République du Sénégal
Ministère de l'Enseignement Supérieur,
de le Recherche et de l'Innovation
(MESRI)

UVS
UNIVERSITE VIRTUELLE DU SENEGAL
foo nekk foofu la

PÔLE SCIENCES, TECHNOLOGIES ET NUMÉRIQUE

MATHÉMATIQUES APPLIQUÉES ET INFORMATIQUE

MÉMOIRE DE MASTER

SUJET : Etudes des risques de sécurités majeurs lier aux cloud et les mécanismes de défense associer cas de Microsoft Azure

PRÉSENTÉ PAR :

Djadji Samba Sow

SOUS LA DIRECTION DE :

Pr Cherif Diallo

Remerciements

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrai témoigner toute ma reconnaissance. Je voudrai tout d'abord adresser toute ma gratitude à mon encadreur Pr Cherif Diallo, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion. Je désire aussi remercier les professeurs de l'UVS, qui m'ont fourni les outils nécessaires à la réussite de mes études universitaires.

Dédicaces

Avec l'expression de ma reconnaissance je dédie ce modeste travail à ceux qui, quels que soient les termes embrassés, je n'arriverais jamais à leur exprimer mon amour sincère.

- ✓ A l'homme, mon précieux offre du Dieu, qui doit ma vie, ma réussite et tout mon respect: mon père
- ✓ A la femme qui a souffert sans me laisser souffrir, qui n'a jamais dit non à mes exigences et qui n'a épargné aucun effort pour me rendre heureux: mon adorable mère.
- ✓ A mon entourage, qui n'ont pas cessés de me conseiller, encourager et soutenir tout au long de mes études. Que dieu les protèges et leurs offre la chance et le bonheur.

Sigles et Abréviations

PAAS: Platform As A Service

SAAS: Software As A Service

IAAS: Infrastructure As A Service

AWS: Amazon Web Service

GCP: Google Cloud Platform

SQL: Structured Query Language

AD: Active Directory

AD DS: Active Directory Domain Service

SSO: Single Sign-On

MFA: Multi-Factor Authentication

RBAC: Role-Based Access Control

IOT: Internet Of Things-

TIC: Technologies de l'information et de la communication

ML: Machine Learning

IA: Intelligence Artificielle

CRM: Customer Relationship Management

CPU: Central Processing Unit

RAM: Random Access Memory

EC2: Elastic Compute 2

ECS: Elastic Container Service

EKS: Elastic Kubernetes Service

S3: Simple Storage Service

EFS: Elastic File System

EBS: Elastic Block Store

RDS: Relational Database Service

VPC: Virtual Private Cloud

ELB: Elastic Load Balancer

IAM: Identity and Access Management

HTTP: HyperText Transfer Protocol

HTTPS: HyperText Transfer Protocol Secure

IP: Internet Protocol

DNS: Domain Name Service

LRS: Locally-Redundant Storage

ZRS: Zone-Redundant Storage

GRS: Geo-Redundant Storage

GZRS: Geo-Zone-Redundant Storage

DDOS: Distributed Denial of Service

APT: Advanced Threat Protection

ID: IDentifier

FIDO2: Fast IDentity Online

B2C: Business to consumer

B2B: Business to Business

LDAP: Lightweight Directory Access Protocol

VPN: Virtual Private Network

JIT: Just-In-Time

JEA: Just Enough Administration

MARS: Microsoft Azure Recovery Services

DPM: Data Protection Manager

CSPM: Cloud Security Posture Management

SIEM; Security Information and Event Management

SOAR: Security Orchestration, Automation and Responses

SSL: Secure Socket Layer

TLS; Transport Layer Security

API: Application Programming Interface

ADE: Azure Disk Encryption

DES: Data Encryption Standard

CLI: Command Line Interface

SOC: Security Operations Center

VM: Virtual Machine

Avant-propos

Pour l'obtention du Diplôme de Master en Systèmes Réseaux et Infrastructures Virtuelles (SRIV), les étudiants doivent présenter un mémoire à la fin de la formation. C'est dans cette optique que nous allons travailler sur un sujet portant l'études des risques de sécurités majeurs lier aux cloud et les mécanismes de défense associer cas de Microsoft Azure dont la teneur est consignée dans ce mémoire.

Liste des Figures et des tableaux

Figure 1: Cloud hybride 4
Figure 2: Les modèles de cloud 5
Figure 3: Structure des Régions Azure 11
Figure 4: Structure d'une zone Géographique Azure 12
Figure 5: Les groupes de ressources Azure 13
Figure 6: Les abonnement 13
Figure 7: Hiérarchie des Groupes d'administration racine 14
Figure 8: Stockage localement redondant 16
Figure 9: Stockage géoredondant (GRS) 16
Figure 10: Stockage redondant interzone (ZRS) 17
Figure 11: Stockage géoredondant interzone (GZRS) 17
Figure 12: Cas d'utilisation des comptes de stockage 18
Figure 13: Sécurité et Commodité des méthodes d'authentifications 22
Figure 14: L'accès Conditionnelle 25
Figure 15: Le contrôle d'accès en fonction du rôle 25
Figure 16: Le modèle Confiance Zéro 26
Figure 17: Azure Backup 27
Figure 18: Les trois exigences de Defender pour le cloud 28
Figure 19: Fonctionnement de Microsoft Sentinel 29
Figure 20: l'exhaustivité d'Azure Monitor 30
Figure 21: Déploiement Azure Monitor (Log Analytics Workspaces 33
Figure 22: Portail Azure 34
Figure 23: Création d'un Groupe de ressource avec PowerShell 34
Figure 24: Création d'une machine virtuelle avec PowerShell 35
Figure 25: Vérification du provisionnement des ressources 35
Figure 26: recherche de log Analytics sur le portail azure 36
Figure 27: création d'un espace de travail Log Analytics 36
Figure 28: configuration des fonctions de base de log Analytics 36
Figure 29: Activer l'extension de machine virtuelle Log Analytics 37
Figure 30: connecter la machine virtuelle à log Analytics 37
Figure 31: vérification de l'état de la connexion du VM à Log Analytics 38
Figure 32: configuration d'un collecteur d'évènement Windows liées aux systèmes 38
Figure 33: configuration de quelques compteurs de performances Windows 39
Figure 34: requetés pour l'interrogation des données 40
Figure 35: Résultat des requêtes sur le CPU et la Mémoire 40
Figure 36: Déploiement de Microsoft Defender pour le Cloud 41
Figure 37: recherche de Microsoft Defender sur le portail azure 42
Figure 38: Mise à jour et installation de l'agent 42
Figure 39: choix de l'abonnement approprier 43
Figure 40: Activation des plans Microsoft defender 43

Figure 41: vérifier si l'approvisionnement est active sur log Analytics 44
Figure 42: Collecte de données de tous les événements 44
Figure 43: inventaire de la machine virtuelle myVM 45
Figure 44: Les recommandations liées à la machine virtuelle myVM 45
Figure 45: Implémenter JIT sur myVM 46
Figure 46: Activation de l'accès JIT sur myVM 47
Figure 47: configuration de l'accès JIT sur myVM 47
Figure 48: Détails de la connexion 48
Figure 49: Déploiement de Microsoft Sentinel 48
Figure 50: Recherche de Microsoft Sentinel sur le portail azure 49
Figure 51: Le panneau de Microsoft Sentinel 49
Figure 52: Ajout d'un espace de travail à Microsoft Sentinel 50
Figure 53: Ajout d'un connecteur d'activité 50
Figure 54: Configurer les journaux d'activité Azure dans le flux vers l'espace de travail Log Analytics 51
Figure 55: ajout de l'espace de travail principale 52
Figure 56: Activation de la gestion d'une tache correction 52
Figure 57: l'affichage de quelques données collectées 53
Figure 58: création d'une règle utilisant Azure Activity 54
Figure 59: Définir la logique de règle 54
Figure 60: configuration du paramètre d'incident 55
Figure 61: visualisation de la règle créée 55
Figure 62: recherche de Déployer un modèle personnalisé sur le portail azure 56
Figure 63: création d'un modèle personnalisé 56
Figure 64: L'ajout de notre Playbooks 57
Figure 65: finalisation de la création 57
Figure 66: la logique Change-Incident-Severity 58
Figure 67: configuration des quatre connexions 59
Figure 68: création d'une règle Scheduled 59
Figure 69: Cette règle identifie la suppression des stratégies d'accès aux machines JIT 60
Figure 70: visualisation de la règle active appelée djadji Playbook 61
Figure 71: Invoquer un incident sur myVM 61
Figure 72: recherche de journal d'activité sur le portail azure 62
Figure 73: apparition de entrée Supprimer les stratégies d'accès réseau JIT 62
Figure 74: une alerte correspondant à la suppression de la stratégie d'accès aux machines virtuelles JIT 63

Tables des matières

Remerciements iii
Dédicaces iv
Sigles et Abréviations v
Avant-propos viii
Liste des Figures et des tableaux ix
Introduction 1
CHAPITRE 1 : Les notions fondamentales du cloud computing 3
1.1 Définition du cloud 3
1.2 Les types de cloud 3
1.2.1 Cloud public 3
1.2.2 Cloud privé 4
1.2.3 Cloud hybride : 4
1.2.4 Cloud communautaire 5
1.3 Modèle de service cloud 5
1.3.1 IAAS 6
1.3.2 PAAS 6
1.3.3 SAAS 7
1.4 Avantage et Inconvénient du cloud 7
1.4.1 Avantages 7
1.4.2 Inconvénients 8
1.5 Les différents fournisseurs de cloud 9
1.5.1 AWS 9
1.5.2 GCP 9
1.5.3 AZURE 10
1.5.3.1 Infrastructure physique d'Azure 10
1.5.3.2 L'infrastructure de gestion Azure 12
1.5.3.3 Les services de calcul et réseau Azure 15
CHAPITRE 2 : Les risques de sécurité majeurs du cloud et les solutions associées 19
2.1 Les risques de sécurité majeurs du cloud computing 19
2.1.1 Les Attaques DDoS 19
2.1.2 Les vulnérabilités par des technologies partagées 19

2.1.3 Une action malveillante 19
2.1.4 Les Attaques de Session Hijacking : 20
2.1.5 Les attaques SQL injection : 20
2.1.6 L'isolation: 20
2.1.7 Vulnérabilités des services 20
2.1.8 Gestion de l'identité et accès médiocre 20
2.1.9 Mauvaises configurations du cloud 21
2.1.10 Attaques sur la chaîne logistique 21
2.1.11 Accès à la plateforme de gestion du cloud 21
2.2 Mécanismes de défense proposés par Microsoft Azure 22
2.2.1 Authentification et Autorisation : 22
2.2.1.1 L'authentification unique (SSO) 22
2.2.1.2 L'authentification multifacteur 23
2.2.1.3 L'authentification sans mot de passe 23
2.2.1.4 Azure Active Directory (AD) : 23
2.2.1.5 Une identité externe 24
2.2.1.6 Azure AD Domain Services : 24
2.2.2 Identité et gestion d'accès 24
2.2.2.1 L'accès conditionnel 24
2.2.2.2 Le contrôle d'accès en fonction du rôle Azure RBAC 25
2.2.3 Confidentialité, Intégrité, et disponibilité 26
2.2.3.1 Le modèle Confiance Zéro 26
2.2.3.2 Azure Backup : 26
2.2.3.3 Azure Disaster Recovery : 27
2.2.4 Surveillance de la sécurité et de réponse aux incidents 27
2.2.4.1 Defender pour le cloud 28
2.2.4.2 Microsoft Defender pour Identity 28
2.2.4.3 Azure Sentinel : 29
2.2.4.4 Azure Monitor 30
2.2.4.5 Azure Log Analytics 31
2.2.5 Gestion politique de sécurité 31
2.2.5.1 Azure Policy : 31
2.2.5.2 Azure AD Identity Governance : 31
2.2.6 Chiffrement 32

2.2.6.1 Azure Key Vault : ... 32
2.2.6.2 Azure Disk Encryptions ... 32
2.2.6.3 Le chiffrement côté serveur du Stockage sur disque Azure ... 32
$2.2.6.4 Le chiffrement sur l'hôte ... 32
2.2.6.5 Le chiffrement de disque confidentiel ... 32
CHAPITRE 3 : Implémentation d'un SIEM sur Azure ... 33
3.1 Mise en place de l'environnement : ... 33
3.1.1 Déploiement azure Monitor ... 33
3.1.1.1 Tâche 1 : Déployer une machine virtuelle Azure ... 34
3.1.1.2 Tâche 2 : Créer un espace de travail Log Analytics ... 35
3.1.1.3 Tâche 3 : Activer l'extension de machine virtuelle Log Analytics ... 37
3.1.1.4 Tâche 4 : Collecter des données d'événement et de performances de machine virtuelle 38
3.1.1.5 Tâche 5 : Afficher et interroger les données collectées ... 39
3.1.2 Déploiement de Microsoft defender pour le cloud : ... 41
3.1.2.1 Tâche 1 : Configurer Microsoft Defender pour le Cloud ... 41
3.1.2.2 Tâche 2 : Examiner la recommandation Microsoft Defender for Cloud ... 44
3.1.2.3 Tâche 3 : Implémenter la recommandation Microsoft Defender for Cloud pour activer l'accès aux machines virtuelles Just in time ... 46
3.1.3 Déploiement de Microsoft Sentinel ... 48
3.1.3.1 Tâche 1 : Intégrer Azure Sentinel ... 49
3.1.3.2 Tâche 2 : configurer Microsoft Sentinel pour utiliser le connecteur de données Azure Activity ... 50
3.1.3.3 Tâche 3 : Créer une règle qui utilise le connecteur de données Azure Activity 53
3.1.3.4 Tâche 4 : Créer un playbook ... 56
3.1.3.5 Tâche 5 : Créer une alerte personnalisée et configurer un playbook en tant que réponse automatisée ... 59
3.2 Tâche 6 : Invoquer un incident et passer en revue les actions associées ... 61
Conclusion ... 64
Bibliographie ... 65
Annexes ... 67

Introduction

Avec l'avènement du cloud computing beaucoup de types de services ont vu le jour notamment le SaaS (Software as a Service), le PaaS (Platform as a Service) et le IaaS (Infrastructure as a Service). Ces derniers offrent des avantages aux entreprise et aux particuliers tels que la réduction de coûts IT (matériel, mises à jour des systèmes et des applications, ressources humaines et consommation d'énergie), la scalabilité, l'optimisation de la collaboration dans les pratiques de travail et de suivi client et l'accès aux mises à jour automatiques. Ce qui fait que ces dernières années, on note une croissance constante de son adoption avec le développement massif de solutions de métadonnées, l'internet des objets (IoT) et la 5G qui s'appuient sur des infrastructures nuagiques.

Cette évolution bien que bénéfique car ayant changé la vie de beaucoup de personnes, elle n'est pas sans conséquence du fait qu'elle attire de nombreux acteurs malveillants à la recherche de gain financier, de secrets liés à la technologie, etc. Dans ces conditions, nul n'est à l'abri de ces menaces, car beaucoup d'organisme sont confrontés à des attaques de types par exemple DDOS qui visent à rendre un serveur, un service ou une infrastructure indisponible. L'attaque peut prendre différentes formes : une saturation de la bande passante du serveur pour le rendre injoignable, un épuisement des ressources système de la machine, l'empêchant ainsi de répondre au trafic légitime. Ce qui nous amène à la question suivante: comment cela est-il possible? Cela est dû au fait qu'il il est très difficile de rendre un système complètement inattaquable pour plusieurs raisons:

- La plupart des systèmes informatiques ont des failles de sécurité qui les rendent vulnérables aux intrusions. Les trouver et les réparer toutes ne sont pas possible pour des raisons techniques et économiques.
- Les systèmes existants ayant des failles connues ne sont pas facilement remplaçables par des systèmes plus sûrs, principalement parce qu'ils ont des fonctionnalités intéressantes que n'ont pas les systèmes plus sûrs, ou parce qu'ils ne peuvent pas être remplacés pour des raisons financières.
- Déployer des systèmes sans failles est très difficile, voire impossible car certaines failles sont inconnues ou inévitables. C'est ce qu'on appelle les zero-day-attacks.
- Même les systèmes les plus sûrs sont vulnérables aux abus de la part d'utilisateurs légitimes qui profitent de leurs privilèges ou souffrent de la négligence des règles de sécurité par ceux-ci.
- La migration des données et des applications vers le cloud peut entraîner des préoccupations en matière de sécurité, en particulier en ce qui concerne la gestion des menaces, l'accès et la conformité réglementaire.

La sécurité d'un environnement informatique en particulier le cloud est donc crucial pour garantir la protection des données et des applications de l'entreprise. Dans ce sens il est important de comprendre les différentes mesures de sécurité mises en place par les fournisseurs de cloud pour protéger les environnements de leurs clients.

Cependant il existe plusieurs fournisseurs de cloud (AWS, Azure, GCP) sur marché, offrant une gamme de services de sécurité cloud public, privé et hybride. Dans ce mémoire nous portons notre choix sur Azure pour des raisons que nous détaillerons ultérieurement (dans les annexes).

La structure de ce mémoire sera la suivante: dans un premier temps, nous présenterons le contexte et les définitions clés liés au cloud et expliquer le fonctionnement du cloud Azure. Ensuite, nous verront les menaces les plus fréquents dans un environnement cloud ainsi que les solutions proposées par Azure pour palier à celles-ci. Enfin nous allons déployer un environnement sur lequel on va mettre en place une preuve de concept de détection et de réponse aux menaces basée sur Microsoft Sentinel en utilisant deux outils pour la collecte de données à savoir Azure Monitor (Log Analytic) et Microsoft Defender, nous allons par la suite invoquer un incident pour voir comment ces solutions Microsoft collabore entre elles pour détecter celles-ci.

CHAPITRE 1 : *Les notions fondamentales du cloud computing*

Il est incontestable que la technologie internet connaît un développement exponentiel depuis sa création. Actuellement, une nouvelle "tendance" a fait son apparition dans le monde des Tics (Technologies de l'information et de la communication), il s'agit du Cloud Computing. Cette technologie, s'appuie sur le WEB 2.0, offre des occasions aux sociétés de réduire les coûts d'exploitation des logiciels par leurs utilisations directement en ligne.

Dans ce chapitre nous présenterons le contexte et les définitions clés liés au cloud et expliquerons le fonctionnement du cloud Azure.

1.1 Définition du cloud

Le cloud computing se réfère à la fourniture de services informatiques, tels que le stockage, le traitement, le réseautage, le logiciel, les analyses et l'intelligence, par l'intermédiaire d'Internet (le cloud). Ces services sont généralement proposés sur la base du pay-as-you-go et les utilisateurs peuvent y accéder au besoin, plutôt que de devoir construire et entretenir leur propre infrastructure physique. Cela permet aux organisations de se concentrer sur leurs compétences clés et de disposer de la possibilité de monter ou descendre en fonction des besoins.

Étant donné que le cloud computing utilise Internet pour fournir ces services, il n'a pas besoin d'être limité par une infrastructure physique de la même manière qu'un centre de données traditionnel. Cela signifie que si vous avez besoin d'augmenter rapidement votre infrastructure informatique, vous n'avez pas besoin d'attendre pour construire un nouveau centre de données : vous pouvez utiliser le cloud pour étendre rapidement votre empreinte informatique.

1.2 Les types de cloud

1.2.1 Cloud public

Le cloud public est un type de cloud computing qui permet aux utilisateurs de louer l'accès à des ressources informatiques, comme des serveurs, des bases de données, du stockage et des réseaux, via le Web. Le cloud public est géré par une entreprise de cloud computing, qui assure la maintenance et la gestion des ressources informatiques. Les utilisateurs paient uniquement pour les ressources qu'ils utilisent, ce qui leur permet de bénéficier d'une grande flexibilité et d'économies importantes par rapport à l'achat et à la gestion de leur propre infrastructure informatique. Les exemples courants de clouds publics incluent Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform.

1.2.2 Cloud privé

Un cloud privé est, à certains égards, l'évolution naturelle d'un centre de données d'entreprise. Il s'agit d'un cloud exclusivement destiné à une seule organisation, offrant un plus grand contrôle pour l'entreprise et son service informatique. Cependant, cela implique également des coûts supplémentaires et moins d'avantages par rapport à un déploiement en cloud public. Le cloud privé peut être hébergé localement dans votre centre de données ou par un tiers en dehors de votre site, exclusivement pour votre entreprise.

1.2.3 Cloud hybride :

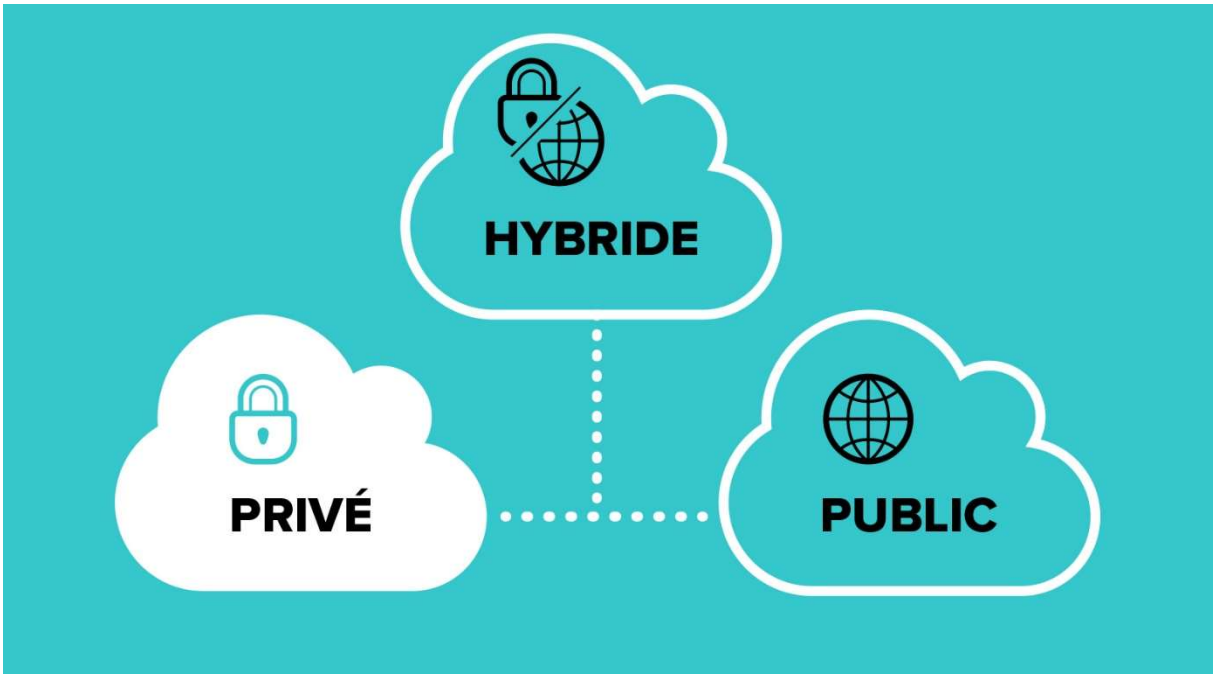


Figure 1: Cloud hybride

Le cloud hybride est un modèle de cloud computing qui combine des ressources informatiques locales avec des ressources de cloud public. Le cloud hybride permet aux utilisateurs de profiter des avantages des deux modèles de cloud computing, à savoir la flexibilité et l'économie du cloud public et le contrôle et la confidentialité du cloud privé.

Le cloud hybride peut être utilisé de différentes manières. Par exemple, une organisation peut choisir de stocker certaines de ses données sensibles sur un cloud privé, tout en utilisant un cloud public pour le stockage de données moins sensibles. Ou bien, une organisation peut utiliser un cloud public pour augmenter la capacité de son infrastructure informatique en cas de pics de trafic ou de demande, tout en conservant une infrastructure informatique locale pour des besoins de base. Le cloud hybride offre une grande flexibilité et permet aux utilisateurs de choisir le modèle de cloud qui convient le mieux à leurs besoins.

1.2.4 Cloud communautaire

Le cloud communautaire est un modèle de cloud computing qui permet à plusieurs organisations de partager des ressources informatiques, comme des serveurs, des bases de données, du stockage et des réseaux, afin de réaliser des économies et de bénéficier d'une infrastructure informatique hautement disponible. Le cloud communautaire est géré par une ou plusieurs organisations participantes, qui s'occupent de la maintenance et de la gestion des ressources informatiques. Il est souvent utilisé par des organisations qui ont des besoins en informatique similaires et qui souhaitent mutualiser leurs coûts. Par exemple, plusieurs universités peuvent décider de mettre en place un cloud communautaire pour héberger leurs systèmes de gestion de l'enseignement et de l'apprentissage. Le cloud communautaire peut également être utilisé par des organisations gouvernementales ou non gouvernementales qui souhaitent mettre en commun leurs ressources informatiques pour atteindre un objectif commun.

1.3 Modèle de service cloud

Le principe de responsabilité partagé est un concept clé dans le cloud computing. Il désigne la répartition des responsabilités entre le fournisseur de cloud et l'utilisateur pour l'exploitation et la gestion du cloud. Selon ce principe, le fournisseur de cloud est responsable de la maintenance et de la gestion des ressources informatiques du cloud, tandis que l'utilisateur est responsable de l'installation et de la configuration des logiciels et des systèmes d'exploitation nécessaires pour ses propres applications.

Le principe de responsabilité partagé permet aux utilisateurs de bénéficier de la flexibilité et de l'économie du cloud computing tout en leur donnant un certain niveau de contrôle sur leur infrastructure informatique. Cependant, il est important de comprendre clairement les responsabilités de chaque partie pour éviter les mauvaises surprises et gérer efficacement les risques. Cette responsabilité varie en fonction du type de services cloud choisit.

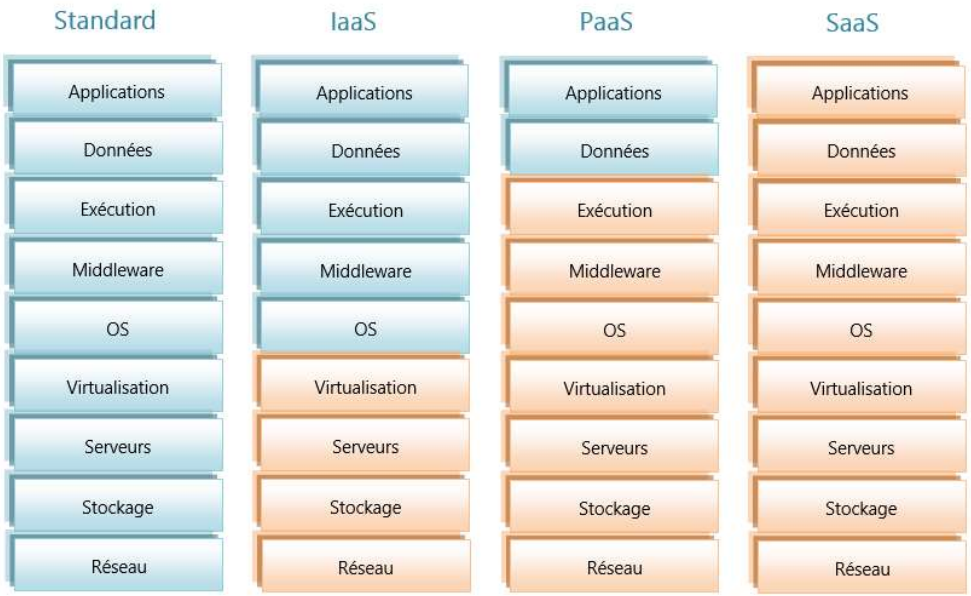


Figure 2: Les modèles de cloud

1.3.1 IAAS

Le modèle IAAS (Infrastructure as a Service, ou "infrastructure en tant que service" en français) est un type de cloud computing qui permet aux utilisateurs de louer l'accès à des ressources informatiques de base, comme des serveurs, du stockage et des réseaux, via le Web. Le fournisseur de IAAS s'occupe de la maintenance et de la gestion de ces ressources, tandis que l'utilisateur est responsable de l'installation et de la configuration des logiciels et des systèmes d'exploitation nécessaires pour ses propres applications.

Le modèle IAAS est souvent utilisé par les développeurs de logiciels et les entreprises qui souhaitent avoir un accès flexible et économique à des ressources informatiques de base pour développer et exécuter leurs applications. Il est également couramment utilisé par les entreprises pour les tests et les déploiements de nouvelles applications, car il leur permet de créer rapidement des environnements de test et de développement sans avoir à acheter et à configurer leur propre infrastructure informatique.

Certains scénarios courants où IaaS pourraient avoir un sens incluent :

- Migration lift-and-shift : vous installez des ressources cloud similaires à votre centre de données sur site, puis vous déplacez simplement les éléments exécutés sur site vers l'infrastructure IaaS.
- Test et développement : vous avez élaboré des configurations pour les environnements correspondants et vous devez les reproduire rapidement. La mise en place ou l'arrêt rapides de ces environnements est rendue possible grâce à une structure IaaS, tout en préservant une totale maîtrise.

1.3.2 PAAS

Le modèle PAAS (Platform as a Service, ou "plateforme en tant que service" en français) est un type de cloud computing qui permet aux utilisateurs de louer l'accès à une plateforme logicielle sur laquelle ils peuvent développer, exécuter et gérer leurs applications. Le fournisseur de PAAS s'occupe de la maintenance et de la gestion de la plateforme logicielle, tandis que l'utilisateur est responsable du développement et de la gestion de ses applications.

Le modèle PAAS est souvent utilisé par les développeurs de logiciels et les entreprises qui souhaitent avoir un accès flexible et économique à une plateforme logicielle pour développer et exécuter leurs applications. Il permet aux développeurs de se concentrer sur le développement de leurs applications, sans avoir à se soucier de la gestion et de la maintenance de la plateforme logicielle sous-jacente. Les exemples courants de PAAS incluent Google App Engine et Heroku.

Certains scénarios courants où PaaS pourraient avoir un sens incluent :

- Cadre de développement : PaaS fournit un cadre sur lequel les développeurs peuvent s'appuyer pour développer ou personnaliser des applications basées sur le cloud. Semblable à la façon dont vous créez une macro Excel, PaaS permet aux développeurs de créer des applications à l'aide de composants logiciels intégrés. Des fonctionnalités cloud telles que l'évolutivité, la haute disponibilité et la capacité

multi-tenant sont incluses, ce qui réduit la quantité de codage que les développeurs doivent effectuer.

- Analytique ou intelligence économique : les outils fournis en tant que service avec PaaS permettent aux organisations d'analyser et d'exploiter leurs données, de trouver des informations et des modèles et de prédire les résultats pour améliorer les prévisions, les décisions de conception de produits, les retours sur investissement et d'autres décisions commerciales.

1.3.3 SAAS

Le modèle SAAS (Software as a Service, ou "logiciel en tant que service" en français) est un type de cloud computing qui permet aux utilisateurs d'accéder à un logiciel en ligne via le Web. Le fournisseur de SAAS s'occupe de l'installation, de la maintenance et de la gestion du logiciel, tandis que l'utilisateur est responsable de son utilisation. Le modèle SAAS est souvent utilisé par les entreprises pour accéder à des applications de gestion, comme les systèmes de gestion de la relation client (CRM) et les systèmes de gestion des ressources humaines (GRH).

Le modèle SAAS présente plusieurs avantages pour les utilisateurs. Tout d'abord, ils n'ont pas à acheter et à maintenir le logiciel eux-mêmes, ce qui leur permet de réaliser des économies importantes. Ensuite, ils n'ont pas à s'inquiéter de la maintenance et de la mise à jour du logiciel, car ces tâches sont effectuées par le fournisseur de SAAS. Enfin, le modèle SAAS permet aux utilisateurs d'accéder au logiciel de n'importe où et à tout moment, ce qui leur offre une grande flexibilité. Les exemples courants de SAAS incluent Microsoft Office 365 et Adobe Creative Cloud.

Certains scénarios courants pour SaaS sont :

- E-mail et messagerie.
- Applications de productivité d'entreprise.
- Suivi des finances et des dépenses.

1.4 Avantage et Inconvénient du cloud

1.4.1 Avantages

Il y a plusieurs avantages à utiliser le cloud computing :

- Economies : les utilisateurs ne paient que pour les ressources informatiques qu'ils utilisent, ce qui leur permet de réaliser des économies importantes par rapport à l'achat et à la gestion de leur propre infrastructure informatique.
- Flexibilité : les utilisateurs peuvent facilement ajouter ou retirer des ressources informatiques en fonction de leurs besoins, ce qui leur offre une grande flexibilité.
- Mobilité : les utilisateurs peuvent accéder à leurs applications et à leurs données de n'importe où et à tout moment, ce qui leur permet de travailler de manière plus efficace et de collaborer plus facilement.

- Mises à jour automatiques : les fournisseurs de cloud s'occupent de la maintenance et des mises à jour des ressources informatiques, ce qui permet aux utilisateurs de se concentrer sur leur cœur de métier plutôt que sur la gestion de leur infrastructure informatique.
- Haute disponibilité : les fournisseurs de cloud mettent en place des mesures de redondance et de tolérance de panne pour assurer la disponibilité des ressources informatiques, ce qui permet aux utilisateurs de bénéficier d'une infrastructure hautement disponible.
- Mise à l'échelle verticale : avec la mise à l'échelle verticale, si vous développiez une application et que vous aviez besoin de plus de puissance de traitement, vous pouvez effectuer une mise à l'échelle verticale pour ajouter plus de CPU ou de RAM à la machine virtuelle. À l'inverse, si vous vous rendez compte que vous avez sur-spécifié les besoins, vous pouvez réduire verticalement en abaissant les spécifications du processeur ou de la RAM.
- Mise à l'échelle horizontale : avec la mise à l'échelle horizontale, si vous subissiez soudainement une forte augmentation de la demande, vos ressources déployées pourraient être mises à l'échelle (automatiquement ou manuellement). Par exemple, vous pouvez ajouter des machines virtuelles ou des conteneurs supplémentaires, en évoluant. De la même manière, s'il y avait une baisse significative de la demande, les ressources déployées pourraient être mises à l'échelle (automatiquement ou manuellement).

1.4.2 Inconvénients

Il y a également quelques inconvénients à utiliser le cloud computing :

- Dépendance : les utilisateurs dépendent du fournisseur de cloud pour l'accès à leurs applications et à leurs données, ce qui peut être un problème en cas de panne ou de perturbation du service.
- Perte de contrôle : les utilisateurs perdent un certain niveau de contrôle sur leur infrastructure informatique, car elle est gérée par le fournisseur de cloud.
- Questions de sécurité : certaines entreprises sont réticentes à utiliser le cloud en raison de préoccupations de sécurité, telles que la perte de données ou les fuites de données.
- Coût à long terme : bien que les utilisateurs paient uniquement pour les ressources informatiques qu'ils utilisent, ils peuvent finir par payer plus à long terme que s'ils avaient acheté et géré leur propre infrastructure informatique.
- Limites de personnalisation : les utilisateurs sont limités dans la personnalisation de leur infrastructure informatique par les options proposées par le fournisseur de cloud.

1.5 Les différents fournisseurs de cloud

Les fournisseurs de cloud sont des sociétés qui offrent des clouds publics, gèrent des clouds privés, ou bien proposent des services de cloud computing à la demande tels que des infrastructures en tant que service (IaaS), des plateformes en tant que service (PaaS) et des logiciels en tant que service (SaaS). Les services cloud ont l'avantage de réduire les coûts des processus métier par rapport à un service informatique sur site. Les fournisseurs les plus populaires sont AWS, Azure et GCP.

1.5.1 AWS

Amazon Web Services (AWS) est une plateforme et une infrastructure de cloud computing créée par Amazon.com pour construire, déployer et gérer des applications et des services à travers un réseau mondial de centres de données. AWS propose une large gamme de services tels que le calcul, le stockage, les bases de données, les analyses, l'apprentissage automatique, les mobiles, l'Internet des objets (IoT), la sécurité et les applications d'entreprise. C'est l'une des plateformes de cloud computing les plus populaires d'aujourd'hui et est utilisée par des entreprises de toutes tailles, des start-ups aux grandes entreprises, pour alimenter leurs applications et services.

1.5.2 GCP

Google Cloud Platform (GCP) est un ensemble de services cloud proposé par Google. Il permet aux entreprises et aux développeurs de créer, de déployer et de gérer des applications et des services sur les infrastructures de Google. GCP propose des services d'infrastructure en tant que service (IaaS), de plateforme en tant que service (PaaS) et de logiciel en tant que service (SaaS).

Voici quelques exemples de services proposés par GCP :

- Compute Engine : ce service permet aux utilisateurs de lancer des instances de serveurs virtuels sur les infrastructures de Google.
- Kubernetes Engine : ce service permet aux utilisateurs de déployer et de gérer des applications en utilisant le système de conteneurs Kubernetes.
- BigQuery : ce service de gestion de données en masse permet aux utilisateurs d'analyser rapidement de grandes quantités de données.
- Cloud Functions : ce service de cloud computing en fonction permet aux utilisateurs de développer et de déployer des applications basées sur des événements sans avoir à gérer les serveurs.

GCP propose également de nombreux autres services, notamment en matière de stockage, de réseau, de Machine Learning et de développement. En utilisant GCP, les entreprises et les développeurs peuvent bénéficier de la scalabilité, de la disponibilité et de la sécurité des infrastructures de Google.

1.5.3 AZURE

Dans cette section nous allons voir en détails le fonctionnement d'azure.

Microsoft Azure est une plate-forme cloud qui fournit une variété de services en évolution constante pour vous aider à atteindre vos objectifs professionnels. Il offre une gamme complète de services, allant de simples services Web pour héberger votre présence en ligne à des ordinateurs virtualisés pour exécuter des solutions logicielles personnalisées. Les services Azure incluent le stockage en ligne, l'hébergement de bases de données, la gestion centralisée des comptes, et des fonctionnalités innovantes telles que l'IA et l'IoT.

Les Composants architecturaux d'Azure :

1.5.3.1 Infrastructure physique d'Azure

La fondation physique d'Azure est composée de centres de données. Conceptuellement, ces centres sont similaires à ceux de grandes entreprises, équipés de racks, d'alimentation électrique, de systèmes de refroidissement et de réseaux dédiés. Les centres sont regroupés dans des régions Azure et des zones de disponibilité pour offrir une résilience et une fiabilité maximales pour vos charges de travail d'entreprise critiques.

- **Régions**

Chaque région Azure est une zone géographique qui comporte un ou plusieurs centres de données proches les uns des autres et connectés par un réseau à faible latence. Azure utilise une gestion intelligente des ressources pour veiller à ce que les charges de travail soient correctement distribuées à l'intérieur de chaque région.

- **Zones de disponibilité**

Les zones de disponibilité Azure sont des centres de données séparés qui se trouvent dans une région donnée. Chacune de ces zones est dotée d'une infrastructure indépendante en termes d'alimentation, de refroidissement et de réseau. Elles sont conçues pour offrir une limite d'isolation pour les charges de travail. Si une zone tombe en panne, l'autre continuera à fonctionner en toute transparence. Les zones sont connectées par des réseaux en fibre optique privés à grande vitesse. Pour garantir une haute disponibilité, chaque région dotée de zones de disponibilité comporte au moins trois zones distinctes. Toutefois, toutes les régions Azure ne prennent pas en charge les zones de disponibilité.

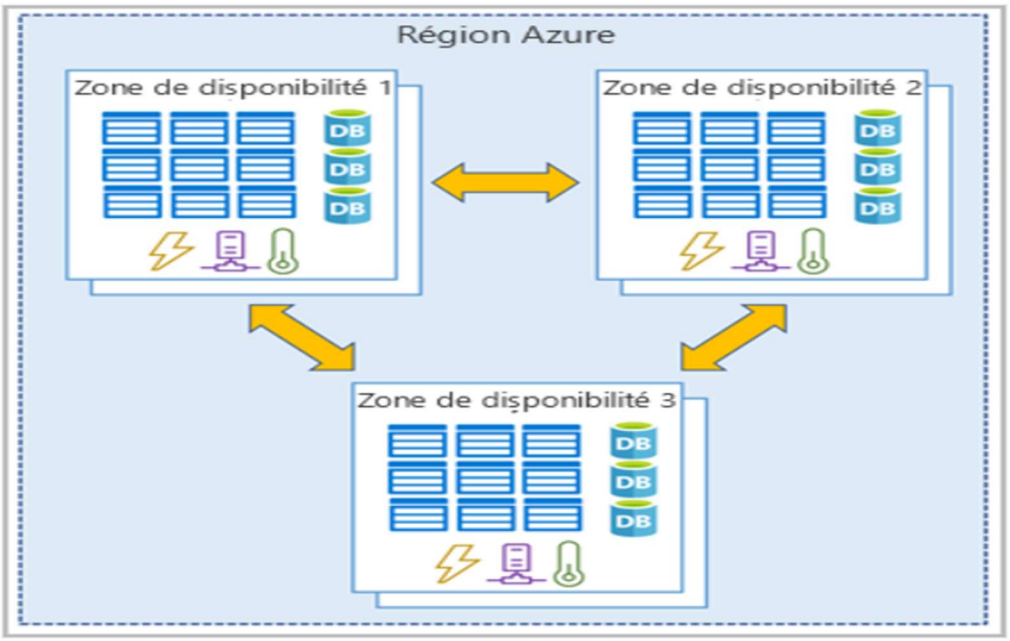


Figure 3: Structure des Régions Azure

- **Paires de régions**

Pour une réduction des risques d'interruptions dus à des événements tels que des désastres naturels, des troubles civils, des pannes d'électricité ou des problèmes de réseau physique, la plupart des régions Azure sont associées à une autre région dans la même zone géographique située à une distance minimale de 480 kilomètres. Cela permet une réplication de ressources à l'échelle géographique. Par exemple, en cas de catastrophe affectant une région paire, les services seront automatiquement basculés vers l'autre région.

Cependant, tous les services Azure ne répliquent pas automatiquement les données. Pour ces cas, la récupération et la réplication doivent être configurées par le client.

Voici des exemples de paires de régions Azure: USA Ouest/USA Est et Asie Sud-Est/Asie Est. Étant directement connectées et suffisamment éloignées des menaces locales, elles peuvent être utilisées pour assurer la redondance de données et la fiabilité des services.

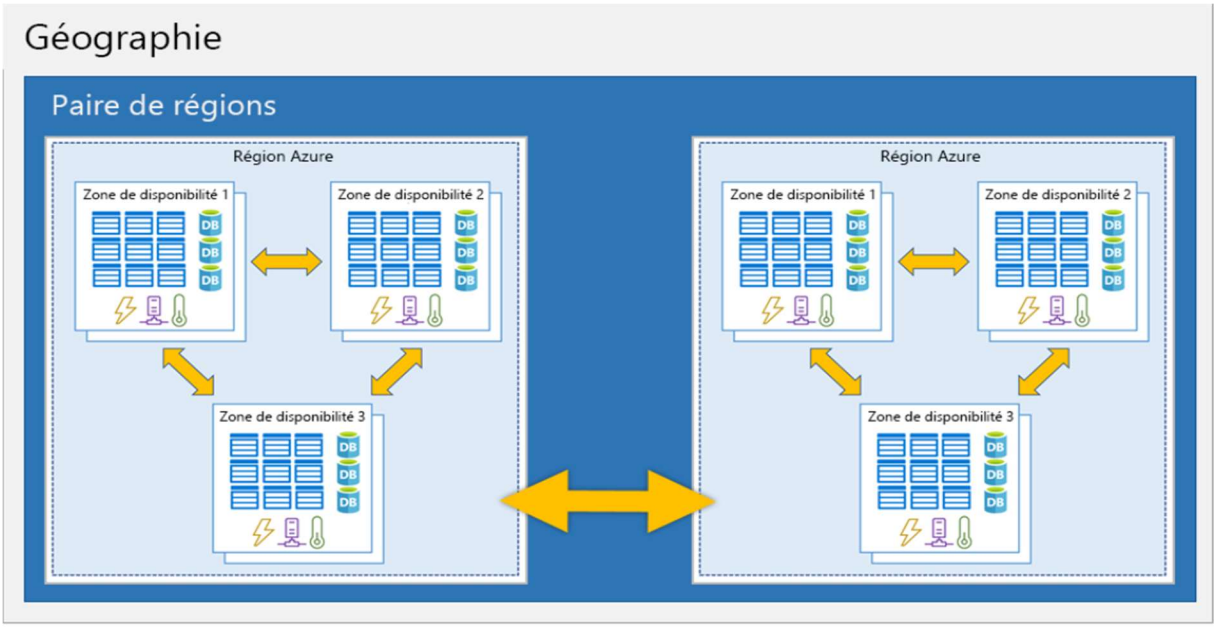


Figure 4: Structure d'une zone Géographique Azure

- **Régions souveraines**

En plus des régions courantes, Azure propose aussi des régions souveraines. Ce sont des instances d'Azure distinctes de l'instance principale d'Azure, qui peuvent être requises pour des raisons légales ou de conformité. Quelques exemples de régions souveraines Azure incluent US DoD Centre, US Gov Virginie, US Gov Iowa, etc., destinées aux agences gouvernementales et aux partenaires du secteur public des États-Unis, et gérées par un personnel autorisé aux États-Unis avec des certifications supplémentaires de conformité. Pour les régions en Chine, telles que Chine Est et Chine Nord, une entente unique a été conclue entre Microsoft et 21Vianet, stipulant que Microsoft ne gère pas directement les centres de données.

1.5.3.2 L'infrastructure de gestion Azure

L'infrastructure de gestion d'Azure est composée de différents éléments, tels que des ressources et des groupes de ressources, des abonnements et des comptes. Connaître la structure hiérarchique de ces éléments est essentiel pour planifier de manière efficace les projets et les produits sur Azure.

- **Ressources et groupes de ressources Azure**

Dans Azure, tout ce que vous configurez pour votre projet ou produit est considéré comme une ressource. Les ressources peuvent inclure des machines virtuelles, des réseaux virtuels, des bases de données, des services cognitifs, etc. Elles sont les éléments fondamentaux qui constituent les différentes parties de votre solution Azure.



Figure 5: Les groupes de ressources Azure

Le regroupement de ressources sous forme de groupes de ressources est une fonctionnalité d'Azure. Lorsque vous créez une ressource, vous devez la classer dans un groupe de ressources pour une meilleure organisation. Chaque ressource ne peut être associée qu'à un seul groupe de ressources à la fois, bien que plusieurs ressources puissent être incluses dans un même groupe. Il est possible de déplacer une ressource d'un groupe à un autre, mais une fois ce déplacement effectué, la ressource n'est plus reliée à son ancien groupe. Il n'est pas non plus possible d'annexer un groupe de ressources à un autre.

- **Abonnements Azure**

Les abonnements Azure sont des outils de gestion, de facturation et d'évolutivité pour vos ressources. Ils fournissent une manière logique d'organiser vos groupes de ressources et de simplifier les facturations. Pour utiliser Azure, vous avez besoin d'un abonnement. Celui-ci vous donne un accès autorisé et authentifié aux produits et services Azure ainsi qu'une possibilité de provisionner des ressources.

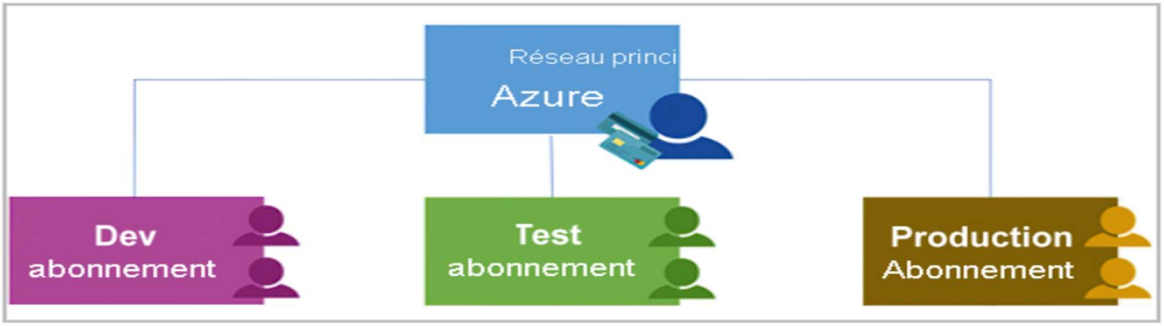


Figure 6: Les abonnement

- **Groupes d'administration Azure**

Le dernier aspect clé de la gestion d'Azure est le groupe d'administration. Les ressources sont regroupées en groupes de ressources, qui sont à leur tour regroupés dans des abonnements. Si vous débutez dans Azure, cette structure peut suffire pour maintenir une organisation adéquate. Cependant, si vous gérez de nombreuses applications, équipes de développement et zones géographiques, vous pourriez avoir besoin d'un moyen plus efficace de gérer l'accès, les politiques et la conformité de vos abonnements. Les groupes

d'administration d'Azure fournissent une couche supérieure de gestion par rapport aux abonnements.

- **Groupe d'administration, abonnements et hiérarchie de groupes de ressources**

Vous pouvez organiser vos ressources dans une hiérarchie structurée en utilisant les groupes d'administration et les abonnements d'Azure pour une stratégie centralisée et un contrôle d'accès. Le schéma ci-dessous démontre comment établir une hiérarchie de gouvernance à l'aide de groupes d'administration.

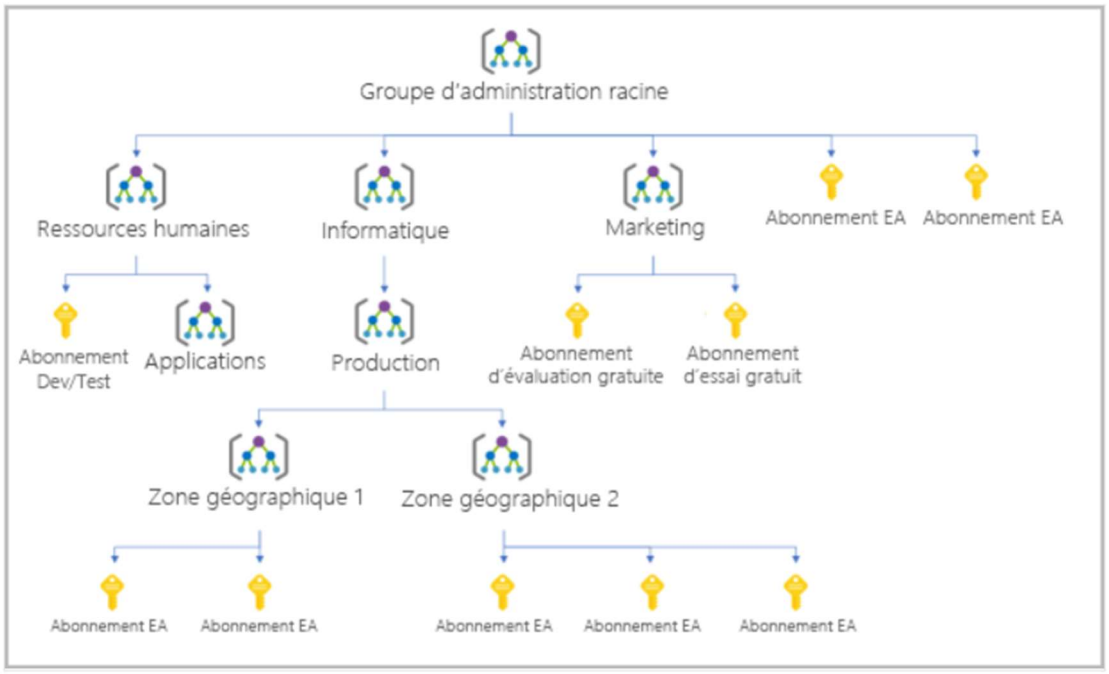


Figure 7: Hiérarchie des Groupes d'administration racine

Voici d'autres façons d'utiliser les groupes d'administration:

- ✓ Imposer une stratégie de sécurité sur l'ensemble de vos ressources en les classant dans un groupe d'administration spécifique. Par exemple, vous pouvez limiter l'emplacement des machines virtuelles au seul West US pour une catégorie nommée Production
- ✓ Fournir à vos utilisateurs un accès à plusieurs abonnements en regroupant ces derniers dans un seul groupe d'administration. En utilisant les autorisations basées sur le rôle (RBAC) sur ce groupe d'administration, vous pouvez facilement contrôler l'accès à toutes les ressources affiliées, sans avoir à créer un script Azure RBAC pour chaque abonnement individuel.

1.5.3.3 Les services de calcul et réseau Azure

- **Machines virtuelles Azure**

Vous pouvez utiliser les Machines virtuelles Azure pour exécuter des systèmes d'exploitation et des logiciels personnalisés dans le cloud sans avoir à vous soucier de l'achat et de la maintenance du matériel physique. Ce service d'infrastructure en tant que service (IaaS) vous offre une virtualisation flexible en vous permettant de personnaliser tout logiciel exécuté sur votre machine virtuelle, ainsi qu'une configuration d'hébergement personnalisée. Cependant, en tant qu'offre IaaS, vous êtes toujours responsable de la configuration, de la mise à jour et de la maintenance des logiciels sur la machine virtuelle.

- **Azure Virtual Desktop**

Avec Azure Virtual Desktop, vous pouvez bénéficier de l'utilisation de Windows 10 ou Windows 11 Enterprise multisession, une plateforme exclusive de Windows pour permettre à plusieurs utilisateurs de se connecter en simultané à une même machine virtuelle. De plus, Azure Virtual Desktop offre une expérience plus homogène en prenant en charge une plus grande variété d'applications par rapport aux systèmes d'exploitation Windows Server.

- **Azure Container Instances**

Réécriture: Azure Container Instances propose la façon la plus rapide et la plus facile d'exécuter un conteneur dans le cloud sans avoir à gérer les machines virtuelles ou adopter d'autres services. Il s'agit d'une plateforme en tant que service (PaaS). Avec Azure Container Instances, vous pouvez charger vos conteneurs et le service s'occupera de les exécuter pour vous.

- **Les comptes de stockage Azure**

Le Stockage Azure propose un espace de stockage unique pour vos données, accessible partout via HTTP/HTTPS. Ce compte offre une sécurité optimale, une haute disponibilité, une durabilité élevée et une scalabilité maximale. Pour le créer, vous devez choisir un type de compte qui déterminera les services de stockage et les options de redondance disponibles, affectant ainsi les différents usages. Parmi les options de redondance nous avons :

- ✓ Le Stockage localement redondant (LRS) : consiste à répliquer vos données à trois reprises dans le même centre de données, dans la région principale.

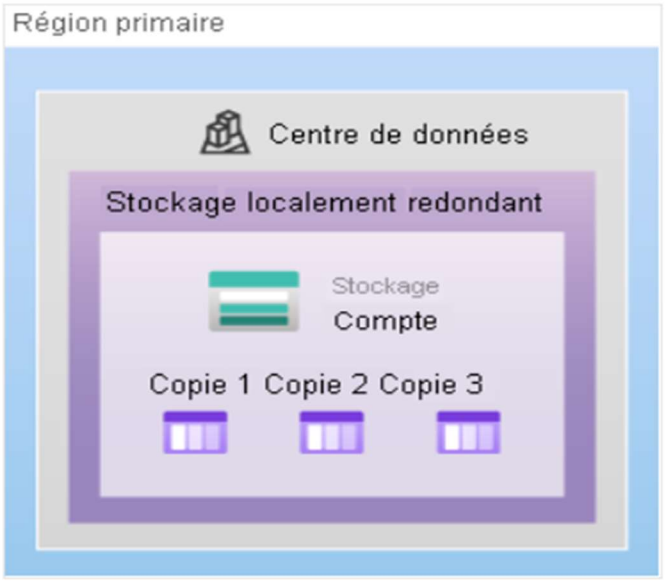


Figure 8: Stockage localement redondant

- ✓ **Stockage géoredondant (GRS)** : assure la duplication de vos données en trois exemplaires dans un même endroit physique à l'intérieur de la région principale avec LRS en temps réel. Elle effectue également la copie asynchrone de ces données vers un seul emplacement physique dans la région secondaire (paire de régions) avec LRS.

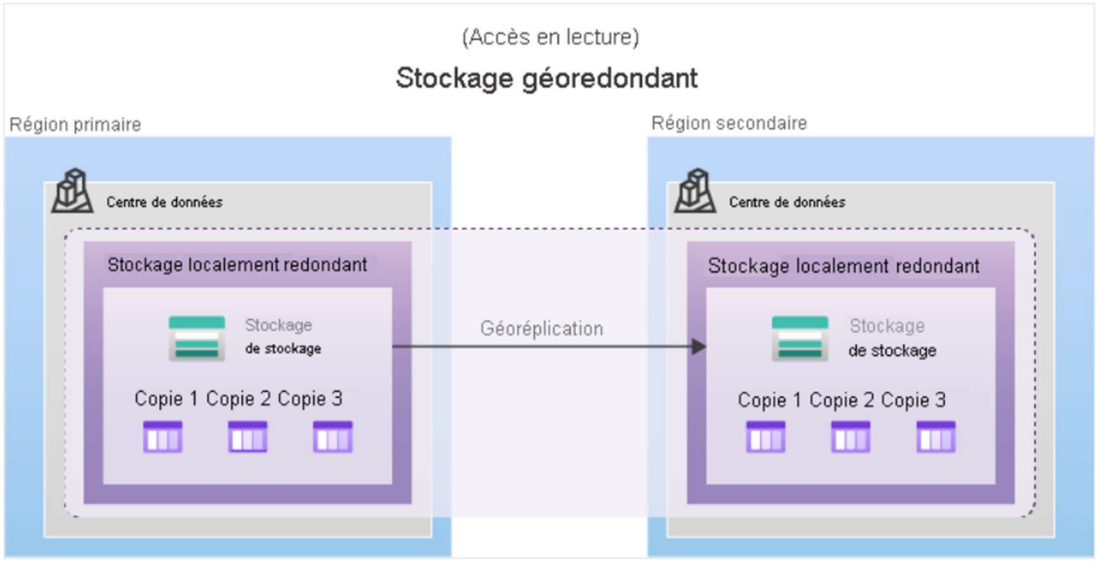


Figure 9: Stockage géoredondant (GRS)

- ✓ **Stockage redondant interzone (ZRS)** : Avec le stockage redondant interzone (ZRS), vos données Stockage Azure sont copiées de manière synchrone dans trois zones de disponibilité différentes, situées dans la même région, pour une meilleure disponibilité. Cette option est uniquement disponible pour les régions qui prennent en charge les zones de disponibilité.

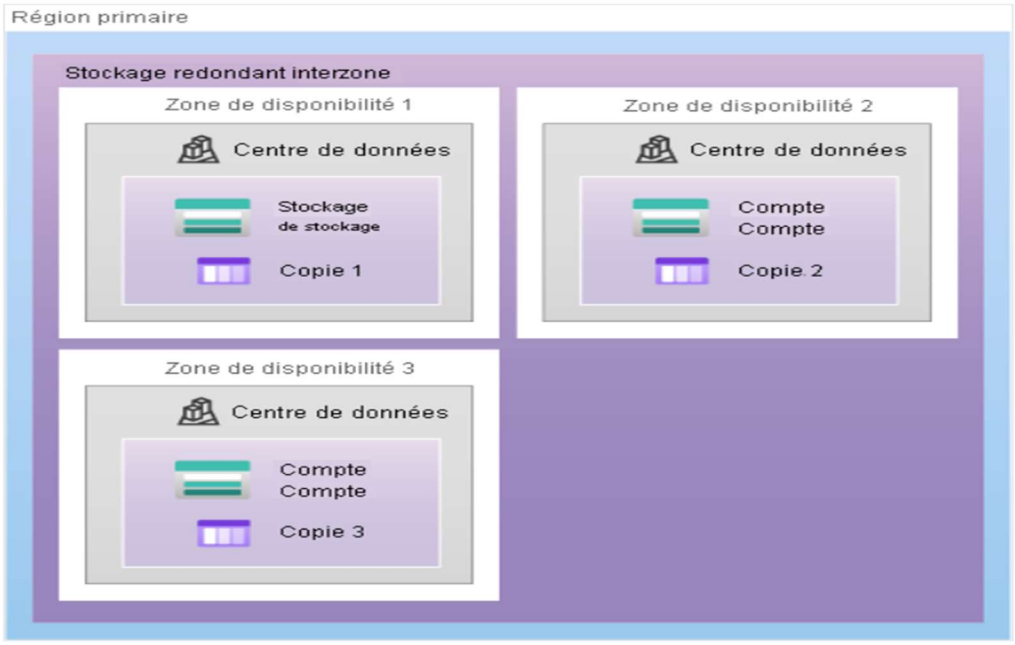


Figure 10: Stockage redondant interzone (ZRS)

- ✓ **Stockage géoredondant interzone (GZRS)** : Le stockage redondant interzone géo (GZRS) assure une protection maximale pour vos données dans le Stockage Azure en combinant la fiabilité des zones de disponibilité avec la protection géographique. Les données sont répliquées en trois zones de disponibilité au sein de la région principale, ainsi qu'une copie de secours vers une région géographique différente avec LRS. La réplication GZRS est fortement recommandée pour les applications nécessitant une disponibilité, une durabilité, une cohérence, une performance et une résilience accrues pour les situations d'urgence.

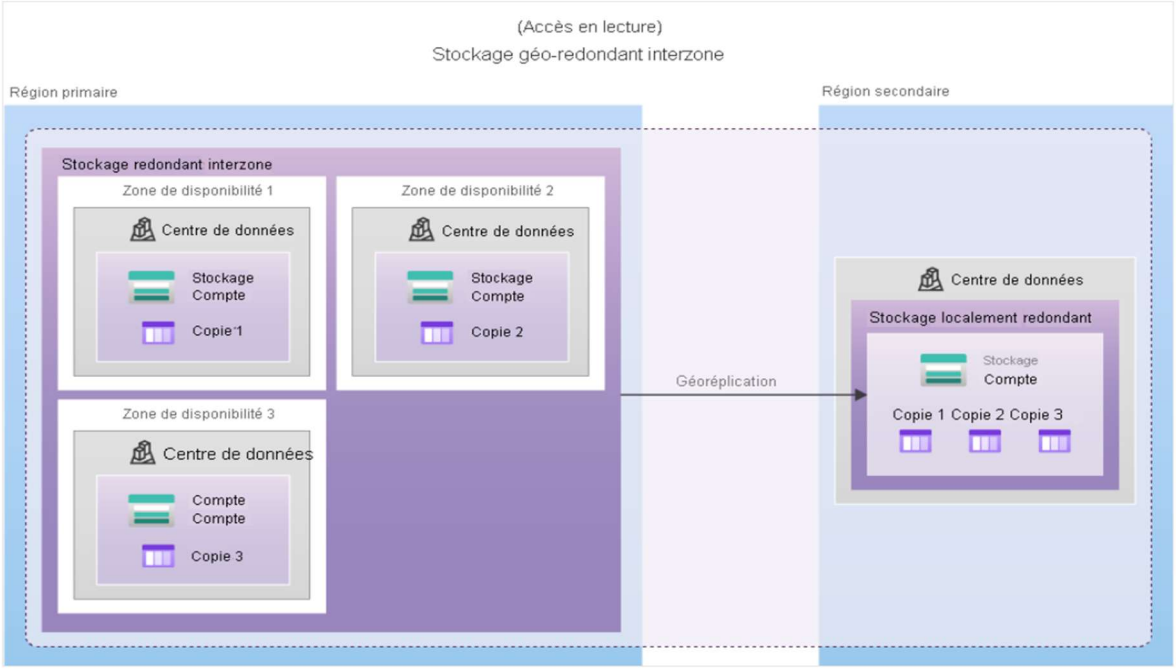


Figure 11: Stockage géoredondant interzone (GZRS)

Le tableau suivant explique les cas d'utilisations des comptes de stockage

Type	Services pris en charge	Options de redondance	Utilisation
Usage général v2 Standard	Stockage Blob (y compris Data Lake Stockage), Stockage File d'attente, Stockage Table et Azure Files	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Type de compte de stockage standard pour les objets blob, les partages de fichiers, les files d'attente et les tables. Recommandé pour la plupart des scénarios utilisant Stockage Azure. Si vous souhaitez prendre en charge le système de fichiers réseau (NFS) dans les fichiers Azure, utilisez le type de compte Partages de fichiers Premium.
Objets blob de blocs Premium	Stockage Blob (y compris Data Lake Storage)	LRS, ZRS	Type de compte de stockage Premium pour les objets blob de blocs et les objets blob d'ajout. Recommandé pour les scénarios à taux élevés de transactions, ceux utilisant des objets plus petits ou nécessitant une latence de stockage faible.
Partages de fichiers Premium	Azure Files	LRS, ZRS	Type de compte de stockage Premium pour les partages de fichiers uniquement. Recommandé pour l'entreprise ou des applications de mise à l'échelle hautes performances. Utilisez ce type de compte si vous voulez un compte de stockage qui prend en charge les partages de fichiers SMB et NFS.
Objets blob de pages Premium	Objets blob de pages uniquement	LRS	Type de compte de stockage Premium pour les objets blob de pages uniquement.

Figure 12: Cas d'utilisation des comptes de stockage

CHAPITRE 2 : *Les risques de sécurité majeurs du cloud et les solutions associées*

Alors que les entreprises continuent de se tourner vers le cloud pour stocker leurs données et accéder à des services, les menaces liées à ces nouvelles technologies ne cessent d'augmenter.

Le paysage de la cybersécurité est en perpétuelle évolution, et il est impératif de se tenir au courant des nouvelles techniques et surfaces d'attaque.

Dans ce chapitre nous allons identifier les risques de sécurité majeurs du cloud ainsi que les solutions proposées par Microsoft azure pour faire face à celle-ci.

2.1 Les risques de sécurité majeurs du cloud computing

2.1.1 Les Attaques DDoS

Les attaques DDoS visent à interrompre les machines ou services et à empêcher les utilisateurs d'accéder à leurs données ou applications. En obligeant un service cloud à utiliser des ressources excédentaires telles que le traitement, la mémoire, le stockage ou la bande passante, les pirates peuvent ralentir les systèmes utilisateurs légitimes ou même les bloquer. Ces attaques sont effectuées à l'aide de réseaux d'équipements connectés à Internet qui ont été infectés par un logiciel malveillant. Ceux-ci sont contrôlés à distance par le pirate et appelés des "bots" formant un "botnet". Le pirate peut alors diriger une attaque en envoyant des instructions à chaque bot. Lorsqu'une cible est attaquée par le botnet, chaque bot envoie des requêtes à l'adresse IP de la cible, causant une saturation du serveur ou du réseau et donc un déni de service du trafic normal. Il peut être difficile de séparer le trafic d'attaque du trafic normal en raison de la nature légitime de chaque bot. Dans le cloud, le coût pour le client peut être plus élevé que ce qu'ils consomment réellement.

2.1.2 Les vulnérabilités par des technologies partagées

Les fournisseurs de services Cloud utilisent une infrastructure physique, une plateforme ou une application partagée pour leur service évolutif. Cependant, cette méthode peut présenter des faiblesses s'ils ne peuvent pas garantir l'isolation des composants de l'infrastructure pour une utilisation multiple par différents clients.

2.1.3 Une action malveillante

Une personne peu scrupuleuse au sein de l'équipe de gestion de centre de données peut facilement causer des dommages à la confidentialité et à l'intégrité des environnements hébergés, en agissant de manière malveillante à l'intérieur du personnel du fournisseur.

2.1.4 Les Attaques de Session Hijacking :

Lorsqu'un système est cible d'une attaque de détournement de session, un individu malveillant prend le contrôle d'une session active entre un client de confiance et un serveur cloud. En utilisant des techniques telles que l'IP Spoofing ou le DNS Spoofing, l'attaquant peut faire croire au serveur cloud qu'il est en communication avec le client de confiance, alors qu'en réalité, c'est l'attaquant qui a accès aux informations sensibles. Cette forme d'accès non autorisé peut mettre en danger la confidentialité et l'intégrité du système.

2.1.5 Les attaques SQL injection :

La technique d'injection SQL consiste à introduire des instructions malveillantes dans une base de données via un champ de saisie. Cela peut permettre au pirate de récupérer ou de modifier des données, de se faire passer pour un utilisateur privilégié, de manipuler des transactions, et même de détruire toutes les données du serveur. En utilisant des commandes SQL spéciales, un attaquant peut accéder aux données sensibles et compromettre la confidentialité et l'intégrité de la base de données.

2.1.6 L'isolation:

Le Cloud Computing permet le partage de ressources et peut potentiellement entraîner des attaques à travers les canaux auxiliaires ou cachés entre les différentes machines virtuelles présentes dans le même environnement. Le manque d'isolement peut se produire lorsqu'une machine virtuelle d'un attaquant se trouve sur la même machine physique que celle d'un utilisateur, ce qui peut permettre à l'attaquant de mettre en place des attaques matérielles ou logicielles pour surveiller ou perturber d'autres machines virtuelles.

2.1.7 Vulnérabilités des services

Les réseaux cloud sont exposés à une menace fréquente de compromission par des services vulnérables. Pour limiter ces risques, il est impératif de tenir les systèmes à jour. La menace principale provient des actions post-compromission telles que la migration des attaques vers les principaux systèmes et ressources d'entreprise hébergés dans le cloud. Les entreprises doivent être en mesure de répondre rapidement et efficacement aux incidents. Malheureusement, beaucoup de scanners de vulnérabilités utilisés pour détecter ces faiblesses sont inefficaces, car les vulnérabilités peuvent être exploitées une semaine avant leur découverte. L'exemple d'Apache Log4J, une vulnérabilité mondialement connue, montre la gravité des conséquences d'une telle menace. Il est donc crucial pour les entreprises de détecter les activités malveillantes avant qu'un service ne soit identifié comme vulnérable.

2.1.8 Gestion de l’identité et accès médiocre

Les cybercriminels qui réussissent à se faire passer pour des utilisateurs authentiques, tels que des opérateurs ou des développeurs d'applications, peuvent accéder, altérer et supprimer des données, voler des informations ou espionner, et introduire des applications ou du code malveillant qui semblent provenir d'un utilisateur légitime. Une mauvaise gestion de l'identité, des clés ou des informations d'identification peut causer de graves conséquences pour l'infrastructure cloud.

2.1.9 Mauvaises configurations du cloud

La source la plus fréquente de fuites de données dans le cloud sont les erreurs de configuration. Les entreprises laissent souvent accidentellement les données de leurs clients accessibles au public, rendant ainsi les informations vulnérables aux cybercriminels. Cependant, ce n'est pas un problème exclusif au cloud, mais plutôt lié à la complexité croissante des configurations dans le cloud. De plus, une attention insuffisante aux configurations ne prévient pas seulement les fuites de données. Il a également été constaté que les hôtes du cloud peuvent être infectés par des logiciels malveillants ou des accès supplémentaires au réseau dus à des modifications système opérées par des attaquants. Par exemple, le groupe de hackers TeamTNT a accédé à des Docker Daemon non sécurisés pour installer et exécuter ses propres images malveillantes, contaminant les victimes via un botnet ou par minage de crypto-monnaie. Il est donc important de noter que les erreurs de configuration peuvent non seulement compromettre les services cloud, mais également fournir une opportunité facile pour les cybercriminels compétents.

2.1.10 Attaques sur la chaîne logistique

Les attaques sur la chaîne d'approvisionnement se multiplient. Certaines sont facilement identifiables, comme l'attaque Solarwinds attribuée à une APT russe, mais il en existe d'autres qui se cachent dans les réseaux et les services cloud. Une méthode d'attaque croissante consiste à compromettre les images sur Docker Hub. TeamTNT, mentionné précédemment, a compromis et continue de compromettre les images Docker Hub, ce qui peut entraîner une compromission pour toute personne qui installe et met à jour ces images. Leurs buts incluent la mise en place d'un botnet générique et le minage. Les administrateurs de Docker doivent être prudents en intégrant de nouvelles images et en installant des logiciels externes sur leur réseau.

2.1.11 Accès à la plateforme de gestion du cloud

La menace qui pèse sur les plateformes de gestion de cloud est de plus en plus préoccupante, avec des attaquants qui visent à accéder aux comptes cloud privilégiés. Cet accès peut donner aux cybercriminels une entrée dans des systèmes sensibles et les informations confidentielles. Les outils open source tels que Purple Panda facilitent l'escalade de privilèges pour les attaquants qui ont obtenu des informations d'identification volées. Les clés peuvent être trouvées dans des référentiels de code et d'images en ligne, ouvrant la voie à des attaques sur la chaîne d'approvisionnement et des vols de données en masse. Des groupes très compétents et bien financiers, comme APT29, ciblent également ces accès pour des missions commanditées par les gouvernements. Il est donc impératif de rester vigilant, car ce type d'accès est particulièrement recherché par les criminels informatiques. Les vulnérabilités des applications, des logiciels libres et des technologies dans le cloud sont de plus en plus ciblées en raison de la complexité et de la taille des réseaux cloud. Les méthodes utilisées par les attaquants peuvent varier, mais elles s'appuient généralement sur les défis posés par la gestion des réseaux cloud vastes et complexes.

2.2 Mécanismes de défense proposés par Microsoft Azure

Les risques que nous venons de voir montre l'importance de sécuriser notre environnement cloud afin de profiter de façon sur aux atouts qu'offrent celui-ci. Il existe plusieurs solutions dans Azure permettant de gérer les aspects suivant :

- Authentification et Autorisation
- Identité et gestion des accès
- Confidentialité, intégrité et disponibilité
- Surveillance de la sécurité et réponse aux incidents
- Gestion de la politique de sécurité
- Le chiffrement des données

Nous allons voir les outils de sécurité qui interviennent dans chaque partie

2.2.1 Authentification et Autorisation :

Le processus d'authentification implique de déterminer l'identité d'un utilisateur, d'un service ou d'un dispositif en obtenant des informations d'identification qui prouvent leur identité. Azure propose diverses méthodes d'authentification, y compris les mots de passe traditionnels, l'authentification unique (SSO), l'authentification multifacteur (MFA) et l'authentification sans mots de passe. Autrefois, sécurité et commodité semblaient incompatibles, mais de nouvelles solutions d'authentification proposent un équilibre entre les deux. La sécurité et la commodité peuvent être visualisées selon un spectre, avec l'authentification sans mots de passe en haut du spectre, offrant une haute sécurité et commodité, tandis que les mots de passe seuls en bas du spectre, proposant une faible sécurité mais une grande commodité.

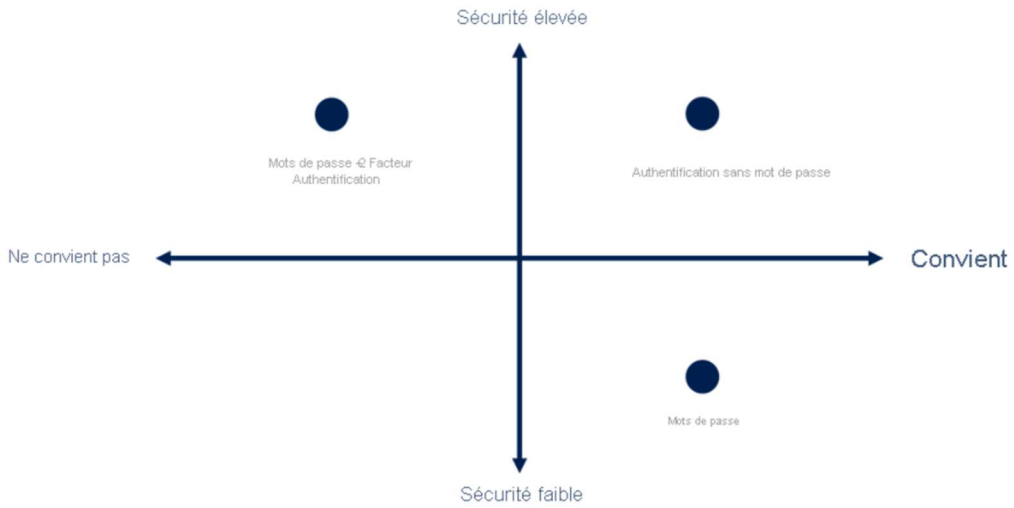


Figure 13: Sécurité et Commodité des méthodes d'authentifications

2.2.1.1 L'authentification unique (SSO)

Le SSO est une méthode qui permet à un utilisateur de s'authentifier une seule fois pour accéder à plusieurs ressources et applications différentes. Pour que cela fonctionne, les applications et les fournisseurs doivent accepter l'authentificateur initial. Avec le SSO, vous n'aurez besoin de retenir qu'un seul identifiant et mot de passe. L'accès à plusieurs

applications est accordé en fonction d'une seule identité liée à l'utilisateur, ce qui simplifie la gestion de la sécurité. Lorsqu'un utilisateur change de rôle ou quitte l'entreprise, l'accès est associé à cette identité unique, ce qui réduit considérablement les efforts pour modifier ou désactiver les comptes. Le SSO facilite la gestion des identités pour les utilisateurs et la gestion des utilisateurs pour l'administration informatique.

2.2.1.2 L'authentification multifacteur

Le processus de l'authentification multifacteur implique l'obtention d'un second facteur d'identification pendant la procédure de connexion. Ce système renforce la sécurité en cas de compromission d'un mot de passe car un autre élément est requis pour s'authentifier. Les facteurs supplémentaires peuvent être une information connue de l'utilisateur, un objet en sa possession ou une propriété biométrique. L'authentification à un seul facteur ne nécessite que l'ID et le mot de passe de l'utilisateur. En comparaison, l'authentification multifacteur apporte une protection supplémentaire. Il est recommandé d'activer cette fonctionnalité chaque fois que possible. Par exemple, Azure AD Multi-Factor Authentication est un service de Microsoft qui propose des fonctions d'authentification multifacteur et permet aux utilisateurs de choisir leur méthode supplémentaire, telles qu'un appel téléphonique ou une notification sur leur application mobile.

2.2.1.3 L'authentification sans mot de passe

La sécurité est cruciale pour les organisations, et l'authentification à plusieurs facteurs (MFA) est une mesure efficace. Cependant, elle peut être source d'irritation pour les utilisateurs qui doivent se souvenir de leurs mots de passe, ajoutant une couche supplémentaire de complexité. C'est pourquoi les méthodes d'authentification sans mot de passe sont préférables : elles sont plus simples et plus pratiques. Elles ne nécessitent plus de mots de passe, mais combinent autre chose que vous avez, êtes ou savez.

Pour utiliser l'authentification sans mot de passe, vous devez configurer l'appareil. Par exemple, votre ordinateur peut être considéré comme quelque chose que vous avez. Une fois enregistré auprès d'Azure, il sera associé à votre identité. Ensuite, en fournissant une information supplémentaire que vous connaissez ou êtes (comme un code secret ou une empreinte digitale), vous pourrez vous connecter sans mots de passe

Azure et Azure Government offrent plusieurs options pour l'authentification sans mots de passe qui peuvent être intégrées à Azure Active Directory : Windows Hello Enterprise, Microsoft Authenticator et les clés de sécurité FIDO2.

2.2.1.4 Azure Active Directory (AD) :

Azure AD est un service de gestion d'identités qui peut être utilisé pour gérer les autorisations et les rôles d'utilisateur dans votre application. Si vous avez déjà un environnement local exécutant Active Directory, vous pouvez le connecter à Azure AD pour une expérience d'identité cohérente entre le cloud et l'environnement local en utilisant Azure AD Connect.

2.2.1.5 Une identité externe

Les identités externes Azure AD désignent les moyens de collaborer en toute sécurité avec des personnes en dehors de votre organisation. Ces identités peuvent correspondre à l'authentification unique et permettent aux utilisateurs externes d'utiliser leurs propres informations d'identité pour se connecter. Azure AD ou Azure AD B2C gère l'accès à vos applications tandis que le fournisseur d'identité de l'utilisateur externe gère son identité.

Les identités externes comprennent la collaboration B2B, la connexion directe B2B, et Azure AD B2C. La collaboration B2B représente les utilisateurs externes en tant qu'utilisateurs invités dans votre annuaire. La connexion directe B2B permet une collaboration transparente avec une autre organisation Azure AD. Avec Azure AD B2C, vous pouvez publier des applications aux consommateurs tout en gérant les identités et les accès via Azure AD B2C.

En fonction de vos besoins de collaboration avec les organisations externes et les ressources à partager, vous pouvez utiliser une combinaison de ces fonctionnalités.

2.2.1.6 Azure AD Domain Services :

Azure Active Directory Domain Services est un service qui vous donne la possibilité d'installer un domaine Active Directory dans le cloud d'Azure et de vous servir des protocoles d'authentification standard, tels que LDAP et Kerberos, pour accéder à vos applications et à vos informations.

2.2.2 Identité et gestion d’accès

Il existe de nombreuses options disponibles dans Azure pour contrôler l'identité et l’accès dans votre application

2.2.2.1 L’accès conditionnel

L'accès conditionnel est un mécanisme utilisé par Azure Active Directory pour déterminer si un utilisateur peut ou non accéder à des ressources en se basant sur des critères tels que son identité, sa localisation et l'appareil utilisé. Pour les administrateurs informatiques, cela signifie une productivité accrue pour les utilisateurs, qui peuvent travailler n'importe où et n'importe quand, ainsi qu'une protection accrue pour les ressources de l'entreprise. Lors de la connexion, l'accès conditionnel collecte des informations sur l'utilisateur et décide s'il peut accéder aux ressources sans fournir un deuxième facteur d'authentification, ou s'il doit en fournir un en cas de signaux inhabituels ou d'une localisation inattendue.

Le diagramme suivant illustre ce flux :

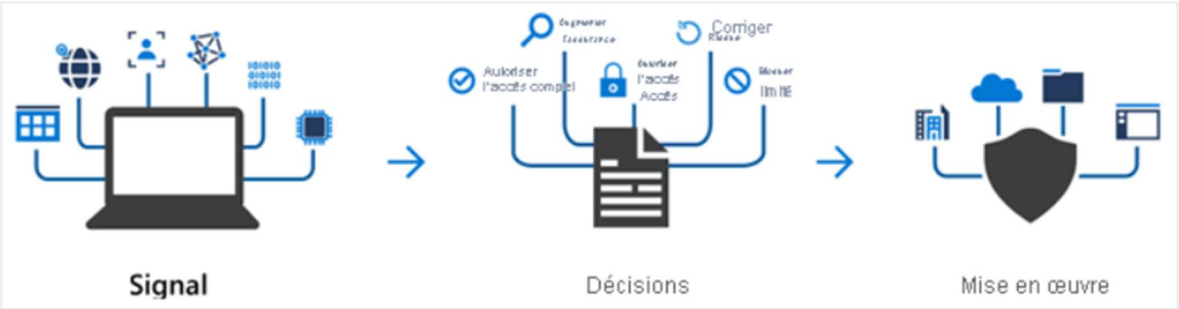


Figure 14: L'accès Conditionnelle

Le système détermine l'accès en utilisant des indicateurs tels que l'emplacement de l'utilisateur, le périphérique ou l'application qu'ils cherchent à accéder. En fonction de ces indicateurs, l'accès peut être autorisé sans restriction si l'utilisateur se connecte à partir de leur emplacement habituel. Cependant, si la connexion est établie à partir d'un emplacement non familier ou considéré comme à haut risque, l'accès peut être entièrement bloqué ou nécessiter une authentification supplémentaire pour être autorisé.

2.2.2.2 Le contrôle d'accès en fonction du rôle Azure RBAC

Pour contrôler l'accès des équipes informatiques et ingénieurs aux ressources dans votre environnement cloud, vous pouvez utiliser le principe du privilège minimum qui implique de n'accorder un accès que si cela est nécessaire pour accomplir une tâche. Azure propose des contrôles d'accès en fonction du rôle (RBAC Azure) pour gérer les autorisations d'accès. Il existe des rôles intégrés dans Azure avec des autorisations d'accès prédéfinies et vous pouvez également définir vos propres rôles. En attribuant un ou plusieurs rôles à des personnes ou des groupes, ils obtiendront les autorisations d'accès associées. Par exemple, en ajoutant un nouvel ingénieur au groupe RBAC Azure des ingénieurs, il obtiendra automatiquement les mêmes autorisations que les autres ingénieurs dans ce groupe. Les autorisations de ce groupe s'étendent aux nouvelles ressources ainsi qu'à celles existantes. Le contrôle d'accès en fonction du rôle s'applique à une étendue spécifique, telle qu'une ressource ou un ensemble de ressources.

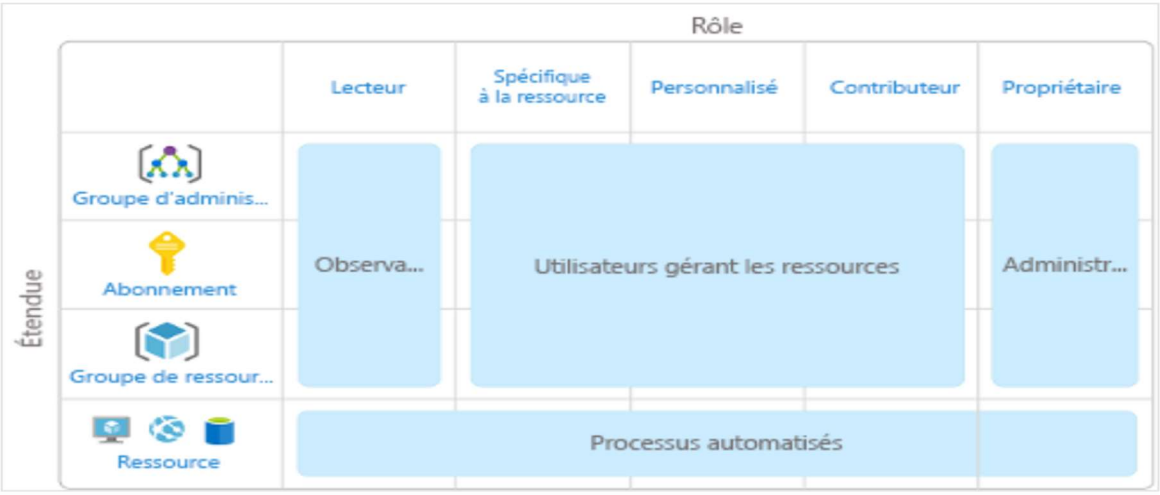


Figure 15: Le contrôle d'accès en fonction du rôle

2.2.3 Confidentialité, Intégrité, et disponibilité

Azure offre plusieurs options pour protéger la confidentialité, assurer l'intégrité et maintenir la disponibilité de vos informations et de vos Applications. Voici quelques exemples :

2.2.3.1 Le modèle Confiance Zéro

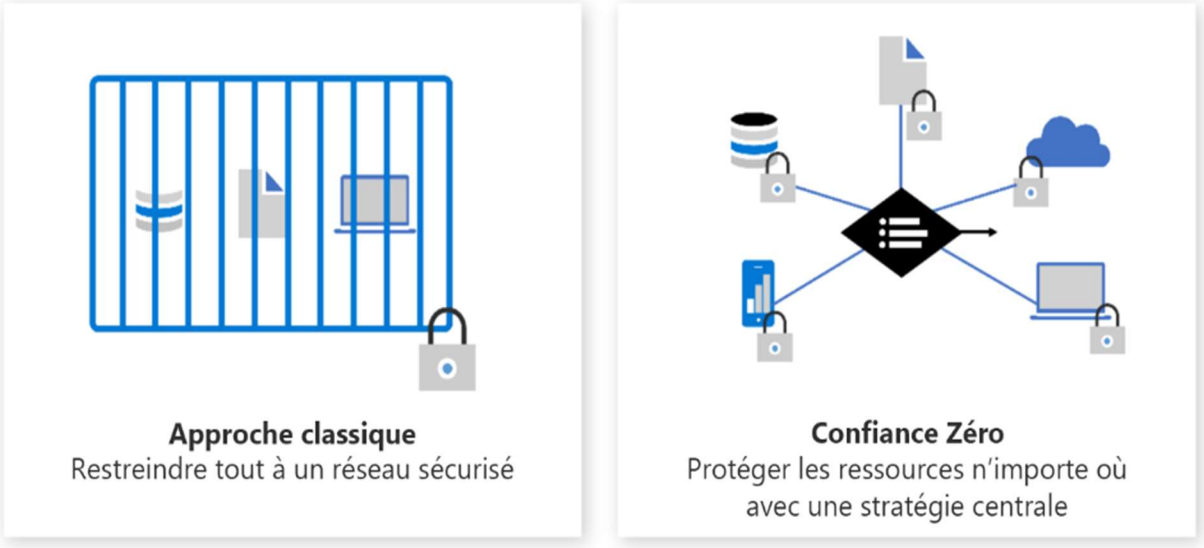


Figure 16: Le modèle Confiance Zéro

Le modèle de sécurité traditionnel pour les réseaux d'entreprise consistait à restreindre l'accès en se basant sur l'appartenance à un réseau géré. Cependant, avec l'augmentation de la mobilité du personnel et la complexité de l'environnement informatique, un nouveau modèle de sécurité est nécessaire. C'est pourquoi Microsoft recommande le modèle de sécurité "Confiance Zéro". Ce modèle se base sur l'authentification systématique et l'autorisation en fonction des données disponibles, l'accès avec le minimum de privilèges nécessaires, et la préparation pour les violations de sécurité en utilisant la segmentation de l'accès, le chiffrement de bout en bout, et l'analytique pour la visibilité et la détection des menaces.

2.2.3.2 Azure Backup :

Avec le service Sauvegarde Azure, vous pouvez protéger vos données critiques en les sauvegardant et en les restaurant en cas de perte ou de corruption de données. Il garantit la sécurité de vos données de sauvegarde, en mettant en place des mesures de sécurité préventives pour lutter contre les attaques de rançongiciel, et en fournissant des outils pour protéger votre entreprise contre les menaces informatiques. La sécurité de vos données est assurée tant lors de leur transfert que lorsqu'elles sont stockées.

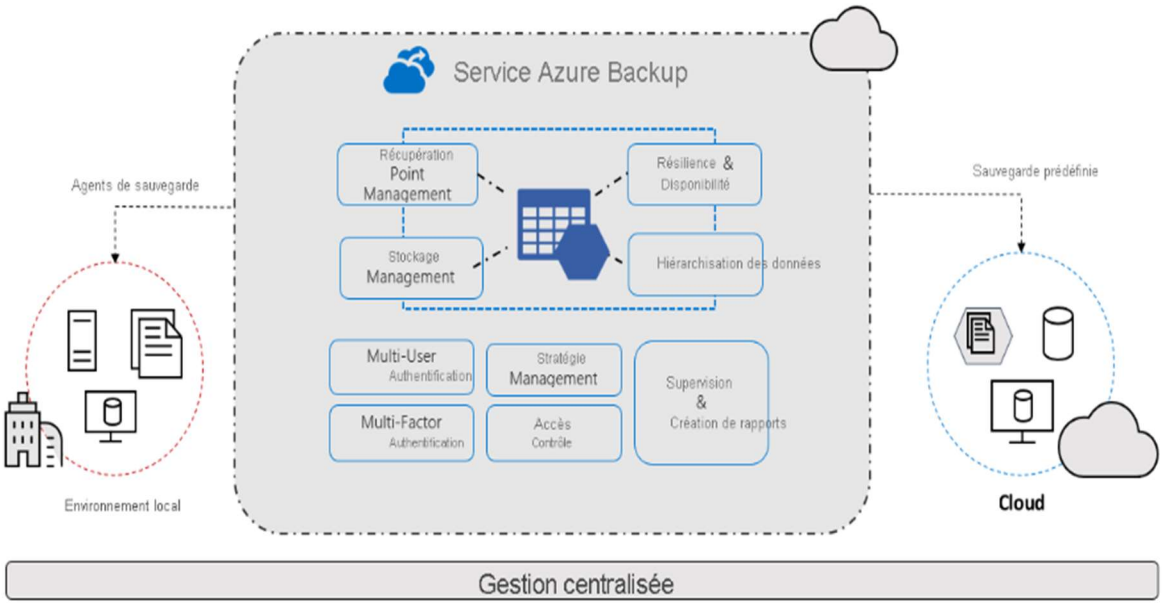


Figure 17: Azure Backup

La Sauvegarde Azure offre maintenant des fonctionnalités de sécurité pour protéger les sauvegardes hybrides. Voici les fonctionnalités :

- Prévention : Une vérification supplémentaire de l'authentification est ajoutée lors de toute opération critique (par exemple, Modifier la phrase secrète). Cela garantit que seuls les utilisateurs avec des informations d'identification Azure valides peuvent effectuer ces opérations.
- Alertes : Un email d'alerte est envoyé à l'administrateur de l'abonnement chaque fois qu'une opération critique (par exemple, Supprimer les données de sauvegarde) est effectuée. Cet email assure une notification rapide à l'utilisateur de ces actions.
- Récupération : Les données de sauvegarde supprimées sont conservées pendant 14 jours de plus après la date de suppression. Cela garantit la possibilité de les récupérer dans un délai donné pour éviter toute perte, même en cas d'attaque. De plus, un plus grand nombre de points de récupération minimum sont conservés pour offrir une protection contre les données corrompues.

2.2.3.3 Azure Disaster Recovery :

Le service de Récupération d'urgence vous offre la possibilité de planifier et de gérer la récupération de vos applications et de vos données en cas de sinistre.

2.2.4 Surveillance de la sécurité et de réponse aux incidents

Voici quelques exemples de solutions Azure qui peuvent vous aider à surveiller la sécurité et à répondre aux incidents de sécurité :

2.2.4.1 Defender pour le cloud

Defender pour le cloud est un outil de sécurité qui surveille vos environnements cloud, locaux, hybrides et multiclouds pour vous aider à renforcer votre posture de sécurité. Le service intégré à Azure surveille de nombreux services sans avoir besoin d'être déployé. Cependant, si vous avez des centres de données locaux ou travaillez avec d'autres environnements cloud, un agent Log Analytics peut être déployé pour collecter des informations sur la sécurité. Les machines Azure sont gérées directement, tandis que les environnements hybrides et multiclouds sont couverts grâce à Azure Arc et à l'étendue des plans Microsoft Defender. Les fonctionnalités CSPM sont également disponibles pour les machines multiclouds sans l'utilisation d'un agent.

Defender pour le cloud s'adresse aux trois principales préoccupations liées à la gestion de la sécurité de vos ressources et de vos charges de travail en nuage et sur site:



Figure 18: Les trois exigences de Defender pour le cloud

Lorsque Defender pour le Cloud détecte une menace, il génère une alerte de sécurité qui décrit les ressources affectées, suggère des mesures correctives et peut déclencher une application logique en réponse. Les alertes peuvent être reçues de produits de sécurité intégrés et exportées. La protection contre les menaces comprend une analyse de la chaîne de frappe de fusion qui corrèle les alertes pour une compréhension complète de la campagne d'attaque, d'où elle a débuté et de son impact sur les ressources.

2.2.4.2 Microsoft Defender pour Identity

Defender pour Identity est une solution de sécurité en nuage qui utilise les informations de votre annuaire Active Directory local pour repérer, détecter et enquêter sur les menaces avancées, les identités compromises et les actions malveillantes d'utilisateurs internes dirigées contre votre entreprise. Cet outil aide les analystes de sécurité et les professionnels de la sécurité à surveiller les activités et comportements des utilisateurs grâce à une analyse basée sur l'apprentissage, à protéger les identités et informations d'identification stockées dans Active Directory, à identifier et examiner les activités suspectes des utilisateurs et les attaques avancées tout au long de la chaîne d'attaque, et à fournir des informations claires sur les incidents dans une chronologie simple pour un triage rapide.

2.2.4.3 Azure Sentinel :

Azure Sentinel est un service de sécurité avancé qui vous permet de surveiller les activités de votre entreprise et de réagir rapidement en cas d'incident de sécurité. Il offre les fonctions suivantes :

- Gestion des informations et des événements de sécurité (SIEM)
- Automatisation et orchestration de la réponse à la sécurité (SOAR)

Avec Azure Sentinel, vous bénéficiez d'une vue d'ensemble de votre entreprise, ce qui vous permet de faire face aux menaces de plus en plus complexes, aux volumes croissants d'alertes et aux délais de résolution prolongés. Il est basé sur les pratiques de protection contre les falsifications et l'immuabilité d'Azure Monitor. Bien que Azure Monitor ne soit qu'une plateforme de données complémentaires, il comporte des dispositions pour la suppression de données en vue de la conformité.

Azure Sentinel collecte des données à grande échelle sur tous les utilisateurs, appareils, applications et infrastructures, tant sur site qu'en multicloud. Il utilise l'analytique et les systèmes d'intelligence sur les menaces fournis par Microsoft pour détecter les menaces non détectées et réduire les faux positifs. L'intelligence artificielle et les années de travail consacrées à la cybersécurité par Microsoft permettent d'investiguer les menaces et de rechercher des activités suspectes à grande échelle. Enfin, les tâches courantes peuvent être automatisées et orchestrées pour une réponse rapide aux incidents.

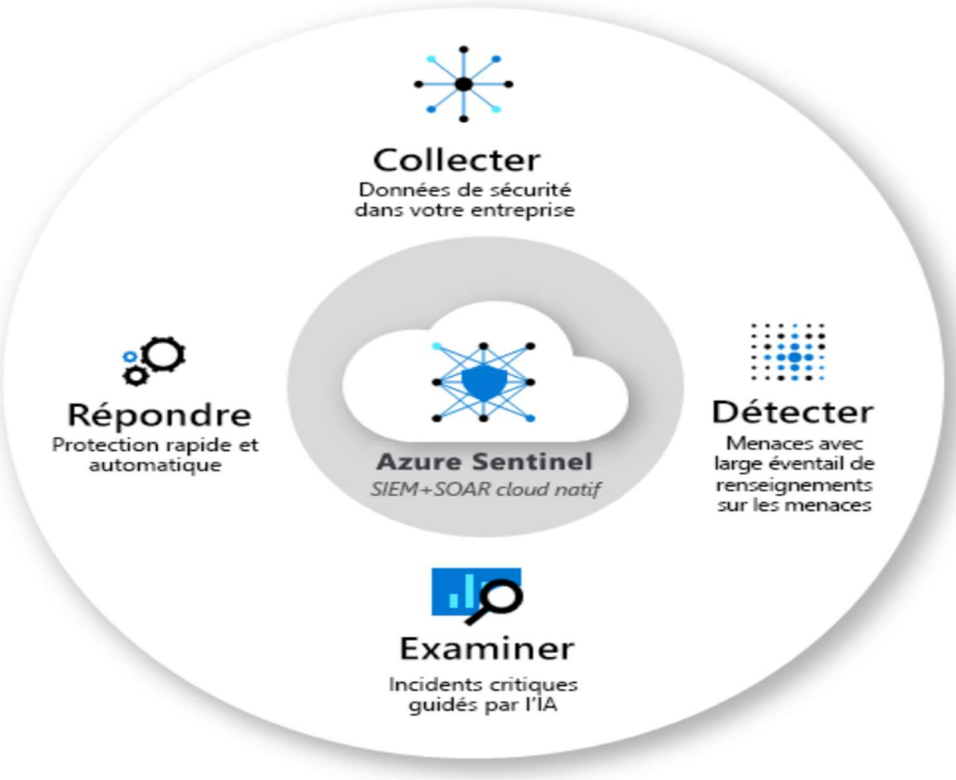


Figure 19: Fonctionnement de Microsoft Sentinel

2.2.4.4 Azure Monitor

Azure Monitor est une plateforme de surveillance qui recueille des données sur vos ressources, les analyse et vous fournit une visualisation claire des informations. Il peut surveiller les ressources Azure, les ressources locales et même les ressources multicloud telles que les machines virtuelles hébergées avec un autre fournisseur. Il offre une vue complète de vos ressources en un seul endroit.

Voici un diagramme qui montre la complétude d'Azure Monitor

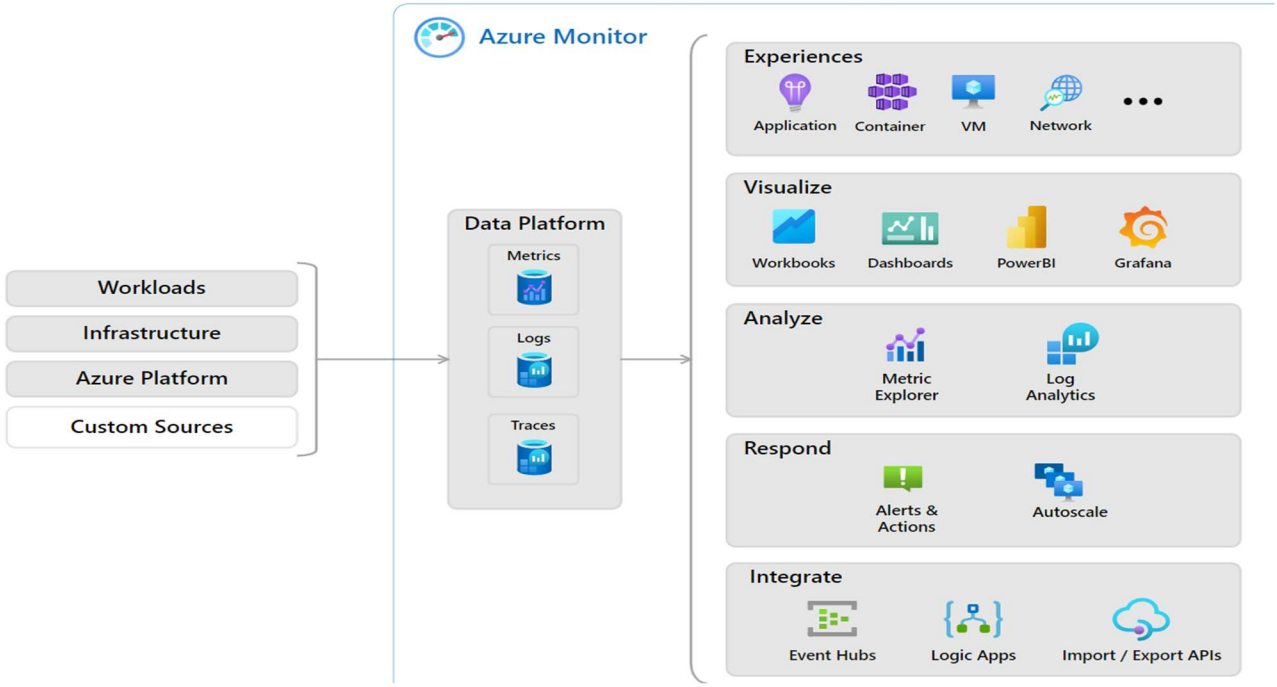


Figure 20: l'exhaustivité d'Azure Monitor

- La collecte de données de journalisation et de métriques peut se faire à différents niveaux de l'architecture d'applications, allant de l'application au système d'exploitation et au réseau. Cela est représenté à gauche dans la liste des sources de données disponibles pour la collecte.
- Au centre, les informations de journalisation et de métriques sont conservées dans des dépôts de données centralisées.
- Les données collectées peuvent être utilisées de plusieurs façons. Les performances en temps réel et historiques de chaque couche de l'architecture peuvent être affichées, ainsi que des informations agrégées et détaillées. Les données sont présentées à différents niveaux pour différents groupes de personnes, à partir de rapports généraux affichés sur le tableau de bord Azure Monitor à des vues personnalisées créées à l'aide de requêtes Power BI et Kusto.

Il est également possible de se servir des données pour réagir immédiatement à des situations critiques, en envoyant des alertes aux équipes par SMS, e-mail, etc. De plus, il est possible de fixer des limites pour déclencher la fonction d'ajustement automatique de la capacité en réponse à la demande.

2.2.4.5 Azure Log Analytics

Le portail Azure offre un outil appelé Azure Log Analytics pour écrire et effectuer des analyses sur les données collectées par Azure Monitor. Cet outil puissant supporte les requêtes simples ou complexes et facilite l'analyse de données. Vous pouvez utiliser des requêtes simples pour afficher un jeu de données, puis les trier, les filtrer et les analyser. Des requêtes plus complexes peuvent être utilisées pour effectuer une analyse statistique avec des résultats affichés sous forme de graphique pour identifier les tendances. Que ce soit pour une utilisation interactive ou en combinaison avec d'autres fonctionnalités d'Azure Monitor telles que les alertes de requête de journal ou les feuilles de calcul, Log Analytics est l'outil que vous utiliserez pour écrire et tester ces requêtes.

2.2.5 Gestion politique de sécurité

Voici quelques exemples de solutions Azure qui peuvent nous aider à gérer notre politique de sécurité :

2.2.5.1 Azure Policy :

Azure Policy est un outil de conformité qui vous aide à établir des normes pour votre organisation en définissant des règles pour vos ressources Azure. Il peut être utilisé pour gérer la sécurité, la conformité réglementaire, la gestion des coûts et la cohérence des ressources. Azure Policy propose des définitions de stratégie prédéfinies pour vous faciliter le démarrage. Les actions de gouvernance incluent la restriction de déploiement de ressources à certaines régions, l'utilisation cohérente de tags, et la collecte de journaux de diagnostic avec Log Analytics.

2.2.5.2 Azure AD Identity Governance :

Azure AD Identity Governance est un service de contrôle d'accès qui vous permet de surveiller et de restreindre l'accès aux ressources de votre organisation. Il vous aide à établir des règles de sécurité pour les utilisateurs afin de s'assurer qu'ils n'ont accès qu'aux ressources nécessaires.

Ce service permet aux organisations de gérer les identités et les accès pour les employés, les partenaires et les fournisseurs à travers divers services et applications en local et dans le cloud. Il couvre les aspects de gestion de vie des identités et des accès, de sécurité de l'accès privilégié pour l'administration.

En particulier, ce service s'efforce de répondre aux questions suivantes :

- Qui doit avoir accès à quelles ressources ?
- Comment les utilisateurs utilisent-ils cet accès ?
- Y a-t-il des contrôles organisationnels pour gérer l'accès ?
- Peuvent-ils être vérifiés par les auditeurs ?

2.2.6 Chiffrement

Voici quelques exemples de solutions Azure qui peuvent nous aider à chiffrer nos données :

2.2.6.1 Azure Key Vault :

Le service de gestion de clés et de secrets Azure Key Vault vous offre un moyen sécurisé de stocker et de gérer vos clés de chiffrement. Il permet également de chiffrer vos données sensibles lors de leur stockage ou transmission. Azure Key Vault aide à résoudre des problèmes liés à la gestion de secrets, de clés de chiffrement et de certificats. Il peut stocker en toute sécurité des jetons, mots de passe, certificats, clés API et autres secrets, tout en contrôlant étroitement leur accès. Il facilite également la création et la gestion de clés de chiffrement pour chiffrer vos données. Azure Key Vault est disponible en deux niveaux de service :

- Standard, qui utilise une clé logicielle pour le chiffrement, et
- Premium, qui inclut des clés protégées par des modules de sécurité matériels (HSM).

2.2.6.2 Azure Disk Encryptions

Afin de satisfaire aux obligations de sécurité et de conformité de votre entreprise, ADE veille à la protection et à la conservation de vos données. Il utilise les fonctionnalités DM-Crypt de Linux ou BitLocker de Windows pour chiffrer les disques de système d'exploitation et de données de vos machines virtuelles Azure. ADE est intégré à Azure Key Vault pour faciliter la gestion sécurisée des clés et des secrets de chiffrement associés à ces disques.

2.2.6.3 Le chiffrement côté serveur du Stockage sur disque Azure

Le chiffrement de données en repos sur le Stockage Azure se charge automatiquement de chiffrer les informations stockées sur les disques gérés d'Azure (disques système et de données) qui persistent dans les clusters de stockage. En étant configuré avec un ensemble de chiffrement de disques (DES), il offre également la possibilité de gérer les clés par le client.

2.2.6.4 Le chiffrement sur l'hôte

Le chiffrement de l'hôte assure la protection de vos données lorsqu'elles sont stockées sur le serveur hôte de votre machine virtuelle, ainsi que pendant leur transit vers les clusters de stockage. Les données seront chiffrées au repos et lors de leur circulation.

2.2.6.5 Le chiffrement de disque confidentiel

Le chiffrement confidentiel de disque relie les clés de chiffrement du disque à la plateforme sécurisée (TPM) de la machine virtuelle, permettant uniquement à cette machine virtuelle d'accéder au contenu du disque protégé. Le code attesté chiffre l'état invité de la machine virtuelle et du TPM à l'aide de clés publiées par un protocole de sécurité qui contourne l'hyperviseur et le système d'exploitation hôte. Ce type de chiffrement est actuellement disponible uniquement pour le disque système d'exploitation, mais le chiffrement sur l'hôte peut également être utilisé pour d'autres disques sur une machine virtuelle confidentielle en plus du chiffrement de disque confidentiel.

CHAPITRE 3 : *Implémentation d'un SIEM sur Azure*

Dans ce chapitre nous allons mettre en place une preuve de concept de détection et de réponse aux menaces basée sur Microsoft Sentinel.

Nous allons donc en premier lieu mettre en place l'environnement qui regroupe Microsoft Sentinel et deux outils pour la collecte de données à savoir Azure Monitor (Log Analytic) et Microsoft Defender for Cloud. Dans un deuxième temps nous allons effectuer quelque attaque pour voir comment les solutions Microsoft collabore entre eux pour détecter celles-ci.

3.1 Mise en place de l'environnement :

La mise en place du lab sera subdiviser en trois parties

3.1.1 Déploiement azure Monitor

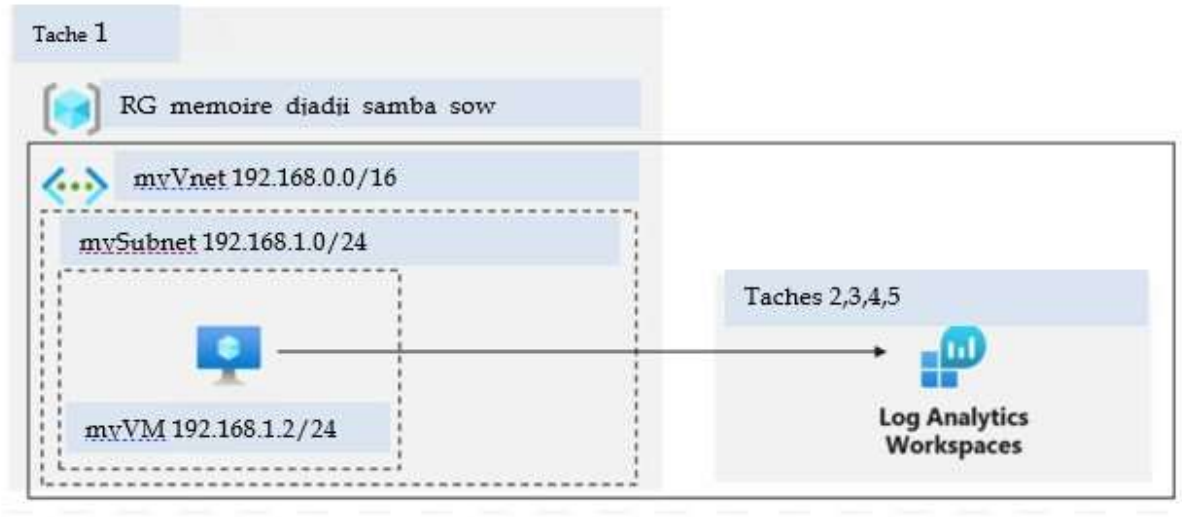


Figure 21: Déploiement Azure Monitor (Log Analytics Workspaces

Avec Azure Monitor, nous allons créer une preuve de concept de surveillance des performances de la machine virtuelle. Pour cela nous devons atteindre les objectifs suivants :

- ✓ Configurer une machine virtuelle de sorte que la télémétrie et les journaux puissent être collectés.
- ✓ Afficher les données de télémétrie et les journaux qui peuvent être collectés.
- ✓ Montrer comment les données peuvent être utilisées et interrogées.

3.1.1.1 Tâche 1 : Déployer une machine virtuelle Azure

Avant de pouvoir déployer des ressources sur azure il faut un compte doté du rôle Propriétaire ou Contributeur dans l'abonnement Azure. Dans notre environnement nous avons utilisé un compte azure pour étudient.

- Pour déployer une machine virtuelle azure nous devons nous Connecter au portail Azure https://portal.azure.com/. Comme illustrer par la figure suivante

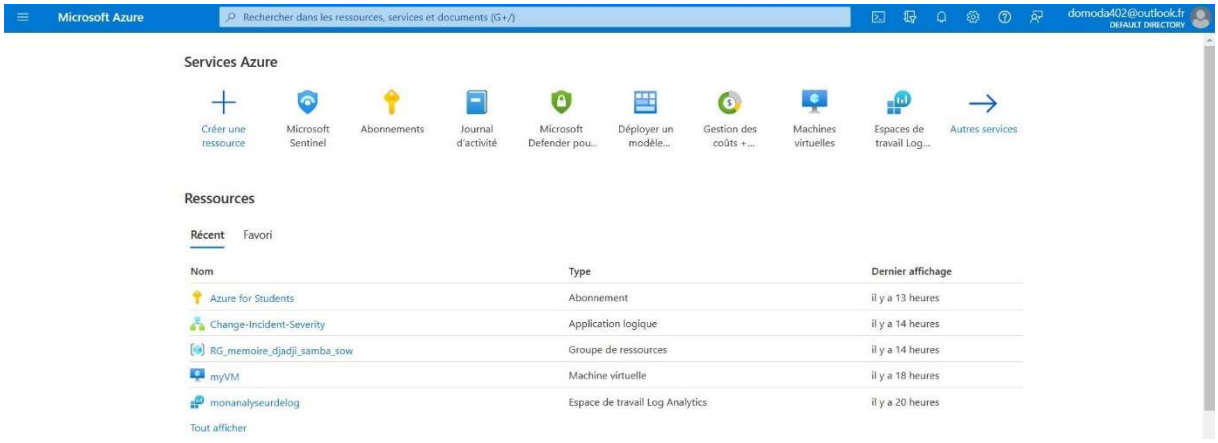


Figure 22: Portail Azure

Une fois sur cette interface nous avons plusieurs façons de créer une machine virtuelle : soit via une interface graphique, soit en utilisant Azure CLI (PowerShell).

- Nous ouvrons le Cloud Shell en cliquant sur la première icône en haut à droite du portail Azure. Une fenêtre va s'ouvrir nous invitant à sélectionner PowerShell et Créer un stockage.
- Dans la session PowerShell du volet Cloud Shell, nous exécutons la commande suivante pour créer un groupe de ressources qui va contenir notre ressource (machine virtuelle) portant le nom RG_memoire_djadji_samba_sow :

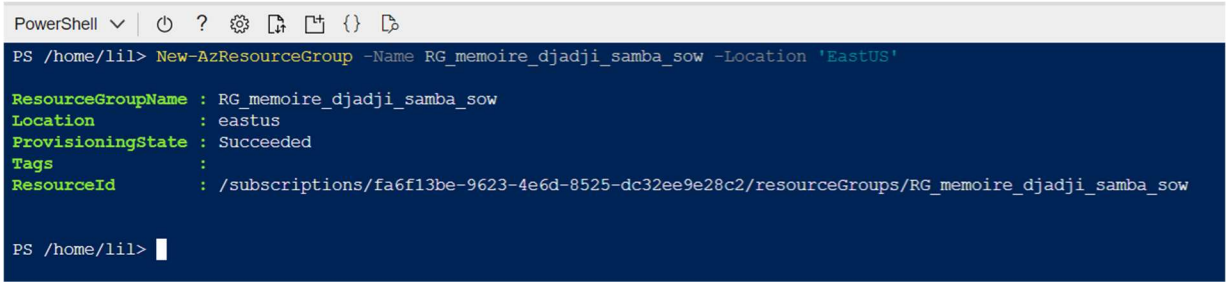


Figure 23: Création d'un Groupe de ressource avec PowerShell

- Toujours dans le même Cloud Shell, exécutons ce qui suit pour créer une machine virtuelle Azure.

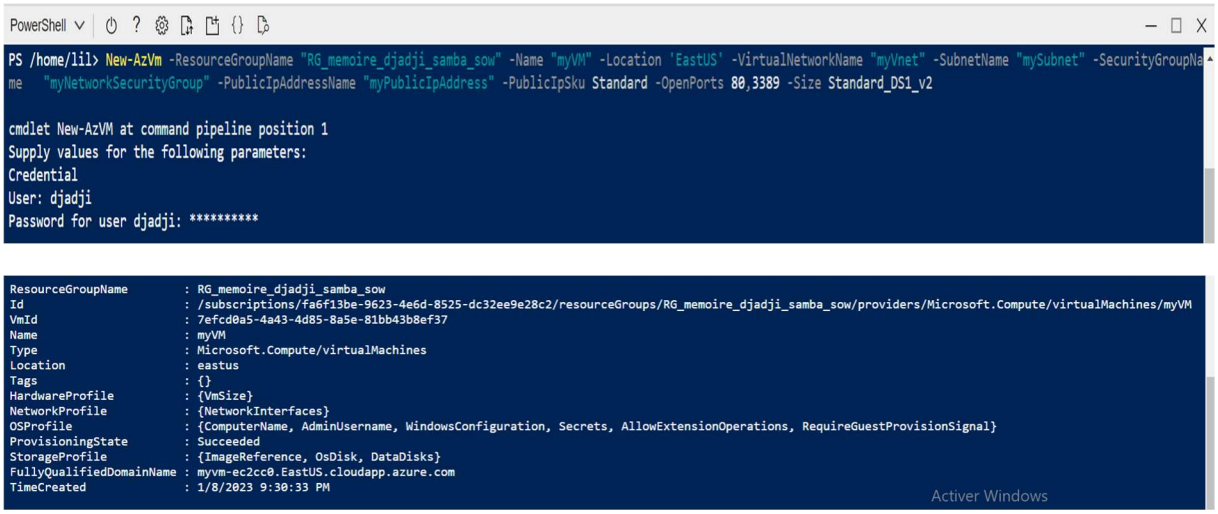


Figure 24: Création d'une machine virtuelle avec PowerShell

- Vérifions que la machine virtuelle nommée **myVM** a été créée et que son **ProvisioningState** est **Succeeded**.

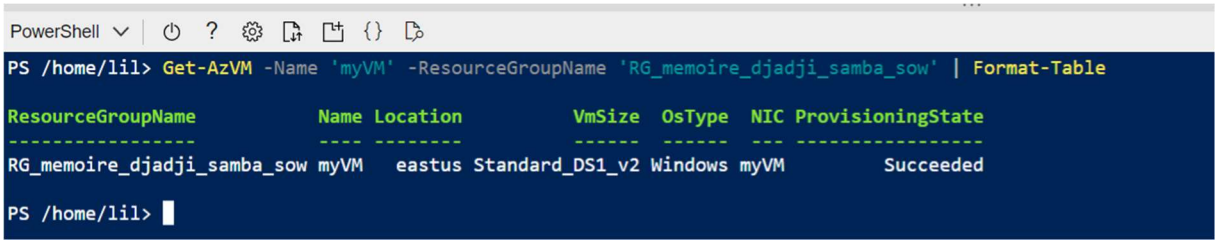


Figure 25: Vérification du provisionnement des ressources

3.1.1.2 Tâche 2 : Créer un espace de travail Log Analytics

Dans cette tâche, nous allons créer un espace de travail Log Analytics.

- Dans le portail Azure, dans la zone de texte Rechercher des ressources, des services et des documents en haut de la page du portail Azure, cherchons Espaces de travail Log Analytics

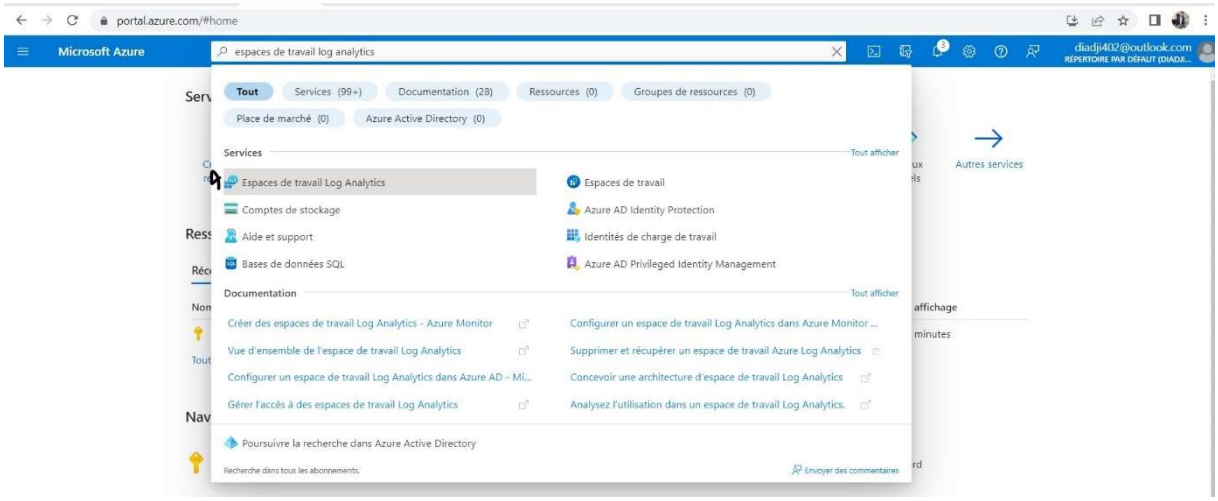


Figure 26: recherche de log Analytics sur le portail azure

- Dans le panneau Espaces de travail Log Analytics, cliquons sur le bouton + Créer.

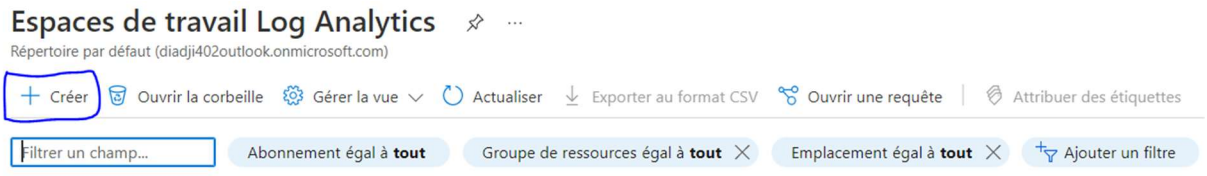


Figure 27: création d'un espace de travail Log Analytics

- Nous spécifions les paramètres suivants : l'abonnement, le groupe de ressources, le nom de l'espace de travail ainsi que la région ou la ressource est déployer. Puis sur vérifier + créer

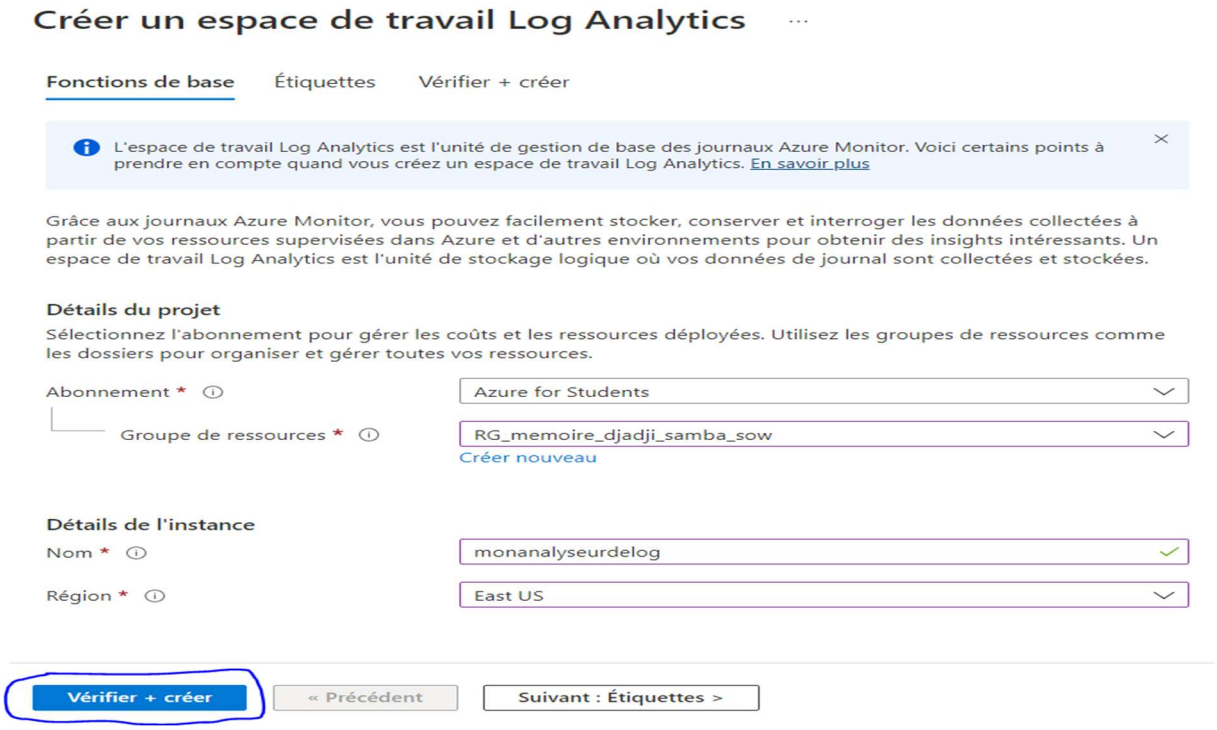


Figure 28: configuration des fonctions de base de log Analytics

Une fois la création effectuer nous devons activer l'extension de machine virtuelle Log Analytic

3.1.1.3 Tâche 3 : Activer l'extension de machine virtuelle Log Analytics

Dans cette tâche, nous allons activer l'extension de machine virtuelle Log Analytics. Cette extension installe l'agent Log Analytics sur les machines virtuelles Windows et Linux. Cet agent collecte les données de la machine virtuelle et les transfère vers l'espace de travail Log Analytics que nous désignons. Une fois l'agent installé, il sera automatiquement mis à niveau, ce qui nous permettra de toujours disposer des dernières fonctionnalités et correctifs.

- Dans le panneau Espace de travail Log Analytics, dans la page Vue d'ensemble, dans la section Connecter une source de données, on choisit l'entrée Machines virtuelles Azure puis on sélectionne la machine **myVM** que nous avons déployée dans la première tâche et notons qu'elle est répertoriée ici comme **Non connectée**. Il faudra veiller à ce que la machine soit en cours d'exécution pour que l'agent soit correctement installé.

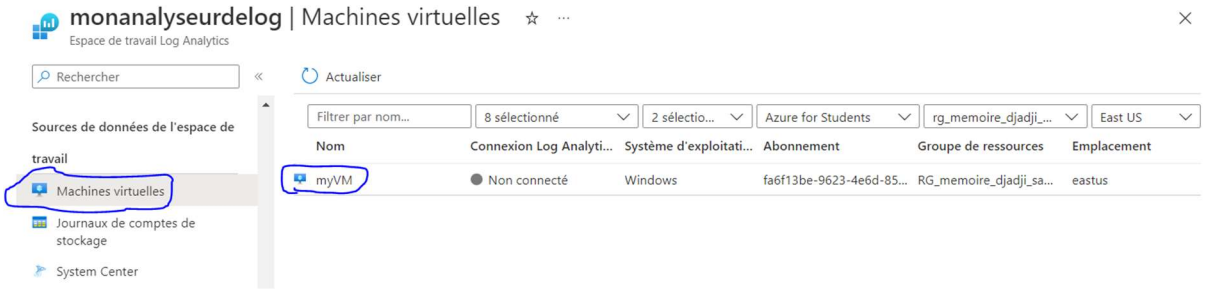


Figure 29: Activer l'extension de machine virtuelle Log Analytics

- Maintenant reste plus qu'à connecter la machine en cliquant sur se connecter

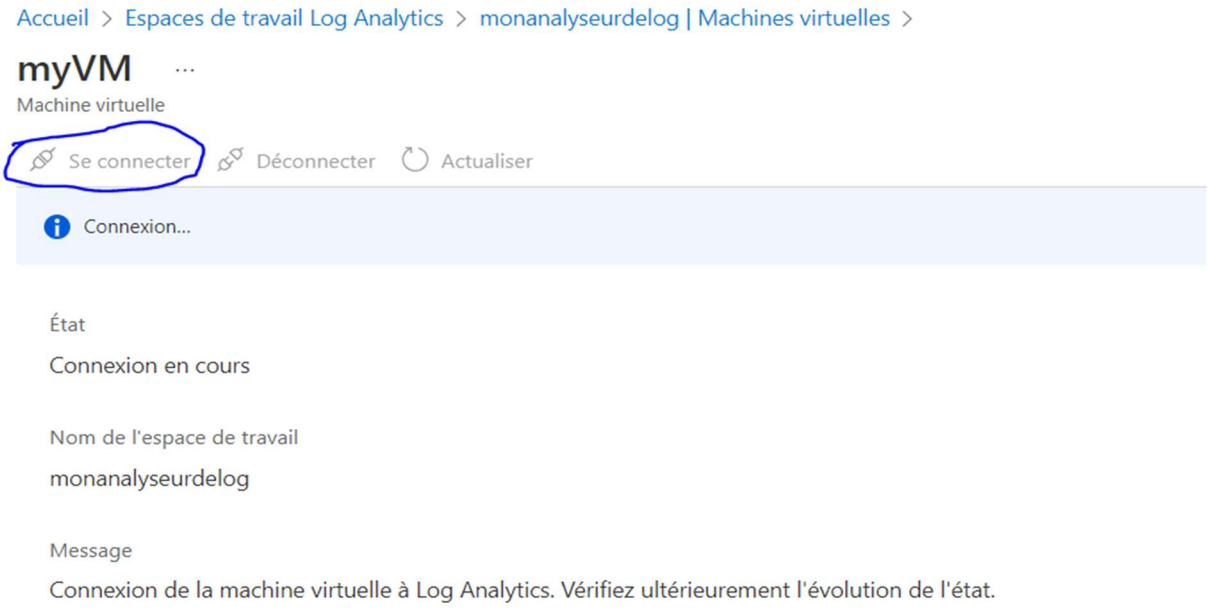


Figure 30: connecter la machine virtuelle à log Analytics

- Attendons que la machine virtuelle se connecte à l'espace de travail Log Analytics. Cela peut prendre quelques minutes. L'état affiché dans le panneau myVM passe de Connexion à **cet espace de travail** comme illustrer ci-dessous.

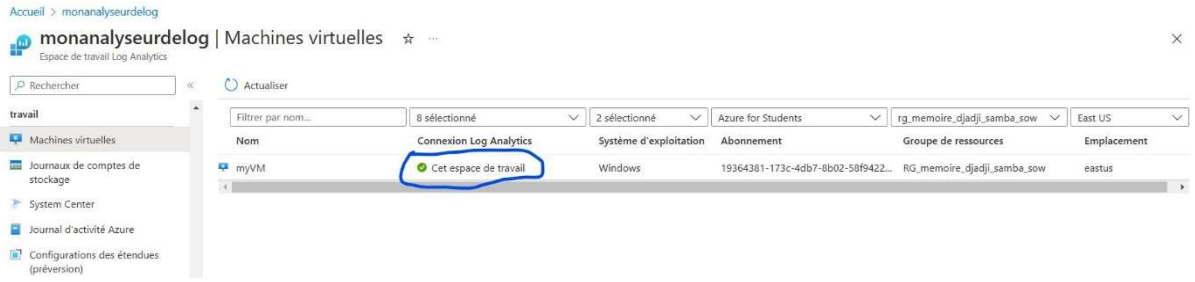


Figure 31: vérification de l'état de la connexion du VM à Log Analytics

3.1.1.4 Tâche 4 : Collecter des données d'événement et de performances de machine virtuelle

Dans cette tâche, nous allons configurer la collection du journal système Windows et plusieurs compteurs de performance courants. Nous examinerons également d'autres sources disponibles.

- Toujours dans l'espace de travail Log Analytics, dans la section Paramètres, nous cliquons sur Gestion des agents hérités. Dans le panneau Configuration des agents, passons en revue les paramètres configurables, notamment les journaux des événements Windows, les compteurs de performance Windows, les compteurs de performance Linux, les journaux IIS et Syslog. Sur l'option Journaux des événements Windows, nous cliquons sur + Ajouter le journal des événements Windows, dans la liste des types de journaux des événements, nous sélectionnons Système.il faudra aussi décocher la case Informations en laissant les cases à cocher Erreur et Avertissement activées. C'est ainsi qu'on ajoute des journaux d'événements à l'espace de travail. D'autres choix incluent, par exemple, les événements matériels ou le service de gestion de clés.

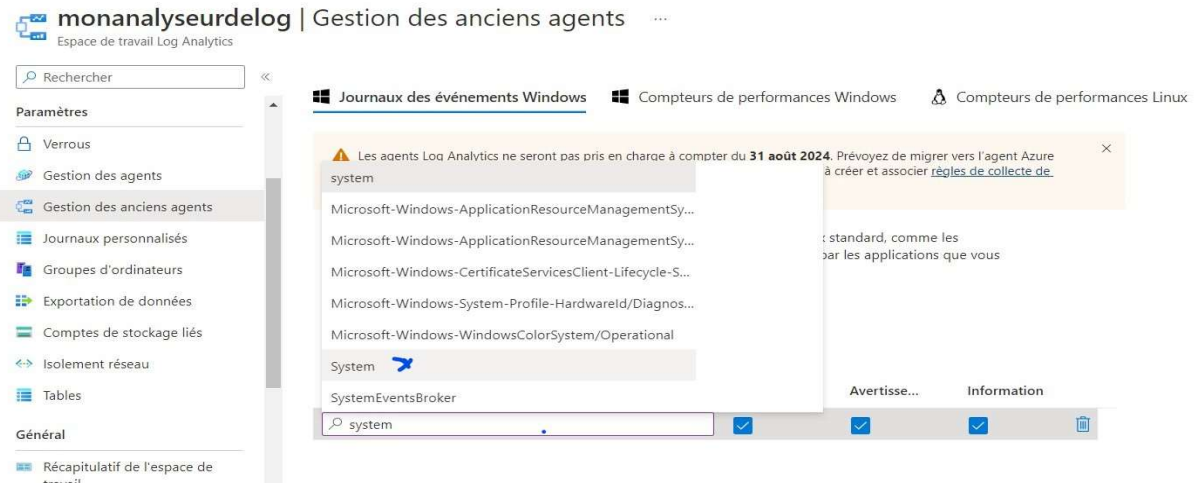


Figure 32: configuration d'un collecteur d'évènement Windows liées aux systèmes

- Sur l'option Compteurs de performance Windows, nous cliquons sur + Ajouter un compteur de performance, et nous ajoutons les compteurs suivants avec un intervalle d'échantillonnage de collecte de 60 secondes :

- ✓ Mémoire (*)\Mo de mémoire disponible
- ✓ Processus (*)\ % Temps processeur
- ✓ Suivi des événements pour Windows\Utilisation totale de la mémoire --- pool non paginé
- ✓ Suivi des événements pour Windows\Utilisation totale de la mémoire --- pool paginé

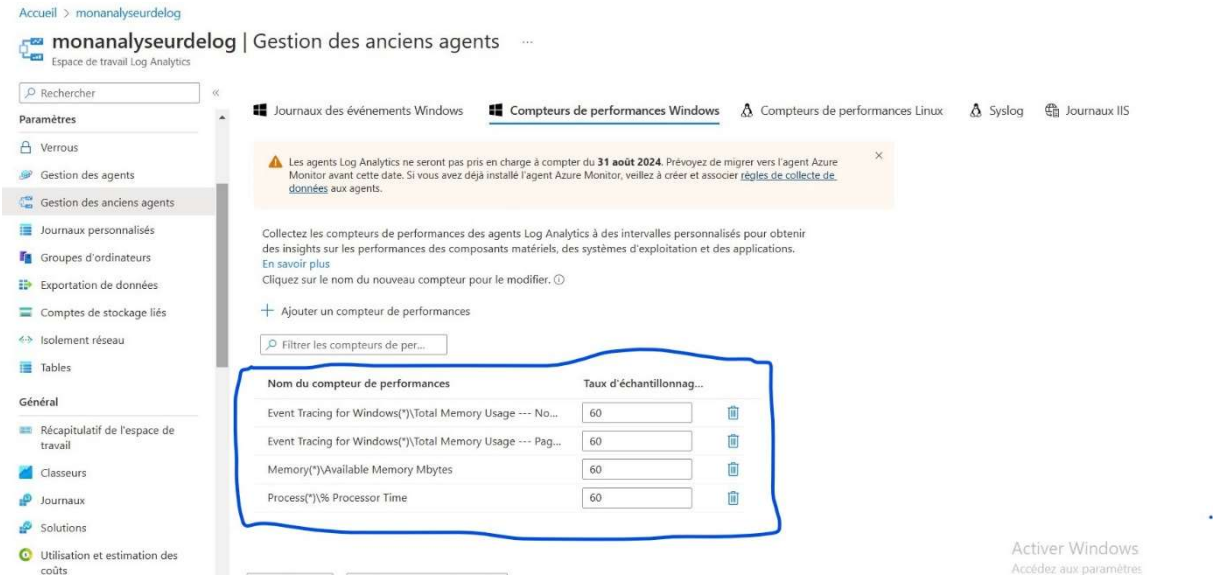


Figure 33: configuration de quelques compteurs de performances Windows

3.1.1.5 Tâche 5 : Afficher et interroger les données collectées

Dans cette tâche, nous allons exécuter une recherche dans les journaux de notre collecte de données.

- Dans l'espace de travail Log Analytics, dans la section Général, cliquez sur Journaux. Si nécessaire, dans le volet Requêtes, dans la colonne Toutes les requêtes, nous choisissons parmi les requêtes prédéfinit pour afficher les données concernant Utilisation de la mémoire et du processeur.

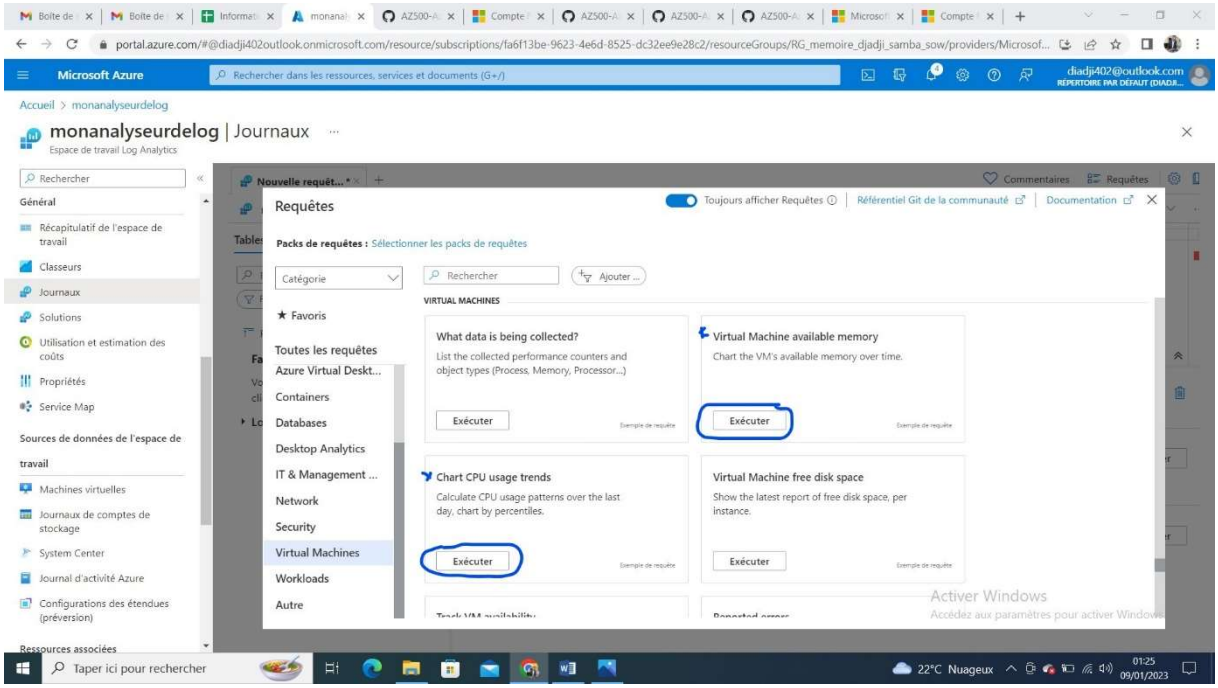


Figure 34: requetés pour l'interrogation des données

La requête s'ouvrira automatiquement dans un nouvel onglet de requête montrant le résultat obtenu. A noter que Log Analytics utilise le langage de requête Kusto. Nous pouvons personnaliser les requêtes existantes ou créer les nôtres. Nous avons également la possibilité d'afficher les données dans différents formats et créer une règle d'alerte basée sur les résultats de la requête. Étant donné que cette machine virtuelle vient d'être créée, il y a peu de données qui s'affichent sur le graphique.

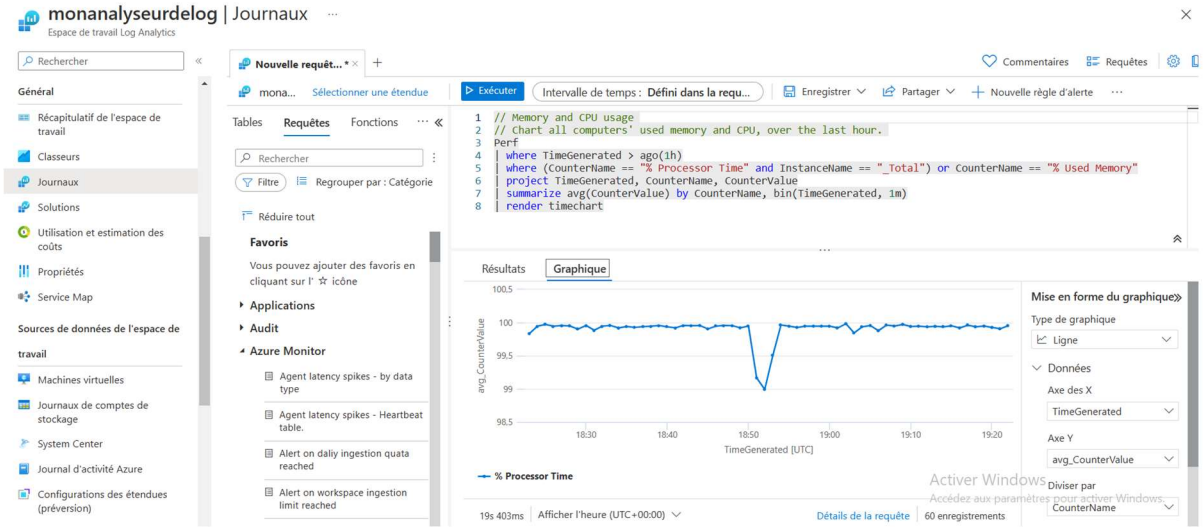


Figure 35: Résultat des requêtes sur le CPU et la Mémoire

Ce qui termine la mise en place d'Azure Monitor

3.1.2 Déploiement de Microsoft defender pour le cloud :

Toujours dans l'optique de mettre en place une infrastructure sécurisée, cet outil nous permet de créer une preuve de concept de Microsoft Defender pour environnement basé sur le cloud. Pour cela, nous souhaitons :

- ✓ Configurer Microsoft Defender pour Cloud pour surveiller une machine virtuelle.
- ✓ Consulter les recommandations de Microsoft Defender for Cloud pour la machine virtuelle.
- ✓ Implémenter des recommandations pour la configuration des invités et l'accès juste à temps aux machines virtuelles.

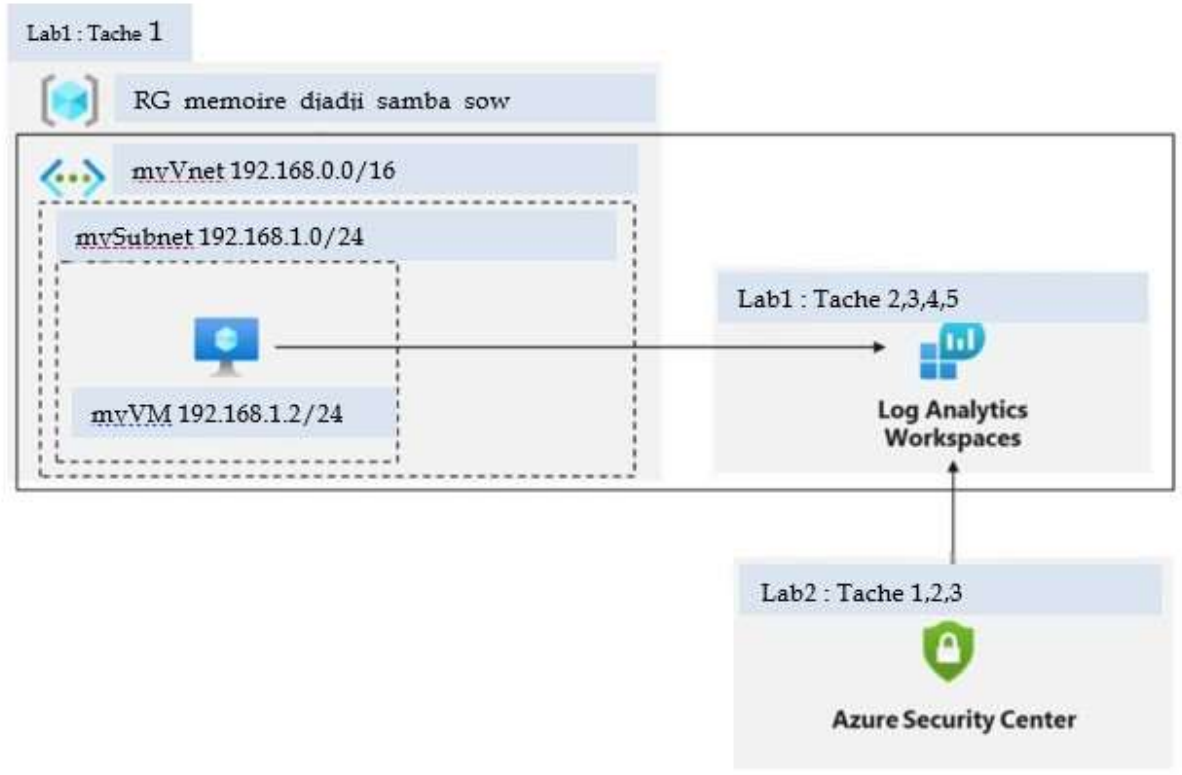


Figure 36: Déploiement de Microsoft Defender pour le Cloud

3.1.2.1 Tâche 1 : Configurer Microsoft Defender pour le Cloud

Dans cette tâche, nous allons intégrer et configurer Microsoft Defender pour Cloud.

- ➢ Dans le portail Azure, dans la zone de texte Rechercher des ressources, nous cherchons Microsoft Defender for Cloud

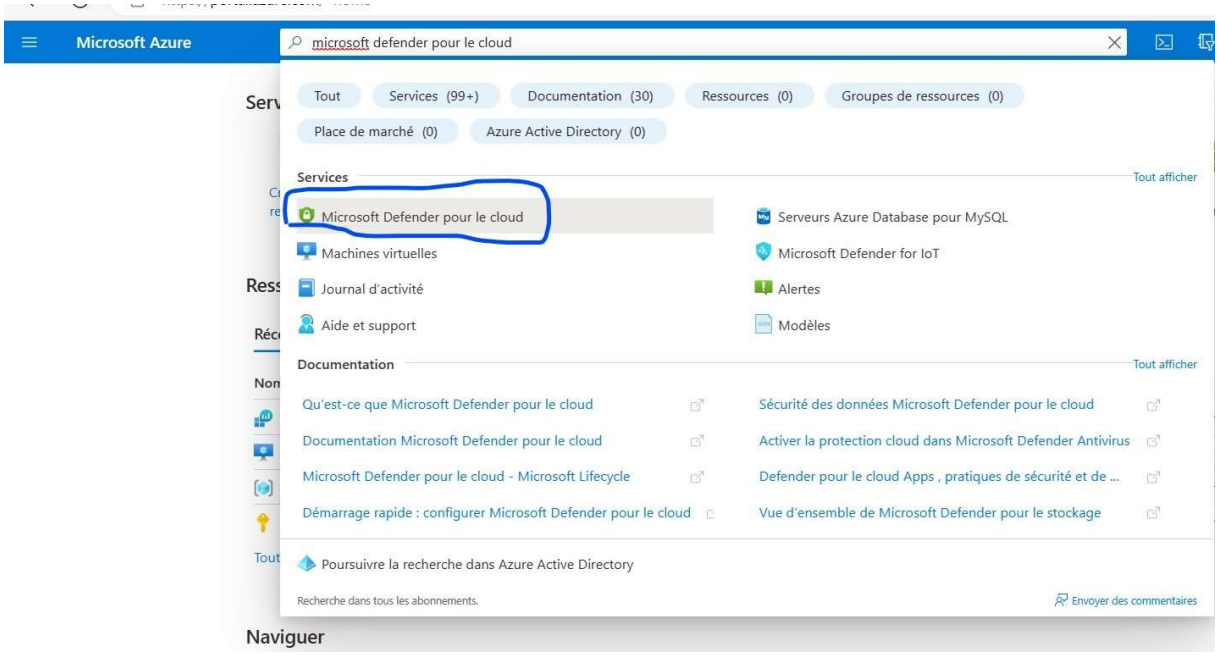


Figure 37: recherche de Microsoft Defender sur le portail azure

- Sur Microsoft Defender pour Cloud, dans le panneau Mise en route, il faudra Mettre à niveau puis Installer les agents.

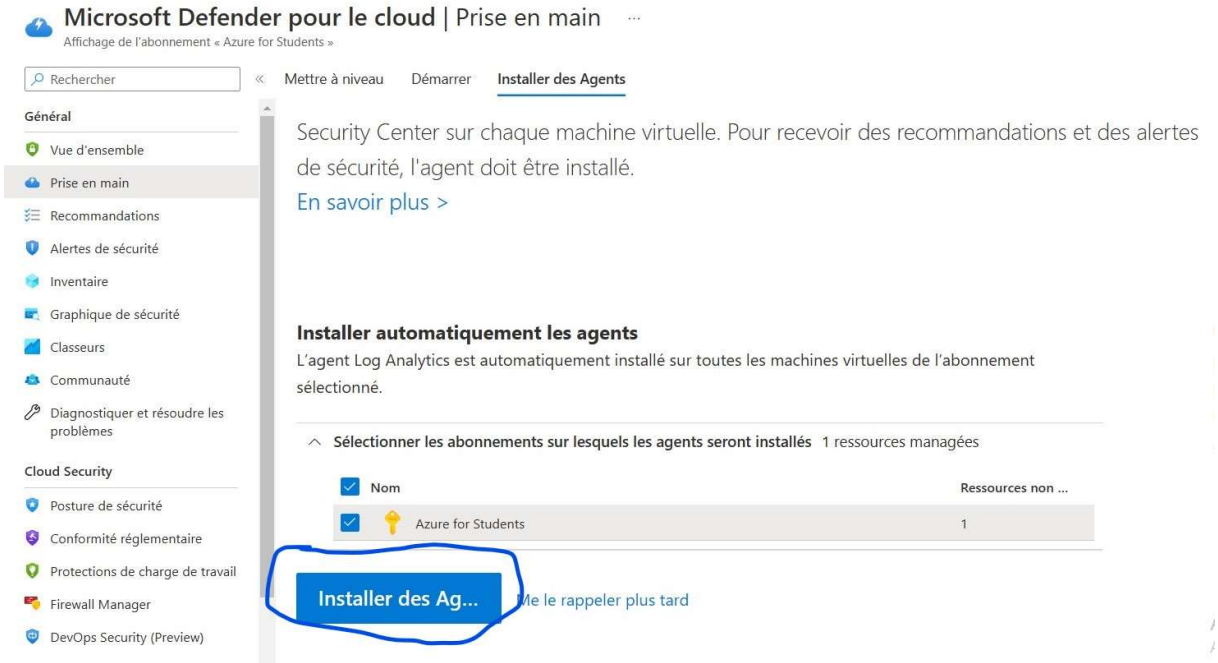


Figure 38: Mise à jour et installation de l'agent

- Puis Sur Microsoft Defender pour Cloud, dans Paramètres d'environnement, nous choisissons l'abonnement approprié.

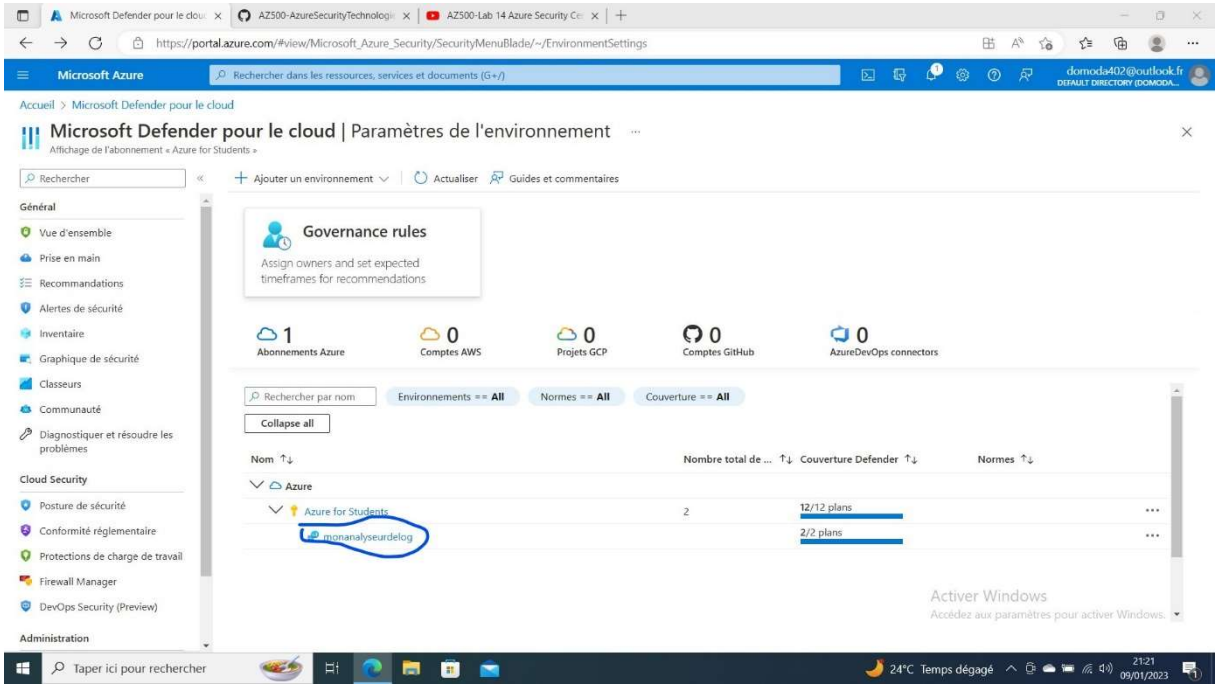


Figure 39: choix de l'abonnement approprier

- Une autre fenêtre apparait nous incitant à Activer tous les plans Microsoft Defender pour Cloud, comme vous pouvez le voir ci-dessous.

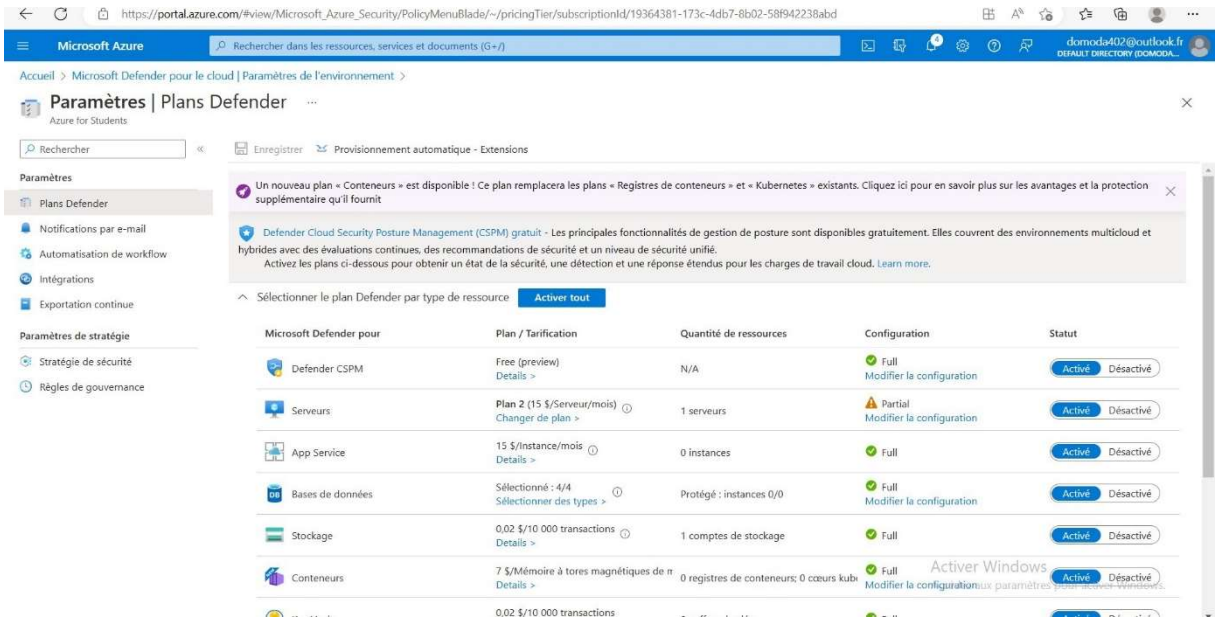


Figure 40: Activation des plans Microsoft defender

- Dans les paramètres, Approvisionnement automatique, il faudra s'assurer que l'approvisionnement automatique est défini sur Activé pour le premier élément Agent Log Analytics pour les machines virtuelles Azure.

.

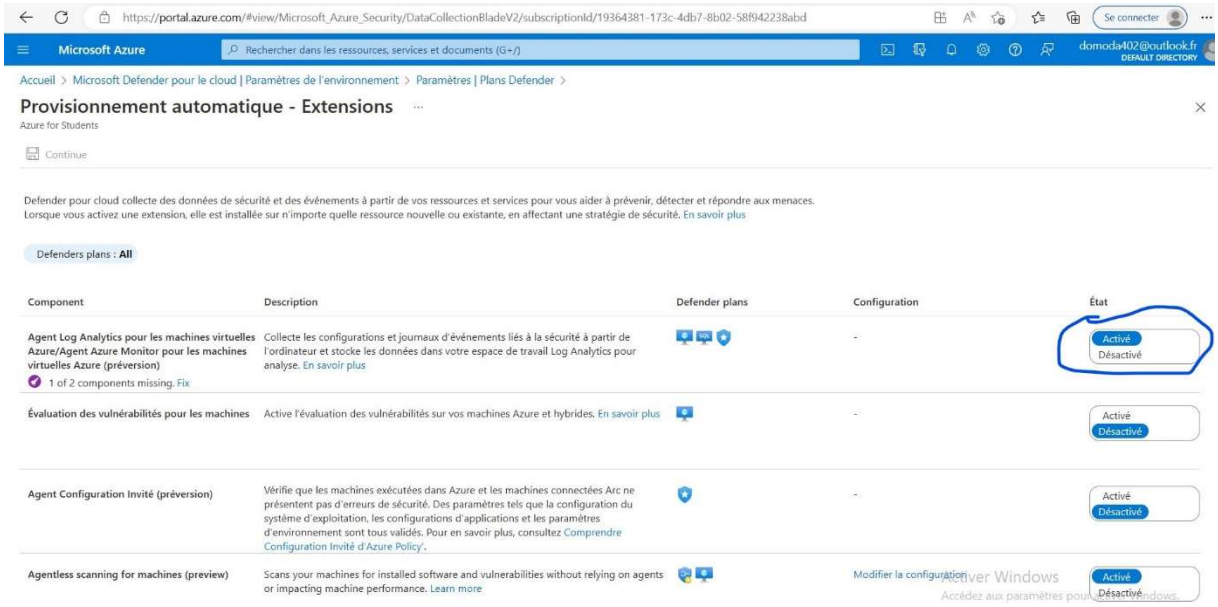


Figure 41: vérifier si l'approvisionnement est active sur log Analytics

- Revenons à Microsoft Defender pour Cloud, dans Paramètres d'environnement, sur l'entrée représentant l'espace de travail Log Analytics nous Sélectionnons Collecte de données dans Microsoft Defender pour Cloud, sur Panneau Paramètres. On choisit Tous les événements puis on enregistre.

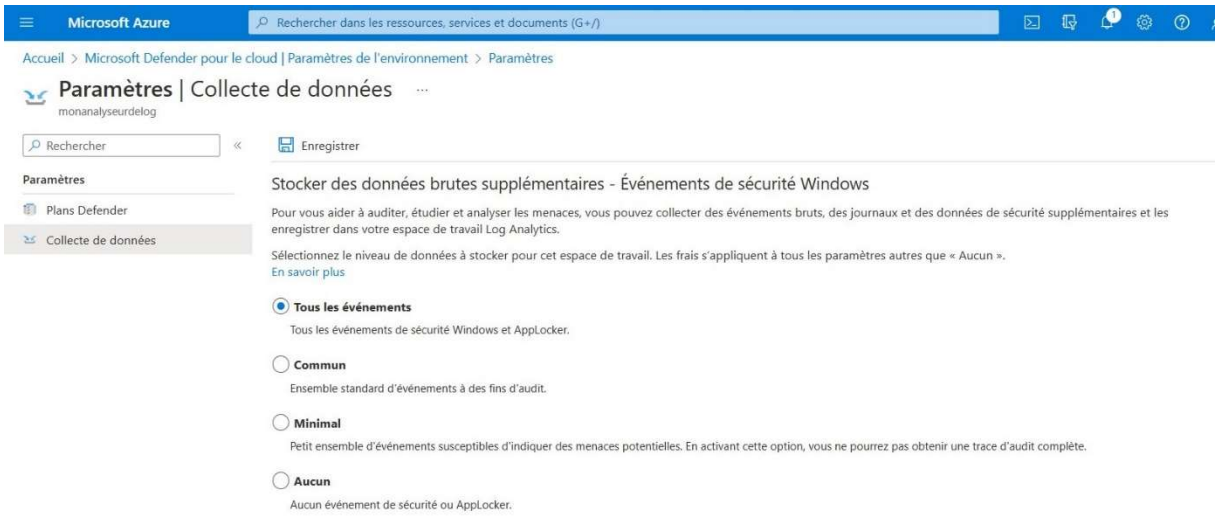


Figure 42: Collecte de données de tous les événements

3.1.2.2 Tâche 2 : Examiner la recommandation Microsoft Defender for Cloud

Dans cette tâche, nous allons passer en revue les recommandations de Microsoft Defender for Cloud.

- Dans Microsoft Defender pour Cloud, Vue d'ensemble, Ressources évaluées, dans le panneau Inventaire, sélectionnons l'entrée **myVM** correspondant à notre machine virtuelle.

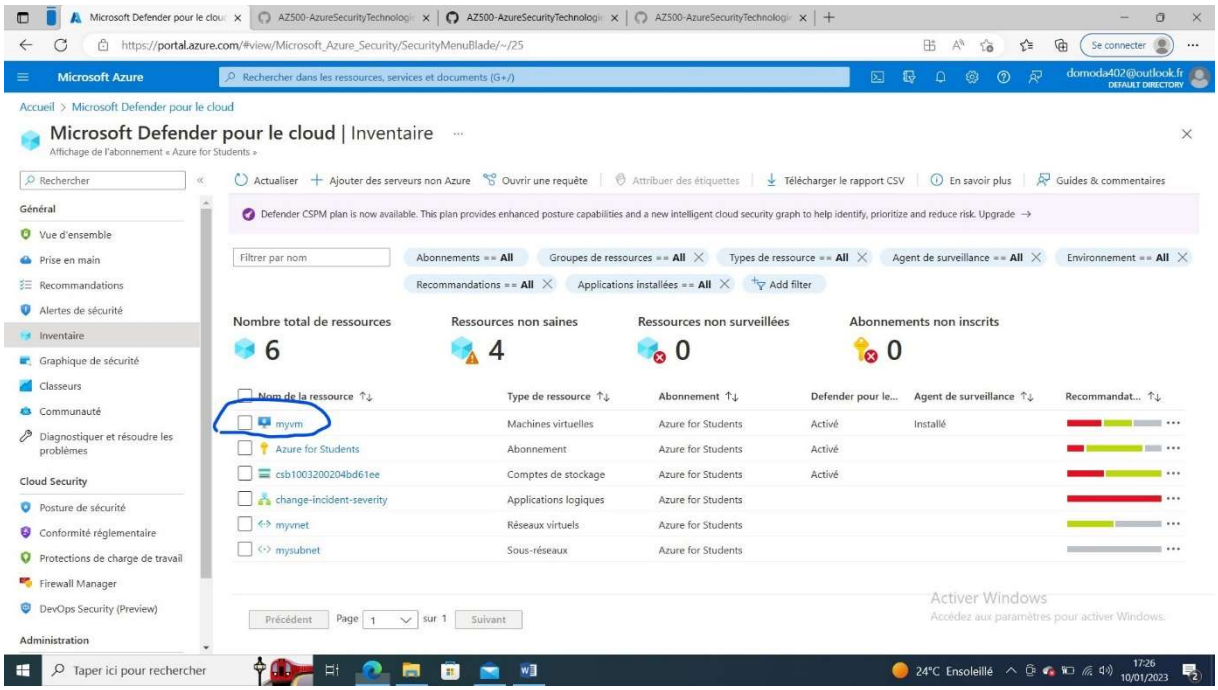


Figure 43: inventaire de la machine virtuelle myVM

- Dans le panneau Intégrité des ressources, sous l'onglet Recommandations, passons en revue la liste des recommandations pour myVM. On s'aperçoit qu'il y a pas mal de recommandation qui sont remontées par exemple l'accès aux machines virtuelles Just in time.

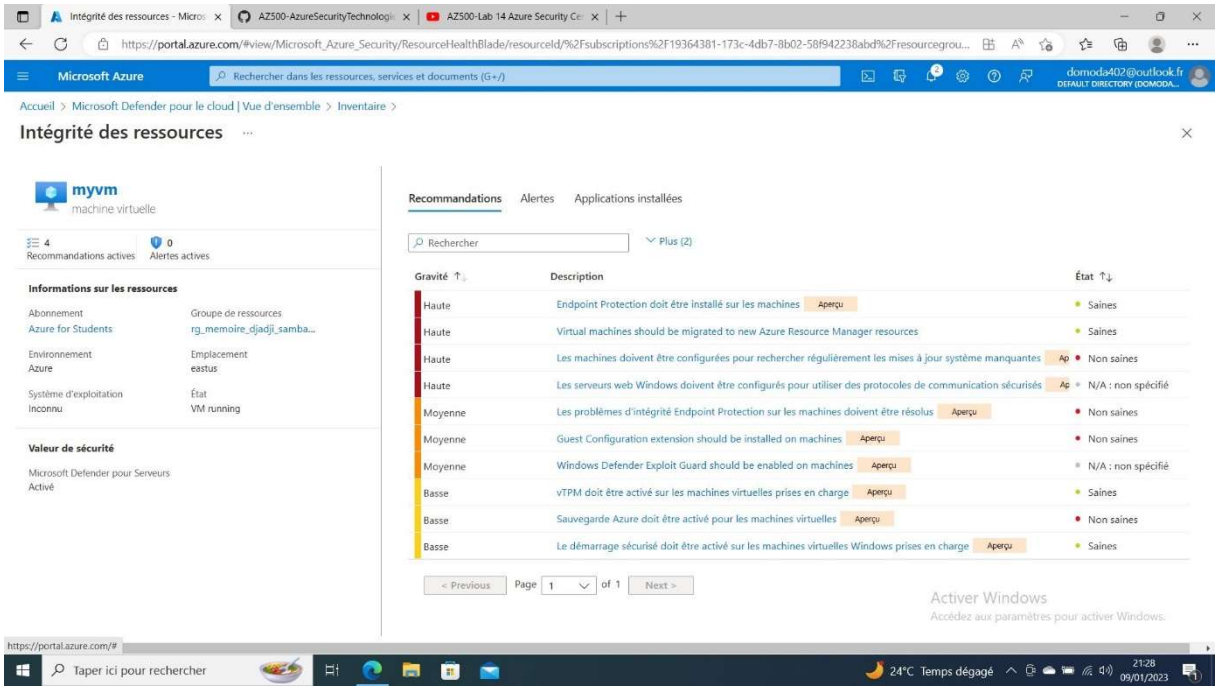


Figure 44: Les recommandations liées à la machine virtuelle myVM

3.1.2.3 Tâche 3 : Implémenter la recommandation Microsoft Defender for Cloud pour activer l'accès aux machines virtuelles Just in time

Dans cette tâche, nous allons implémenter la recommandation Microsoft Defender for Cloud pour activer l'accès juste à temps aux machines virtuelles sur la machine virtuelle.

- Dans le portail Azure, revenons à Microsoft Defender pour Cloud, dans le panneau Protection contre la charge de travail, dans la section Protection avancée, nous cliquons sur la vignette Accès juste à temps aux machines virtuelles et, dans le panneau Accès juste à temps aux machines virtuelles, nous cliquons sur Essayer d'accéder juste à temps aux machines virtuelles. Il peut arriver que les machines virtuelles ne soient pas répertoriées, dans ce cas il faut accéder au panneau Machine virtuelle et cliquer sur Configuration, puis sur l'option Activer les machines virtuelles juste-à-temps sous l'accès de la machine virtuelle juste-à-temps. Répéter l'étape ci-dessus pour revenir à Microsoft Defender pour Cloud et actualiser la page, la machine virtuelle apparaîtra.

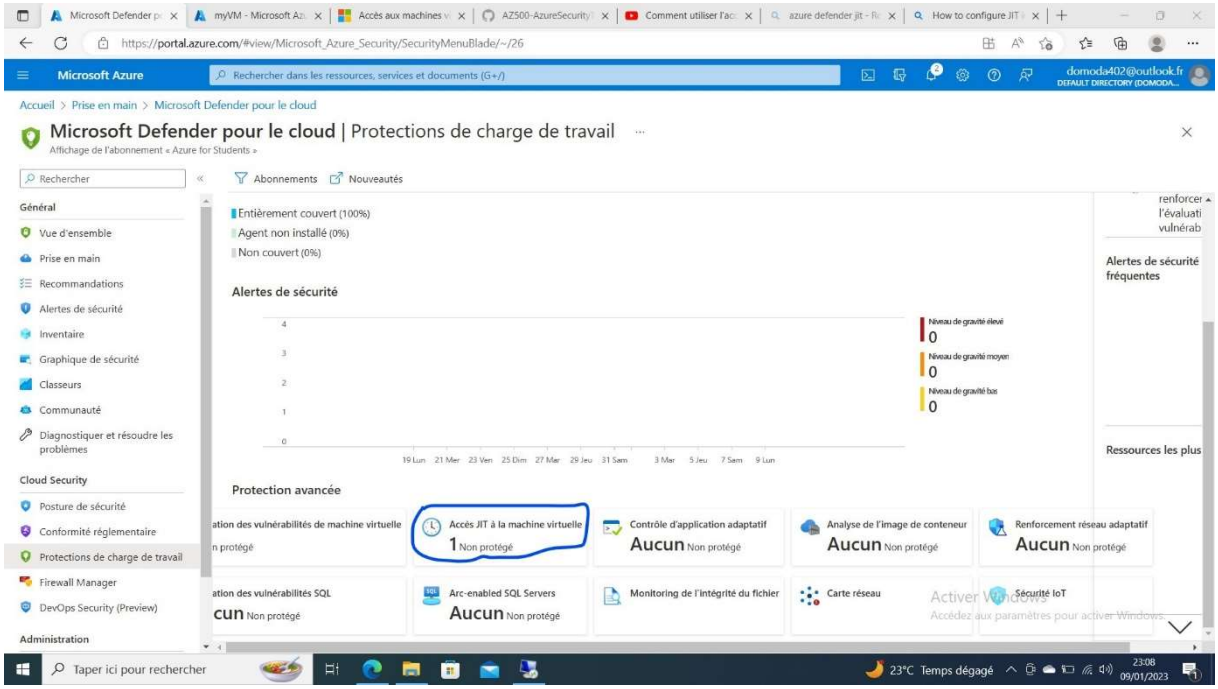


Figure 45: Implémenter JIT sur myVM

- Sur l'accès à la machine virtuelle juste à temps, sélectionnons **Non configuré**, puis cliquer sur l'entrée myVM. Il faudra peut-être attendre quelques minutes avant que l'entrée myVM ne soit disponible. Et puis nous Sélectionnons Activer JIT sur 1 machine virtuelle.

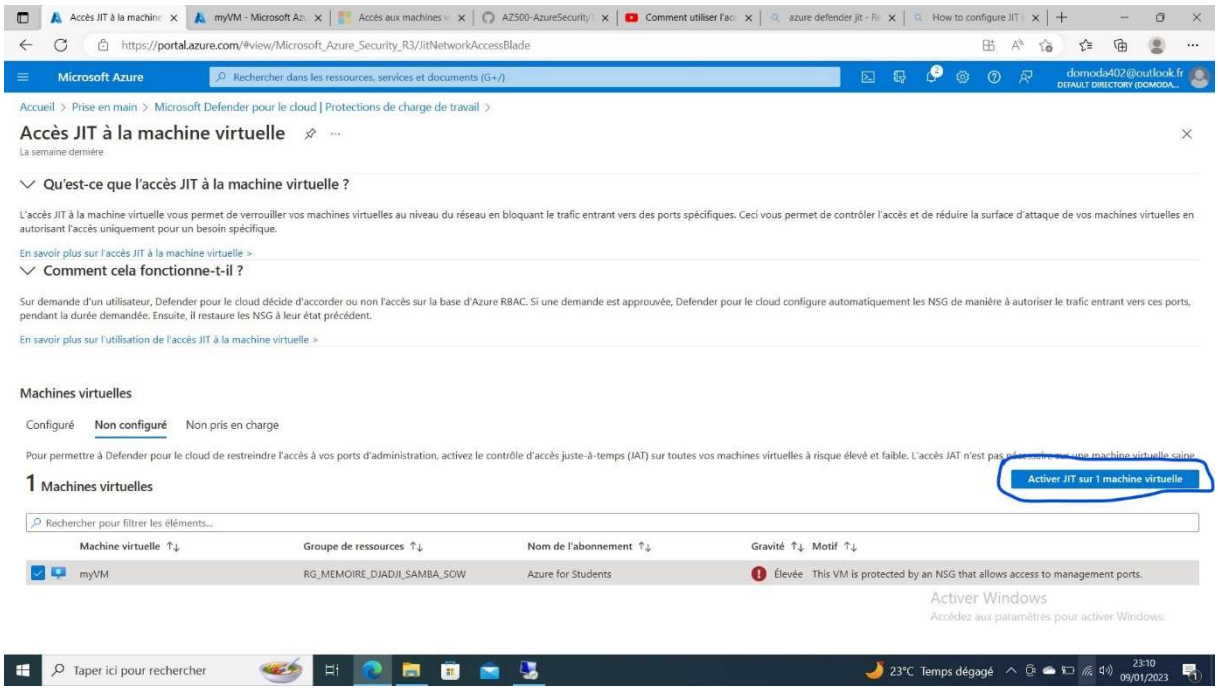


Figure 46: Activation de l'accès JIT sur myVM

- Dans le panneau Configuration de l'accès à la machine virtuelle JIT, à l'extrême droite de la ligne faisant référence au port 22, nous cliquons sur le bouton de sélection puis sur Supprimer.



Figure 47: configuration de l'accès JIT sur myVM

- Pour finir on enregistre la configuration de l'accès à la machine virtuelle JIT. Nous avons aussi la possibilité de configurer l'accès sur les autres ports dépendamment de nos besoins en sécurité d'accès.

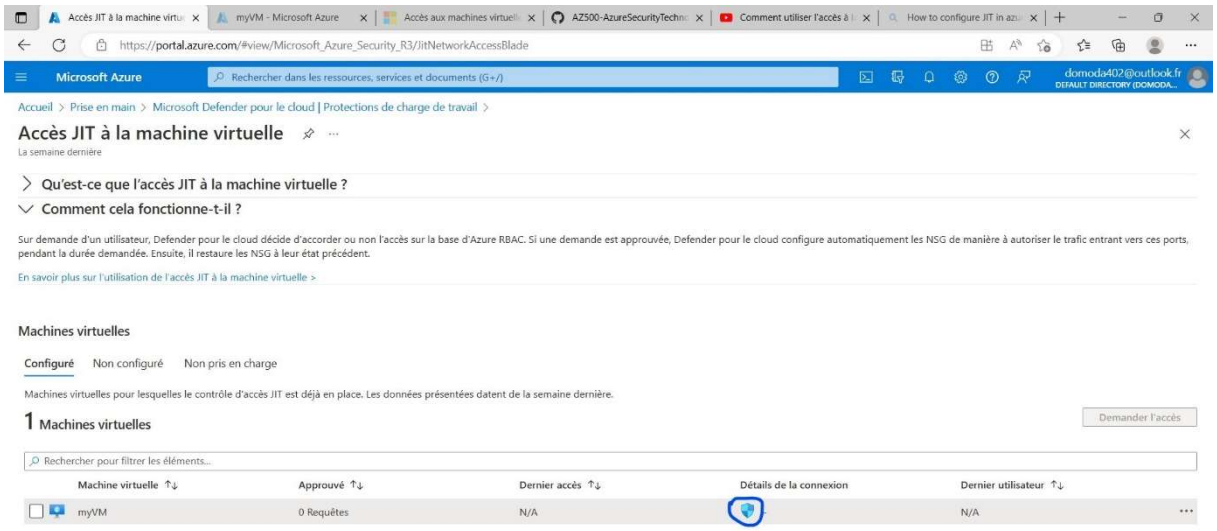


Figure 48: Détails de la connexion

Nous avons intégré Microsoft Defender for Cloud et implémenté des recommandations de machines virtuelles.

3.1.3 Déploiement de Microsoft Sentinel

Après la mise place d'Azure Monitor et de Microsoft Defender pour le cloud, nous en arrivons à l'objectif final qui est la création d'une preuve de concept de détection et de réponse aux menaces basée sur Microsoft Sentinel. Pour, nous allons :

- ✓ Commencer à collecter des données à partir d'Azure Activity et de Microsoft Defender pour le Cloud.
- ✓ Ajouter des alertes intégrées et personnalisées
- ✓ Découvrir comment les Playbooks peuvent être utilisés pour automatiser une réponse à un incident.

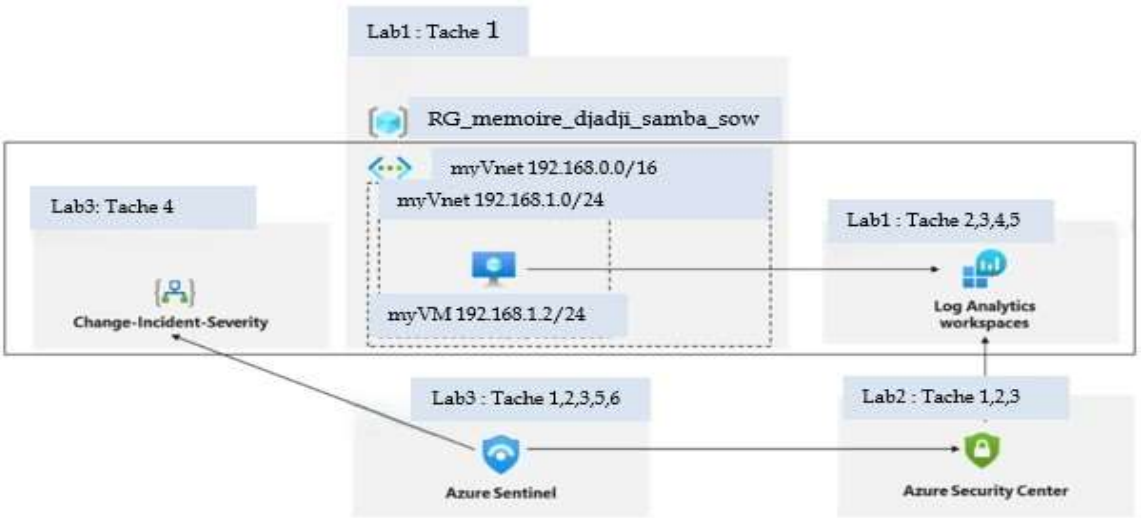


Figure 49: Déploiement de Microsoft Sentinel

3.1.3.1 Tâche 1 : Intégrer Azure Sentinel

Dans cette tâche, nous allons intégrer Microsoft Sentinel et connecter l'espace de travail Log Analytics.

- Il s'agit de notre première tentative d'action Microsoft Sentinel dans le tableau de bord Azure, effectuons les étapes suivantes : Dans le portail Azure, dans la zone de texte Rechercher des ressources, des services et des documents en haut de la page du portail Azure, tapons Microsoft Sentinel, sélectionnons Microsoft Sentinel dans la vue Services et appuyons sur la touche Entrée.

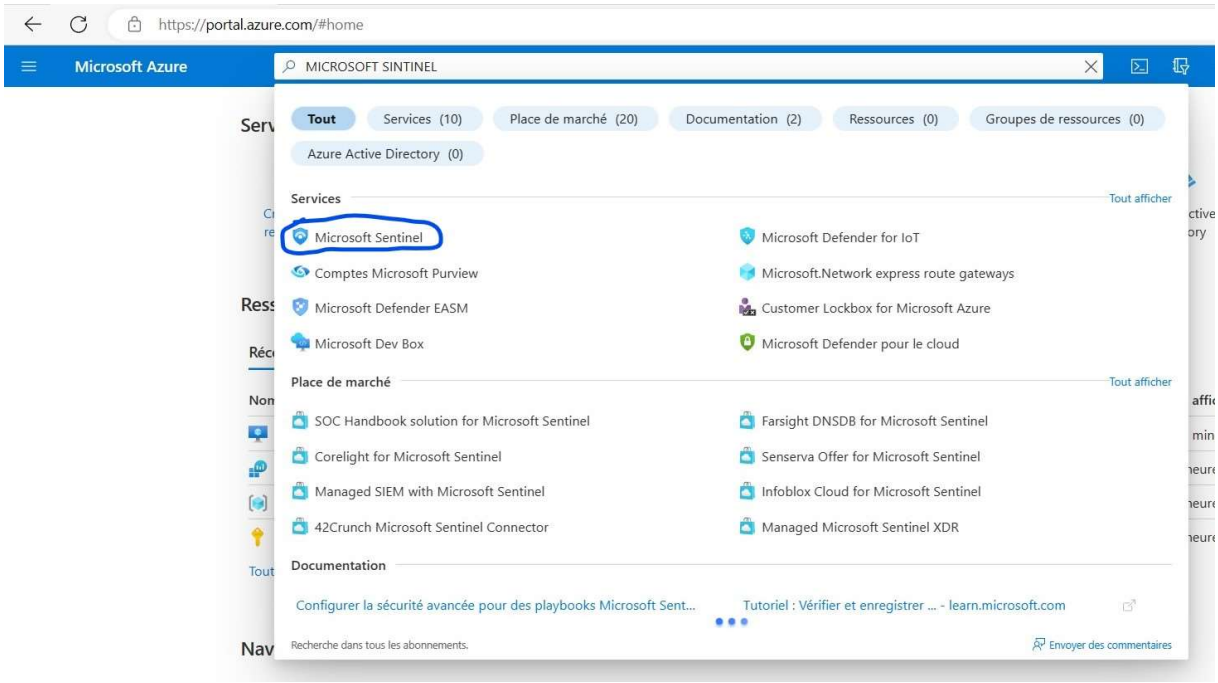


Figure 50: Recherche de Microsoft Sentinel sur le portail azure

- Dans le panneau Microsoft Sentinel, nous cliquons sur le bouton + Créer.

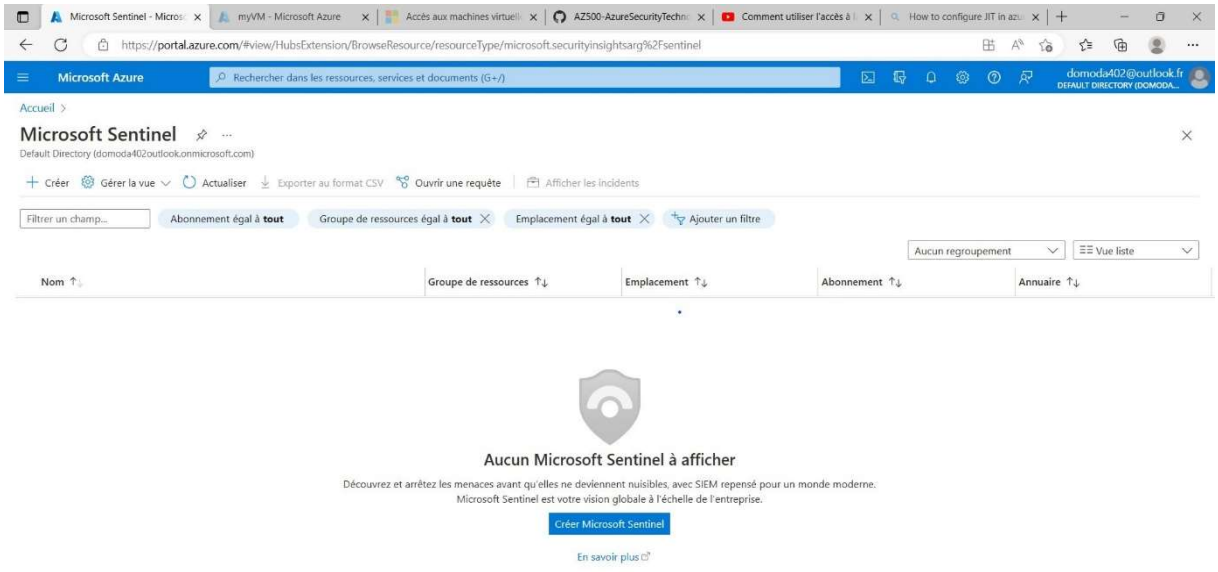


Figure 51: Le panneau de Microsoft Sentinel

- Dans le panneau Ajouter Microsoft Sentinel à un espace de travail, nous sélectionnons l'espace de travail Log Analytics que nous avons créé dans le laboratoire Azure Monitor, puis cliquons sur Ajouter.

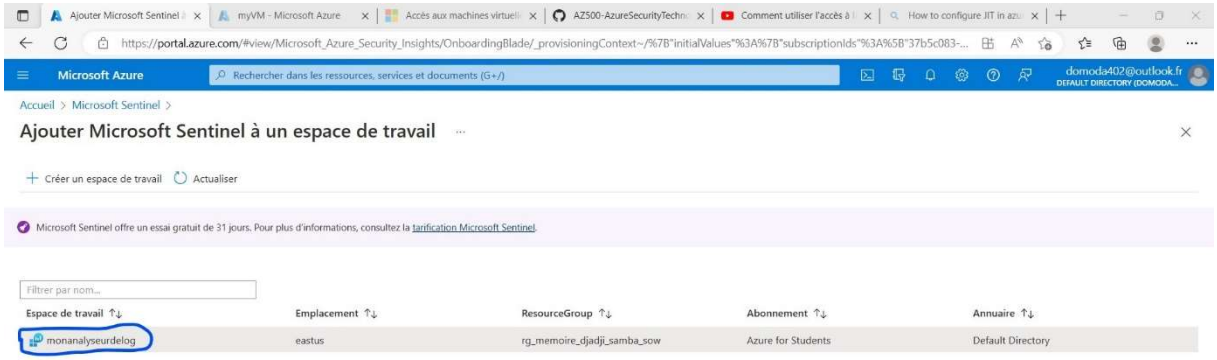


Figure 52: Ajout d'un espace de travail à Microsoft Sentinel

Il est à noter que Microsoft Sentinel a des exigences très spécifiques pour les espaces de travail. Par exemple, les espaces de travail créés par Microsoft Defender for Cloud ne peuvent pas être utilisés.

3.1.3.2 Tâche 2 : configurer Microsoft Sentinel pour utiliser le connecteur de données Azure Activity.

Dans cette tâche, nous allons configurer Sentinel pour utiliser le connecteur de données Azure Activity.

- Sur Microsoft Sentinel, Connecteur de données, passez en revue la liste des connecteurs disponibles, sélectionnons l'entrée représentant le connecteur d'activité, nous vérifions sa description et son état, puis nous cliquons sur Ouvrir la page du connecteur.

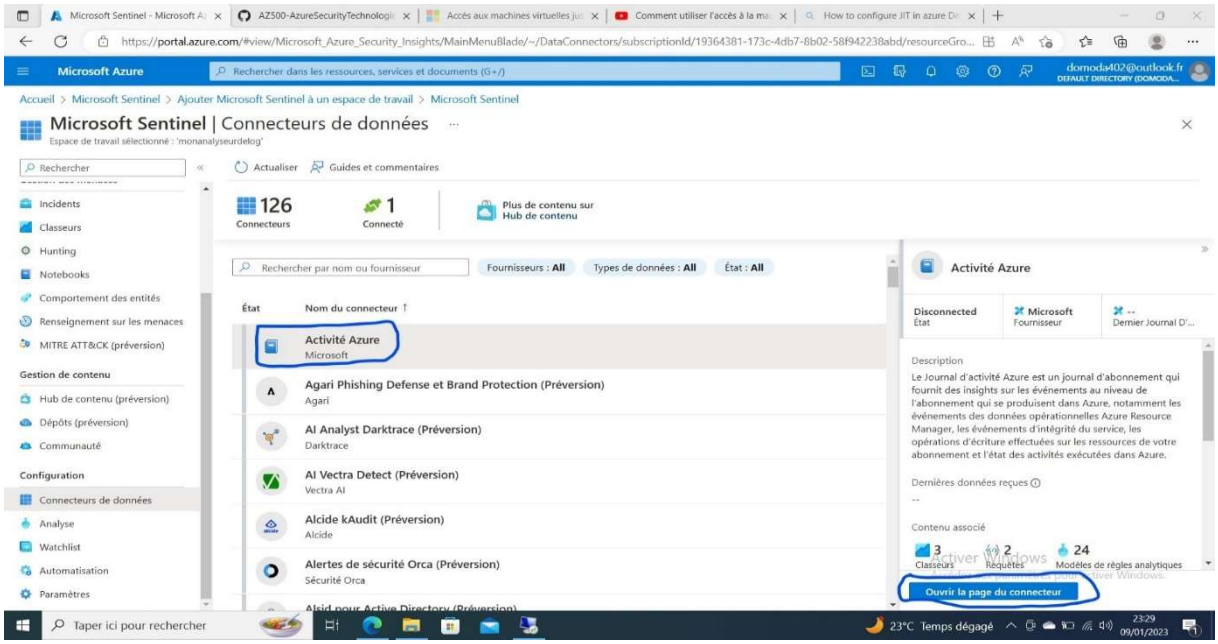


Figure 53: Ajout d'un connecteur d'activité

- Dans l'onglet Configurer les journaux d'activité Azure pour les diffuser vers l'espace de travail Log Analytics spécifié (page Affecter une stratégie), cliquons sur le bouton Points de suspension de l'étendue (...). Dans la page Étendue, choisissons notre abonnement Azure dans la liste déroulante des abonnements, puis cliquons sur le bouton Sélectionner en bas de la page.

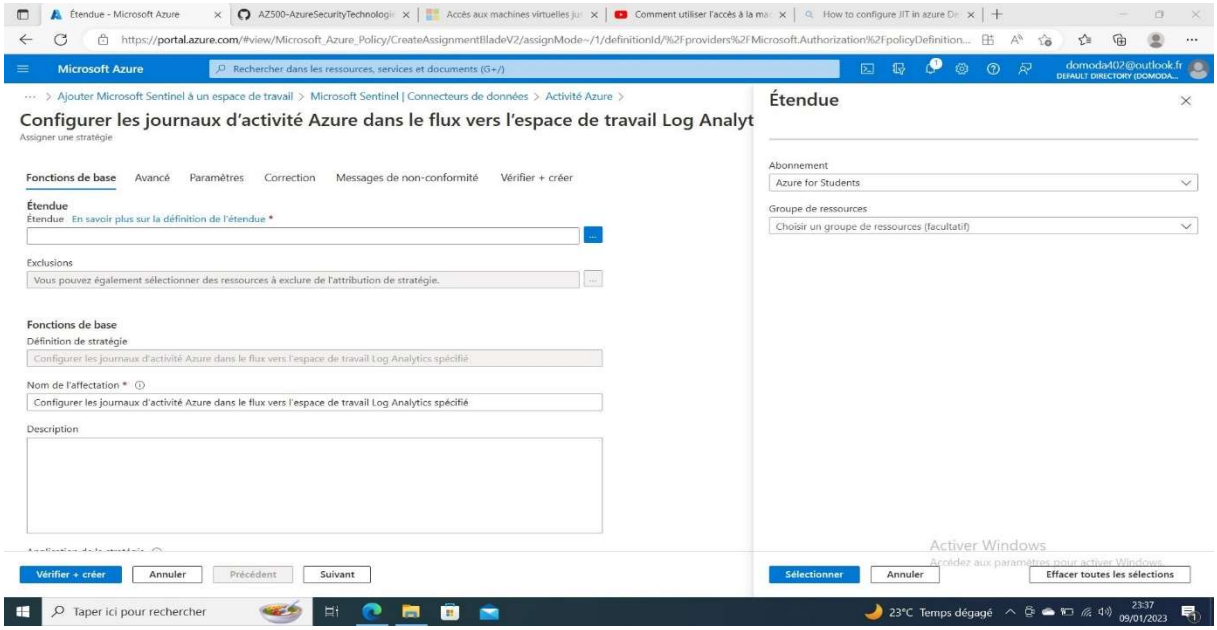


Figure 54: Configurer les journaux d'activité Azure dans le flux vers l'espace de travail Log Analytics

- Sur le bouton Suivant en bas de l'onglet Notions de base pour passer à l'onglet Paramètres. Sous l'onglet Paramètres, sur le bouton ellipse (...) de l'espace de travail Primary Log Analytics (...). Dans la page Espace de travail Log Analytics principal, assurons-nous que notre abonnement Azure est sélectionné et utilisons la liste déroulante Espaces de travail pour sélectionner l'espace de travail Log Analytics que nous utilisons pour Sentinel. Puis le bouton Sélectionner en bas de la page.

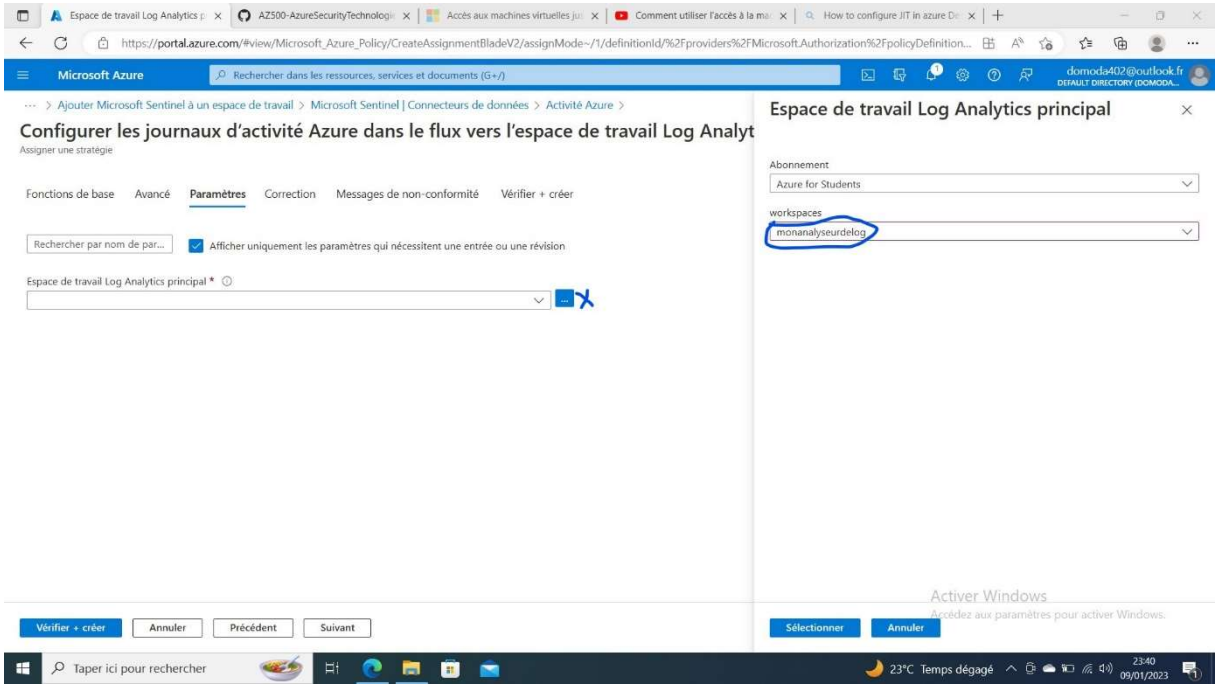


Figure 55: ajout de l'espace de travail principale

- Sur l'onglet Correction, nous cochons la case Créer une tâche de correction. Cela activera la liste déroulante « Configurer les journaux d'activité Azure pour diffuser vers l'espace de travail Log Analytics spécifié » dans la liste déroulante Stratégie pour corriger. Dans la liste déroulante Emplacement de l'identité attribuée au système, nous sélectionnons la région (dans notre cas États-Unis de l'Est) que nous avons utilisée précédemment pour votre espace de travail Log Analytics.

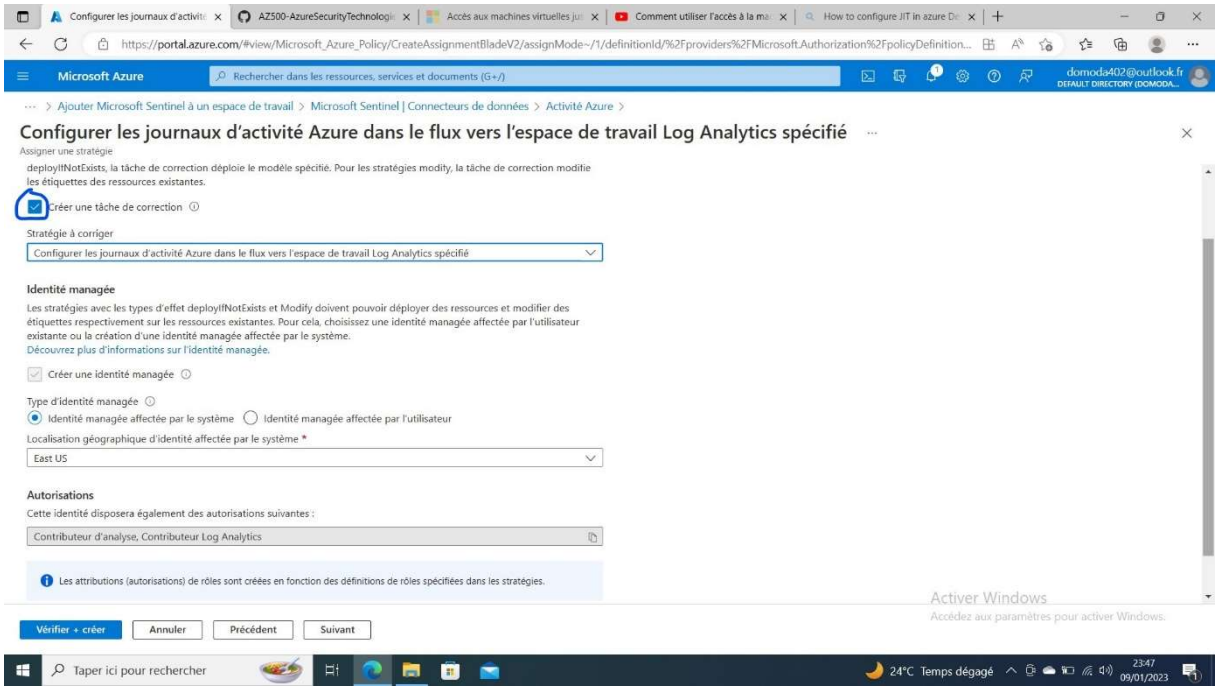


Figure 56: Activation de la gestion d'une tache correction

- Sur l'onglet Message de non-conformité, nous pouvons entrer un message de non-conformité si nous le souhaitons (facultatif), enfin sur le bouton +créer. Sur la page activité azure on peut s'apercevoir l'affichage de quelques données collectées.

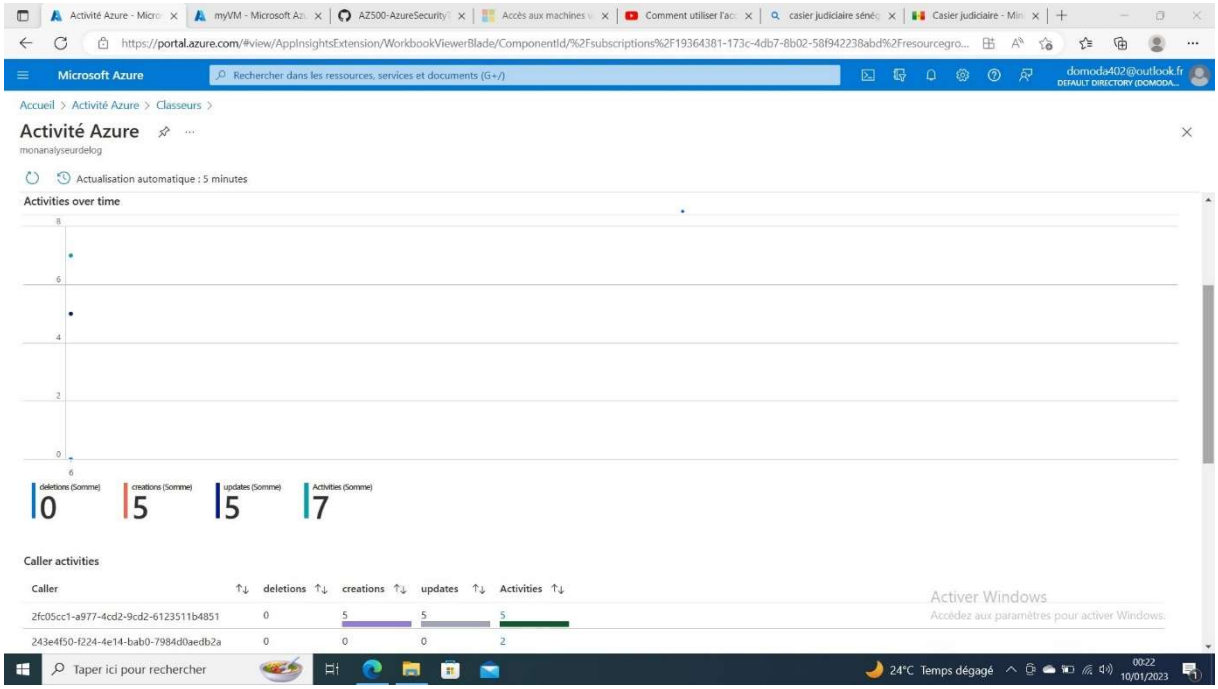


Figure 57: l'affichage de quelques données collectées

3.1.3.3 Tâche 3 : Créer une règle qui utilise le connecteur de données Azure Activity

Dans cette tâche, nous allons examiner et créer une règle qui utilise le connecteur de données Azure Activity.

- Sur Microsoft Sentinel, Analyse, dans la liste des modèles de règles, choisissons **Nombre suspect de création ou de déploiement de ressource** associée à la source de données Azure Activity. Ensuite, dans le volet affichant les propriétés du modèle de règle, on clique sur Créer une règle. Cette règle a la gravité moyenne.

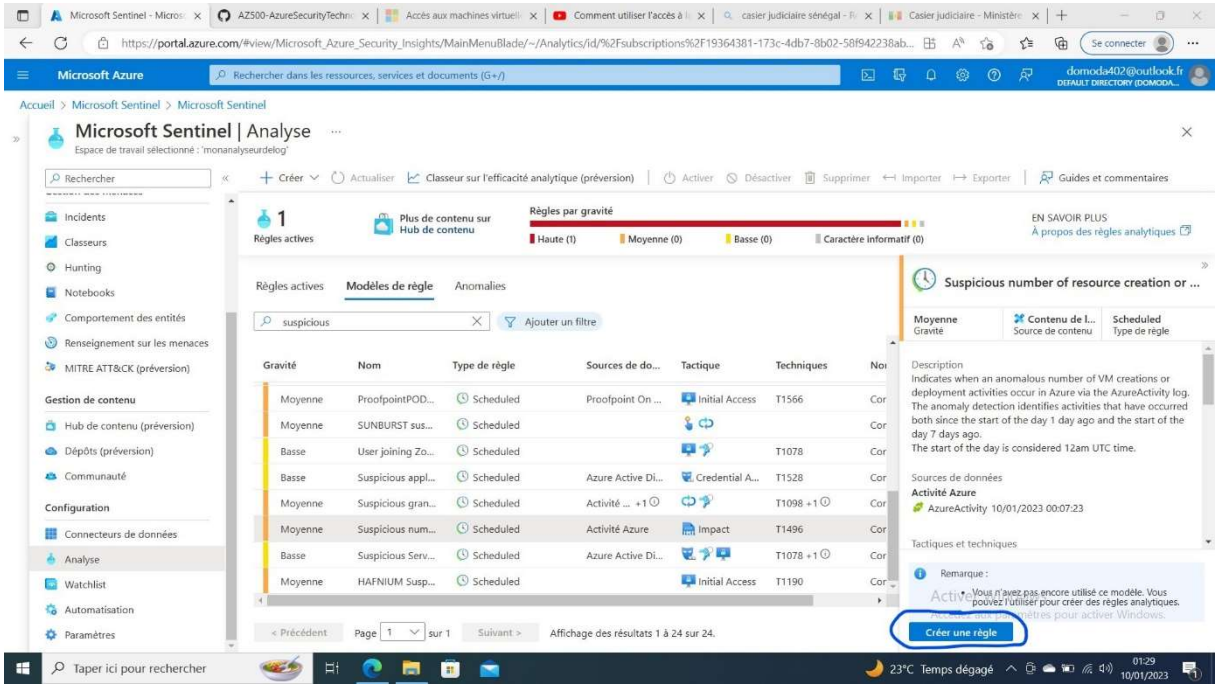


Figure 58: création d'une règle utilisant Azure Activity

- Sous l'onglet Général de l'Assistant Règle analytique - Créer une règle à partir du panneau Modèle, acceptons les paramètres par défaut et cliquons sur Suivant : Définir la logique de règle.

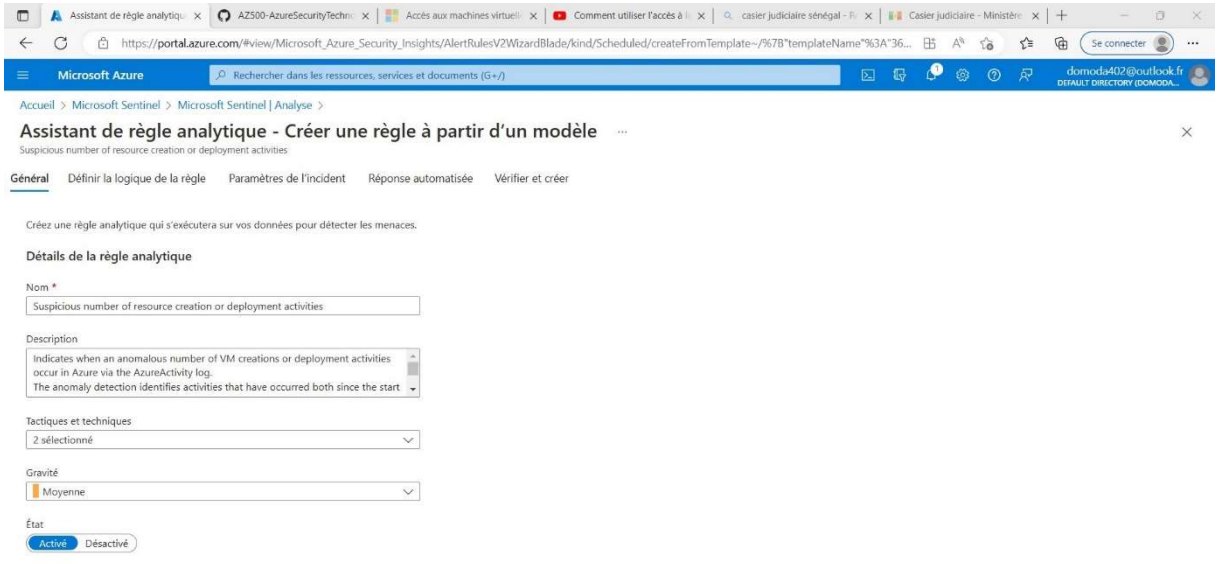


Figure 59: Définir la logique de règle

- Sous l'onglet Définir la logique de la règle de l'Assistant Règle analytique - Créer une règle à partir du panneau Modèle, acceptons les paramètres par défaut et cliquons sur Suivant : Paramètres d'incident.

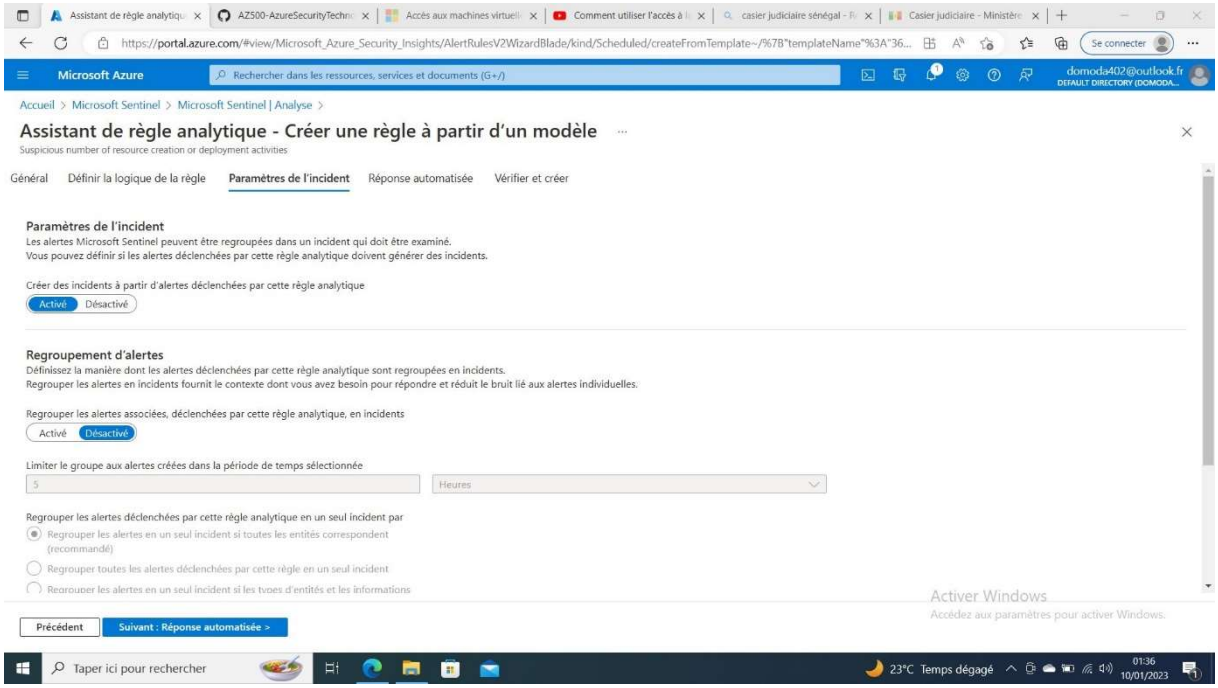


Figure 60: configuration du paramètre d'incident

- Sous l'onglet Paramètres d'incident de l'Assistant Règle analytique - Créer une règle à partir du panneau Modèle, acceptons les paramètres par défaut et cliquons sur Suivant : de réponse automatisée. C'est ici que nous pouvons ajouter un playbook, implémenté en tant qu'application logique, à une règle pour automatiser la correction d'un problème. Après création nous avons une règle active.

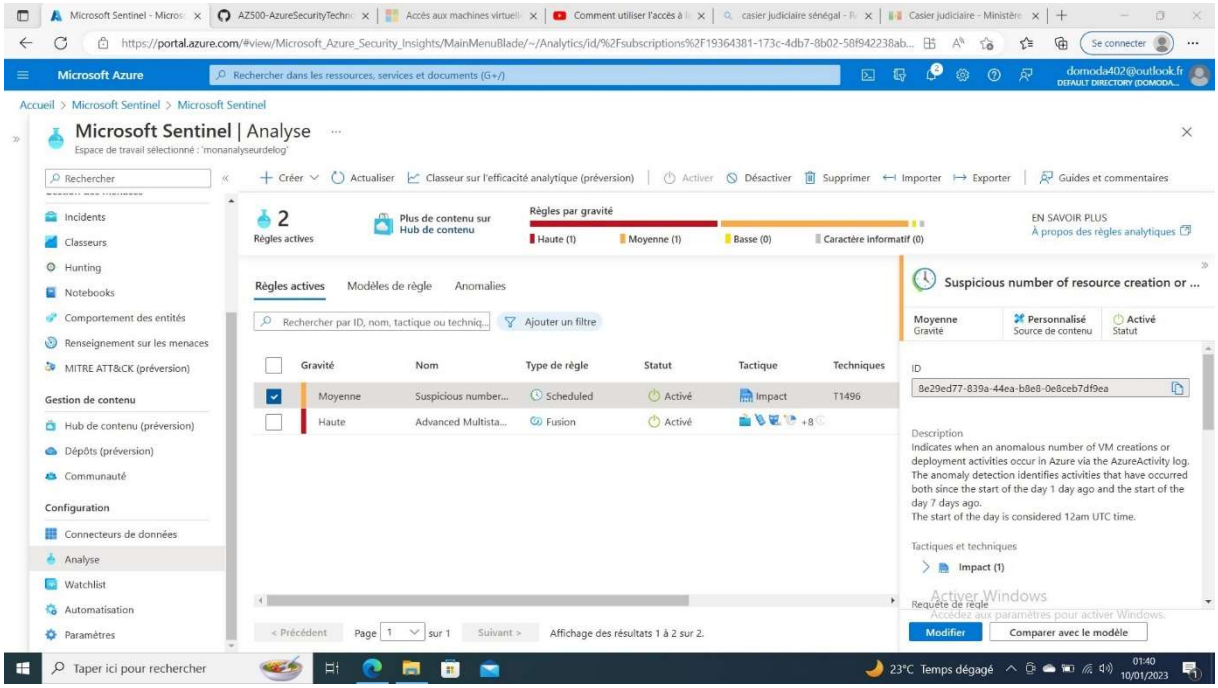


Figure 61: visualisation de la règle créée

3.1.3.4 Tâche 4 : Créer un playbook

Dans cette tâche, nous allons créer un playbook. Un playbook de sécurité est un ensemble de tâches qui peuvent être appelées par Microsoft Sentinel en réponse à une alerte.

- Dans le portail Azure, dans la zone de texte Rechercher des ressources, des services et des documents en haut de la page du portail Azure, tapons Déployer un modèle personnalisé et appuyons sur la touche Entrée.

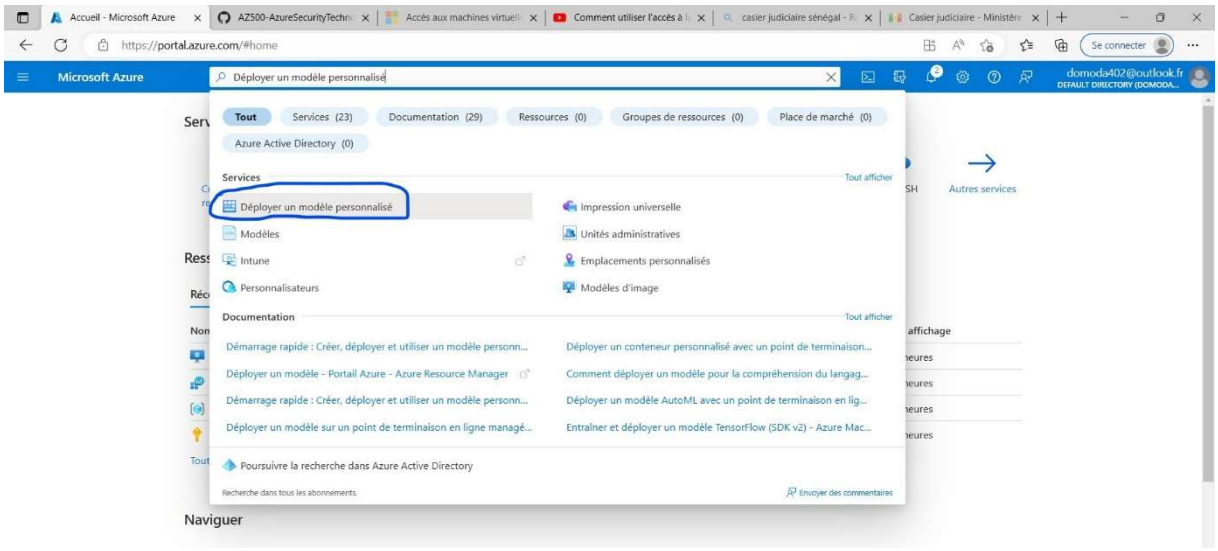


Figure 62: recherche de Déployer un modèle personnalisé sur le portail azure

- Dans le panneau Déploiement personnalisé, cliquons sur l'option Créer votre propre modèle dans l'éditeur.

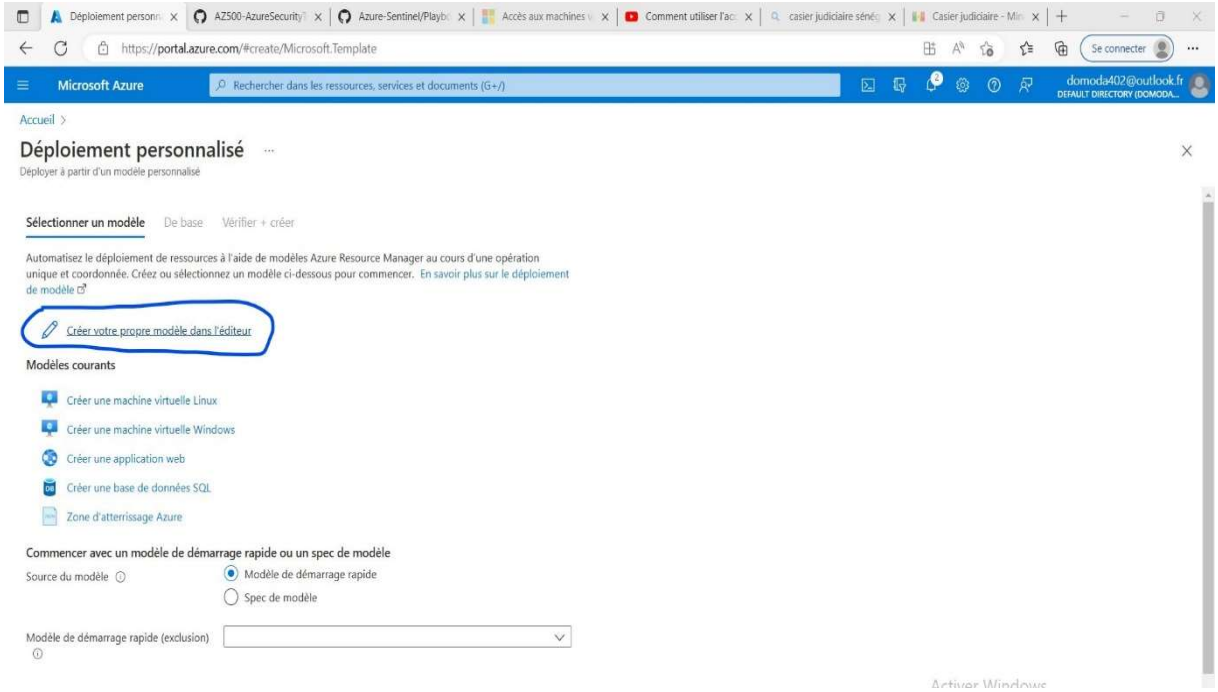


Figure 63: création d'un modèle personnalisé

- Dans le panneau Modifier le modèle, cliquez sur Charger le fichier, recherchez le fichier stocké sur notre machine en local pour l'ouvrir. Dans le panneau Modifier le modèle, cliquons sur Enregistrer. Selon différents scénarios y a des Playbooks correspondants et disponible sur la page GitHub de Microsoft Azure https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks.

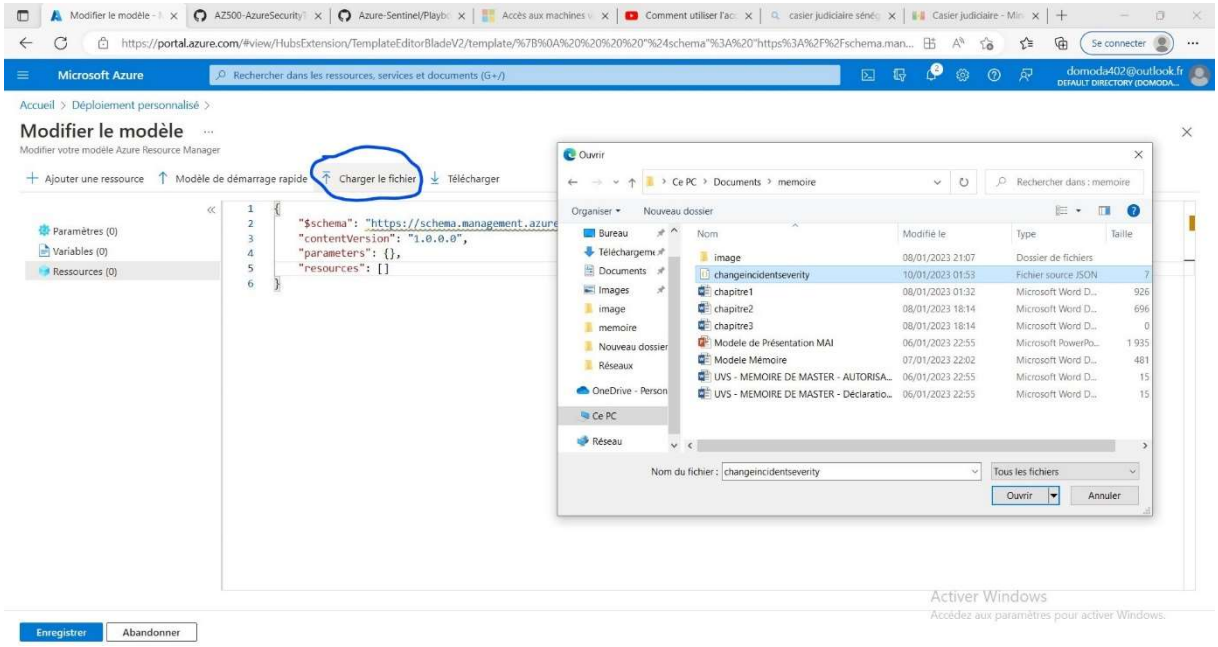


Figure 64: L'ajout de notre Playbooks

- Sur Vérifier + créer, puis sur Créer.

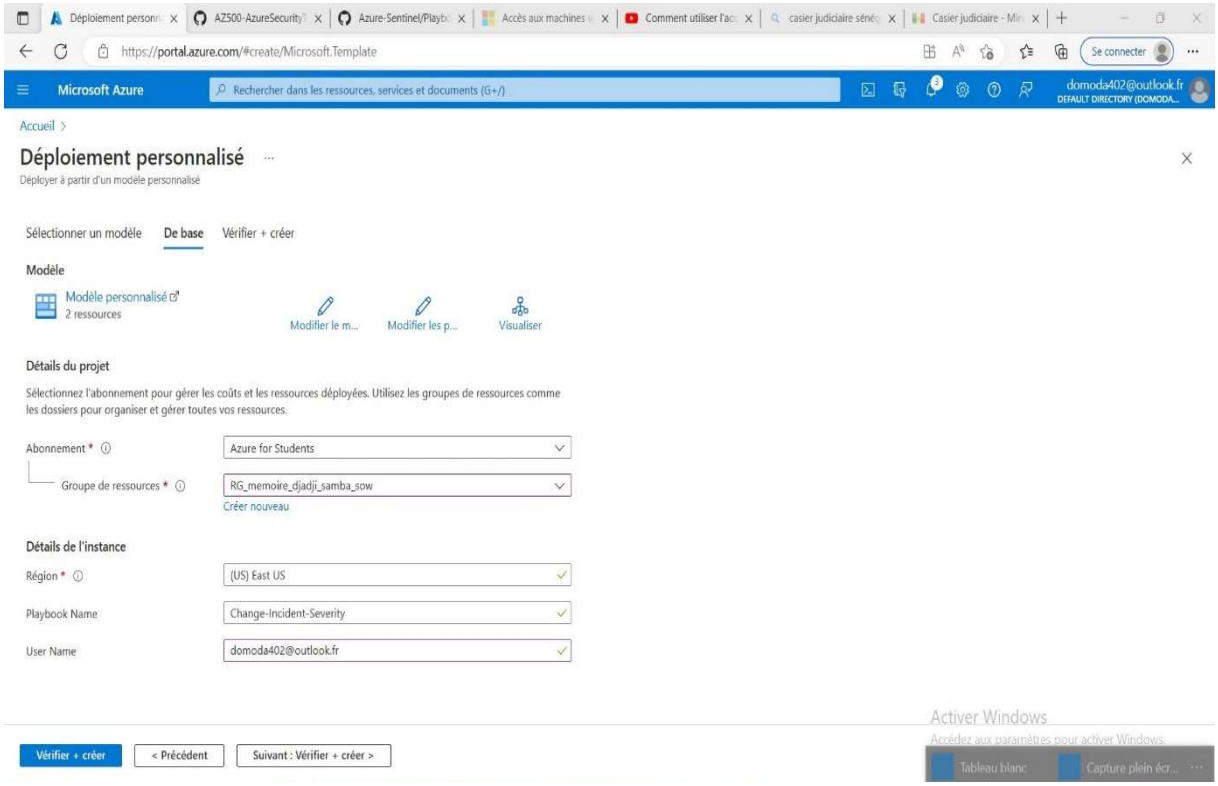


Figure 65: finalisation de la création

- A la fin du déploiement, dans le panneau Groupes de ressources, dans la liste des groupes de ressources RG_memoire_djadji_samba_sow, dans la liste des ressources, choisissons l'entrée représentant l'application logique Change-Incident-Severity nouvellement créée

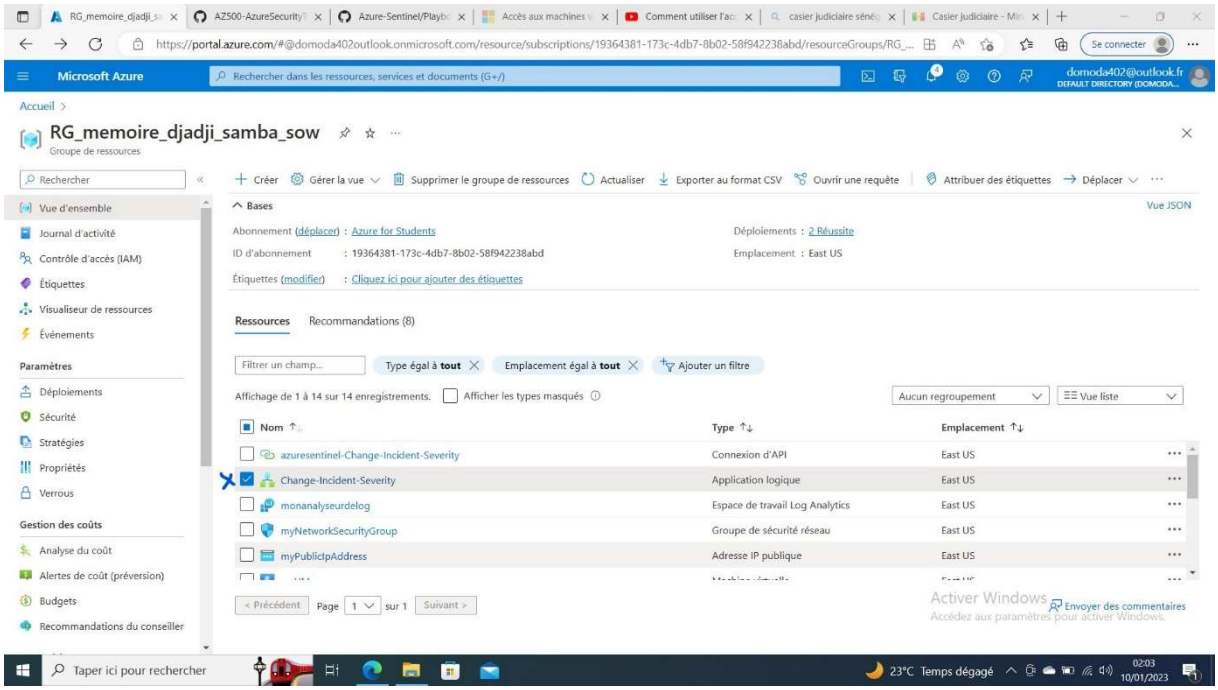


Figure 66: la logique Change-Incident-Severity

- Dans le panneau Concepteur d'applications logiques, chacune des quatre connexions affiche un avertissement. Cela signifie que chacun doit être revu et configuré. Cliquons sur Ajouter nouveau, vérifions que l'entrée de la liste déroulante Locataire contient notre nom de locataire Azure AD, puis cliquons sur Connexion. Nous allons répéter l'étape précédente pour les trois autres étapes de connexion en s'assurant qu'aucun avertissement ne s'affiche sur aucune des étapes. Pour finir enregistrons nos modifications.

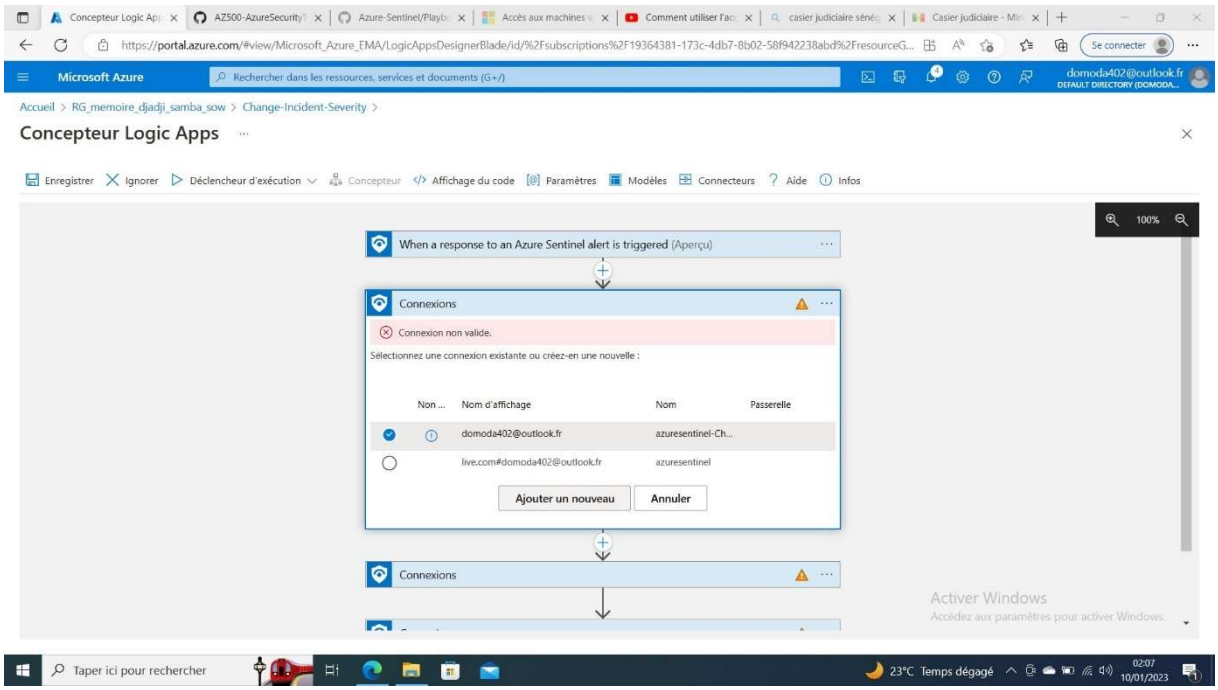


Figure 67: configuration des quatre connexions

3.1.3.5 Tâche 5 : Créer une alerte personnalisée et configurer un playbook en tant que réponse automatisée

- Sur Microsoft Sentinel, Analyse, sur Règle de requête planifiée, Créons une règle en spécifiant les paramètres suivants : nom du playbooks **djadji playbooks**, les autres paramètres sont par défaut.

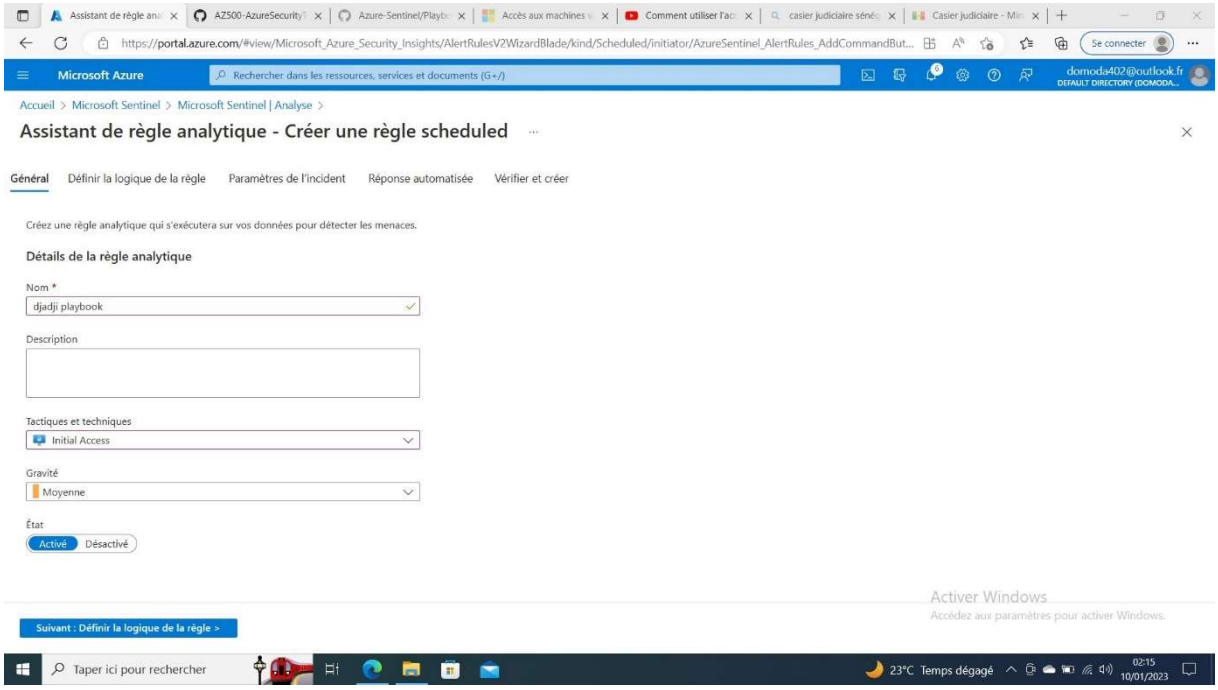


Figure 68: création d'une règle Scheduled

- Sous l'onglet Définir la logique de la règle de l'Assistant Règle analytique, dans la zone de texte Requête de règle, mettons la requête de règle suivante. Cette règle identifie la suppression des stratégies d'accès aux machines virtuelles juste-à-temps.

```
AzureActivity | where ResourceProviderValue =~ "Microsoft.Security"  | where
OperationNameValue =~ "Microsoft.Security/locations/jitNetworkAccessPolicies/delete"
```

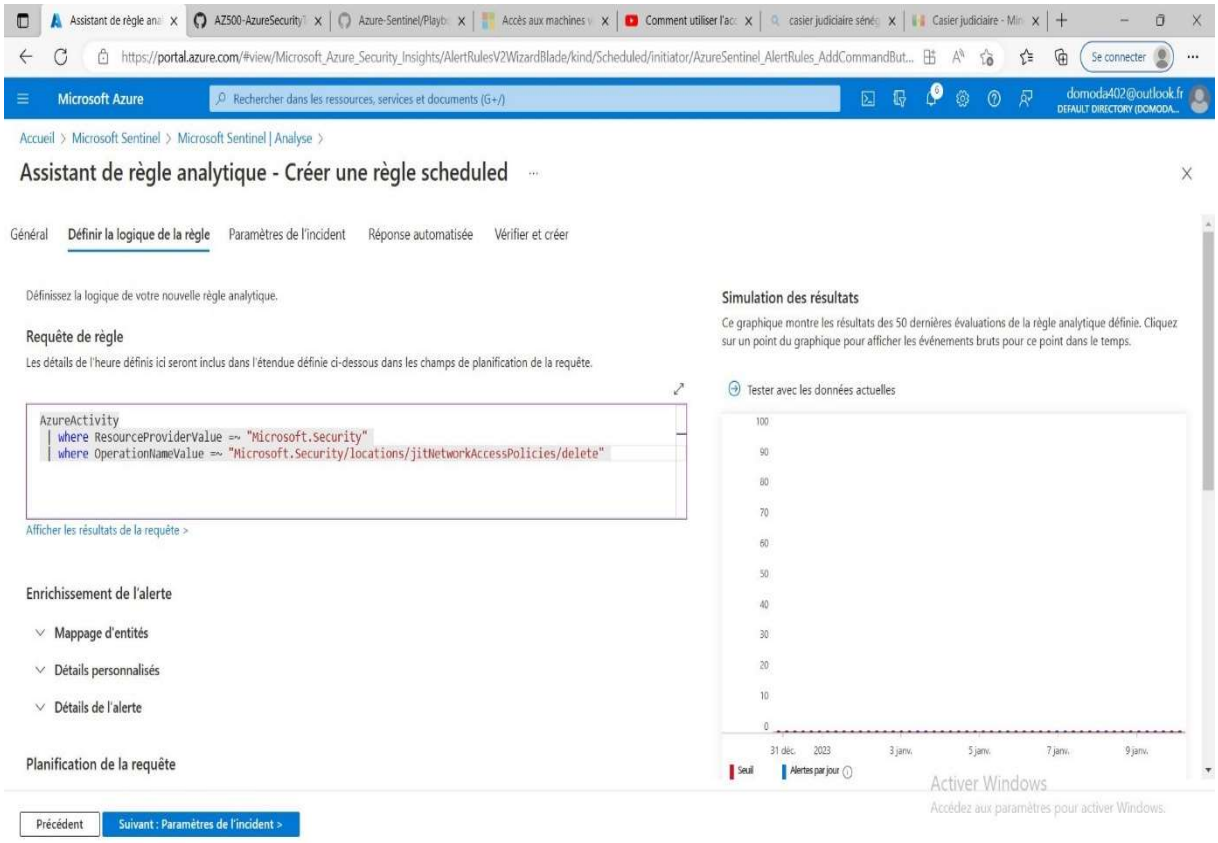


Figure 69: Cette règle identifie la suppression des stratégies d'accès aux machines JIT

- Pour les autres onglets, on laisse les paramètres par défaut et on valide pour créer la règle. Nous avons maintenant une nouvelle règle active appelée **djadji Playbook**. Si un événement identifié par la logique se produit, il en résultera une alerte de gravité moyenne, qui générera un incident correspondant.

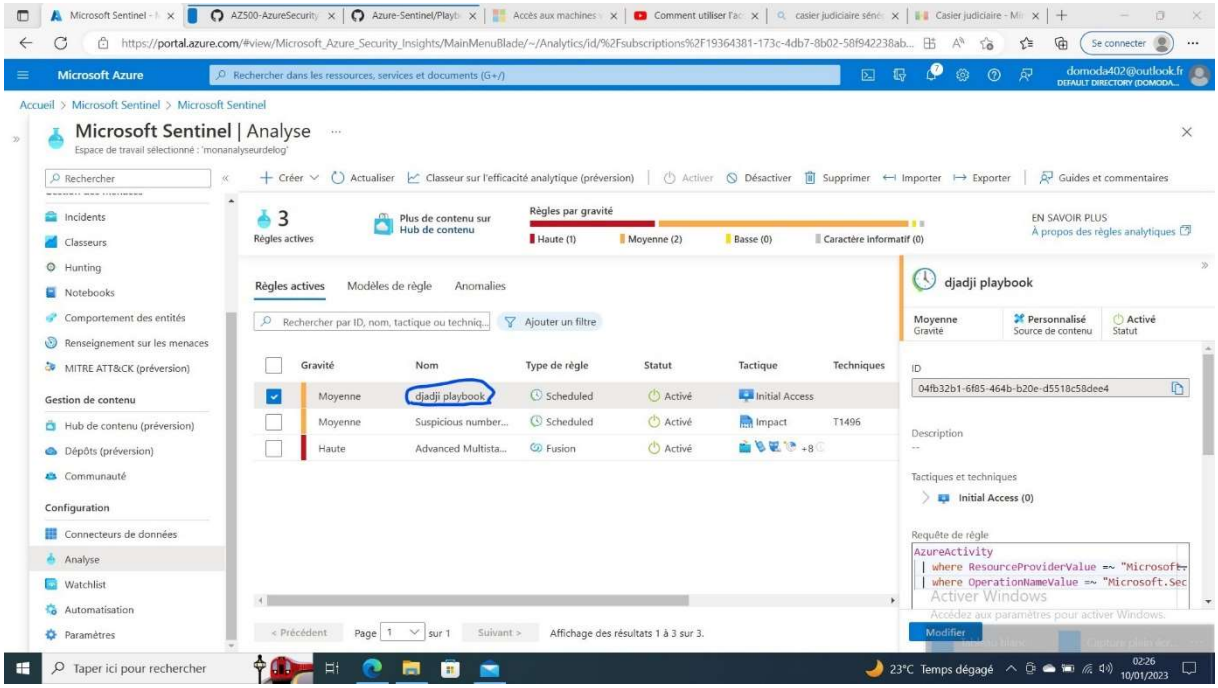


Figure 70: visualisation de la règle active appelée djadji Playbook

3.2 Tâche 6 : Invoquer un incident et passer en revue les actions associées

- Sur Microsoft Defender pour Cloud, Panneau Protection contre les charges de travail, cliquons sur la section Accès juste à temps aux machines virtuelles sous Protection avancée. Sur le côté droit de la ligne référençant la machine virtuelle myVM, cliquons sur le bouton de points de suspension, puis sur Supprimer.

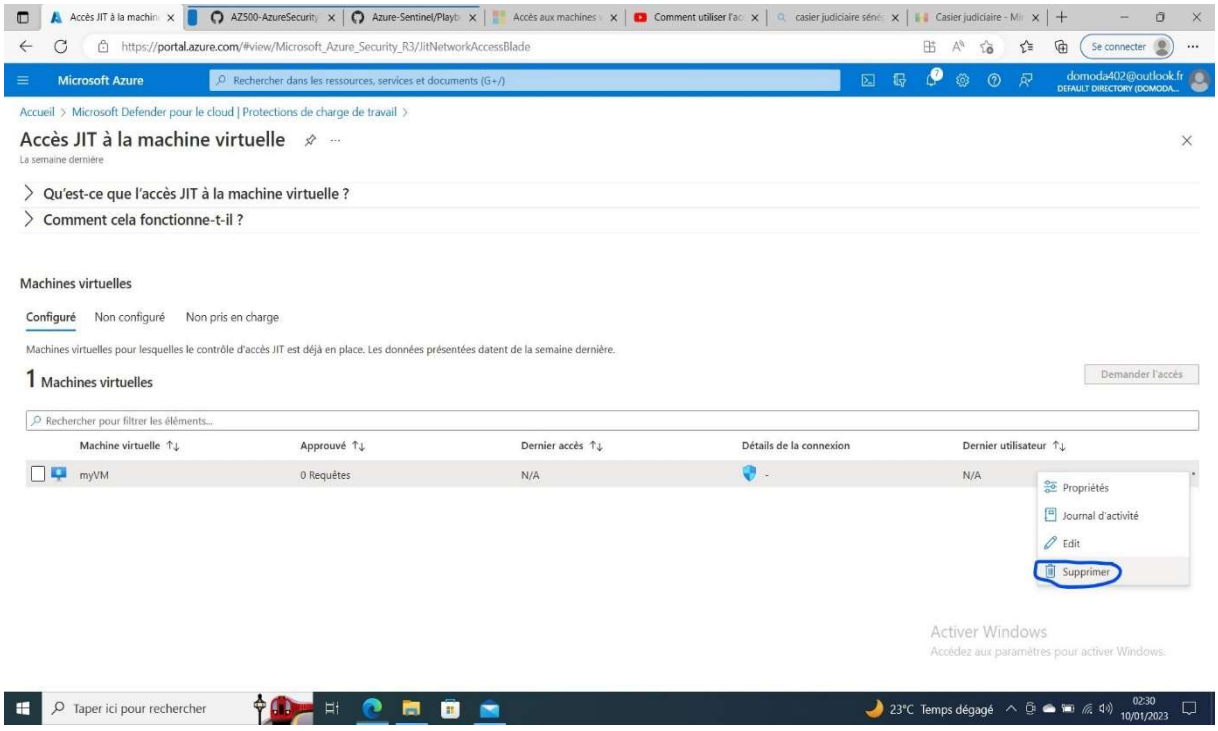


Figure 71: Invoquer un incident sur myVM

- Dans le portail Azure, dans la zone de texte Rechercher des ressources, des services et des documents en haut de la page du portail Azure, tapons Journal d'activité et appuyons sur la touche Entrée.

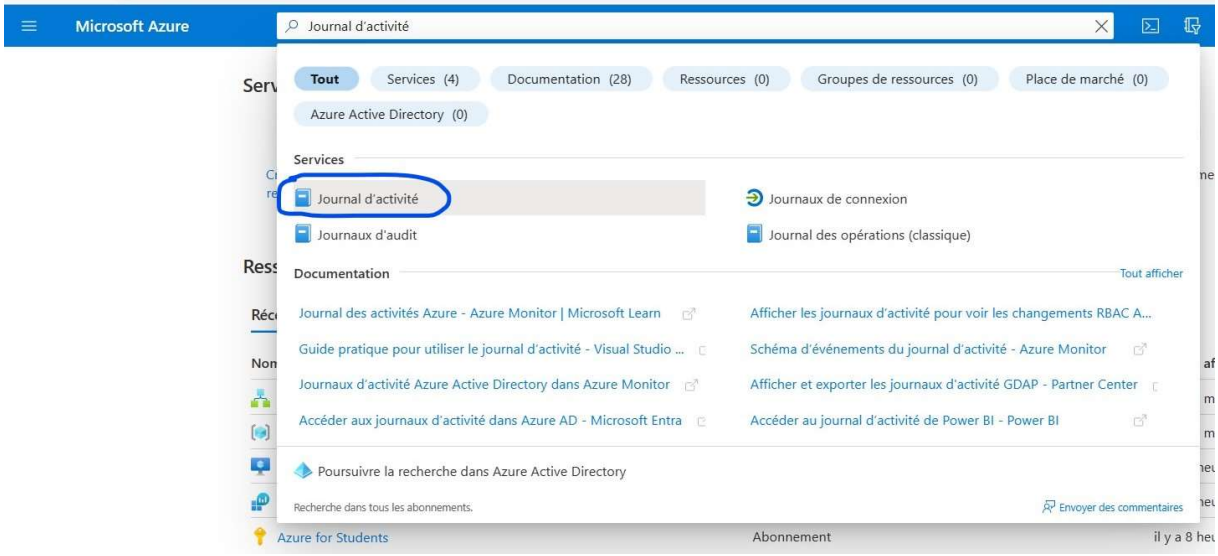


Figure 72: recherche de journal d'activité sur le portail azure

- En accédant au panneau Journal d'activité, nous pouvons noter une entrée **Supprimer les stratégies d'accès réseau JIT** qui apparait.

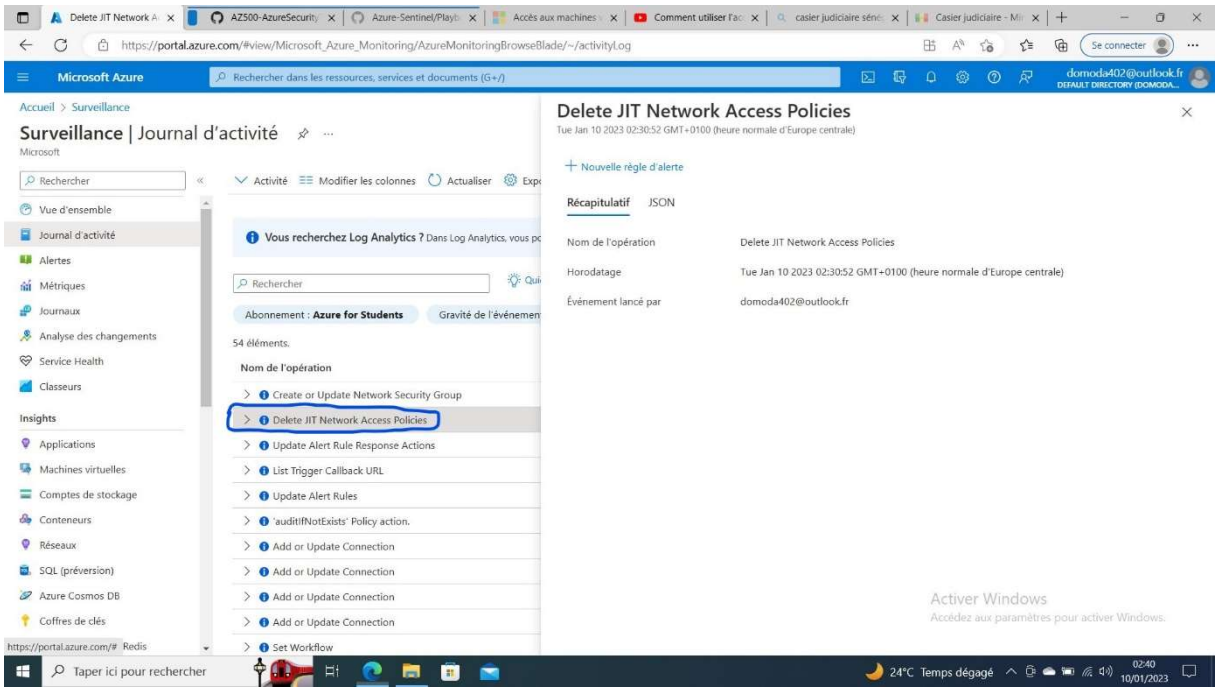


Figure 73: apparition de entrée Supprimer les stratégies d'accès réseau JIT

- Sur Microsoft Sentinel Vue d'ensemble, passons en revue le tableau de bord et vérifions qu'il affiche une alerte correspondant à la suppression de la stratégie d'accès aux machines virtuelles juste-à-temps. Nous pouvons apercevoir ci-dessous qu'une alerte à belle et bien était détecter.

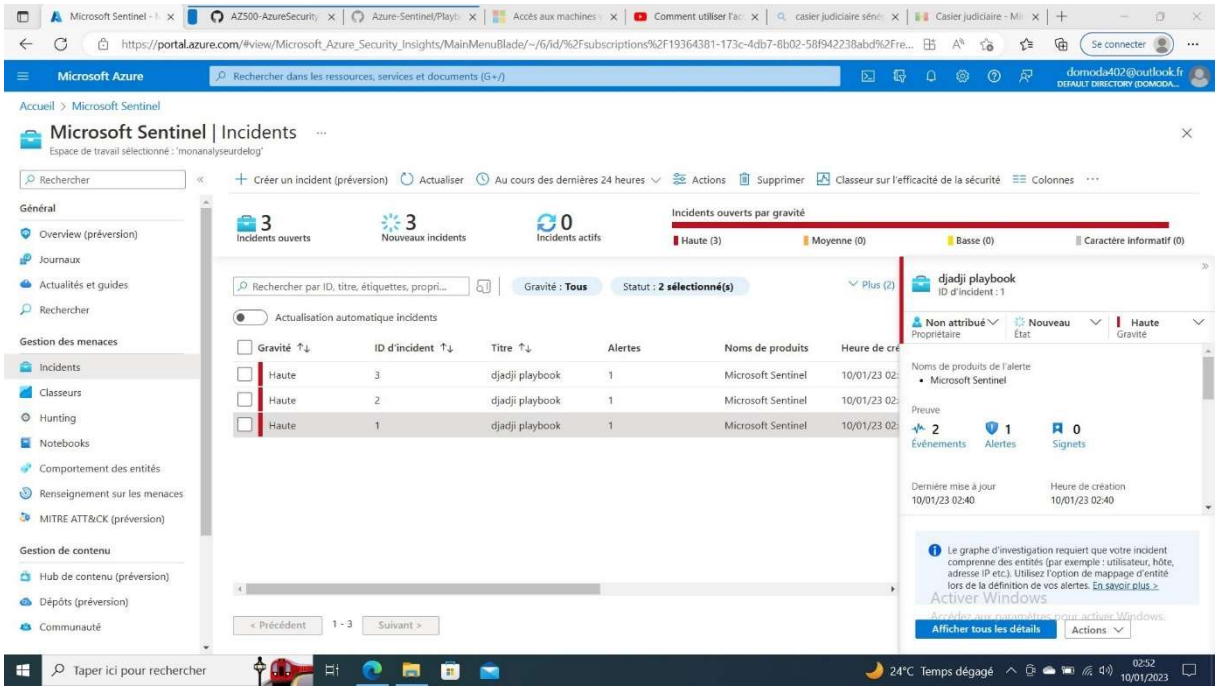


Figure 74: une alerte correspondant à la suppression de la stratégie d'accès aux machines virtuelles JIT

Nous avons créé un espace de travail Microsoft Sentinel, l'avons connecté aux journaux d'activité Azure, créé un playbook et des alertes personnalisées déclenchées en réponse à la suppression des stratégies d'accès aux machines virtuelles juste-à-temps, et vérifié que la configuration est valide. Maintenant pour aller plus loin votre équipe SOC à travers les informations fournit par Sentinel poussé l'investigation.

Conclusion

Le choix d'un fournisseur dépendant de plusieurs facteurs, il faudra prendre le temps de faire une étude approfondie afin de voir quel fournisseur satisfait le plus nos exigences. Cependant, la migration des données et des applications vers le cloud peut entraîner des préoccupations en matière de sécurité, en particulier en ce qui concerne la gestion des menaces, l'accès et la conformité réglementaire. Il est important de penser en amont les aspects liés à la sécurité de son environnement. Car comme nous venons de voir les menaces sont omni présent et de plus en plus sophistiqué. La surveillance en permanence est donc une nécessité. D'où la mise en place d'un système de Gestion de l'information et des événements de sécurité comme Microsoft Sentinel qui collabore avec des outils de collectes de données pour mieux détecter les incidents de sécurité au sein votre environnement cloud.

Bibliographie

[1] documentation sur GCP, disponible sur https://cloud.google.com/docs?hl=fr

[2] documentation sur AWS, disponible sur https://docs.aws.amazon.com/index.html

[3] documentation sur Azure, disponible sur https://azure.microsoft.com

[4] documentation sur Azure Monitor, disponible sur https://learn.microsoft.com/fr-fr/azure/azure-monitor/overview

[5] Hoby RATSITOBAINA, OAuth : Comment ça marche ?, 2014. Disponible sur : http://blog.netapsys.fr/ oauth-comment-ca-marche/comment-page-1

[6] TOOLS4EVER, Qu'est-ce que le Role Based Access Control (RBAC) ? Disponible sur : https://www. tools4ever.fr/logiciel/iam-solution-gestion-des-identites/ quest-ce-que-le-role-based-access-control

[7] Yann Desmarest, Identification et authentification dans le cloud avec SAML, 2015. Disponible sur : https://www.e-xpertsolutions.com/e-news/ identification-et-authentification-dans-le-cloud-avec-saml

[8] Systancia, Le Cloud Computing, Les différents modèles et niveaux de services du Cloud Computing. Disponible sur : http://www.systancia.com/fr/modeles-du-cloud-computing

[9] wikiversity, Cloud computing et entreprise : Les modèles de déploiement du Cloud, 2016. Disponible sur : https: //fr.wikiversity.org/wiki/Cloud_computing_et_entreprise/Les_mod%C3%A8les_de_d%C3%A9ploiement_du_Cloud

[10] Martin Gilje Jaatun, Cloud Computing First International Conference, CloudCom 2009 Beijing, China, December 2009 Proceedings, page 159, 2009. Disponible sur: https: //books.google.co.ma/books?id=VKHwHChUFtUC&pg=PR1&lpg=PR1&dq=Cloud+Comuting+First+International+Conference,+CloudCom+2009+Beijing,+China,+December+2009+Proceedings&source=bl&ots=2zK_t38pxt&sig=3nHW9BUKYVYSPh3GUNBWW2HECU4&hl=fr&sa=X&redir_esc=y#v=onepage&q=Cloud%20Computing%20First%20International%20Conference%2C%20CloudCom%202009%20Beijing%2C%20China%2C%20December%202009%20Proceedings&f=false

[11] CSA, The Treacherous 12, Cloud Computing Top Threats in 2016. Disponible sur: https://downloads. cloudsecurityalliance.org/assets/research/top-threats/ Treacherous-12_Cloud-Computing_Top-Threats.pdf

[12] Le cloud computing, Les différents types et niveaux de cloud computing. Disponible sur: http://www-igm.univ-mlv.fr/~dr/ XPOSE2009/cloudcomputing/types.html

[13] ACP, Analyses et Synthèses, Les risques associés au Cloud computing, 2013. Disponible sur : http://www.banque-france.fr/uploads/media/ 201307-Risques-associes-au-Cloud-computing_01.pdf

[14] K. Saurabh et B. Rajkumar, «NetworkCloudSim : Modelling Parallel Applications in Cloud Simulations,» Proceedings of the 4th IEEE International Conference on Utility and Cloud Computing, Victoria, Canada, n° %1105-113, 2011.

[15] A. Poggi, G. Rimassa et M. Tomaiuolo, «Multi-user and security support for multi-agent systems,» Proceedings of WOA, Dagli oggetti agli, 2001 .

[16] K. Govinda et E. Sathiyamoorthy, «Agent based security for cloud computing using obfuscation',,» International Conference On Modelling Optimization And Computing Procedia Engineering, vol. 38, p. 125–129, 2012.

[17] J. Rittinghouse et J. Ransome, «Cloud Computing: Implementation, Management, and Security,» Inc. Boca Raton, FL, USA, CRC Press, 2009, p. Chapter 6

[18] M. K. I., K. A. et A. M., «Cloud computing security: A survey,» Computers, vol. 3, n° %11, p. 1–35, 2014.

[19] R. SHIREY, « Internet security glossary,» version 2, 2007.

[20] P. RANE, Securing SaaS applications: a cloud security perspective for application providers, Information Security Management Handbook, vol. 5, 2010.

[21] R. CHOW, P. GOLLE, M. JAKOBSSON, E. Shi, J. Staddon, R. Masuoka et J. Molina, «Controlling data in the cloud: outsourcing computation without outsourcing control,» In : Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, pp. 85-90, 2009.

Annexes

A. Comparaisons des fournisseurs de cloud

Il existe plusieurs critères pour comparer les plateformes cloud d'Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP) :

- Couverture géographique : AWS est présent dans plus de 190 pays, Azure dans 140 pays et GCP dans plus de 100 pays.
- Gamme de services : AWS propose plus de 175 services, Azure propose plus de 600 services et GCP propose plus de 100 services.
- Coûts : Les coûts peuvent varier en fonction de l'utilisation, mais en général, AWS est considéré comme étant légèrement plus cher que les autres plateformes, tandis que GCP est souvent considéré comme étant le moins cher. Azure se situe généralement entre les deux.
- Intégration avec les produits Microsoft : Azure est une plateforme cloud intégrée à la suite de produits Microsoft, ce qui peut être un avantage pour les entreprises utilisant déjà les produits Microsoft.
- Machine learning et analyse de données : Toutes les trois plateformes proposent des services de machine learning et d'analyse de données, mais GCP est considéré comme étant particulièrement fort dans ce domaine.
- Soutien : Toutes les trois plateformes proposent une documentation détaillée et un soutien par téléphone et e-mail. Cependant, AWS est considéré comme étant le plus fort en matière de soutien.

En fin de compte, la plateforme cloud qui conviendra le mieux dépendra des besoins spécifiques de l'entreprise en termes de coûts, de gamme de services, d'intégration avec les produits existants et de soutien. Il est recommandé de faire une analyse approfondie des besoins de l'entreprise et de tester les différentes plateformes pour déterminer la meilleure solution.

B. Justificatif de notre choix sur Azure

Les raisons pour lesquelles Microsoft Azure peut être un choix avantageux pour certaines entreprises sont :

- Intégration avec les produits Microsoft : Azure est intégré à la suite de produits Microsoft, ce qui peut simplifier la migration des applications et des données vers le cloud. Par exemple, les développeurs peuvent utiliser Visual Studio, le système de gestion de source de code Microsoft, pour développer et déployer des applications dans Azure. Les entreprises peuvent également utiliser Azure Active

Directory pour gérer les identités et les accès des utilisateurs, ce qui peut simplifier la gestion des autorisations et la sécurité des données.

- Gamme de services : Azure propose plus de 600 services, ce qui signifie qu'il offre une gamme plus large de services que les autres plateformes. Cela peut être important pour les entreprises qui ont besoin de services spécifiques pour leurs opérations. Par exemple, Azure propose des services de base de données, de développement, de machine learning, d'analyse de données, de déploiement et de gestion de la mobilité.

- Conformité et sécurité : Azure est conforme à de nombreux standards de sécurité et de conformité, ce qui peut être important pour les entreprises soucieuses de la protection de leurs données. Azure prend en charge les normes de sécurité telles que ISO 27001, SOC 1, 2 et 3, et PCI DSS. Les entreprises peuvent également utiliser des services de sécurité tels que Azure Security Center pour surveiller la sécurité de leur environnement cloud.

- Outils de développement : Azure propose des outils de développement intégrés, notamment Visual Studio et GitHub, ce qui peut faciliter le développement et la gestion des applications. Les développeurs peuvent également utiliser des services de développement tels que Azure Devops pour planifier, développer, tester et déployer des applications dans le cloud.

- Soutien : Azure propose une documentation détaillée et un soutien par téléphone et e-mail, ce qui peut aider les entreprises à résoudre les problèmes rapidement. En outre, Azure propose des options de support premium pour les entreprises qui ont besoin de soutien supplémentaire.

- Partenariats et écosystème : Microsoft travaille étroitement avec un large éventail de partenaires pour offrir une gamme étendue de services et d'applications dans le cloud. Les entreprises peuvent également utiliser des services tiers proposés par des partenaires pour étendre les fonctionnalités d'Azure.

C. Fonctionnalité de sécurité réseaux offert par les réseaux virtuels :

Les réseaux virtuels et sous-réseaux virtuels dans Azure permettent à des ressources d'Azure de communiquer entre elles et avec d'autres ressources, tant locales qu'internet. Un réseau Azure peut-être considérer comme une extension de votre réseau local, connectant différentes ressources. Les réseaux virtuels Azure offrent des fonctionnalités clés telles que l'isolement, la communication internet, le routage et la filtration du trafic. Ils prennent en charge des points de terminaison publics et privés pour permettre la communication entre les ressources externes et internes. Les points de terminaison publics ont une adresse IP publique accessible partout dans le monde, tandis que les points de terminaison privés sont restreints à un réseau virtuel avec une adresse IP privée.

❖ **Isolement et segmentation**

Le réseau virtuel Azure vous permet de séparer votre infrastructure en plusieurs réseaux distincts pour une meilleure sécurité et une organisation plus efficace. Lors de la configuration d'un réseau virtuel, vous pouvez choisir entre utiliser des adresses IP publiques ou privées et définir une plage d'adresses IP uniquement utilisable dans ce réseau virtuel. Il est également possible de scinder ce réseau en sous-réseaux pour une gestion plus avancée des adresses IP. Pour la résolution de noms, vous avez le choix entre le service de résolution de noms intégré à Azure ou un serveur DNS interne ou externe.

❖ **Communications Internet**

Vous pouvez activer les connexions entrantes depuis Internet en attribuant une adresse IP publique à une ressource Azure ou en plaçant la ressource derrière un équilibreur de charge public.

❖ **Communiquer entre des ressources Azure**

Il est important de permettre une communication sécurisée entre les ressources Azure. Pour ce faire, vous pouvez utiliser deux méthodes :

- ✓ Connecter des ressources Azure, telles que des machines virtuelles, App Service Environment pour Power Apps, Azure Kubernetes Service, et des groupes de machines virtuelles identiques Azure, via des réseaux virtuels.
- ✓ Lier des ressources Azure telles que des comptes de stockage et des bases de données Azure SQL à des réseaux virtuels en utilisant des points de terminaison de service. Cette méthode permet d'améliorer la sécurité et d'assurer un routage optimal entre les ressources.

❖ **La communication avec des ressources locales**

Les réseaux virtuels Azure permettent de connecter différentes ressources ensemble, que ce soit dans votre environnement local ou sur votre abonnement Azure. Il existe trois moyens de maintenir cette connexion :

- ✓ Les connexions VPN point-à-site, où un ordinateur en dehors de votre organisation se connecte à votre réseau d'entreprise à travers une connexion VPN sécurisée.
- ✓ Les VPN site-à-site qui relient votre passerelle VPN local ou votre appareil VPN à la passerelle VPN Azure sur un réseau virtuel, donnant l'impression aux appareils Azure d'être sur le réseau local.
- ✓ Azure ExpressRoute qui offre une connexion privée dédiée et sécurisée vers Azure sans passer par Internet, idéale pour les environnements nécessitant une bande passante élevée et une sécurité renforcée.

- **Router le trafic réseau**

Par défaut, Azure dirige le trafic entre les sous-réseaux via les réseaux virtuels connectés, les réseaux locaux et Internet. Toutefois, vous pouvez également contrôler la façon dont le trafic est acheminé en utilisant des tables de routage ou le protocole BGP (Border Gateway Protocol). Les tables de routage vous permettent de créer des règles de routage personnalisées pour contrôler la façon dont les paquets sont acheminés entre les sous-réseaux, tandis que le BGP peut travailler avec les passerelles VPN Azure, le Serveur de routes Azure ou Azure ExpressRoute pour annoncer des routes BGP locales à des réseaux virtuels Azure.

- **Filtrer le trafic réseau**

Le filtrage du trafic entre les sous-réseaux sur Azure peut-être effectuer à l'aide de deux méthodes:

  - ✓ Les groupes de sécurité réseau qui permettent de définir des règles de sécurité d'entrée et de sortie pour contrôler le trafic.
  - ✓ Les Appliances virtuelles réseau qui sont des machines virtuelles spécialisées utilisées pour remplir une fonction réseau particulière, telle que la gestion de pare-feu ou d'optimisation WAN.

- **Connecter des réseaux virtuels**

Vous pouvez relier différents réseaux virtuels ensemble en utilisant le peering de réseaux virtuels. Ce processus permet à deux réseaux virtuels de se connecter directement l'un à l'autre sans avoir à passer par l'Internet public. Le trafic réseau échangé entre les réseaux appairés reste privé et est géré par le réseau principal Microsoft. Le peering vous permet de faire communiquer les ressources de chaque réseau virtuel et de créer un réseau interconnecté global à l'aide d'Azure, même si les réseaux virtuels sont situés dans des régions différentes.

Les routes définies par l'utilisateur (UDR) vous permettent de contrôler la façon dont les paquets sont acheminés entre les sous-réseaux d'un réseau virtuel ou entre les réseaux virtuels, vous offrant ainsi un meilleur contrôle sur le flux de trafic réseau.