- la rentabilité : modele basé sur la consommation, c'est à dire que l'on ne paye que ce que l'on consomme

- la scalabilité : il s'agit de l'augmentation ou de la diminution des resources et services en fonction de la demande

- l'élasticité : il automatise la mise a l'echelle pendant les pics et la baisse de la demande

- doit toujours etre a jour

- la fiabilité :

- il est normal :

- il est securisé :

- il est global c'est à dire qu'il fonctionne partout a travers le monde

modeles de services cloud :

- Saas pour les clients

- Pass pour les eveloppeurs

- Iaas avantages : il permet le deploiement rapide de nouveaux appareils informatiques

ont migrent vers le cloud car celui ci permet d'avancer plus rapidement et d'innover dans des voies qui etaient jusqu'ici inimaginable

Azure : est un ensemble de services cloud en constante evolution qui aide votre organisation(votre entreprise) a faire face aux defis actuels

le portail Azure est une console web unifie qui vous permet de gerer votre abonnement azure a l'aide d'une IHM

service de plateforme(l'analytique et l'Iot; intelligence artificielle; services de developpement;Computes services) et service d'infrastructure(calcul, mise en reseau, stockage; multimedia et CDN; donnees)

les services de AZURE

- DevOps : Azure DevOps, Azure DevTest Labs

Combinant développement (Dev) et opérations (Ops), DevOps est l'union des personnes, des processus et des technologies destinés à fournir continuellement de la valeur aux clients.

- Calcul : Machine Virtuelles Azure, Aure Batch, Azure Container Instances, Azure Kubernetes services, Azure Functions, Azure Service Fabric, Azure Virtual Machine Scale Sets

- Reseau : Reseau Virtuel Azure, Azure load Balancer, passerelle VPN azure, Azure DNS, Azure DDOS protection, Azure application GateWay

- Stockage : Stockage Blob Azure, Fichier Azure, Table Azure, File d'attente

- Web : Azure app service, Azure Notification Hubs, Gestion des API Azure, Service Azure SignalR

machines virtuelles : sont des émulations logicielles d'ordinateurs physiques.

elles fournissent une infrastructure Iaas

Azure Container Instances et Azure Kubernetes Services sont des ressources de calcul que vous pouvez utiliser pour deployer et geres des conteneurs.

modeles de deploiement de cloud computing :

- cloud public

avantages :

\* couts inferieurs : c a d que vous n'avez pas besoin de payer du materiel ou du logiciel, et vous payez uniquement le service que vous utilisez.

\* Absence de maintenance : votre fournisseur de service assure la maintenance.

\* Scalabilité presque illimité :

\* Haute fiabilité : car un vaste reseau de serveur offre une garantie contre les pannes.

- cloud privé :

avantages :

\* Flexibilité accrue

\* Controle accrue

\* Scalabilité accrue

- cloud hybride : est un type de cloud qui associe un cloud privé(ou infrastructure locale) à un cloud public.

les clouds hybrides permettent aux donnees et aux applications de se deplacer entre les deux environnements.

avantages :

\* Controle

\* Flexibilité

\* Rentabilité

\* Facilité

avantages que offre un environnement cloud par rapport a un environnement physique

- Haute disponibilite

- Extensibilite

- Elasticite

- Agilite

- Geodistribution

- Reprise d'activite apres sinistre

depenses d'investissement (CapEx, capital Expenditure)

depenses de fonctionnement (OpEx, Operational Expenditure)

IoT (Internet Of Things) : permet aux appareils de collecter et de transmettre des informations pour analyse des données.

Azure Iot Central est une plateforme d'application Iot qui réduit les charges et les couts associés au développement, a la gestion et à la maintenance de solutions Iot de qualité professionnelle.

Azure IoT Hub : est un service managé, hébergé dans le Cloud et qui agit en tant que hub central de messages pour la communication bidirectionnelle entre votre application IoT et les appareils gérés.

Azure IoT Central s’appuie sur IoT Hub et ajoute un tableau de bord vous permettant de vous connecter à vos appareils IoT, de les surveiller et de les gérer.

Azure Security Center est un service de supervision qui fournit une visibilité de votre posture de sécurité sur l’ensemble de vos services, à la fois sur Azure et localement.

Azure Key Vault est un service Cloud centralisé conçu pour le stockage des secrets d’une application, à un emplacement central unique.

L’authentification est le processus qui consiste à établir l’identité d’un utilisateur ou d’un service voulant accéder à une ressource

L’autorisation est le processus qui vise à établir le niveau d’accès dont dispose un utilisateur ou un service authentifié. Elle détermine les données auxquelles ils ont accès et l’utilisation qu’ils peuvent en faire.

Azure AD est le service Cloud de Microsoft qui gère les identités et les accès.

L’authentification unique permet à un utilisateur de se connecter une fois et d’utiliser ces informations d’identification pour accéder à plusieurs ressources et applications auprès de différents fournisseurs.

Services Azure AD :

Authentification

Ce processus inclut la vérification de l’identité avant d’accéder aux applications et aux ressources, ainsi que des fonctionnalités comme la réinitialisation de mot de passe en libre-service, l’authentification multifacteur, une liste de mots de passe interdits personnalisée, et des services de verrouillage intelligent.

Authentification unique

Avec l’authentification unique, vous n’avez qu’un seul nom d’utilisateur et un seul mot de passe à retenir pour accéder à plusieurs applications. Une même identité est liée à un utilisateur, ce qui simplifie le modèle de sécurité. Quand un utilisateur change de rôle ou quitte l’organisation, les modifications d’accès s’appliquent à cette identité, ce qui réduit considérablement le travail nécessaire pour changer ou désactiver les comptes.

Gestion des applications

Vous pouvez gérer vos applications Cloud et locales à l’aide d’Azure AD. Certaines fonctionnalités comme le proxy d’application, les applications SaaS, le portail Mes applications (également appelé Volet d’accès) et l’authentification unique offrent une meilleure expérience utilisateur.

Gestion des appareils

En plus des comptes individuels des personnes, Azure AD prend en charge l’inscription des appareils. L’inscription permet de gérer les appareils avec des outils comme Microsoft Intune. Il est également possible d’appliquer des stratégies d’accès conditionnel basées sur les appareils pour limiter les tentatives d’accès aux seuls appareils connus, quel que soit le compte d’utilisateur qui en fait la demande.

Azure AD Multi-Factor Authentication est un service Microsoft qui offre des fonctionnalités d’authentification multifacteur. Azure AD Multi-Factor Authentication permet aux utilisateurs de choisir une autre forme d’authentification pendant la connexion, par exemple un appel téléphonique ou une notification d’application mobile.

Voici les services qui proposent les fonctionnalités d’Azure AD Multi-Factor Authentication :

Azure Active Directory

Azure Active Directory Free permet aux administrateurs ayant le niveau d’accès Administrateur général d’activer Azure AD Multi-Factor Authentication via l’application Microsoft Authenticator, un appel téléphonique ou un code SMS. Vous pouvez également mettre en œuvre Azure AD Multi-Factor Authentication pour tous les utilisateurs via l’application Microsoft Authenticator uniquement, en activant les paramètres de sécurité par défaut de votre locataire Azure AD.

Azure Active Directory Premium (licences P1 ou P2) permet une configuration complète et précise d’Azure AD Multi-Factor Authentication via des stratégies d’accès conditionnel (comme indiqué ci-dessous).

Authentification multifacteur pour Office 365

Une partie des fonctionnalités d’Azure AD Multi-Factor Authentication est intégrée à votre abonnement Office 365.

L’authentification multifacteur est un processus par lequel l’utilisateur est invité à fournir une autre forme d’identification pendant la connexion. Il peut s’agir d’entrer un code sur le téléphone portable ou de fournir une analyse d’empreinte digitale.

L’accès conditionnel est un outil dont se sert Azure Active Directory pour autoriser (ou refuser) l’accès aux ressources en fonction de signaux d’identité. Par signaux, il faut entendre l’identité de l’utilisateur, sa localisation et l’appareil à partir duquel il demande l’accès.

Domain Services(Services de Domaine) : c'est l'outil utilisé par Azure pour fournir des services de domaine managé comme la jonction de domaine, la stratégie de groupe, le protocole LDAP et l'authentification Kerberos/NTLM.

Privileged Identity Management(PIM) : est un service dans azure AD qui vous permet de superviser l'acces aux ressources importantes de votre organisation.

Pour les administrateurs informatiques, l’accès conditionnel offre les avantages suivants :

Il permet aux utilisateurs d’être productifs en tout lieu et à tout moment.

Il protège les ressources de l’organisation.

Quand utiliser l’accès conditionnel ?

L’accès conditionnel est utile dans les cas suivants :

Exiger l’authentification multifacteur pour accéder à une application.

Vous pouvez imposer l’authentification multifacteur à tous les utilisateurs ou uniquement à certains d’entre eux, comme les administrateurs.

Vous pouvez aussi décider d’appliquer l’authentification multifacteur aux accès émanant de tous les réseaux ou seulement des réseaux non approuvés.

Vous devez autoriser l’accès aux services uniquement à partir d’applications clientes approuvées.

Par exemple, vous pouvez souhaiter autoriser les utilisateurs à accéder aux services Office 365 à partir d’un appareil mobile, à condition qu’ils utilisent des applications clientes approuvées, comme l’application Outlook Mobile.

Vous devez exiger des utilisateurs qu’ils accèdent à votre application à partir d’appareils gérés uniquement.

Un appareil géré est un appareil qui répond à vos standards de sécurité et de conformité.

Vous devez bloquer l’accès aux sources non approuvées, par exemple aux localisations inconnues ou inattendues.

L’environnement du système azure se compose des réseaux suivants :

\* Réseau de production Microsoft Azure (réseau Azure)

\* Réseau d'entreprise Microsoft (réseau Corpnet)

Sécurité Dans le Cloud

L’architecture réseau d'un centre de données Azure se compose des éléments suivants :

\* Réseau de périphérie

\* Réseau étendue

\* Réseau de passerelles régionales

\* Réseau du centre de données

Microsoft Defender pour le Cloud : vous aide à prévenir; détecter et répondre aux menaces avec une visibilité et un contrôle accrus sur la sécurité de vos ressources Azure.

Les piliers de la sécurité du Cloud :

* La gestion de la posture de sécurité
* La protection des charges de travail Cloud

Defender pour le Coud répond a trois besoins essentiels :

* Evaluation continue
* Sécurisation
* Défense

Types d'attaques DDOS:

\* Attaques Volumétriques :

\* Attaques de protocole :

\* Attaques de la couche Ressource(Application) :

Azure DDOS protection : est un service conçu pour aider à protéger vos applications et serveurs en analysant le trafic réseau et en ignorant tout ce qui ressemble à une attaque DDOS.

Azure DDOS protection est disponible en deux niveaux :

\* De base et Standard

Le Pare-feu Azure est un service de sécurité réseau managé dans le Cloud qui protège vos ressources Réseau virtuel Azure contre les attaques.

Les fonctionnalités du pare-feu Azure :

* Zone de disponibilité et de haute disponibilité
* Filtrage au niveau du réseau et de l’application
* DNATs SNAT sortants et entrants pour communiquer avec les ressources Internet
* Plusieurs adresses IP publiques
* Renseignement sur les menaces
* L’intégration à Azure Monitor

Azure Bastion protège vos machines virtuelles contre l’exposition des ports RDP/SSH au monde extérieur tout en fournissant un accès sécurise à l’aide de RDP/SSH. Il fournit une connectivité RDP/SSH sécurise et fluide à vos machines virtuelles directement depuis le portail Azure via le protocole TLS (Transport Layer Security).

Microsoft Sentinel est une solution évolutive, Cloud native, **de gestion des informations et des événements de sécurité (SIEM)** et **d’orchestration, d’automatisation et de réponse de sécurité (SOAR).**