

METTRE EN ŒUVRE DES SOLUTIONS CLOUD SÉCURISÉES

COMPRENDRE LES CONCEPTS DE SÉCURITÉ AZURE

IDENTITY AND ACCESS MANAGEMENT (IAM)

- Gérer les **accès** et les **autorisations** dans Azure
- **Utilisateurs, groupes, rôles et permissions**

PARE-FEU AZURE

- **Protéger** les ressources réseau
- **Configuration et fonctionnement**

RÉSEAU VIRTUEL

- Création et gestion de **réseaux privés**
- Isolation et **segmentation** du réseau

GESTION DES CERTIFICATS

- **Déployer** et **gérer** des certificats **SSL/TLS**
- **Renouvellement** et **révocation**

IDENTITY AND ACCESS MANAGEMENT (IAM)

UTILISATEURS ET GROUPES

- **Création et gestion d'utilisateurs**
- **Attribution d'utilisateurs dans des groupes**

RÔLES ET PERMISSIONS

- **Rôles** pour contrôler les accès
- Assignment de **permissions** aux rôles

PARE-FEU AZURE

FONCTIONNEMENT

- **Filtrage du trafic** entrant et sortant
- Protection contre les **attaques** et les **menaces**

CONFIGURATION

- Règles de pare-feu
- Interface utilisateur ou ligne de commande

RÉSEAU VIRTUEL

CRÉATION ET CONFIGURATION

- Configuration du réseau privé
- Paramètres IP et routage

ISOLATION ET SEGMENTATION DU RÉSEAU

- **Sous-réseaux**
- **Réseaux privés virtuels (VPN)**

GESTION DES CERTIFICATS

DÉPLOIEMENT

- Procédure de demande de certificat
- Installation sur les services Azure

RENOUVELLEMENT

- Processus de renouvellement automatique
- Suivi des dates d'**expiration**

RÉVOCATION

- **Retrait** des certificats **compromis**
- Mise à jour des **services concernés**

METTRE EN ŒUVRE DES SOLUTIONS CLOUD SÉCURISÉES : AUTHENTIFICATION ET AUTORISATION

AZURE ACTIVE DIRECTORY (AAD)

Azure Active Directory est un service d'identité et d'accès basé sur le **cloud** qui permet de gérer les **identités** et les **accès** des utilisateurs aux ressources.

FONCTIONNEMENT

AAD fournit des services tels que :

- L'**authentification** des utilisateurs
- La gestion des **groupes** et des **rôles**
- La **synchronisation** avec les annuaires locaux

INTÉGRATION AVEC DES APPLICATIONS

Intégrer **AAD** avec des applications permet de gérer l'accès et les **rôles des utilisateurs** directement via AAD, simplifiant ainsi la gestion des identités.

Avantages	Exemples
Centralisation	Gestion des utilisateurs
Sécurité renforcée	Authentification multi-facteurs
Simplification	SSO

UTILISATION DU SINGLE SIGN-ON (SSO)

Le SSO est une fonctionnalité d'**Azure AD** qui permet aux utilisateurs de se connecter une seule fois pour accéder à **plusieurs applications et services**.

Avantages	Exemples d'utilisation
Simplifie la gestion des mots de passe	Accès à Microsoft 365
Améliore la sécurité	Accès aux applications internes de l'entreprise
Augmente la productivité	Accès aux applications SaaS tierces

OAUTH2 ET OPENID CONNECT

OAuth2 est un protocole d'autorisation et **OpenID Connect** est une couche d'identité basée sur OAuth2.

OAuth2	OpenID Connect
Protocole d'autorisation	Couche d'identité
Gestion des accès	Gestion de l'authentification et de l'identité
Basé sur des jetons d'accès	Basé sur des jetons d'accès et des jetons d'identité

PRINCIPE DE FONCTIONNEMENT

OAuth2 permet aux applications d'obtenir un **accès limité** aux comptes des utilisateurs, tandis qu'**OpenID Connect** permet aux utilisateurs de **s'authentifier** auprès des applications en utilisant leurs identifiants de fournisseurs d'identité.

IMPLÉMENTATION DANS AZURE

AAD prend en charge **OAuth2** et **OpenID Connect**, facilitant ainsi leur implémentation et leur utilisation dans les applications et services Azure.

GESTION DES CLÉS ET DES SECRETS

Stockez et gérez les **secrets**, les **clés** et les **certificats** de manière sécurisée avec **Azure Key Vault**.

AZURE KEY VAULT

Azure Key Vault est un service de **gestion des secrets** qui permet de stocker et de gérer les clés, les secrets et les certificats de manière sécurisée.

Avantages	Exemples d'utilisation
Centralisation des secrets	Clés de chiffrement
Sécurité accrue	Certificats SSL/TLS
Gestion des accès	Connexions à des services

FONCTIONNEMENT

Key Vault stocke les données sensibles sous forme d'objets, tels que des **clés**, des **secrets** ou des **certificats**, et permet un **accès contrôlé** à ces objets.

UTILISATION

Intégrer **Key Vault** dans les applications et services pour stocker et accéder aux **secrets** de manière sécurisée, sans révéler les secrets directement dans le code.

Avantages	Explications
Sécurité	Stockage et accès sécurisé aux secrets
Centralisation	Gestion centralisée des secrets
Contrôle d'accès	Contrôle d'accès basé sur les rôles

SÉCURISATION DES DONNÉES

Key Vault permet de protéger les données stockées en utilisant des **contrôles d'accès**, de l'**audit** et du **chiffrement**, garantissant ainsi la sécurité des données sensibles.

METTRE EN ŒUVRE DES SOLUTIONS CLOUD SÉCURISÉES

SURVEILLANCE DE LA SÉCURITÉ

La **surveillance de la sécurité** est essentielle pour **déetecter** et **prévenir** les menaces, ainsi que pour protéger les **ressources** et les **applications** dans Azure.

AZURE SECURITY CENTER

Azure Security Center est un service de **surveillance de la sécurité** qui détecte les **menaces** et protège les **ressources** dans le cloud.

Avantages	Exemples d'utilisation
Surveillance continue	Analyse des vulnérabilités et recommandations
Protection adaptative	Protéger les ressources du cloud
Détection des menaces	Déetecter et réagir aux menaces en temps réel

FONCTIONNEMENT

Azure Security Center collecte et analyse les données des **ressources Azure** pour fournir une vue d'ensemble de la **sécurité** et des **recommandations** pour renforcer la protection.

SURVEILLANCE DES MENACES

Security Center utilise des **algorithmes avancés** pour détecter et surveiller les **menaces en temps réel**.

Avantages	Exemples d'utilisation
Détection rapide	Tentatives de force brute
Prévention des incidents	Malwares
Réponse immédiate	Exploits connus

PROTECTION DES RESSOURCES

Security Center applique des **stratégies de sécurité** et surveille leur conformité pour protéger les ressources Azure.

Avantages de Security Center	Exemples d'utilisation
Surveillance continue	Analyse des menaces
Conformité	Audit de conformité
Protection contre les attaques	Détection d'intrusions

AZURE MONITOR

Azure Monitor est un service de **surveillance des performances** et de l'**état de santé** des **ressources Azure**.

SURVEILLANCE DES PERFORMANCES

Azure Monitor collecte des données de **métriques** et de **journalisation** pour surveiller les performances et l'état de santé des applications et des ressources.

ALERTES ET NOTIFICATIONS

Azure Monitor génère des **alertes** en fonction de seuils **prédéfinis** et envoie des **notifications** pour informer sur les incidents potentiels.

Types d'alertes	Description
Alertes de métriques	Basées sur des métriques, comme l'utilisation du processeur ou la quantité de mémoire disponible
Alertes d'activité	Basées sur des événements, comme la création ou la suppression de ressources
Alertes de journal	Basées sur des données de journaux, comme la détection d'erreurs spécifiques

JOURNAUX D'AUDIT

Les **journaux d'audit** sont essentiels pour suivre les **activités** et analyser les **données de journalisation**.

- Suivi des activités des utilisateurs
- Analyse des accès aux ressources
- Déetecter les problèmes de sécurité
- Vérification de la conformité

COLLECTE ET STOCKAGE DES JOURNAUX

Les **journals d'audit** sont collectés et stockés dans des services Azure tels que **Log Analytics** et **Azure Storage**.

Service Azure	Description
Log Analytics	Un service qui aide à collecter, analyser et agir sur les journaux Azure
Azure Storage	Un service de stockage pour les données non structurées, telles que les journaux d'activité

ANALYSE DES DONNÉES DE JOURNAL

Les données de journal peuvent être analysées pour détecter les **tendances**, les **schémas** et les **anomalies** qui peuvent aider à identifier les problèmes de sécurité.

SUIVI DES ACTIVITÉS

Le suivi des activités permet de surveiller les **actions** effectuées par les **utilisateurs** et les **applications** sur les **ressources Azure**.

- Les actions effectuées par les utilisateurs et les applications peuvent inclure :
 - La création, la modification ou la suppression de ressources
 - Les modifications apportées aux paramètres de configuration
 - Les actions de contrôle d'accès (Ex : ajout d'utilisateurs)

SÉCURITÉ DES APPLICATIONS ET DES DONNÉES

CHIFFREMENT DES DONNÉES

Le **chiffrement** est un mécanisme de protection qui garantit la **confidentialité** et l'**intégrité** des données en les rendant inintelligibles sans la clé de déchiffrement appropriée.

CHIFFREMENT AU REPOS

Le chiffrement au repos protège les **données stockées** sur des supports persistants (disques, bases de données) contre les **accès non autorisés** ou les **vols de supports physiques**.

Type de support	Exemple de chiffrement en Azure
Disque	Azure Disk Encryption (ADE)
Base de données	Azure SQL Database Transparent Data Encryption (TDE)

CHIFFREMENT EN TRANSIT

Le **chiffrement en transit** protège les données transmises entre deux systèmes sur un réseau, empêchant les **attaques d'interception** des données et de l'écoute passive.

SÉCURITÉ DES APPLICATIONS WEB

AZURE WEB APPLICATION FIREWALL (WAF)

Azure WAF est un **pare-feu** qui protège vos applications web contre les attaques courantes, comme les **injections SQL** et les attaques par **script intersites (XSS)**.

FONCTIONNEMENT

Le **WAF** agit comme une **barrière de protection** entre votre application et les clients pour inspecter et filtrer le trafic en fonction de **règles spécifiques**.

CONFIGURATION

La configuration du **WAF Azure** nécessite la création de **règles** et de **politiques de filtrage** pour déterminer quels types de trafic sont autorisés ou bloqués.

AZURE DDOS PROTECTION

Azure DDoS Protection protège vos **applications** contre les **attaques par déni de service distribué (DDoS)** qui cherchent à rendre vos services inaccessibles.

COMPRENDRE LES ATTAQUES DDOS

Les attaques DDoS sont des tentatives **malveillantes** de rendre un service en ligne **indisponible** en inondant le réseau avec un volume massif de trafic.

Type d'attaque	Description
Inondation SYN	Inonde le serveur avec des requêtes SYN
Attaque par réflexion	Utilise des serveurs intermédiaires
Attaque par amplification	Amplifie le trafic via des serveurs tiers

MÉCANISMES DE PROTECTION

Azure DDoS Protection utilise des techniques de **mitigation automatique**, telles que l'absorption et la dispersion du trafic, pour protéger vos applications et minimiser l'impact des attaques.

RÉCUPÉRATION APRÈS SINISTRE ET CONTINUITÉ DES ACTIVITÉS

AZURE SITE RECOVERY

Azure Site Recovery (ASR) est un service permettant la réPLICATION des **VMs**, la récupération d'urgence et la migration pour garantir la **continuité** des activités.

FONCTIONNEMENT

ASR permet de configurer un **basculement automatique** ou **manuel** vers une réplica VM en cas de défaillance de la VM principale.

CONFIGURATION

1. Créer un **Recovery Services vault**
2. Définir les **paramètres de réplication** et de **récupération**
3. Configurer la **VM source** et la **cible**

AZURE BACKUP

Azure Backup est un service intégré qui permet de **sauvegarder** et de **restaurer** les données dans l'environnement Azure.

Avantages	Exemples d'utilisation
Sécurité des données	Bases de données
Facilité d'utilisation	Fichiers et dossiers
Fiabilité	VMs Azure

SAUVEGARDE DES DONNÉES

1. Créer un **Recovery Services vault**
2. Définir la **politique de sauvegarde**
3. Sélectionner les **éléments à sauvegarder**

RESTAURATION DES DONNÉES

1. Sélectionner l'élément à restaurer dans le **Recovery Services vault**
2. Choisir un point de récupération
3. Restaurer les données

TESTS DE BASCULEMENT

Les tests de basculement permettent de valider le fonctionnement du **plan de récupération d'urgence** sans impacter les opérations en cours.

Avantages	Inconvénients
Valide le plan	Peut être coûteux
Réduit les risques	Nécessite des ressources
Améliore la confiance	Peut être complexe

- Test complet
- Test partiel
- Test de table ronde

PLANIFICATION

1. Définir les **objectifs de point de récupération (RPO)** et de **temps de récupération (RTO)**
2. Planifier les tests à **intervalles réguliers**

EXÉCUTION

1. Utiliser **Azure Site Recovery** pour effectuer un test de basculement
2. Vérifier les résultats et ajuster le **plan de récupération** si nécessaire

