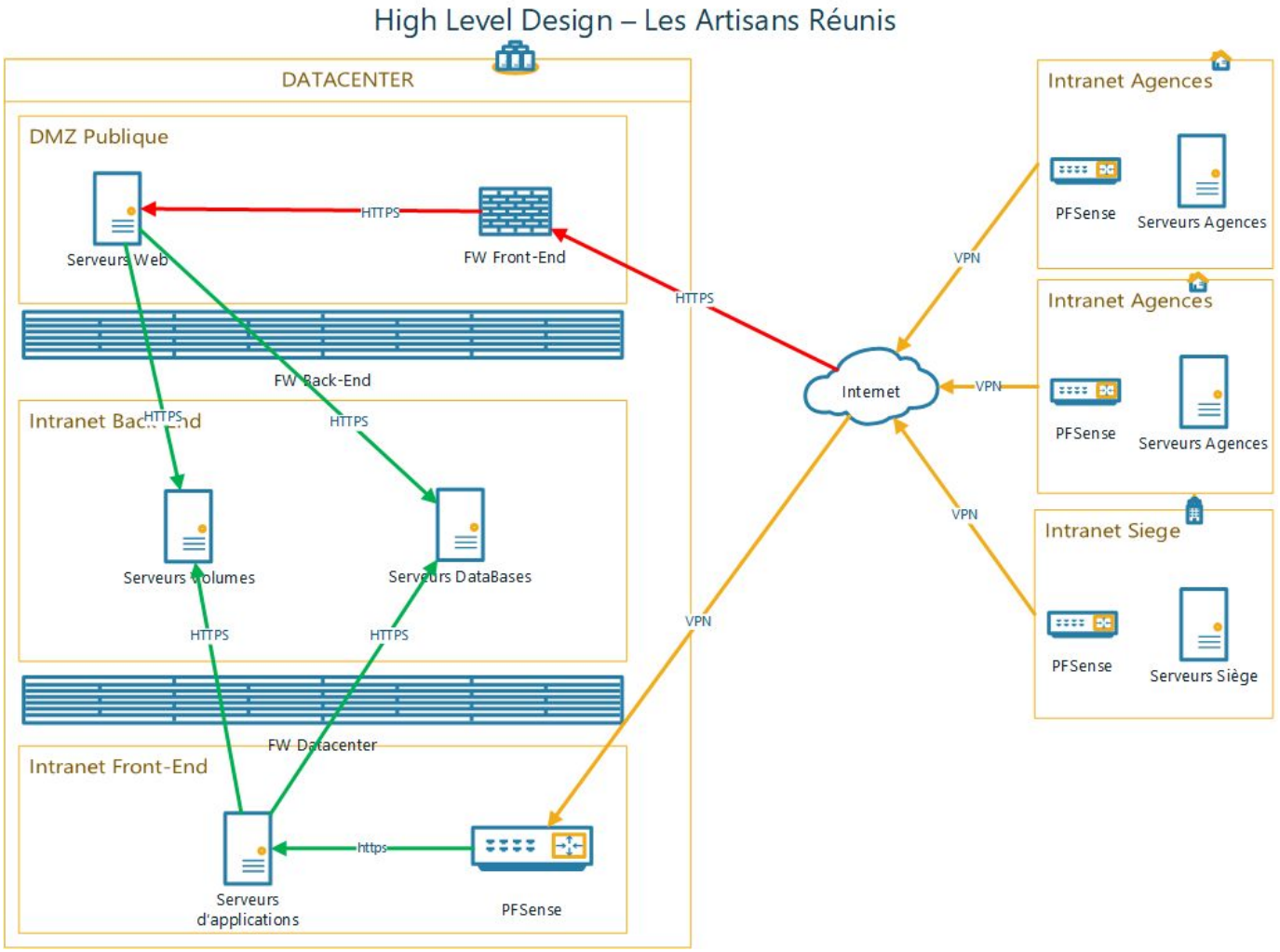
C3

Application non-critique pouvant supporter une interruption de service de 2 jours consécutifs en heures ouvrées.
=> Aucune exigence d'architecture.

Diagrammes d'architecture

Les agences sont connectées au siège au travers d'un VPN, les utilisateurs et les postes de travail se connectent au réseau de l'entreprise et sont authentifiés via un serveur Active Directory.

Vue générale



Data center

Authentification

Active Directory

LDAP

Pour toute application interactive (web ou Windows), un écran d'authentification permet à l'utilisateur de se connecter au travers de LDAP.
Pour toute application batch, la connexion au LDAP est réalisée via l'utilisateur technique user_ldap_xxx.

Siège social

Agence type

Transfert de fichiers

L'entreprise ne détient aucun outil du marché pour les transferts de fichiers entre les sites.
À défaut d'outils, le protocole préconisé est SFTP sur le port 22.
Préconisation : lorsque c'est possible, c'est le serveur télécollecte qui initie le téléchargement de fichiers sur le serveur de fichiers agence.

Bases de données

MySQL : à partir du 01/06/2019, MySQL est à proscrire pour tout nouveau projet.

PostgreSQL
Version à utiliser pour chaque nouveau projet : 11.5.
Les applications utilisant la version 10.10 devront être migrées avant le 10/11/2022.

Oracle
Oracle, en raison du coût de la licence, n'est à utiliser que dans le cadre d'applications nécessitant :

- plus de 1 000 connexions simultanées ;
- des tables contenant plus de 1 000 000 de lignes.

Couches de persistance

Quelle que soit la base de données ciblée, chaque application devant se connecter utilisera un "User Applicatif" dont les login et password sont normalisés.

- Login : user_app_xxx => xxx représentant le Trigrame de l'application.
- Password : le password sera communiqué par l'équipe Sécurité lors de la création du user applicatif.

Droits en lecture/écriture sur la base de données.
À noter : l'accès aux bases Access n'est quant à lui pas protégé.

Règles d'hébergement

Data center

L'entreprise dispose d'une infrastructure serveurs et réseau hébergée dans un data center.
Les applications centralisées sont hostée sur des serveurs virtuels VMWare.

Local Technique
Chaque site (siège social y compris) dispose d'un local technique conçu et maintenu dans les règles de l'art par la société "SMRG".

Cloud
Lorsque cela sera pertinent et sur proposition des chefs de projet, l'entreprise pourra décider d'héberger ses applications web sur le Cloud AWS.

Règles relatives aux serveurs agence

Plan d'adressage IP
VPN agences : 192.168.999.0/24 avec 999 = Code agence
Serveurs agence

Système d'exploitation
OS : Windows Server Standard 2019.
Services :

- Terminal Services
- DHCP
- DNS
- AD Secondaire
- Serveur de fichiers

Files system
- Le système est installé sur C:\
- Fichier de configuration : C:\config\config.inf
- Les applications sont installées sur D:\apps\trigramme_application
- Les données applicatives sont installées sur E:\apps\trigramme_application
- Les fichiers à envoyer au siège sont dans E:\Data\Out\trigramme_application
- Les fichiers reçus du siège sont dans E:\Data\In\trigramme_application
- Après traitement, les fichiers traités sont déplacés dans E:\Data\Old\trigramme_application
- Les fichiers de log et d'erreur sont dans : E:\apps\data\trigramme_application\log

Contenu de config.inf
[AGE]
AGE=XXX

Règles relatives aux postes de travail

Système d'exploitation

OS : Windows 10 Entreprise LTSC 2019

Files system

- Le système est installé sur C:\
- Les applications sont installées sur D:\

Règles relatives aux serveurs data center

Plan d'adressage IP

Siège : 10.0.999.0/24 avec 999 = Code société

Nom DNS

XXXYYY999999
XXX = Géographie (MPL = Montpellier - LYO = Lyon)
YYY = OS (WIN = Windows - LNX = Linux)
99999 = Numéro chronologique

Système d'exploitation

OS : Windows Server Standard 2019.
Services :

- Terminal Services
- DHCP
- DNS
- AD Primaire
- Serveur de fichiers

Serveurs Infrastructure

- Active Directory : 10.0.1.1
- LDAP : 10.0.1.2
- PFsense : 10.0.1.3

Files system

- Le système est installé sur C:\
- Les applications sont installées sur D:\apps\trigramme_application

- Les données sont installées sur E:\apps\data\trigramme_application
- Les fichiers à envoyer aux agences sont dans E:\Data\Out
- Les fichiers reçus des agences sont dans E:\Data\In
- Après traitement, les fichiers traités sont déplacés dans E:\Data\Old
- Les fichiers de log et d'erreur sont dans : E:\apps\data\trigramme_application\log

Règles relatives aux serveurs web et application

Sauf exception justifiée :

- OS - Ubuntu Serveur 18.04 LTS
- Serveur web : Apache 2.4.41
- Serveur d'application : Tomcat

Dans tous les cas :

- Port HTTPS (443)
- Certificat : SHA256

Règles relatives aux serveurs d'application

Cette section n'est pas consultable.

Règles relatives au patching

"Les Artisans Réunis" sont intransigeants sur la sécurité. Aussi, un planning annuel de mise à jour de sécurité est mis en œuvre de manière à ce que tous les serveurs de l'entreprise soient patchés et rebootés une fois par mois.

Périmètre :

- Système d'exploitation : Windows - Linux
- Base de données : Oracle - SQL Servers - MySQL - PostgreSQL - HFSQL
- Middleware : WAS - TOMCAT - APACHE - EAI

Impact sur les applications :

Dans le souci de garantir un niveau de service acceptable, notamment pour les applications en 24/7, l'architecture technique doit être redondante sur toutes ses couches.
Lorsque la redondance n'est pas justifiée (application 10/5), les applications concernées par l'intégration applicative devront être "bouchonnées" et les plans batch devront prévoir un "plan de reprise".

Stratégies de sauvegarde

Les sections suivantes ne sont pas consultables :

- *Applications C1*

- *Applications C2*
- *Applications C3*

Bases de données

Fréquence	Type	Rétention
Journalière	Log	14 jours
Hebdomadaire	Dump	5 semaines
Mensuelle	Dump	13 mois

Système d’exploitation

Fréquence	Type	Rétention
Journalière	Incrémentale	14 jours
Hebdomadaire	Différentielle	5 semaines
Mensuelle	Full	13 mois

Système de fichiers

Fréquence	Type	Rétention
Journalière	Incrémentale	14 jours
Hebdomadaire	Incrémentale	5 semaines
Mensuelle	Full	13 mois

VM (Machine Virtuelle)

Fréquence	Type	Rétention
Journalière	Full	14 jours

Règles relatives aux développements spécifiques

Visual Basic.NET

L'essentiel du patrimoine applicatif "Client Lourd" pour Windows est développé en Visual Basic.NET sur le framework Visual Studio.NET.
20/10/2018 : Un projet de décommissionnement sur 3 ans des applications Visual Basic a été ouvert. Sauf dérogation, ce framework est désormais à proscrire chez "Les Artisans Réunis".

WinDev et WinDev Mobile 24

20/10/2018 : À compter de ce jour, tout nouveau projet de développement pour Windows ou application mobile sera réalisé sous WinDev en WLangage.
Les cibles concernées sont :

- les clients lourds ;
- les services Windows.

Applications web

20/10/2018 : À compter de ce jour, les applications web de la société "Les Artisans Réunis" doivent être développées en PHP / Symfony.
En cas d'incompatibilité avec un projet, et sur dérogation, il sera possible de s'appuyer sur le serveur d'application Java J2EE.

Règles de sécurité

Gestion des droits d'accès

AD pour Users et Computers.
Accès aux applications géré par LDAP.

Comptes techniques

(xxx = trigramme de l'application)
(999 = code site)

Batchs : user_batch_xxx
LDAP : user_ldap_xxx
Database : user_dba_xxx
SFTP Siège : user_sftp_soc999
SFTP agences : user_sftp_age999

Antimalware

La mise à jour des antivirus et antimalwares des serveurs de l'entreprise est prise en charge par un serveur SEP.

Ports serveur

Par défaut, lors du build des serveurs, tous les ports d'écoute sont fermés.
Les chefs de projet sont chargés de demander l'ouverture des ports nécessaires au bon fonctionnement de leur application.

Firewall

Chaque site de l'entreprise est équipé d'un routeur pfSense protégé par les fonctionnalités Firewall et VPN.