NOM: PRÉNOM: CLASSE:

MR ROLIN 2026

[DIVERS] Cloud Computing

Objectifs

- Expliquer le principe du Cloud Computing et ses usages professionnels
- Identifier le rôle du Cloud dans les interventions informatiques
- Comprendre et comparer les méthodes de sauvegarde via le Cloud
- Décrire la connectivité entre le Cloud et un réseau local
- Expliquer les mécanismes d'identification et d'authentification Cloud
- Appliquer les bonnes pratiques de sécurité dans un contexte Cloud

Introduction

Le Cloud Computing désigne une manière moderne d'utiliser l'informatique. Contrairement aux systèmes traditionnels où les données et les logiciels sont stockés localement sur un ordinateur ou sur un serveur dans l'entreprise, le Cloud permet d'accéder à ces ressources à distance, via Internet. Les fichiers, les applications et parfois même les serveurs ne se trouvent plus physiquement chez l'utilisateur, mais dans des centres de données gérés par des fournisseurs spécialisés.

Dans le monde professionnel, cette approche a profondément modifié les méthodes de travail. Les employés peuvent accéder à leurs documents depuis différents appareils, les équipes peuvent collaborer en temps réel et les entreprises peuvent réduire leurs coûts liés au matériel informatique. Pour un technicien en maintenance PC et réseaux, le Cloud n'est donc pas une technologie abstraite, mais un environnement de travail quotidien qu'il faut comprendre et maîtriser.

Le Cloud Computing dans les interventions informatiques

Lors d'une intervention informatique, le Cloud joue un rôle central. De nombreuses actions qui nécessitaient auparavant un déplacement physique peuvent aujourd'hui être réalisées à distance. Le technicien peut accéder aux données d'un utilisateur, vérifier des configurations ou rétablir un service sans se rendre sur place. Cela permet de gagner du temps et d'intervenir plus rapidement en cas de problème.

Le Cloud est également utilisé pour fournir des outils indispensables à l'intervention, comme des plateformes de gestion, des systèmes de tickets ou des solutions de supervision. Dans beaucoup d'entreprises, les comptes utilisateurs, les droits d'accès et même certaines configurations de postes sont gérés directement via des interfaces Cloud. Le technicien doit donc être capable de naviguer dans ces environnements et de comprendre leur fonctionnement.

Les services Cloud proposés par des acteurs comme Microsoft Azure, Amazon Web Services ou Google Cloud sont devenus des références dans le monde professionnel et sont fréquemment rencontrés lors des interventions.

Les types de services Cloud et leurs usages

Le Cloud ne propose pas un seul type de service, mais plusieurs niveaux d'utilisation. Certains services fournissent simplement une infrastructure virtuelle, comme des serveurs ou de l'espace de stockage, tandis que d'autres proposent directement des logiciels prêts à l'emploi accessibles via un navigateur web. Dans le cadre de la maintenance informatique, ce sont surtout les services applicatifs et de stockage qui sont utilisés.

Ces services permettent par exemple de gérer des messageries professionnelles, de stocker et partager des documents ou encore d'héberger des sauvegardes. Pour le technicien, il est important de comprendre que plus le service est "clé en main", moins il a de contrôle sur l'infrastructure, mais plus l'utilisation est simple pour l'utilisateur final.

IaaS – Infrastructure as a Service
Ce modèle fournit une infrastructure informatique virtuelle : serveurs, disques, réseaux.

Le client gère le système d'exploitation et les applications.

Exemple : création d'un serveur virtuel pour héberger un service interne.

PaaS – Platform as a Service
Le fournisseur met à disposition une plateforme complète (système, base de données, outils).
Le client se concentre uniquement sur le développement ou l'utilisation.

SaaS – Software as a Service
Les applications sont accessibles directement via Internet, sans installation locale.

Exemples très courants :
- messagerie professionnelle
- stockage de fichiers
- outils collaboratifs

Les méthodes de sauvegarde via le Cloud

La sauvegarde des données est l'un des usages les plus importants du Cloud en entreprise. Une sauvegarde consiste à conserver une copie de sécurité des données afin de pouvoir les récupérer en cas de problème. Les pertes de données peuvent être causées par une panne matérielle, une erreur de manipulation, un vol, un incendie ou encore une attaque informatique. Sans sauvegarde, ces données peuvent être perdues définitivement.

Le Cloud permet de stocker ces copies de sécurité dans un endroit distant, ce qui protège les données même si le matériel local est endommagé. Il existe plusieurs méthodes de sauvegarde, qui diffèrent par leur fonctionnement et leur efficacité. Certaines copient l'ensemble des données, tandis que d'autres ne sauvegardent que les éléments modifiés. Le choix de la méthode dépend du volume de données, de la fréquence des sauvegardes et des besoins de restauration.

Il est très important de faire la distinction entre une véritable sauvegarde et une simple synchronisation Cloud. Une synchronisation permet d'avoir les mêmes fichiers à plusieurs endroits, mais elle ne protège pas contre la suppression ou la corruption des données. Le rôle du technicien est souvent d'expliquer cette différence aux utilisateurs, qui pensent à tort que leurs fichiers sont automatiquement protégés.

Avantages et limites des sauvegardes Cloud

Les sauvegardes Cloud présentent de nombreux avantages. Elles permettent d'accéder aux données depuis n'importe quel endroit, offrent un haut niveau de sécurité et évitent la dépendance à un support physique unique. Elles sont également automatisées, ce qui réduit les oublis et les erreurs humaines.

Cependant, elles présentent aussi certaines limites. Une sauvegarde Cloud dépend fortement de la qualité de la connexion Internet. Si le débit est insuffisant ou instable, les sauvegardes peuvent être lentes ou incomplètes. De plus, le stockage Cloud a un coût, souvent calculé en fonction du volume de données. Le technicien doit donc être attentif à ces contraintes et s'assurer que la solution mise en place correspond aux besoins réels de l'entreprise.

Connectivité entre le Cloud et le réseau local

Pour accéder aux services Cloud, une connexion réseau fiable est indispensable. Le Cloud repose entièrement sur Internet, ce qui signifie que la qualité de la connexion influence directement les performances et la disponibilité des services. Une coupure Internet peut rendre les applications Cloud inaccessibles, même si elles fonctionnent parfaitement côté fournisseur.

Le réseau local joue un rôle essentiel dans cette connectivité. Le routeur, le pare-feu et les paramètres réseau doivent être correctement configurés pour autoriser les communications avec le Cloud. Des protocoles sécurisés sont utilisés afin de protéger les données échangées. Dans certains cas, un réseau privé virtuel (VPN) est mis en place pour renforcer la sécurité des connexions entre l'entreprise et le Cloud.

Lors d'une intervention, le technicien doit être capable de diagnostiquer un problème de connectivité Cloud. Il doit vérifier si le problème provient du réseau local, de la connexion Internet ou du service Cloud lui-même, avant de prendre les mesures appropriées.

Identification sur le Cloud

L'identification correspond à l'identité numérique d'un utilisateur dans un système Cloud. Chaque utilisateur dispose d'un compte qui lui est propre, généralement lié à une adresse e-mail professionnelle. Cette identité permet au système de savoir qui est l'utilisateur et quels services il est autorisé à utiliser.

Dans un environnement professionnel, la gestion des identités est essentielle. Le technicien peut être amené à créer, modifier ou supprimer des comptes utilisateurs, ainsi qu'à attribuer des droits d'accès. Une mauvaise gestion des identités peut entraîner des problèmes de sécurité ou des erreurs d'accès aux ressources.

Authentification sur le Cloud

L'authentification est le mécanisme qui permet de vérifier que l'utilisateur est bien celui qu'il prétend être. Le moyen le plus simple d'authentification reste le mot de passe, mais celui-ci est souvent insuffisant à lui seul pour garantir un niveau de sécurité élevé.

C'est pourquoi les services Cloud utilisent de plus en plus l'authentification multifacteur. Cette méthode combine plusieurs éléments de vérification, par exemple un mot de passe et un code temporaire envoyé sur un smartphone. Cette approche réduit fortement les risques d'accès non autorisé, même si le mot de passe est compromis.

Pour le technicien, il est essentiel de comprendre ces mécanismes afin de pouvoir les configurer correctement et aider les utilisateurs en cas de difficulté de connexion.

Bonnes pratiques de sécurité dans le Cloud

La sécurité dans le Cloud repose à la fois sur le fournisseur et sur l'utilisateur. Même si les infrastructures Cloud sont très sécurisées, une mauvaise configuration ou des pratiques inadéquates peuvent créer des failles importantes. Le technicien joue un rôle clé dans la mise en place de règles de sécurité adaptées, comme l'utilisation de mots de passe robustes, l'activation de l'authentification multifacteur et la limitation des droits d'accès.

Il doit également sensibiliser les utilisateurs aux risques liés au phishing, aux connexions depuis des réseaux non sécurisés et au partage excessif de données. La sécurité Cloud est donc un travail continu qui nécessite vigilance et rigueur.

Conclusion

Le Cloud Computing est aujourd'hui au cœur des systèmes informatiques professionnels. Il facilite les interventions, améliore l'accessibilité des données et renforce la sécurité lorsqu'il est correctement utilisé. Pour un technicien en maintenance PC et réseaux, la compréhension du Cloud, des sauvegardes, de la connectivité réseau et des mécanismes d'authentification est indispensable.

Maîtriser ces notions permet non seulement de résoudre des problèmes techniques, mais aussi d’adopter une posture professionnelle attendue dans le monde du travail actuel, où le Cloud est devenu une composante incontournable de l’informatique.