19/04/2024

Lucas DEGRET, François BRASY, Julien LEBRIS, Théodore PALIANI

wILD cODE sCHOOL

EcoSolar Solutions

Dossier Projet

[Contexte 1](#_Toc235184752)

[Historique 1](#_Toc1715855509)

[Installation et processus 1](#_Toc1603457538)

[Enjeux 1](#_Toc1299983899)

[Besoins 1](#_Toc885233327)

[Réseau 2](#_Toc723183464)

[Infrastructure actuelle 2](#_Toc1092665504)

[Conception du réseau proposé 2](#_Toc1527343054)

[Topologie physique 2](#_Toc498749900)

[Topologie logique 2](#_Toc2038278360)

[Composants réseau 2](#_Toc719439516)

[Switches et routeurs 2](#_Toc509888988)

[Points d'accès sans fil 2](#_Toc2113751318)

[Matériel de Datacenter 3](#_Toc586159057)

[Protocoles et services 3](#_Toc183836276)

[DHCP, DNS, SMTP 3](#_Toc2047304469)

[VPN, MPLS, QoS 3](#_Toc117130774)

[Redondance et haute disponibilité 3](#_Toc757776508)

[WAN et LAN 3](#_Toc1322158190)

[Services réseaux et web 3](#_Toc548564088)

[Connectivité 3](#_Toc1239151859)

[Interne (LAN, WLAN) 3](#_Toc1843876908)

[Externe (WAN, Internet) 3](#_Toc122918806)

[Plan d’adressage IP 3](#_Toc1311679665)

[Sécurité réseau 3](#_Toc785072280)

[Firewall, Proxy, Reverse proxy 3](#_Toc97505807)

[Sécurité 3](#_Toc1139054758)

[Analyse des risques 4](#_Toc2105088409)

[EBIOS, Mehari 4](#_Toc33278504)

[Politique de sécurité 4](#_Toc685778923)

[ISO 27000 4](#_Toc1175060951)

[Sécurité physique et logique du Datacenter 4](#_Toc108399299)

[Sécurité des données 4](#_Toc2010632292)

[Cryptographie, PKI et certificats 4](#_Toc1292769276)

[Contrôle d'accès 4](#_Toc53885722)

[LDAP/LDAPS, MFA, Zero trust 4](#_Toc1383847148)

[Protection des endpoints 4](#_Toc330906101)

[Antivirus, EDR 4](#_Toc656966519)

[Sécurité des communications 4](#_Toc89951583)

[SSH, SSL/TLS, DNSSEC 4](#_Toc1747479697)

[Supervision de la sécurité 4](#_Toc981444914)

[SIEM, SOC 4](#_Toc1277233940)

[Plan de réponse aux incidents 5](#_Toc1058921909)

[Détection, réaction et reporting 5](#_Toc173469836)

[Documentation 5](#_Toc1046879079)

[Documentation technique 5](#_Toc1208341667)

[Diagrammes de réseau 5](#_Toc1544477698)

[Spécifications des équipements 5](#_Toc1563224022)

[Manuels d'exploitation 5](#_Toc130063192)

[Procédures opérationnelles 5](#_Toc1883219274)

[Guides d’utilisation 5](#_Toc1242344629)

[Documentation de configuration 5](#_Toc996825622)

[Scripts d'automatisation 5](#_Toc602912458)

[Configurations des équipements 5](#_Toc1694086936)

[Documentation de sauvegarde 5](#_Toc833703483)

[Plans de sauvegarde et restauration 5](#_Toc986742798)

[Documentation de sécurité 5](#_Toc1497651121)

[Politiques de sécurité 6](#_Toc1654718622)

[Plans de réponse aux incidents 6](#_Toc1867179409)

[Sauvegarde 6](#_Toc1089077250)

[Stratégie de sauvegarde 6](#_Toc1071284229)

[Sauvegardes sur site et hors site 6](#_Toc644296094)

[Plan de continuité d’activité (PCA) 6](#_Toc334352102)

[PRA/PCA, Redondance des données 6](#_Toc1292834688)

[Solutions de sauvegarde 6](#_Toc310291932)

[Logiciels et matériel utilisés 6](#_Toc1655110604)

[Tests et validation 6](#_Toc2011608210)

[Fréquence des tests de restauration 6](#_Toc1607894542)

[Stockage sécurisé 6](#_Toc1089848317)

[Solutions de stockage distribué 6](#_Toc150179562)

[Système 6](#_Toc1602274101)

[Infrastructure serveur 7](#_Toc846072127)

[Hyperviseurs, serveurs physiques et virtuels 7](#_Toc1821641107)

[Systèmes d’exploitation 7](#_Toc2000485960)

[Windows Server, Linux 7](#_Toc178731711)

[Services systèmes 7](#_Toc941074452)

[Active Directory, Serveur de fichiers, Serveur de messagerie 7](#_Toc1099833919)

[Gestion des applications métier 7](#_Toc1979310026)

[ERP, CRM 7](#_Toc863162265)

[Automatisation et gestion de configuration 7](#_Toc943684592)

[Scripts, Ansible, etc. 7](#_Toc640662341)

[Supervision 7](#_Toc1304095881)

[Outils et indicateurs de performance 7](#_Toc240120755)

[Virtualisation 7](#_Toc461998826)

[Proxmox, Cluster d'hyperviseur 7](#_Toc202825750)

Cloud Computing 7

[Annexe 8](#_Toc1879647820)

[Tableau 1: Liste du personnel 16](#_Toc164258124)

# Contexte

## Historique

Entreprise fondée, implémentée à Toulouse en 2010 et pionnière spécialisée dans les énergies renouvelables, dédiée au développement et à la fabrication de panneaux solaires à haut rendement. L’entreprise dispose d’un petit Datacenter à Marseille. Elle emploie actuellement une cinquantaine de personne avec une perspective de passer à 80 voire plus.

## Installation et processus

L’ensemble des bureaux, ateliers et entrepôt se trouvent à Toulouse dans un bâtiment plein pied et possède un Datacenter à Marseille.

La production est semi-industrielle :

* Automate non-connecté au SI, conduis par conducteurs de machine et opérateur d’atelier
* Gestion de stock par ERP (Dolibarr), saisie d’information via tablette industriel
* Données et documents lié aux processus et aux produits : Factures, bon de commandes, demandes d’achat, secret industriel … (certains en papier).

## Enjeux

### Croissance Exponentielle :

Avec une demande croissante pour ses panneaux solaires haute performance, SolarEco Solutions doit moderniser son infrastructure informatique pour gérer l'augmentation rapide des données et assurer une gestion efficace de la production.

### Sécurité des accès :

Les commerciaux de l'entreprise ont besoin d'accéder à l'ERP/CRM de l'entreprise de manière distante pour gérer efficacement leurs activités, accéder aux informations clients, et mettre à jour les données en temps réel. Cela soulève des enjeux spécifiques liés à la sécurité, à la disponibilité, et à la performance de ces accès distants.

### Sécurité des Brevets et Données :

La protection des brevets et des données de conception est une priorité cruciale pour assurer la pérennité de la technologie exclusive de SolarEco Solutions. Des mesures de sécurité informatique renforcées sont nécessaires pour garantir la confidentialité et l'intégrité des informations sensibles.

### Optimisation de la Chaîne d'Approvisionnement :

Avec l'engagement d'utiliser exclusivement des matériaux français, SolarEco Solutions doit optimiser sa chaîne d'approvisionnement grâce à des solutions informatiques efficaces pour suivre les stocks, les commandes et garantir la traçabilité des matériaux.

### Expansion du Datacenter :

Avec l'investissement dans un petit datacenter, SolarEco Solutions doit planifier son expansion pour répondre aux besoins croissants de stockage de données tout en garantissant la sécurité et la disponibilité des informations cruciales.

## Objectif

L’enjeu majeur est de faire une refonte totale du Service Informatique actuel :

* Modernisation de l’infrastructure actuel
* Aménager le Datacenter
* Mise en place des bonnes pratiques, démarche de gestion des risques, accès distant
* Informatiser l’activité (gestion de prod, gestion commerciale, communication vers l’extérieur)

# Modernisation de l’infrastructure

## Etat des lieux

### Architecture Locale

#### Schéma topologique

Voici une représentation logique de l’infrastructure informatique local de l’entreprise.

Une image contenant texte, diagramme, ligne, Parallèle

Description générée automatiquement

#### Adressage

L’entreprise comprend un seul réseau IPv4 de classe C privé 192.168.128.0/24. Il a une étendueDHCP pour les 200 premières machines, les 54 dernières adresses sont fixes pour serveurs, imprimantes, etc.

#### Topologie

La connexion des équipements réseaux est effectuée de façon directe. L’entreprise comprend :

* Un boitier type « box Internet » fourni par le Fournisseur d’Accès Internet (FAI) qui lui attribue une adresse IP publique, un service DNS, internet fibré et d’un service de relais SMTP.
* Un Firewall, Appliance Pfsense, avec pour règle « permit all any any » qui est définie sur l’interface LAN.
* De switches de niveau 2 administrables où dessus n’existe qu’un seul VLAN et où tous les nœuds sont raccordés sur ce switch (serveurs, NAS, périphériques, etc.).
* 2 points d’accès wifi en WPA2

### Socle Système

La majeure partie des services de l’entreprise fonctionne sur un hyperviseur Proxmox VE contenant 5 VM :

* 1 Serveur Windows 2019 Standard avec fonctionnalités AD, DNS, DHCP
* 1 Serveur Debian avec l’ERP DOLIBARR
* 1 serveur téléphonie
* 1 serveur mail
* 1 serveur Debian 12 avec GLPI installé. Utilisateurs importés depuis l’AD, l’agent GLPI est installé sur Serveur Windows et Linux mais pas sur les postes ni les périphériques type tablette ou smartphone.

Il contient aussi un NAS servant de serveur de fichier.

### Périphériques

L’infrastructure utilise plusieurs types de périphériques :

* Tablettes Android
* Smartphones
* Téléphones IP + softphones
* Ordinateurs portables et fixes sous Windows intégrés au domaine
* Imprimantes

### Architecture Datacenter

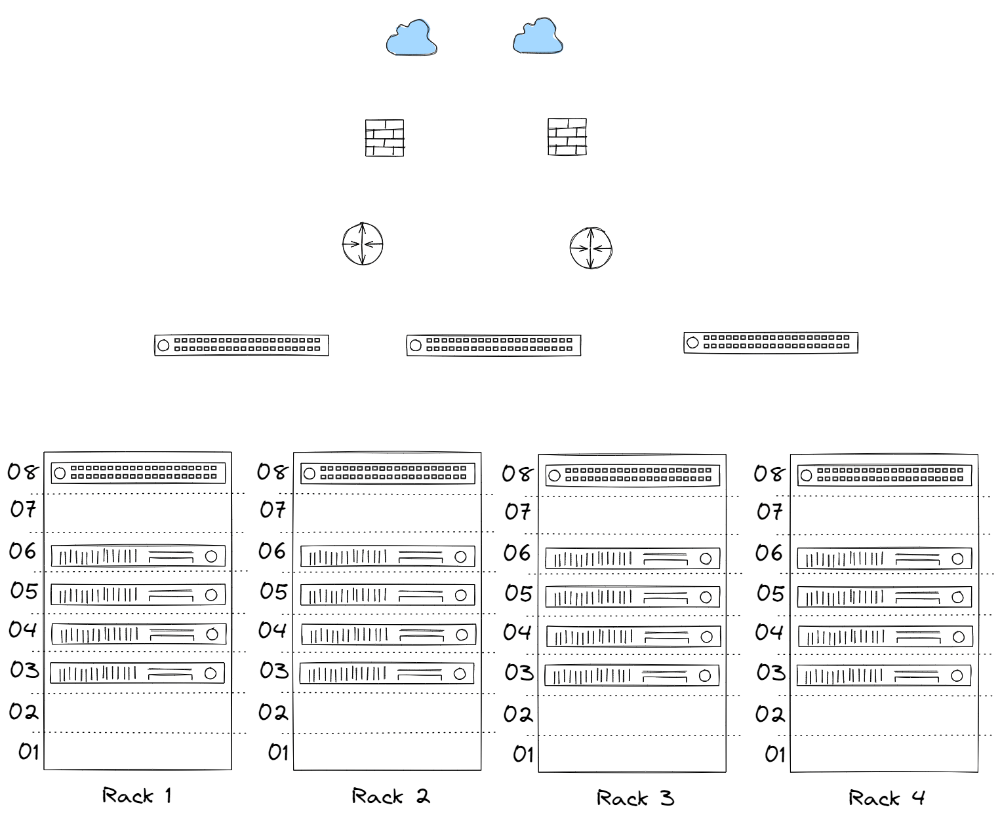
#### Accès

Le datacenter, d'une superficie de 50 M2, a été racheté en début d'année, et dispose de tous le nécessaire en termes de sécurité :

* Sécurité physique : contrôle d'accès par badge et biométrie
* Surveillance vidéo sur tout le site
* Gardiennage
* Sécurité électrique (multi-arrivées électriques, secours onduleurs et groupe électrogène)
* Sécurité anti-incendie (détection par aspiration d'air et analyseur laser, extinction par gaz inerte dans la salle DataCenter)
* Climatisation free-cooling basse consommation environnementale et aller froide sou pression
* Et bien entendu, une magnifique ferme de **panneaux solaires** et des accumulateurs électriques permettant de stocker l'énergie produite non consommée, et venant compléter l'installation électrique traditionnelle.

#### Schéma Topologie

Voici une représentation logique de l’infrastructure informatique du Datacenter.



#### Topologie

L'infrastructure du bâtiment est opérationnelle, le DataCenter dispose de 4 baies 19 pouces, il reste à concevoir la partie infrastructure informatique au niveau architecture réseau (switchs, serveurs, routeurs, firewall) pour répondre aux besoins des communications externe (nord/sud) et interne (est/ouest).

Chaque baie est équipée de 4 serveurs physiques et d'un switch de type "leaf switches".  
On retrouve aussi 3 switchs de type "Spine switches", 2 routeurs, 2 firewalls et 2 liaisons WAN fibrées.

Tout cet ensemble n'est ni brassé ni configuré et donc pas opérationnel.

## Problématiques

### Sécurité

#### Firewall unique

La topologie montre qu'il y a un seul pare-feu reliant l'ensemble du réseau interne à l'Internet. Cela crée un point de défaillance unique et expose potentiellement le réseau interne aux attaques externes si le pare-feu est compromis.

#### Accès Wi-Fi

L'accès Wi-Fi semble être disponible à la fois dans les bureaux et l'atelier sans indication de mesures de sécurité spécifiques.

#### Hyperviseur et VMs

Les machines virtuelles (VM) sur l'hyperviseur semblent être directement connectées au même réseau que le reste des bureaux. Cela peut exposer les VMs à des menaces internes.

### Disponibilité

#### Points de défaillance uniques (SPOF – Single Point Of Failure)

Le schéma montre plusieurs points de défaillance uniques, comme un seul commutateur reliant toutes les sections du réseau et un seul hyperviseur.

#### NAS unique

Le stockage NAS (Network Attached Storage) est un point de défaillance unique pour les données.

### Intégrité

#### Protection des données :

Il n'y a pas de mention de sauvegardes ou de mesures de protection des données.

#### Contrôle d'accès :

L'absence de segmentation claire du réseau pourrait permettre à des utilisateurs non autorisés d'accéder à des ressources sensibles.

## Améliorations proposées

### Sécurité

#### Firewall double

Un second firewall sera dans l’infrastructure pour créer une redondance.

Actif/Passif avantages => Couvert en cas de panne actif tombe = passif prend le relais.

DOC + VM par Théodore à faire pour vendredi 26/07

#### Accès Wi-Fi

A FAIRE, A VOIR PAR QUI

### Disponibilité

#### Redondance

Une implémentation d’une redondance au niveau des commutateurs càd ajout de 2 switches N3 neufs et 1 switch N2 neuf, nous garderons les anciens switches N2 qui sont déjà présent de l’entreprise. Pourquoi ? Permet de segmenter le réseau en plusieurs VLAN pour isoler les différentes sections de l’entreprise et de configurer une haute disponibilité au sein du réseau.

#### Hyperviseur et VMs

A FAIRE, A VOIR PAR QUI

#### NAS Secondaire

Un second NAS sera ajouté à l’infrastructure de façon à créer un cluster haute disponibilité. Le terme « haute disponibilité » fait référence à une solution de configuration de serveur conçue pour réduire les interruptions de service causées par des dysfonctionnements du serveur. On utilise deux hôtes pour former un « cluster high-availability » dans lequel un hôte assume le rôle de « serveur actif » et l'autre hôte agit comme un « serveur passif » de secours.

Dans un cluster high-availability, les données du serveur actif sont répliquées en continu sur le serveur passif, de sorte que des copies en miroir de tous les fichiers existent sur les deux hôtes. Par conséquent, en cas de panne ou de dysfonctionnement du serveur actif, le serveur passif peut prendre en charge tous les services, minimisant ainsi les temps d'arrêt du système.

### Intégrité

#### Protection des données :

L’utilisation de protocole sécurisée (HTTPS, SFTP…) permettront de protéger les données en transit.

Un VPN sera mis en place pour assurer les connexions à distance.

A REMPLIR LORSQUE NOUS AURONS FAIT LE COURS

#### Contrôle d'accès :

Pour les routeurs et les commutateurs, nous mettrons en place des ACL (Access Control List). L’utilisation des politiques RBAC (Role By Access Control) servira à limiter l’accès aux ressources critiques seulement aux utilisateurs autorisés. De plus, nous ajouterons et créerons des politiques strictes.