

Les caractéristiques techniques de logiciel COMDEV ERP/CRM

Le présent document a pour but de vous décrire les principales caractéristiques de notre solution ComDev CRM/ERP v3.7.

Alger le, 11/03/2024

Objet :

Ce document a pour objectif de présenter **Les caractéristiques techniques de logiciel ComDev ERP/CRM**

La Sarl Intel Dev Software Algérie Inscrire au registre de commerce d'Alger, sous le N° 16/00-1202337B21, dont le siège est situé à :
RUE BOUBAGUELA N°09 LOCAL N°02B
OUED SEMAR ALGER. (Ci-après appelée **INTEL DEV Software Algérie**).

Description technique de l'ERP ComDev v3.7 :

Notre solution ComDev ERP/CRM est un logiciel modulaire (on n'active que les fonctions que l'on désire) de gestions de TPE/PME, d'indépendants, d'entrepreneurs ou d'associations. C'est un progiciel exécutable au sein d'un serveur Web et peut donc être accessible depuis n'importe quel lieu disposant d'une connexion Internet.

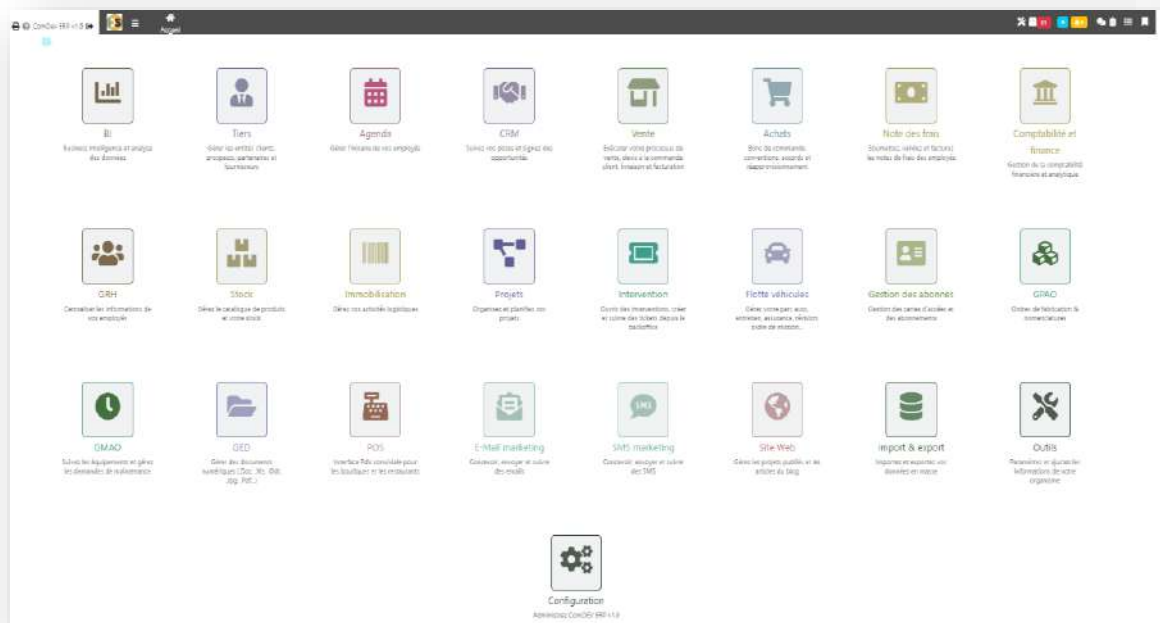
ComDev ERP v3.7 est disponible pour toute plateforme Web (Windows, MAC, Linux, Aix...) et tourne grâce aux technologies : [PHP](#) v80.026, Python, [MySQL](#) v8.0.31, Serveur Web HTTPS. Il a été conçu pour fonctionner chez le plus grand choix d'hébergeurs ou de serveurs. Ainsi ComDev ERP v 3.7 fonctionne avec toutes les configurations PHP et ne requiert aucun module PHP spécifique ou complémentaire. Il ne supporte pour l'instant que les bases de données [MySQL](#) et [PostgreSQL](#).

Notre solution se démarque des autres suites de gestion d'entreprise par sa plus grande simplicité (règle des 3 S) :

Simple pour le déploiement (nous déployons le logiciel sur votre propre serveur, nous ne conservons ni n'hébergeons vos données)

Simple pour l'utilisation (fonctions modulaires pour ne pas surcharger les menus, informations claires à la saisie)

Simple pour le développement (pas de Framework lourds). Le cœur du système intègre en effet sa propre architecture (design patterns) permettant à tout développeur d'être tout de suite opérationnel sans connaissances particulières autre que le PHP.



MODULES PRINCIPAUX :

COMDEV ERP/CRM est une solution modulaire complète dotée des fonctionnalités et d'analytique permettant de faire avancer votre entreprise.

Supporte l'évolution de la société : multi-activités, multi-sites, multi-sociétés,....

Intuitif et facile à utiliser, appropriation rapide, accès basé sur rôle/fonction de l'utilisateur.

Modernité : web, mobilité, Android,...

Large écosystème technique et fonctionnel.

Flexible et facile à adapter.

Plusieurs gestionnaires de menus (possibilité de différencier les menus pour le backoffice des utilisateurs internes ou le front office pour les clients ou fournisseurs)

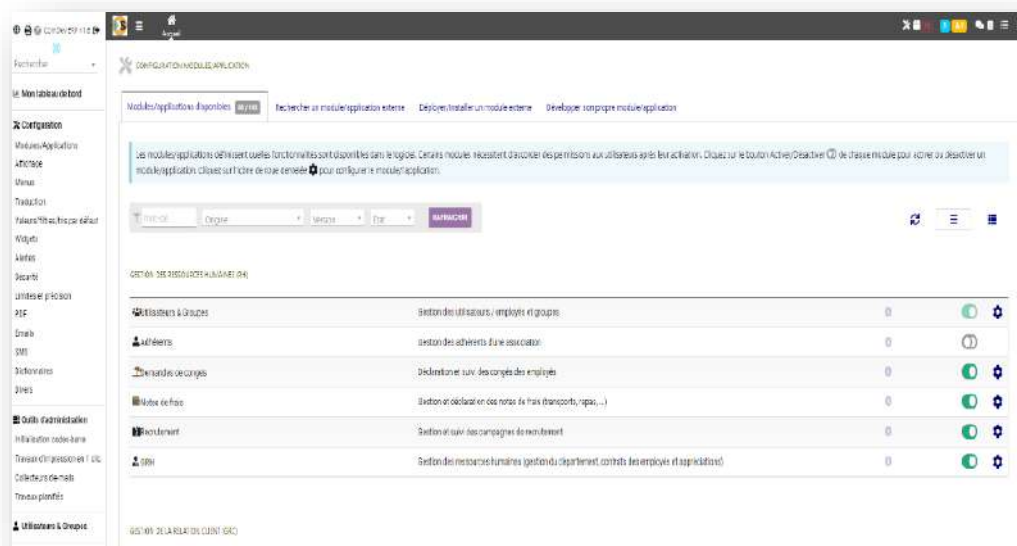
Agenda : est un outil qui permet d'ajouter un calendrier dans ComDev ERP/CRM et de gérer les événements pour collaborer avec les groupes de travail.

Le module Notification : permet d'envoyer des notifications (emails, sms) lors d'évènements ComDev ERP/CRM.

Compatibilité avec tous les outils Google Agenda, Google Calandre, Google Suite,...

Les modules de ComDev ERP/CRM :

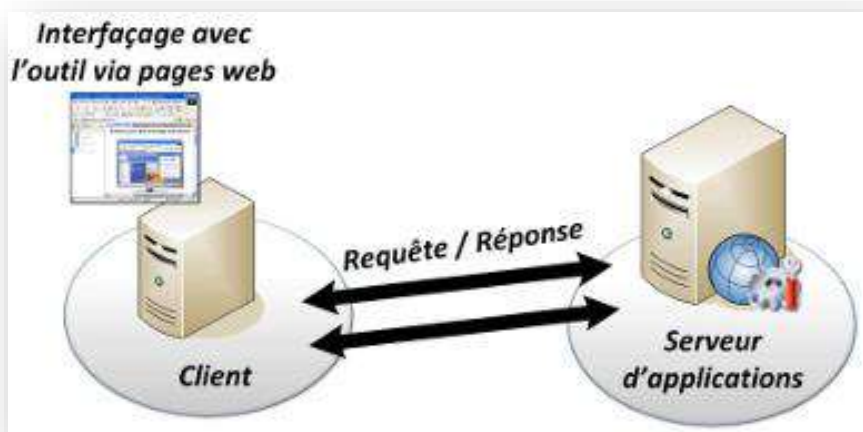
- CRM,
- Marketing,
- Comptabilité,
- Stock,
- GPAO,
- GMAO,
- Finances,
- Achat,
- Vente,
- GRH,
- Logistique,
- Annuaire des prospects et/ou clients et/ou fournisseurs,
- Annuaire des contacts/adresses,
- Point de vente/Caisse enregistreuse
- Réalisation de sondages
- Mailing de masses vers les clients, prospect ou utilisateurs Dolibarr
- Rapports et statistiques
- Export PDF de tous les éléments (factures, propositions commerciales, commandes, bons expéditions, etc...)
- Imports et exports (CSV ou Excel).
- Connectivité LDAP



- Le produit intègre des technologies ouvertes et modernes :
 - Forte intégration des services web,
 - Développement d'une interface web entièrement personnalisable.
- Intègre également de nombreuses fonctionnalités dédiées aux réseaux informatiques (messagerie instantanée, smsing, système de time line, liens avec réseaux sociaux...)

Architecture technique :

L'application ComDev ERP/CRM est réalisée suivant le modèle classique « client-serveur » avec un client dit de type « léger » qui accède à l'outil au moyen de pages web.



Les règles de sécurité générales dans notre ERP ComDev v3.7

Sécuriser votre espace de travail contre les attaques internes et externes

Sécurité pour notre logiciel métier en mode Saas

Intel Dev s'engage à préserver votre confiance à l'égard de la confidentialité des données que nous recueillons auprès de vous. Veuillez lire la présente politique de protection des données en mode Saas avec attention afin de comprendre nos pratiques en matière de collecte, d'utilisation et de partage de vos données.

Comment fonctionne le Saas pour ComDev ERP ?

Le système Saas consiste à mettre à disposition des usagers des logiciels accessibles par internet, et ce **de manière centralisée**. Chaque utilisateur crée un compte et s'acquitte tous les mois ou tous les ans des coûts lui permettant d'utiliser les services. Les applications ne « tournent » donc plus sur votre ordinateur, mais elles sont **utilisées en ligne**. La mise à disposition, l'entretien et les mises à jour des logiciels relèvent alors des obligations de votre prestataire. Les utilisateurs doivent cependant gérer l'utilisation des logiciels au moyen d'un navigateur Internet. Ceci est généralement possible avec n'importe quel appareil connecté à Internet. Il vous suffit alors de vous identifier sur la page d'accueil de l'utilitaire en ligne.



LE CLOUD DE L'INTÉGRATEUR

Pour profiter **des avantages de l'hébergement Saas pour ComDev ERP v3.7**, vous pouvez choisir le cloud de votre intégrateur. Il s'agit d'une solution beaucoup plus économique que le mode sur site car vous économiserez la maintenance fastidieuse et les coûts liés à votre propre infrastructure informatique. Tout est géré par votre intégrateur. Il vous offre également un confort supplémentaire en termes de maintien. En cas de

problème avec votre **système ERP**, votre service informatique ne sera pas directement impliqué. Les utilisateurs peuvent contacter l'équipe d'assistance fournie par l'intégrateur.

Il en va de même pour les mises à jour du **ComDev ERP v3.7** : elles ne seront réalisées qu'avec votre accord et avec l'assurance que les développements sur mesure ne seront pas affectés, par exemple en créant au préalable des environnements de test. Cela vous donnera une confiance accrue et un risque moindre ! Selon le contrat que vous contractez, vos données peuvent être sauvegardées à intervalles réguliers sur plusieurs serveurs distants, et vous bénéficierez par exemple d'un temps de réparation garanti inférieur à 24 heures

Les avantages du SaaS

L'avantage le plus évident et le plus important de **SaaS** est la réduction des dépenses d'hébergement grâce à une utilisation optimale des ressources, mais il existe d'autres avantages très importants que cette architecture peut apporter à votre entreprise :

- Une mise à l'échelle rapide et facile, qui permet d'allouer autant de ressources que nécessaire sans temps d'arrêt et sans beaucoup de routines administratives.
- Niveau élevé de protection contre les logiciels malveillants.
- Les mises à jour et la maintenance des logiciels sont prises en charge par les fournisseurs de **SaaS**.
- Réduction des coûts et du temps consacrés à la gestion du matériel.
- Mise en œuvre et mise à disposition rapides des services pour le client : au lieu d'envoyer des packs de logiciels et d'attribuer des licences, le service doit être « disponible en ligne » afin d'être immédiatement accessible à l'entreprise.
- Intégration d'un nouveau collaborateur facile : il n'est plus nécessaire de commander de nouvelles licences ou d'installer le logiciel sur de nouveaux postes. Dans la plupart des cas, il suffit d'enregistrer un nouvel utilisateur en ligne. Cela facilite le processus d'intégration de nouveaux employés qui seront plus vite opérationnels dans leur service.
- Utilisation des services en mode stationnaire et mobile avec toutes sortes de terminaux : le logiciel n'est plus obligatoirement associé à un poste de travail fixe. Grâce à leurs identifiants, les utilisateurs pourront accéder à leurs applications en toute mobilité ou à partir d'autres systèmes. Cela facilite également le concept du télétravail.
- Les nouvelles fonctionnalités et les mises à jour sont déployées et intégrées plus rapidement : comme les logiciels « tournent » chez le prestataire, ils sont aussi directement gérés par celui-ci. Vous disposez ainsi à tout moment de la version de services la plus récente.
- Les architectures de Cloud ont l'avantage d'offrir à tous les utilisateurs le même niveau de sécurité : les données étant toutes enregistrées de manière délocalisée sur un serveur du Cloud, les problèmes matériels et logiciels locaux n'entraînent que rarement des pertes de données. Les petites entreprises bénéficient ainsi du même niveau de sécurité que les grandes.

Serveurs privé virtuel (VPS)

Un serveur privé virtuel (VPS) est une machine qui héberge tous les logiciels et les données nécessaires au fonctionnement d'une application ou d'un site web. La dénomination virtuelle tient au fait qu'il ne consomme qu'une partie des ressources physiques sous-jacentes du serveur, qui sont gérées par un fournisseur tiers. Cependant, vous avez accès à vos ressources dédiées sur ce matériel.

Serveurs Privés Virtuels (VPS)

Simple et rapide – sécuritaire et personnalisable

- Bande passante illimitée, jusqu'à 2 Gbit/s*
- Protection DDoS inclus

Notre hébergement cloud et la sécurisation de nos logiciels

Les logiciels de gestion que nous développons sont hébergés dans le cloud privé de OCTANUIM. En effet, OCTANUIM dispose de son propre Datacenter situé en France, et certifié ISO 27001 – HDS. La norme ISO 27001 est une référence en matière de sécurité de l'information. Elle garantit l'efficacité de notre Système de Management de la Sécurité de l'Information (SMSI), audité et certifié chaque année par l'AFNOR :

- Traitement et confidentialité des données,
- Maîtrise des risques,
- Sécurité des informations stockées.

Les bonnes pratiques pour protéger ComDev ERP v3.7 :

La sécurité ERP nécessite de connaître les risques auxquels on peut être exposé, de se renseigner sur les menaces, d'identifier ses lacunes ainsi que d'appliquer au mieux les bonnes pratiques suivantes.

Sécuriser l'accès au logiciel ERP :

Comme pour toute application, l'authentification contribue grandement à la sécurité des comptes. **Pour offrir un niveau de sécurité maximal, l'authentification multi-facteur**

Est un moyen de protéger les accès. Dans ce cas, les utilisateurs doivent valider l'accès sur une application smartphone ou saisir un code reçu sur un token par exemple.

Les protocoles d'authentification OAuth2 (*autorisation*) et SAML 2.0 (*fournisseur d'identité*) sont devenus incontournables pour la sécurité des accès d'un ERP.

Certificat SSL Comodo :

Le certificat SSL (Secure Socket Layer) est un certificat de sécurité numérique délivré par l'Autorité de certification pour un nom de domaine particulier. Comodo est un type de certificat SSL. Un certificat SSL validera votre site web ou un système ERP en chiffrant les données installées dans le réseau du site. Le chiffrement est effectué après l'achat et la validation du certificat.

Les certificats de sécurité SSL sécurisent la connexion de votre site web ou l'ERP et le navigateur. Une fois que votre certificat SSL a été installé, vous bénéficierez d'une sécurité en ligne ininterrompue.

Les certificats SSL Comodo utilisent le chiffrement SHA2 & ECC 128/256 bits, qui est une norme de l'industrie. Il est disponible avec plusieurs longueurs de bits, le plus populaire étant le 256. Le chiffrement garantit que les données transmises via le réseau restent sécurisées. Si vous disposez d'un certificat avec un certificat SHA1, nous vous recommandons vivement de mettre à jour votre certificat vers SHA2 car des risques ont été identifiés avec l'ancien.

L'émission d'un certificat de validation étendue ou EV fournit à votre site web le nom de votre entreprise sur une barre verte et un cadenas dans le navigateur Web où votre site web est affiché. L'adresse du site web passe de HTTP à HTTPS, ce qui signifie également que le site web est sécurisé. Il s'agit d'un affichage visuel universellement reconnu d'une propriété en ligne sécurisée. Vos clients se sentiront plus en confiance pour effectuer des paiements en ligne sur votre site web.

Sécurisez tous vos sous-domaines de site web avec un seul plan, c'est-à-dire le plan Wildcard. Les plans Wildcard couvrent votre domaine principal (www.domain.com/domain.com) ainsi que tous les autres sous-domaines tels que mail.domain.com, login.domain.com, etc.

Notre fournisseur Octenium propose 4 types différents de plans de certificats SSL Comodo Positive, en fonction des besoins spécifiques du site Web ou système ERP.

Chiffrer les données d'entreprise :

Pour prévenir tout accès malveillant ou exploitation illégale au système ERP, **il est recommandé de chiffrer l'ensemble des données**. Plusieurs niveaux de cryptage viennent protéger les informations et seuls l'éditeur-intégrateur ou le fournisseur Cloud sont propriétaires des clés de décryptage. En cas de menace ou de fuite de données, les données récupérées deviennent illisibles.

Mettre en place un système de sauvegarde de l'ERP :

Pour veiller à la sécurité ERP, le système de sauvegarde des données et la configuration du logiciel ERP jouent un rôle important face aux risques d'attaques, mais également à l'erreur humaine. **En mettant en œuvre une gestion performante des sauvegardes, il est possible de revenir à une situation antérieure récente ou un état antérieur plus ancien, en minimisant la perte de données.**

Comment utiliser le service Backup Storage ?

Parés la réception de vos identifiants, connectez-vous à votre espace de Backup Storage, en utilisant le protocole de votre choix FTP ou FTPS, sur votre serveur à sauvegarder ou sur votre client FTP et archiver vos documents sur un serveur sécurisé et supervisé 24/7.

Module «Sécurité» de ComDev ERP/CRM :

Le module "**Sécurité**" vous permet de contrôler la sécurité de votre plateforme **ComDev ERP/CRM v3.7** et veuillez sur la maîtrise et la surveillance de vos données hébergées ainsi vos montres le niveau de sécurité actuel de votre **ComDev ERP/CRM** et finalement il vous aide à atteindre le niveau optimal.

Le plugin "**Sécurité**" vous montre dans un tableau de bord tous les indicateurs nécessaires pour connaître le niveau de sécurité de votre plateforme et l'indique comme le fait un antivirus : sécurité faible, moyenne ou forte. Nous fournissons avec le module un tableau de bord détaillé sur toutes les informations critique de votre système et plateforme dans une seule page.

Ci-dessous les éléments contrôlés par notre module :

1. Contrôler et corriger les permissions du fichier de configuration (s'il respecte les normes de sécurité ou pas)
2. Contrôler et corriger les permissions du dossier Documents.
3. Désactiver les outils d'installation/migration.
4. Chiffrer les mots de passe stockés dans la base de données.

5. Chiffrer le mot de passe de la base dans les fichiers de configuration.
6. Veillez sur l'utilisation de la technique: Force the HTTPS mode.
7. Cacher le lien "Mot de passe oublié" sur la page de connexion.
8. Activer l'option : Enable CSRF protection.
9. Détecter les adresses IP bloquées.
10. Gérer le délai d'expiration des sessions.
11. Contrôler la Taille maximum des fichiers envoyés (0 pour interdire l'envoi).
12. Activer le scan de vos fichiers ComDev ERP/CRM à l'aide de l'option : Antivirus activé sur la télé versement des fichiers.
13. Contrôler les Adresses IP qui ne peuvent pas atteindre votre plate-forme.

HACKS ET CRACKS

- ☐ Support du mode register_globals on ou off (off sérieusement recommandé).
- ☐ Support du mode safe_mode on ou off de PHP (non recommandé).
- ☐ Option de production pour inhiber toute remontée d'information technique comme débogage, info d'erreurs, info de version.
- ☐ Système de protection anti injection SQL.
- ☐ Système de protection anti injection XSS (Cross Site Scripting).

Notez qu'il reste préférable d'ajouter la protection du côté du serveur Web en désactivant l'option Apache « AcceptPathInfo Off »

- ☐ Système de protection anti CSRF (Cross Site Request Forgery).



ACCES PAGES ET FICHIERS

- ☐ Pages et contenus protégés par un système centralisé de vérification des habilitations accordées aux groupes ou utilisateurs pour chaque module fonctionnel.
- ☐ Isolation des fichiers stockés par ComdEV ERP/CRM dans une arborescence différente de la racine web (donc non téléchargeable sans passer par le wrapper).
- ☐ Système de protection anti scan dire (tout répertoire contient un fichier index pour limiter la visibilité si le serveur web à l'option "Indexes" active.).

PROTECTION LOGIN

- ☐ Retardateur anti brute force cracking sur la page de login.
- ☐ Code graphique optionnel anti robot (CAPTCHA) sur la page de login.
- ☐ Aucun traçage de mot de passe dans les logs (ni techniques ni fonctionnelles).
- ☐ Système d'audit interne pour enregistrer de manière permanente les événements en rapport avec l'administration utilisateurs et les logins en succès ou en échec.

Intel Dev Software Algérie prend des précautions pour protéger vos données contre les pertes, le vol, le mésusage et l'accès, la divulgation, la modification et la destruction non autorisés, par le biais de mesures de sécurité appropriées sur les plans administratif, physique et technique.

[\(Solution disponible en ligne en mode Saas\).](#)

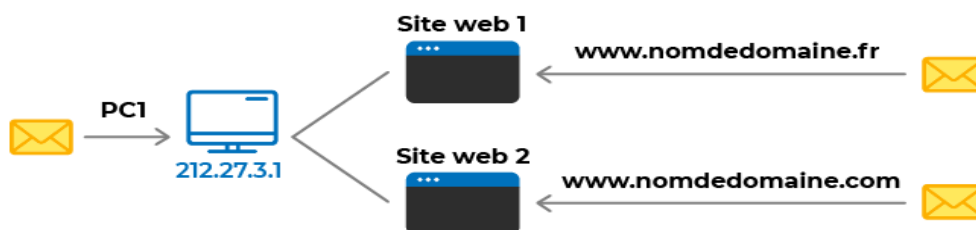
Accès à distance avec DDNS dynamique

Configurer un serveur DDNS :

DDNS (Dynamics Domain Name System) : Ce service permet de faire la correspondance entre des noms du domaine fixe et des adresses IP de votre réseau domestique. On peut le voir comme une sorte d'un service d'accès. Ce service repose sur un protocole également appelé DDNS.

Il existe 2 types de nommage pour une machine :

- le **nom de domaine** ;
- le **nom d'hôte**, couramment appelé "host Name".



Que signifie Dyn DNS (DDNS) ?

DNS dynamique (Dyn DNS) signifie **Dynamics Domain Name System** (également abrégé en « **DDNS** »). Il vous aide à transférer les adresses IP de votre réseau domestique en évolution constante vers un nom de domaine fixe. Vous devez vous enregistrer auprès d'un service DDNS sous un nom disponible (par ex : *.exemple.com*). Sous celui-ci, votre ordinateur est toujours accessible même si vous ne connaissez pas son adresse IP actuelle.

Quelle est la différence entre DDNS et DNS?

DDNS ou Dyn DNS peut être compris comme une extension du DNS : Domain Name System. Le DNS est un système d'annuaire mondial qui connaît l'adresse IP de chaque domaine enregistré (c'est-à-dire qu'il peut résoudre les noms en adresse) pour permettre l'accès aux sites Web, aux emails ou au FTP. Le processus fonctionne comme une sorte de service de renseignement téléphonique, où les coordonnées actuelles sont tenues prêtes et diffusées sur demande. Le DNS « recherche » l'adresse IP qui appartient au nom d'hôte (si elle ne se trouve pas encore dans le cache DNS) et est en échange constant avec la base de données DNS du fournisseur d'accès Internet correspondant. Dans le meilleur des cas, on répond à la demande avec l'adresse IP correspondante. Les adresses IP peuvent aussi être traduites dans les noms de domaine respectifs de la manière inverse. Cependant, cela s'avère plus difficile car le DNS Reverse n'est pas un standard Internet exigé et le DNS n'est pas optimisé pour cela.

La méthode de service DDNS prend cependant en charge l'attribution d'adresses IP dynamiques à un domaine spécifique. Une comparaison avec les bases de données DNS du fournisseur d'accès Internet s'effectue automatiquement. Le DynDNS s'assure de manière automatique que les changements d'adresse IP sont détectés et que les entrées DNS sont mises à jour en conséquence. Tout ce dont vous avez besoin pour établir une connexion à votre ordinateur est l'adresse de domaine enregistrée dans le service DDNS.

Comment fonctionne le Dynamics Domain Name System (Dyn DNS) ?

Comme l'adressage se fait généralement avec des noms de domaine et non avec des adresses IP, vous avez besoin d'un DNS dynamique qui met à jour les adresses IP qui changent constamment et les assigne alors à un nom de domaine fixe. Dès que l'adresse IP du routeur change, le routeur signale l'adresse IP actuelle au service DDNS, qui met à jour la requête DNS sous son propre domaine et répond à l'adresse IP. Si vous établissez maintenant une connexion à votre ordinateur, cette procédure se présente comme suit :

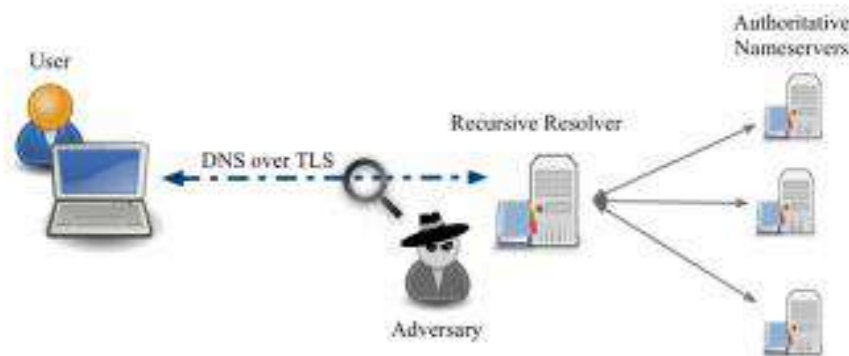
1. Le routeur notifie le service DDNS de l'adresse IP attribuée par le fournisseur d'accès. Celui-ci est attribué dans le DynDNS au nom de domaine que vous avez spécifié. Avec ce domaine, le serveur local est désormais accessible à tout moment.
2. Si l'adresse IP change après 24 heures, le service DDNS recevra automatiquement la nouvelle adresse IP. Le serveur DDNS répond aux requêtes DNS et met à jour la nouvelle adresse IP sous le domaine fixe.
3. Si vous souhaitez vous connecter à votre ordinateur (par exemple via la connexion bureau à distance), envoyez une requête DNS à votre domaine enregistré. Le serveur DDNS délivre alors automatiquement l'adresse IP actuelle de votre fournisseur d'accès Internet stockée sous le nom.
4. Une connexion client-serveur est maintenant possible avec l'adresse IP obtenue.

“La sécurité des données et les pratiques en termes de « Cyber sécurité » sont devenus des sujets prioritaires dans le déploiement d'un ERP”.

Qu'est-ce que le cyber sécurité ?

Le cyber sécurité fait référence à l'ensemble des mesures et outils déployés pour protéger les réseaux et les systèmes informatiques contre les intrusions et les attaques malveillantes. Les attaques par déni de service, de phishing, de malware, d'ingénierie sociale ou encore de type « man in the middle » sont de potentielles menaces pour la sécurité des données de toute entreprise.

Aujourd'hui, les risques cyber sont des enjeux de taille auxquels les industriels sont confrontés avec leur système ERP. Avec la montée en puissance du travail à distance, la digitalisation des usines, l'utilisation de terminaux mobiles, les ERP sont plus que jamais exposés à des risques ou failles de sécurité. Ces systèmes, capables de gérer les processus critiques d'une entreprise tels que la gestion de la production, la relation client, la logistique ou encore la gestion financière, stockent un important volume de données sensibles, notamment des données clients. Face à la multiplication des tentatives d'intrusion qui prennent diverses apparences, la sécurité devient un sujet dont l'impact doit être pleinement mesuré par l'entreprise. Dans un contexte d'ultra-digitalisation, la sécurité des systèmes d'information reste plus que jamais un défi critique et sensible pour de nombreuses entreprises industrielles.



Quels sont les moyens de se protéger contre les attaques basées sur le DDNS ?

Un pare-feu DNS :

Est un outil qui peut fournir plusieurs services de sécurité et de performance aux serveurs DNS. Un pare-feu DNS est érigé entre le résolveur récursif de l'utilisateur et le serveur de noms faisant autorité du site web ou du service qu'il essaie d'atteindre. Le pare-feu peut fournir des [services de rate limiting](#) pour bloquer les pirates qui tentent de submerger le serveur. Si le serveur subit un temps d'arrêt suite à une attaque ou pour toute autre raison,

le pare-feu DNS peut maintenir le site ou le service de l'opérateur en utilisant les réponses DNS présentes dans le cache.

En plus de ses fonctionnalités de sécurité, un pare-feu DNS peut également fournir à l'opérateur des solutions de performance, telles que des recherches DNS plus rapides et des coûts de bande passante réduits pour l'opérateur DNS.

DNS comme outil de sécurité :

Les résolveurs DNS peuvent également être configurés pour fournir des solutions de sécurité à leurs utilisateurs finaux (les internautes). Certains résolveurs DNS offrent des fonctionnalités telles que le [filtrage de contenu](#), ce qui peut bloquer des sites connus pour distribuer des logiciels malveillants et du [spam](#), et la protection contre les botnets, ce qui bloque les communications avec les botnets connus. De nombreux résolveurs DNS sécurisés sont gratuits et un utilisateur peut activer l'un de ces services [DNS récurifs](#) en modifiant un simple paramètre de son routeur local. Le [DNS Cloudflare](#) met l'accent sur la sécurité.

Imposer des critères obligatoires aux mots de passe :

Quelques règles élémentaires suffisent à renforcer la complexité du mot de passe. Si certains employés peuvent s'en agacer, les mots de passe forts sont indispensables dans le monde actuel où menaces et vulnérabilités abondent.

1. Chiffrer les mots de passe stockés dans la base de données.
2. Chiffrer le mot de passe de la base dans les fichiers de configuration.

Equipez-vous d'un firewall (pare-feu) pour sécuriser vos données :

« Pare-feu » sont une nécessité de sécurité qui restreint l'accès non autorisé aux systèmes et réseaux, et sont l'une des lignes fortes de défense contre les attaques d'utilisateurs extérieurs. Les pare-feu sont installés en utilisant un logiciel ou sont intégrés par défaut dans le matériel de mise en réseau tels que les routeurs. Les pare-feu peuvent filtrer le trafic IP, les ports et les protocoles TCP /IP. Les pare-feu peuvent être configurés pour être indulgent ou agressif au moment d'accepter le trafic entrant.

Exemple :

- Windows Firewall
- Comodo Firewall
- GlassWire

Munissez-vous d'un antivirus :

Pour sécuriser vos données installé un antivirus. Un antivirus est un logiciel informatique destiné à identifier et à effacer des logiciels malveillants, appelés virus, sur votre support numérique.

Son fonctionnement est simple, l'antivirus va analyser les fichiers entrants (ce sont les fichiers que vous téléchargez ou vos courriers électroniques), la mémoire vive aussi appelée RAM de votre ordinateur et les périphériques de stockage comme les disques durs, les clés USB etc.

Exemple :

Kaspersky DDoS Protection couvre l'ensemble des étapes permettant de protéger votre entreprise contre les attaques DDoS :

Analyse de votre trafic Internet 24h/ 24 et 7j/7. Alerte en cas d'attaques potentielles.

Redirection de votre trafic vers le centre de nettoyage du cyber sécurité qui a toujours une longueur d'avance.

Sécuriser vos données en les sauvegardant :

La sauvegarde informatique est le fait de faire une copie des données sur un support indépendant pour faire face à toute éventualité, comme des pannes matérielles, des pertes, des infections par des logiciels malveillants, etc. Elle permet de récupérer rapidement des informations depuis une version précédente ou d'être restauré.

Sauvegarde interne

La sauvegarde interne se fait sur un support grâce à un équipement physique comme des disques durs externes ou des serveurs NAS (Network Attached Storage). La sauvegarde se fait automatiquement. La restauration est le plus souvent une opération manuelle en cas de perte des données.

Le bémol, c'est que les données sont stockées au sein même de l'entreprise et en cas de sinistres comme un incendie, un vol, etc. elles peuvent être perdues. Le stockage interne nécessite une personne ayant les capacités nécessaires pour assurer la maintenance du stockage.

Planifications de la sauvegarde automatique Backup :

ComDev backup est un module de ComDev ERP/CRM dédié à la création automatisée de sauvegardes. Ce module enregistre des copies de l'ensemble des données de ComDev ERP/CRM de manière régulière, à une période sélectionnée par l'administrateur BD.

ComDev backup vous évite d'avoir à vous soucier de la perte de vos données.

Dès la fin de sa configuration, le module commence la sauvegarde automatique de vos données logicielles. ComDev backup fait 15 sauvegardes avant de procéder à la suppression de la plus ancienne. Vous aurez ainsi 15 copies de vos données logicielles en cours disponible et consultable à tout moment. Le module vous notifie par mail en cas de problème inhérent à vos sauvegardes. Vous pourrez ainsi vérifier par vous-même et régler le problème à temps.

Sauvegarde externe

La sauvegarde externe se fait vers un service en ligne comme un cloud. Elle permet une synchronisation permanente des données. Le prestataire s'occupe des opérations, il n'est pas nécessaire d'avoir en interne, une personne compétente dans ce domaine. De plus, les données sont stockées en dehors de l'entreprise, ce qui fait qu'elles sont moins exposées aux risques d'incendie ou autres mais, elles ne sont pas totalement exonérées de tout risque.

Concernant votre ERP vous pouvez faire vos sauvegardes autant en interne qu'en externe. C'est à vous de choisir lequel est le plus adapté à votre fonctionnement

Sauvegarde ComDev ERP/CRM Nas

Synology

Sauvegarde données ComDev ERP/CRM vers Nas Synology réalisée par réplication synchronisée (Rsync) quotidienne sur votre NAS Synology.

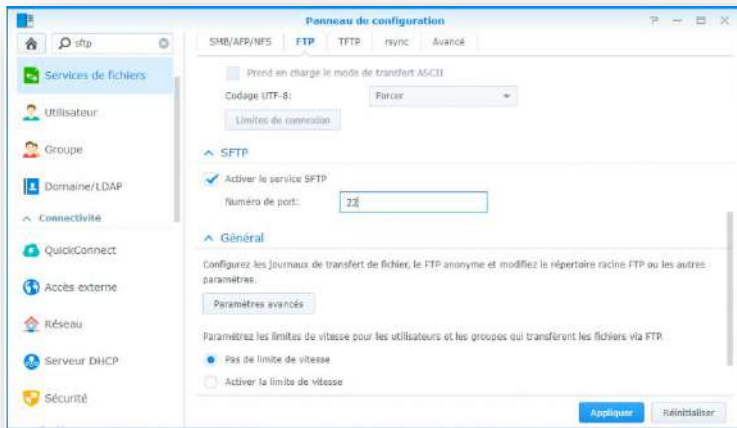
S'applique sur le dossier des données de votre instance lors d'un traitement de nuit vers un dossier autorisé de votre Serveur. Afin d'éviter des transferts trop lourds, le système synchronise un dossier de données déposé en réplique sur votre serveur de manière sécurisé en protocole SSH.

Seuls les changements apportés à vos données sur votre instance ComDev ERP/CRM en ligne sont modifiés sur le serveur distant (ajout et suppression).

Le dossier des données comprend les fichiers et les sauvegardes des bases de données de votre session.

Il est ensuite également possible de construire une rétention plus importante.

Voici le résultat avec le dossier «documents» de la session ComDev ERP/CRM télé versé dans le dossier backup. Ce dossier contient la sauvegarde de la base de données ainsi que les fichiers des GED.



Installer un certificat SSL/TLS sur un serveur web :

Le certificat SSL est destiné à la sécurisation des données sensibles, essentiellement dans le cadre des paiements en ligne. Par la suite, le SSL s'est imposé comme la **norme pour protéger l'accès aux comptes utilisateurs, l'envoi de documents dématérialisés ou les déclarations fiscales** (entre autres). Même les réseaux sociaux ont adopté le protocole SSL : vous pouvez constater, en vous connectant sur Facebook, Twitter ou LinkedIn, que ces plateformes affichent bien le protocole HTTPS et le fameux cadenas.

Les droits utilisateurs pour sécuriser vos accès :

Les droits utilisateurs sont une **autorisation d'accès aux données, à certaines personnes d'une entreprise** par exemple. Ces dernières auront la possibilité d'accéder à des dossiers, informations, ou faire des actions auxquelles, elles seules auront accès.

Le but des droits utilisateurs est de donner un accès suffisant aux salariés pour qu'ils puissent faire leur travail correctement, mais **sans qu'ils se perdent avec des données** qui ne les concernent pas. Cela évite de les encombrer, et qu'ils ne fassent pas de mauvaises manipulations.

Ces droits existent aussi sur les ERP. Et heureusement ! Car avec toutes les données qu'ils peuvent centraliser, les salariés peuvent être rapidement débordés. N'hésitez pas à demander leur mise en place pour sécuriser l'ensemble de vos données.

Sécurité des serveurs Windows NT :

Qu'est-ce que Windows NT ?

Windows New Technology (NT) est une famille de systèmes d'exploitation développée par Microsoft. Il a été conçu pour être un système d'exploitation (OS) haut de gamme fiable et sécuritaire pour les serveurs et les postes de travail et il est toujours le fondement de la famille des systèmes d'exploitation Windows de Microsoft, qui comprend les versions de serveur et de bureau du système d'exploitation.

Windows NT a joué un rôle important dans l'industrie de l'informatique d'entreprise en offrant une plateforme fiable, évolutive et sécurisée pour les entreprises. Il a gagné en popularité dans les environnements d'affaires grâce à sa robustesse, sa prise en charge pour le réseau et sa compatibilité avec les applications d'affaires. Le succès de Windows NT a conduit à l'adoption à grande échelle des technologies Microsoft dans l'informatique d'entreprise.

La sécurité des serveurs Windows s'applique en deux temps :

- Application d'un script de post installation lors de l'installation du serveur.
- Application des stratégies de groupe lors de l'intégration au sein d'un domaine AD.

Les points suivants sont mis en œuvre dans le cadre de la sécurisation des serveurs Windows :

- Arrêt des services inutiles
- Suppression des packages système inutiles
- Création de comptes locaux de secours et renommage du compte Administrateur
- Intégration de la machine dans l'authentification Active Directory
- Configuration de l'externalisation des logs
- Configuration des sauvegardes
- Configuration du monitoring
- Configuration de l'inventaire automatique
- Configuration de la synchronisation temporelle
- Configuration de la politique de mise à jour
- Configuration de la stratégie de mot de passe
- Configuration des accès distants
- Mise en place de droits spécifique sur l'arborescence.

Par la suite, des scripts de sécurisation standards sont mises en œuvre en fonction du rôle du serveur (serveur Web, serveur BDD, serveur applicatif).

Sécurité des mots de passe :

- Le personnel **d'Intel Dev** n'a pas accès à votre mot de passe et ne peut pas le récupérer pour vous. Votre seule option en cas de perte est de le réinitialiser.
- Les identifiants de connexion sont toujours transmis de manière sécurisée via HTTPS.
- Les administrateurs des bases de données clients ont même l'option de configurer la limitation de tentatives et la durée de refroidissement en cas de tentatives de connexion répétées.
- Les mots de passe des clients sont protégés par des chiffrements PBKDF2+SHA512 conformes aux normes industrielles (salage + étirement pour des milliers de tours).

Accès par nos employés :

- L'équipe **d'Intel Dev** Assistance peut se connecter à votre compte pour accéder aux paramètres liés à votre problème d'assistance. Pour cela, elle utilise ses propres identifiants, pas votre mot de passe (qu'elle n'a aucun moyen de connaître).
- Cet accès spécial du personnel améliore l'efficacité et la sécurité : l'équipe peut immédiatement reproduire le problème que vous rencontrez, vous n'avez jamais besoin de partager votre mot de passe et nous pouvons auditer et contrôler les actions du personnel séparément !
- Notre équipe d'assistance s'efforce à respecter votre vie privée autant que possible et n'accède qu'aux fichiers et paramètres nécessaires pour diagnostiquer et résoudre votre problème.
- Seuls quelques ingénieurs de confiance **d'Intel Dev** ont l'autorisation de gérer les serveurs à distance - et l'accès n'est possible qu'en utilisant une paire de clés SSH personnelles chiffrées, depuis un ordinateur avec chiffrement de disque.

Version d'ERP COMDEV 3.7

Editeur/licence : INTEL DEV SOFTWARE ALGERIE

CONTACT :

Téléphone : +213-(0)23 82 44 11

Mobile : +213-(0) 774146415 / +213-(0)792489187

Email : contact@inteldevsoft.com

Site web : <https://comdevweb.inteldevsoft.com/>

Rue boubaguella Adresse : n°09 local n°02b oued OuedSmar Alger