TRAVAUX PRATIQUES – FILIÈRE INFRASTRUCTURE DIGITALE

M213 - Sécuriser un environnement Cloud propriétaire en ligne public

50,5 heures

SOMMAIRE

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

PARTIE 1

SE PRÉPARER POUR LA SÉCURITÉ DANS LE CLOUD

Dans ce module, vous allez :

- Connaitre les enjeux de sécurité Cloud
- Découvrir des aspects de sécurité Cloud

8,5 heures

ACTIVITE n°1

Réalisation d'une recherche Internet sur les enjeux de sécurité Cloud

Compétences visées :

- Développer l'activité de benchmarking
- Etablir un comparatif des clauses du contrat fournisseur Cloud
- Etablir une stratégie de sortie du Cloud Azure
- Etablir un comparatif des normes et standards de sécurité adoptés par les fournisseurs Cloud

Recommandations clés :

- Se référer au cours
- Utiliser des sources internet fiables

4,5 heures

CONSIGNES

Pour le formateur

- Initier les stagiaires à la réalisation d'une recherche sur internet
- Sensibiliser les stagiaires à l'utilisation des sources fiables et à noter les références pendant leur recherche sur internet
- Discuter les résultats de la recherche et proposer éventuellement qu'un stagiaire ou deux fassent un exposé devant ses camarades

Pour l'apprenant

- Travailler en groupe et partager l'information avec les collègues
- Répartir les tâches entre les membres du groupe pour faciliter le travail
- Discuter les résultats de la recherche entre le groupe
- Consolider et préparer un support de présentation synthétisant l'ensemble des tâches demandées

- En groupe de 3 à 4 personnes
- Des ordinateurs dotés d'une connexion internet, et sur lesquels MS PowerPoint est installé
- Un projecteur dans le cas d'une présentation

- Travail en groupe
- Qualité du livrable en terme du contenu
- Qualité du livrable en terme de présentation

Activité 1

Réalisation d'une recherche Internet sur les enjeux de sécurité Cloud

Réalisation d'une recherche Internet sur les enjeux de sécurité Cloud

Pour la réalisation de ce TP, vous allez devoir accomplir 3 tâches. Deux tâches communes et la 3ème tâche sera à traiter par groupe :

Tâche 1 : Réaliser une étude comparative des éléments Confidentialité, Sécurité et Disponibilité pour les fournisseurs Cloud Azure et Amazon (AWS).

Tâche 2 : Etablir une stratégie de sortie du Cloud Azure pour une entreprise souhaitant se retirer du Cloud.

Tâche 3 : Réaliser une recherche internet sur les normes et standards de sécurité adoptés par le top 4 des fournisseurs Cloud. Chaque groupe doit choisir un fournisseur à traiter :

- Normes et standards de sécurité au niveau du Cloud Azure
- Normes et standards de sécurité au niveau du Cloud Amazon
- Normes et standards de sécurité au niveau du Cloud Google
- Normes et standards de sécurité au niveau du Cloud Alibaba

Activité 1

Réalisation d'une recherche Internet sur les enjeux de sécurité Cloud

Eléments de réponse

Tâche 1 : Réaliser une étude comparative des éléments Confidentialité, Sécurité et Disponibilité pour les fournisseurs Cloud Azure et Amazon (AWS).

L'objectif est de comparer les clauses contractuelles pour les fournisseurs Azure et AWS pour les points suivants Confidentialité, Sécurité et Disponibilité.

Clauses	Azure	AWS
Confidentialité	**Vous choisissez l'emplacement de vos données** Lorsque vous utilisez Azure, vous choisissez l'emplacement de vos données. Via notre réseau de centres de données étendu et en constante expansion dans le monde entier, Microsoft offre la résidence des données et Azure vous permet de choisir parmi plus de 60 régions liées par l'un des plus grands réseaux interconnectés de la planète, qui inclut plus de 150 centres de données (et ce nombre ne cesse d'augmenter). Toutefois, quel que soit le lieu où vos données sont stockées, Microsoft ne contrôle ni ne limite les emplacements depuis lesquels vos utilisateurs finaux peuvent les consulter, les copier ou les déplacer. La plupart des services Azure vous permettent de spécifier la région dans laquelle vos données client sont stockées et traitées. Azure propose des outils qui vous aident à contrôler l'emplacement de vos données : par exemple, vous pouvez utiliser Azure Policy ou Azure Blueprint pour restreindre l'accès aux régions sélectionnées pour votre abonnement.	Confidentialité des données. Vous pouvez préciser les régions AWS dans lesquelles Votre Contenu sera stocké. Vous consentez au stockage et au transfert de Votre Contenu dans les régions AWS que vous sélectionnez. Nous n'accéderons pas à Votre Contenu et ne l'utiliserons pas, à moins que cela soit nécessaire pour maintenir ou fournir les Offres de Services, ou dans la mesure nécessaire pour respecter la loi ou une ordonnance exécutoire d'un organisme gouvernemental. Nous (a) ne divulguerons Votre Contenu à aucun gouvernement ou tiers ou (b) ne déplacerons pas Votre Contenu des régions AWS que vous avez sélectionnées ; sauf, dans chaque cas, dans la mesure nécessaire pour respecter la loi ou une ordonnance exécutoire d'un organisme gouvernemental. À moins que cela n'enfreigne une loi ou une ordonnance exécutoire d'un organisme gouvernemental, nous vous avertirons de toute exigence légale ou ordonnance décrite à la présente Clause 3.2. Nous utiliserons uniquement les Informations relatives à votre Compte conformément à l''Avis de Confidentialité et vous consentez à ladite utilisation. L''Avis de Confidentialité ne s'applique pas à Votre Contenu. https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement_French_Translation_2022-09-20.pdf
Sécurité	Azure met en place un ensemble de pratiques et stratégies de sécurité pour les Services en Ligne qui respectes : SSAE 18 SOC 1 Type II et SSAE 18 SOC 2 Type II https://www.microsoft.com/licensing/terms/fr-FR/product/PrivacyandSecurityTerms/all	Sécurité AWS. Sans préjudice de la Clause 10 ou de vos obligations en vertu de la Clause 4.2, nous instaurerons des mesures raisonnables et adaptées pour vous aider à sécuriser Votre Contenu à l'encontre de toute perte, accès ou divulgation, accidentel(le) ou illégal(e). Nous pouvons, périodiquement, modifier ou interrompre tout Service. Nous vous informerons en respectant un préavis d''au moins 12 mois si nous interrompons des fonctionnalités substantielles d'un Service que vous utilisez ou si nous modifions, avec une incompatibilité ascendante, une API visible par le client que vous utilisez, excepté qu'un tel avis ne pourra être exigé si la période de préavis de 12 mois (a) pose un problème lié aux Services ou nous pose un problème lié à la sécurité ou à la propriété intellectuelle, (b) est particulièrement contraignant au plan économique ou technique, ou (c) nous amène à enfreindre des exigences légales.
Disponibilité	Azure garantie un taux de disponibilité SLA par service offert : https://azure.microsoft.com/fr-fr/support/legal/sla/summary/	AWS garantie un taux de disponibilité SLA par service offert : https://aws.amazon.com/fr/legal/service-level-agreements/

PARTIE 1

Activité 1

Réalisation d'une recherche Internet sur les enjeux de sécurité Cloud

Eléments de réponse

Tâche 2 : Etablir une stratégie de sortie du Cloud Azure pour une entreprise souhaitant se retirer du Cloud.

La stratégie de sortie du Cloud devra être axée autour des 4 aspects clés suivants :

- ✓ **L'inventaire des plateformes :** Connaître son patrimoine est essentiel. Les stratégies de sortie ne s'appliquent souvent qu'aux fonctions critiques de l'entreprise. Il est donc important de savoir ce que vous avez en cours d'exécution dans quel Cloud – un inventaire Cloud à jour est d'une grande aide.
- ✓ **L'infrastructure open source et portabilité :** Les composants d'infrastructure open source tels que Kubernetes ou les clusters OpenShift ou les bases de données open source peuvent faciliter le passage d'un Cloud à l'autre. Plus vous utilisez de services propriétaires, plus il sera difficile d'adapter votre application pour qu'elle s'exécute dans un nouvel environnement Cloud.
- ✓ **Multi-Cloud dès le début :** Vu les délais important des négociations contractuelles entre les entreprises et les fournisseurs Cloud. Il est plus judicieux d'avoir des contrats établis avec plusieurs fournisseurs Cloud dès le début.
- ✓ **Blocage entreprise :** Même si, d'un point de vue technique, votre application peut facilement être déplacée vers un autre fournisseur Cloud. Si vous exécutez des applications Cloud à grande échelle, la configuration des environnements Cloud correspondants en transférant les autorisations et les configurations est extrêmement complexe.

PARTIE 1

Activité 1

Réalisation d'une recherche Internet sur les enjeux de sécurité Cloud

Eléments de réponse

Tâche 3 : Réaliser une recherche internet sur les normes et standards de sécurité adoptés par le top 4 des fournisseurs Cloud. Chaque groupe doit choisir un fournisseur à traiter :

- Normes et standards de sécurité au niveau du Cloud Azure (https://learn.microsoft.com/fr-fr/compliance/regulatory/offering-cis-benchmark)

Monde	Amérique	ASIE	EMEA
Point de référence CIS Attestation CSA-STAR Certification CSA-STAR Auto-évaluation CSA-STAR ISO 20000-1-2011 ISO 22301 ISO 27001 ISO 27017 ISO 27018 ISO 27701 ISO-9001 SOC 1 SOC 2 SOC 3 WCAG	CJIS CNSSI 1253 DFARS DoD IL2 DoD IL5 DoE 10 CFR Part 810 EAR FedRAMP FIPS 140-2 IRS 1075 ITAR Section NDAA 889 NIST 800-161 NIST 800-171 NIST 800-53 NIST 800-63 NIST CSF Section 508 VPATs PDPA Argentine Lois sur la confidentialité du Canada CCPA (États-Unis)	IRAP Australie GB 18030 Chine DJCP Chine (MLPS) TCS Chine Inde MeitY CS Mark Japon (Gold) ISMAP Japon My Number Act (Japon) K-ISMS Corée ISPC Nouvelle-Zélande MTCS Singapour	EU EN 301 549 EU ENISA IAF RGPD de l'UE Clauses contractuelles types de l'UE C5 Allemagne IDW PS 951 Allemagne IT Grundschutz Workbook Allemagne BIR 2012 Pays-Bas Localisation de données personnelles Russie ENS High Espagne LOPD Espagne DESC Émirats arabes unis Cyber Essentials plus Royaume-Uni G-Cloud Royaume-Uni PASF Royaume-Uni

PARTIE 1

Activité 1

Réalisation d'une recherche Internet sur les enjeux de sécurité Cloud

Eléments de réponse

Tâche 3 : Normes et standards de sécurité au niveau du Cloud Amazon AWS (https://aws.amazon.com/fr/compliance/programs/)

Monde	Amérique	ASIE	Europe et Afrique
CSA CyberGRX CyberVadis ISO 9001 ISO 22301 ISO 27001 ISO 27017 ISO 27701 ISO 27018 PCI DSS, niveau 1 SOC 1 SOC 2 SOC 3	CCCS CJIS Guide des exigences de sécurité (SRG) FedRAMP FERPA FIPS FISMA GxP HIPAA HITRUST CSF ITAR MPAA Article 508 du VPAT NIST LPRPDE Règle SEC 17a-4(f)	FinTech Directives concernant les informations médicales FISC MTCS niveau 3 IRAP NISC K-ISMS ISMAP OSPAR	HDS C5 CISPE Rapport de la FINMA ISAE 3000 type 2 G-Cloud GSMA Cyber Essentials Plus ENS High PiTuKri Rapport ISAE 3000 de type II TISAX

PARTIE 1

Activité 1

Réalisation d'une recherche Internet sur les enjeux de sécurité Cloud

Eléments de réponse

Tâche 3 : Réaliser une recherche internet sur les normes et standards de sécurité adoptés par le top 4 des fournisseurs Cloud. Chaque groupe doit choisir un fournisseur à traiter :

- Normes et standards de sécurité au niveau du Cloud Google (https://cloud.google.com/security/compliance/offerings#/regions=Global)

Google Cloud offre une gamme très large de norme et standards (148) de conformité de sécurité réparties par région et industrie :

- Global
- Asie
- Canada
- EMEA
- Amérique latine
- USA

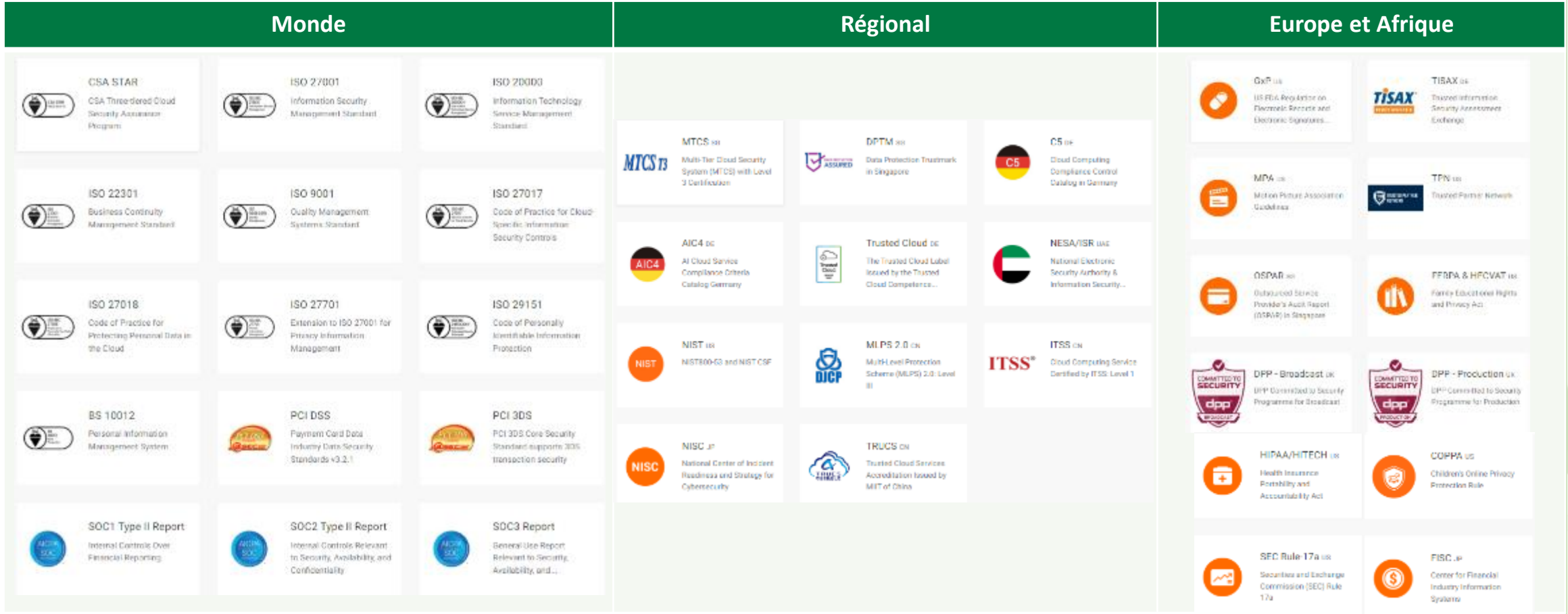
PARTIE 1

Activité 1

Réalisation d'une recherche Internet sur les enjeux de sécurité Cloud

Eléments de réponse

Tâche 3 : Normes et standards de sécurité au niveau du Cloud Alibaba (https://www.alibabacloud.com/fr/trust-center/compliance?spm=a2c6w.11657460.4547953020.1.5f87e561oxIAWW)



PARTIE 1

ACTIVITE n°2

Travaux pratiques sur les aspects de sécurité Cloud

Compétences visées :

- Développer l'activité de benchmarking
- Etablir un comparatif des clauses du contrat fournisseur Cloud
- Etablir une stratégie de sortie du Cloud Azure
- Etablir un comparatif des normes et standards de sécurité adoptés par les fournisseurs Cloud

Recommandations clés :

- Se référer au cours
- Utiliser des sources internet fiables

4 heures

CONSIGNES

Pour le formateur

- Initier les stagiaires à la réalisation d'une recherche sur internet
- Sensibiliser les stagiaires à l'utilisation des sources fiables et à noter les références pendant leur recherche sur internet
- Discuter les résultats de la recherche et proposer éventuellement qu'un stagiaire ou deux fassent un exposé devant ses camarades

Pour l'apprenant

- Travailler en groupe et partager l'information avec les collègues
- Répartir les tâches entre les membres du groupe pour faciliter le travail
- Discuter les résultats de la recherche entre le groupe
- Consolider et préparer un support de présentation synthétisant l'ensemble des tâches demandées

- En groupe de 3 à 4 personnes
- Des ordinateurs dotés d'une connexion internet, et sur lesquels MS PowerPoint est installé
- Disposer d'un abonnement Cloud Azure Gratuit ou Payant
- Connaissance basic du langage JavaScript

- Travail en groupe
- Qualité du livrable en terme du contenu et présentation
- Travaux pratiques opérationnels

Activité 2

Réalisation d'une recherche Internet sur les aspects de sécurité Cloud

PARTIE 1

Réalisation d'une recherche Internet et d'un TP sur les aspects de sécurité Cloud

Pour la réalisation de ce TP, vous allez devoir accomplir 2 tâches par groupe :

Tâche 1 : Réaliser un benchmark des outils natifs de gestion de la posture de sécurité Cloud (CSPM) disponibles chez les fournisseurs Cloud Azure et Google Cloud.

Tâche 2 : Une entreprise développe ses activités au niveau du Cloud Azure moyennement le déploiement d'applications Web JavaScript.

- Quel est le meilleur moyen pour protéger les clés et chaines de connexion Bd au niveau d'Azure ?
- Procéder à la création d'une machine virtuelle Linux au niveau d'Azure ainsi que le déploiement d'une application JavaScript sandalone permettant de récupérer un secret depuis Azure key vault. Les actions devront être réalisées via les commands Azure CLI.

Indices :

1. Création d'un coffre de clés
2. Stocker un secret dans Key Vault
3. Créer une machine virtuelle Azure Linux et Installer les bibliothèques **Node.js et npm**
4. Activer une identité managée pour la machine virtuelle
5. Octroyer les autorisations nécessaires à l'application console pour lire les données provenant de Key Vault
6. Récupérer un secret à partir de Key Vault

Activité 2

Réalisation d'une recherche Internet sur les aspects de sécurité Cloud

Eléments de réponse : Tâche 1

L'objectif recherché à travers cette action et de réaliser une étude comparative des principales fonctionnalités entres les deux solutions **Microsoft Defender pour Azure** et **de Security Command Center pour Google Cloud**.

L'étude comparative devra comprendre les offres de tarifications disponibles ainsi qu'une comparaison de la tarification entre les deux services pour un abonnement similaire avec les mêmes ressources.

- Security Commande Center : https://cloud.google.com/security-command-center/
- Microsoft Defender :
  - Fonctionnalités : https://learn.microsoft.com/fr-fr/azure/defender-for-cloud/defender-for-cloud-introduction
  - Tarification : https://azure.microsoft.com/fr-fr/pricing/details/defender-for-cloud/?cdn=disable#pricing

PARTIE 1

Activité 2

Réalisation d'une recherche Internet sur les aspects de sécurité Cloud

Eléments de réponse : Tâche 2

1. Création d'un coffre de clés :

   ❖ Création Ressource Groupe et région : az group create --name **"Nom-resource-groupe"** -l **"EastUS"**

   ❖ Création Azure keyVault : az keyvault create --name **"your-unique-keyvault-name"** -g **"Nom-resource-groupe"**

2. Stocker un secret dans Key Vault :

   ❖ az keyvault secret set --vault-name **"your-unique-keyvault-name"** --name **"mySecret"** --value **"Success!"**

3. Créer une machine virtuelle Azure Linux :

   ❖ az vm create --resource-group **"Nom-resource-groupe"** --name **"myVM"** --image **"UbuntuLTS"** --admin-username **"azureuser"** --generate-ssh-keys

4. Activer une identité managée pour la machine virtuelle :

   ❖ az vm identity assign --name **"myVM"** --resource-group **"Nom-resource-groupe"**

   Notez l'identité affectée par le système qui est affichée dans le code suivant. La sortie de la commande ci-dessus doit être la suivante :

   { "systemAssignedIdentity": **"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",**

   "userAssignedIdentities": {}}

5. Octroyer les autorisations nécessaires à l'application console pour lire les données provenant de Key Vault :

   ❖ az keyvault set-policy --name **"your-unique-keyvault-name"** --object-id **"systemAssignedIdentity"** --secret-permissions get list

6. Récupérer un secret à partir de Key Vault

   Se connecter à la machine virtuelle : ssh azureuser@<PublicIpAddress>

PARTIE 1

Activité 2

Réalisation d'une recherche Internet sur les aspects de sécurité Cloud

Eléments de réponse : Tâche 2

7. Installer des bibliothèques **Node.js et npm** sur la machine virtuelle :

   ❖ Sur la machine virtuelle, installez les deux bibliothèques npm que nous utiliserons dans notre script JavaScript : @azure/keyvault-secrets et @azure/identity.

   a) Dans le terminal SSH, installez Node.js et npm avec les commandes suivantes :

      ❖ curl -sL https://deb.nodesource.com/setup_14.x | sudo -E bash - && sudo apt-get install -y nodejs

   b) Créez un répertoire d'applications et initialisez le package Node.js :

      ❖ mkdir app && cd app && npm init -y

   c) Installez les packages de service Azure à l'aide de npm :

      ❖ npm install @azure/keyvault-secrets @azure/identity

8. Créez et modifiez le fichier JavaScript standalone :

   i. Sur la machine virtuelle dans le répertoire app, créez un fichier JavaScript nommé **index.js .**

      ❖ touch index.js

   ii. Ouvrez le fichier avec un éditeur de texte vim :

      ❖ vim index.js

   iii. Copiez le code suivant en remplaçant **your-unique-keyvault-name** par le nom de votre coffre de clés, et collez-le dans l'éditeur vim :

PARTIE 1

Activité 2

Réalisation d'une recherche Internet sur les aspects de sécurité Cloud

Eléments de réponse : Tâche 2

```
// index.js
const { SecretClient } = require("@azure/keyvault-secrets");
const { DefaultAzureCredential } = require("@azure/identity");
 // Your Azure Key Vault name and secret name
 const keyVaultName = "<your-unique-keyvault-name>";
 const keyVaultUri = `https://${keyVaultName}.vault.azure.net`;
 const secretName = "mySecret";
 // Authenticate to Azure
const credential = new DefaultAzureCredential();
const client = new SecretClient(keyVaultUri, credential);
 // Get Secret with Azure SDK for JS
 const getSecret = async (secretName) => { return (await client.getSecret(secretName)).value; }
getSecret("mySecret").then(secretValue => {
 console.log(`The value of secret 'mySecret' in '${keyVaultName}' is: '${secretValue}'`);
}).catch(err => {
 console.log(err);
 })
```

iv. Enregistrez le fichier avec **:qw!**

9. Exécuter l'application standalone Node.js

Node index.js The value of secret **'mySecret'** in **'your-unique-keyvault-name'** is: **'Success!'**

10. Nettoyer les ressources :

- az group delete -g **"Nom-resource-groupe"**

PARTIE 1

PARTIE 2

ADOPTER UNE INFRASTRUCTURE CLOUD SÉCURISÉE

Dans ce module, vous allez :

- Procéder au déploiement des mécanismes de sécurité des VM dans le Cloud

33 heures

ACTIVITÉ 1

QCM sur le système d’identité et d’authentification Azure

Compétences visées :

- Approfondir les connaissances sur la gestion des identités et l’Active Directory Azure.

Recommandations clés :

- Lire le support de cours

4 heures

CONSIGNES

1. Pour le formateur

- Connaissances solide de la sécurité, Conformité et identité sur le Cloud Azure
- Débloquer les stagiaires en cas de difficulté
- Laisser un peu de temps aux stagiaires pour qu'ils puissent réaliser les tâches eux-mêmes
- Demander des explications quant aux réponses fournies

2. Pour l'apprenant

- Lire attentivement les questions.
- En cas de problème ou blocage, le faire savoir à votre formateur
- Parcourir les réponses proposées
- Comparer vos réponses à celles proposées pour évaluer votre niveau de compréhension du cours

3. Conditions de réalisation :

- Seul
- Des ordinateurs dotés d'une connexion internet
- Un projecteur dans le cas d'une présentation à faire par le formateur pour présenter les réponses

4. Critères de réussite :

- +70% de réponses correctes

Activité 1
QCM sur le système d'identité et d'authentification Azure

PARTIE 2

QCM

1. Azure AD fournit une _____ .

A. Authentification de base

B. Authentification fédérée

C. Authentification synchronisée

D. Toutes les options

2. Azure AD fournit _____.

A. Un accès mobile (à distance) sécurisé aux applications sur site.

B. Une authentification unique

C. Un accès n'importe où et n'importe quel appareil

D. Toutes les options

3. RBAC peut être utilisé _____.

A. Pour contrôler l'autorisation d'accès aux applications

B. Uniquement pour l'administration

C. Pour contrôler les autorisations d'accès aux applications et l'administration

D. Aucune des options

Activité 1
QCM sur le système d'identité et d'authentification Azure

PARTIE 2

QCM

4. Vous envisagez d'implémenter la gestion des groupes en libre-service dans Microsoft Azure. Qui est responsable de l'approbation des demandes des utilisateurs pour rejoindre un groupe ?

A. Un co-administrateur

B. Un administrateur de domaine

C. Un propriétaire de groupe

D. Un administrateur de services

5. Si vous créez un utilisateur dans Azure AD, il s'appelle _____ Identité.

A. Domaine

B. Synchroniser

C. Fédéré

D. Cloud

6. Quels sont les trois types de contrôles RBAC (Role Basic Access) dans Microsoft Azure ?

A. Abonnement

B. Groupe de ressources

C. Ressource

D. Toutes les options

Activité 1
QCM sur le système d'identité et d'authentification Azure

PARTIE 2

QCM

7. Qui peut gérer l'accès aux abonnements Azure et aux groupes de gestion dans le locataire ?

A. Administrateur global et Propriétaire

B. Administrateur global et contributeur

C. Lecteur mondial et contributeur

D. Administrateur d'applications

8. Qui peut gérer tous les aspects d'Azure AD et des services Microsoft qui utilisent les identités Azure AD ?

A. Lecteur mondial

B. Administrateur global

C. Propriétaire du groupe

D. Administrateur d'applications

9. Les rôles _____ sont utilisés pour accorder l'accès aux actions privilégiées dans Azure AD.

A. Administratif

B. RBAC

C. Utilisateur

D. Membre

Activité 1
QCM sur le système d'identité et d'authentification Azure

QCM

10. Pour créer un rôle personnalisé, votre organisation a besoin d'Azure AD Premium _____.

A. P1

B. P2

C. Soit P1 ou P2

D. P1 et P2

11. Si le compte sur le site est désactivé, combien de temps faut-il pour accéder au compte cloud ?

A. 300 minutes

B. 500 minutes

C. 100 minutes

D. Aucune des options

12. Dans Azure, la gestion des groupes inclut _____.

A. Attribution d'un propriétaire de groupe

B. Création d'un groupe

C. Ajouter des utilisateurs au groupe

D. Toutes les options

PARTIE 2

Activité 1
QCM sur le système d'identité et d'authentification Azure

PARTIE 2

QCM

13. Quel est le nombre d'attributions de rôles par abonnement dans Azure ?

A. 100 attributions de rôles

B. 1000 attributions de rôles

C. 2000 attributions de rôles

D. 50 attributions de rôles

14. Combien d'applications cloud peuvent être associées à une stratégie d'accès conditionnel Azure AD ?

A. 10 000 objets

B. 50 000 Objets

C. 500 objets

D. 5000 objets

15. Quel est l'avantage significatif pour l'utilisateur obtenu en mettant en œuvre l'intégration d'applications SaaS ?

A. Authentification unique aux applications SaaS

B. Accès anonyme aux applications SaaS

C. Accès multi-comptes aux applications SaaS

D. Accès multi-niveaux aux applications SaaS

Activité 1
QCM sur le système d'identité et d'authentification Azure

PARTIE 2

QCM

16. Un nom de domaine est une partie importante de l'identifiant de _____.

A. Nom d'utilisateur ou adresse e-mail

B. Adresse pour un groupe

C. URI d'ID d'application pour une application

D. Toutes les options

17. Pour quels types de comptes la réécriture du mot de passe fonctionne-t-elle ?

A. Identifiants synchronisés

B. ID de domaine

C. ID cloud

D. Toutes les possibilités

18. Lequel des éléments suivants a le niveau d'accès le plus élevé dans le portail Azure ?

A. Administrateur global

B. Administrateur d'applications

C. Administrateur d'utilisateurs

D. Propriétaire de l'abonnement

E. Contributeur d'abonnement

Activité 1
QCM sur le système d'identité et d'authentification Azure

QCM

19. Quels sont les deux types d'utilisateurs de base dans Azure AD ?

A. Membre

B. Utilisateur et inviter un utilisateur

C. Accéder à l'administrateur

D. Membre et Utilisateur

20. Le nom de domaine de base est principalement destiné à être utilisé comme mécanisme d'amorçage jusqu'à ce qu'un nom de domaine personnalisé soit vérifié.

A. Vrai

B. Faux

21. Quel est l'avantage du contrôle d'accès de base de rôle (RBAC) dans Microsoft Azure ?

A. Gestion de groupe/rôle

B. Grandes attributions d'autorisations

C. Attribution d'autorisations de gestion granulaire

D. Gestion des services/abonnements

PARTIE 2

Activité 1
QCM sur le système d'identité et d'authentification Azure

QCM

22. Le domaine de base d'Azure AD se présente sous la forme _____.

A. sample01.onmicrosoft.com

B. exemplexyz.domain.onmicrosoft.com

C. abc123.azure.microsoft.com

D. Aucune des options

23. Contoso.com est votre domaine personnalisé vérifié, alors l'UPN de l'utilisateur1 sera _____.

A. utilisateur1@contoso.com

B. utilisateur1@contoso.microsoft.com

C. utilisateur1@contoso.onmicrosoft.com

24. Pour gérer Azure Ad, le privilège requis est _____.

A. Administrateur global

B. Administrateur de services

C. Administrateur d'entreprise

D. Administrateur AD

PARTIE 2

QCM

25. Quel type d'applications de galerie SaaS prend en charge le provisionnement automatique de Microsoft Azure Active Directory ?

A. Applications Windows

B. Applications publiées

C. Applications en vedette

D. Applications intégrées

26. Qu'est-ce que la forme complète d'Azure ?

A. Expérience de libération d'upwelling en zone aurorale

B. Expérience de libération Auroral Zero Upwelling

27. Azure AD n'est pas disponible dans Azure Free Edition.

A. Vrai

B. Faux

Activité 1
QCM sur le système d'identité et d'authentification Azure

QCM

28. Vous devez choisir entre utiliser un service d'authentification multifacteur (MFA) sur site et un service basé sur le cloud hébergé dans Azure. Parmi les fonctionnalités suivantes, lesquelles sont disponibles uniquement dans le service MFA sur site ?

A. IP de confiance

B. Sécurisation des applications SaaS dans la galerie d'applications

C. Alertes à la fraude

D. SMS bidirectionnel

29. Votre entreprise utilise O365. L'administrateur de locataire s'inscrit à un abonnement Azure gratuit et crée un locataire Azure Active Directory (Azure AD). Il associe ensuite le locataire Azure AD à l'abonnement Azure. L'authentification multifacteur (MFA) n'est pas activée. Vous souhaitez activer la fonction de réinitialisation de mot de passe en libre-service pour vos utilisateurs cloud. Laquelle des affirmations ci-dessous est vraie concernant votre locataire et la fonctionnalité de réinitialisation de mot de passe en libre-service ?

A. Vous ne pouvez pas activer cette fonctionnalité tant que vous n'avez pas effectué la mise à niveau vers un abonnement Premium Azure.

B. Vous ne pouvez pas activer cette fonctionnalité tant que vous n'avez pas effectué la mise à niveau vers un abonnement Azure de base.

C. La fonction de réinitialisation de mot de passe en libre-service est disponible, car elle fait partie de votre licence O365 payante

D. Vous ne pouvez pas activer cette fonction tant que vous n'avez pas configuré MFA.

PARTIE 2

Activité 1
QCM sur le système d'identité et d'authentification Azure

PARTIE 2

QCM

30. Votre entreprise utilise Windows Azure et a publié plusieurs applications. Votre équipe réseau vous a informé qu'il y a beaucoup de trafic provenant d'un sous-réseau spécifique. Vous pensez que l'une des applications les plus couramment utilisées peut être à blâmer. Vous devez vérifier quelles applications sont les plus utilisées et d'où provient le trafic. À partir de quelle lame du portail Azure devez-vous commencer votre recherche ?

A. Azure Active Directory

B. Utilisateurs et groupes

C. Applications d'entreprise

D. Services d'applications

31. Votre réseau contient un domaine Active Directory Domain Services (AD DS) nommé contoso.com et un domaine Azure Active Directory (Azure AD) nommé contoso.onmicrosoft.com. Vous utilisez des stratégies de contrôle d'accès basées sur les rôles (RBAC) pour vérifier qui a des droits dans l'abonnement Azure. Vous êtes un administrateur global et avez le rôle intégré « propriétaire ». Un membre de votre équipe nommé Mary doit être autorisée à créer et à gérer tous les objets de l'abonnement, mais ne doit pas être en mesure d'ajouter ou de supprimer des attributions de rôle. Vous devez donner à Mary uniquement les droits dont elle a besoin. Cela doit être accompli avec le moins d'efforts administratifs. Que devez-vous faire ?

A. Ajouter Marie au rôle de propriétaire

B. Créer un rôle RBAC personnalisé pour Mary

C. Ajouter Marie au rôle Contributeur

D. Ajouter Marie au rôle de lecteur

Activité 1
QCM sur le système d'identité et d'authentification Azure

PARTIE 2

QCM

32. Vous êtes l'administrateur de l'abonnement Azure de votre entreprise et le locataire Azure Active Directory (Azure AD). Votre entreprise dispose d'un Active Directory sur site. Votre patron vous demande de faire des recherches, permettant aux utilisateurs de l'entreprise d'accéder aux applications SaaS (Software as a Service) de la ligne d'activité (LOB) en utilisant les règles d'accès conditionnel. Vous devez vous assurer que votre locataire remplit les conditions préalables pour l'accès conditionnel aux applications SaaS. Quel est le niveau d'abonnement Azure le plus bas requis pour activer l'accès conditionnel aux applications SaaS ?

A. Abonnement Azure gratuit

B. Abonnement Azure Premium

C. Licences O365 payantes

D. Abonnement Azure Basic

33. Votre entreprise a un abonnement Azure. Vous créez 5 groupes de ressources dans l'abonnement : RG1, RG2, RG3, RG4 et RG5. Vous souhaitez donner à un partenaire nommé John le droit de gérer entièrement toutes les ressources de RG3. Le Live ID de John est john@outlook.com. John ne doit pas être en mesure de gérer les ressources d'un autre groupe de ressources. Que devrais tu faire?

A. Connectez-vous au portail Azure, accédez à RG3 et ajoutez le Live ID de John en tant que propriétaire.

B. Ajoutez John à votre Azure Active Directory. Cliquez sur l'abonnement et ajoutez la connexion Azure de John en tant que propriétaire.

C. Connectez-vous au portail Azure, cliquez sur Abonnement et ajoutez l'identifiant Live de John en tant que propriétaire.

D. Ajoutez John à votre Azure Active Directory. Accédez à RG3 et ajoutez la connexion Azure de John en tant que propriétaire.

Activité 1
QCM sur le système d'identité et d'authentification Azure

Eléments de réponse : QCM

1. D
2. D
3. B
4. C
5. D
6. D
7. A
8. B
9. A
10. C
11. D
12. D
13. C
14. B
15. A

PARTIE 2

Eléments de réponse : QCM

16. D
17. A
18. A
19. D
20. A
21. A
22. A
23. A
24. D
25. A
26. A
27. B
28. D
29. C
30. C

Eléments de réponse : QCM

31. B

32. D

33. D

ACTIVITÉ 2

Implémenter les mécanismes de sécurité des VM

Compétences visées :

- Déployer les règles de renforcement de la sécurité des VM sur le Cloud

Recommandations clés :

- Appréhender les mécanismes de sécurité des VM

6 heures

CONSIGNES

1. Pour le formateur

- Connaissances solide du fonctionnement des VM au niveau du Cloud
- Maitrise des aspect sécurité des VM

2. Pour l’apprenant

- Travailler en groupe et partager l’information avec les collègues
- Avoir des connaissances avancées sur l'utilisation du Cloud Azure volet machine virtuelle

3. Conditions de réalisation :

- Des ordinateurs dotés d’une connexion internet
- Disposer d’un abonnement Cloud Azure Gratuit ou Payant.

4. Critères de réussite :

- Répondre aux différentes questions soulevées au niveau de l’énoncé
- Travail en groupe
- Qualité du livrable en terme du contenu et présentation
- Travaux pratiques opérationnels

Activité 2
Implémenter les mécanismes de sécurité des VM

Travail demandé

Une entreprise souhaite procéder au déploiement d'une solution répartie composée de plusieurs machines virtuelles au niveau du Cloud Azure. Vu le secteur d'activité critique de l'entreprise, la solution ainsi que les machines virtuelles doivent être disponibles et opérationnelles 24h/24h 7J/7J avec un niveau de sécurité élevé.

Tâche 1 : Indiquer les mécanismes que doit déployer l'entreprise pour assurer la haute disponibilité ainsi qu'un bon fonctionnement de la solution. Fournir une définition des concepts identifiés.

Tâche 2 : Expérimenter les concepts identifiés précédemment à travers la création de VMs Azure. En indiquant les étapes de paramétrage;

Tâche 3 : Sachant que la solution effectue l'envoi des notifications par mail en utilisant le protocole SMTP sécurisé et expose une interface Web accessible over internet via Https. Indiquer et implémenter la matrice des flux (sortant et entrant) à adopter pour la VM applicative;

Tâche 4 : Indiquer les mesures de sécurité qui seront déployées pour assurer une sécurité renforcée de la VM et procéder au déploiement d'un bastion pour accès aux machines.

PARTIE 2

Activité 2
Implémenter les mécanismes de sécurité des VM

Eléments de réponse

Tâche 1 : Indiquer les mécanismes que doit déployer l'entreprise pour assurer la haute disponibilité et un bon fonctionnement de la solution;

Les mécanismes à mettre en place sont :

Création des VMs dans un Groupe à haute disponibilité : Les groupes à haute disponibilité veillent à ce que les machines virtuelles que vous déployez sur Azure soient distribuées sur plusieurs clusters matériels isolés. Leur utilisation garantit qu'en cas de défaillance matérielle ou logicielle dans Azure, seul un sous-ensemble de vos machines virtuelles est affecté et que votre solution globale reste disponible et opérationnelle.

Equilibrage de charge des machines virtuelles : L'équilibrage de charge offre un niveau plus élevé de disponibilité en répartissant les demandes entrantes sur plusieurs machines virtuelles.

Mise à l'échelle horizontale : également appelée augmentation ou diminution de la taille des instances, consiste à ajouter ou supprimer des instances d'une ressource. Pendant que de nouvelles ressources sont approvisionnées, l'application continue à s'exécuter sans interruption. Une fois le processus d'approvisionnement terminé, la solution est déployée sur ces ressources supplémentaires. Si la demande diminue, les ressources supplémentaires peuvent être correctement arrêtées et libérées.

PARTIE 2

Activité 2
Implémenter les mécanismes de sécurité des VM

PARTIE 2

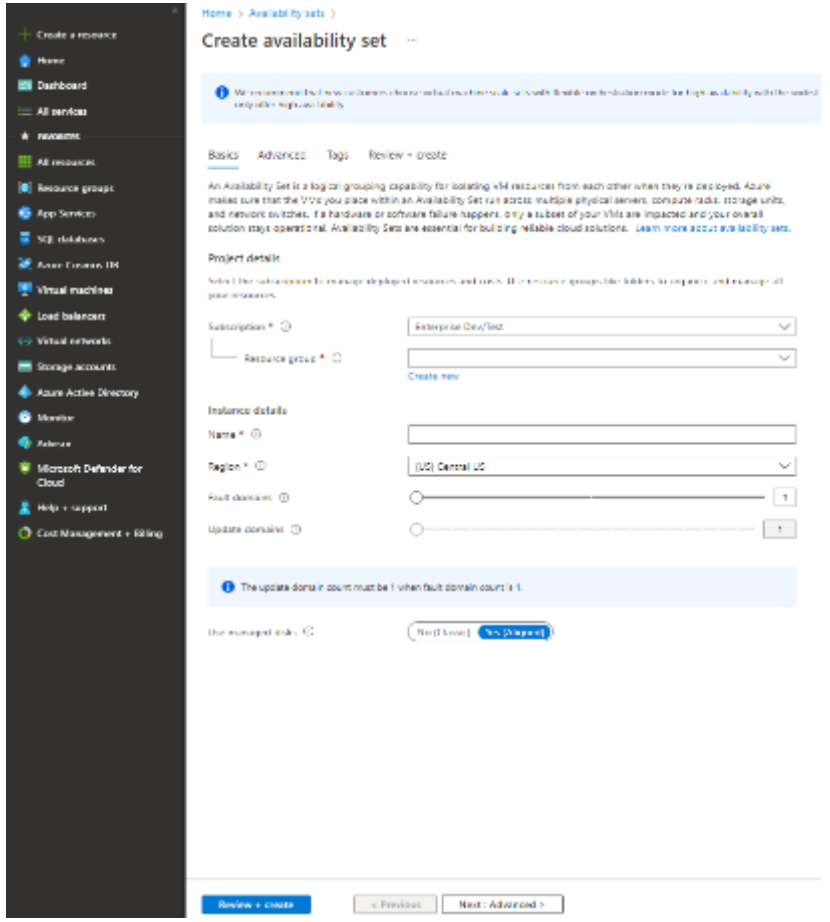
Eléments de réponse

Tâche 2 : Expérimenter les concepts identifiés précédemment à travers la création de VM Azure. En indiquant les étapes de paramétrage;

❑ **Création des VMs dans un Groupe à haute disponibilité :**

Dans ce TP, nous allons procédé à :

1. Créer un groupe à haute disponibilité
2. Créer une machine virtuelle dans un groupe à haute disponibilité
3. Vérifier l'affectation des machines virtuelles



1. Créer un groupe à haute disponibilité

Le matériel situé à un emplacement est divisé en plusieurs domaines de mise à jour et d'erreur.

Un **domaine de mise à jour** est un groupe de machines virtuelles et d'équipements physiques sous-jacents pouvant être redémarrés en même temps.

Les machines virtuelles d'un même **domaine d'erreur** partagent un espace de stockage commun ainsi qu'une source d'alimentation et un commutateur réseau.

Choisir dans la zone de recherche « **Zone de disponibilité »** puis choisir le « **nom du ressource Groupe » (créer un nouveau si besoin),** fournir **le nom de la zone de disponibilité** et la **région.**

Renseigner la valeur **1** pour **Domaine d'erreur** et **Domaine de Mise à jour** puis **valider la création**.

Activité 2
Implémenter les mécanismes de sécurité des VM

PARTIE 2

Eléments de réponse

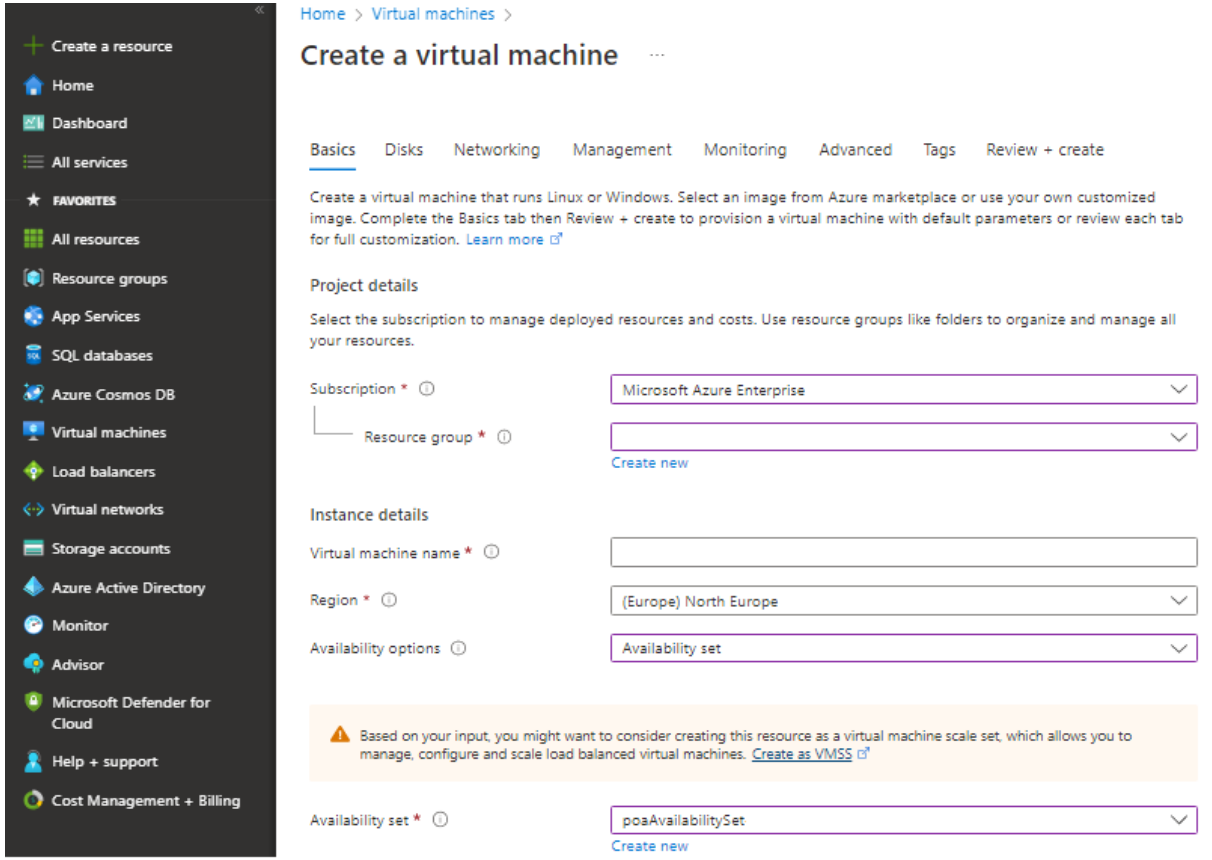
2. Créer une machine virtuelle dans un groupe à haute disponibilité

- Choisir dans le menu vertical du portail Azure l'onglet **Machines virtuelles**
- Renseigner les informations obligatoires en choisissant le même ressource group et zone utilisés précédemment pour la zone de disponibilité et choisir par la suite la zone de disponibilité créée dans l'étape 1.

- Créer une deuxième machine en répétant la même démarche.

3. Vérifier l'affectation des machines virtuelles

Choisir dans la zone de recherche « **Zone de disponibilité** » puis sélectionner la zone de disponibilité créée. (Deux machines doivent apparaître)

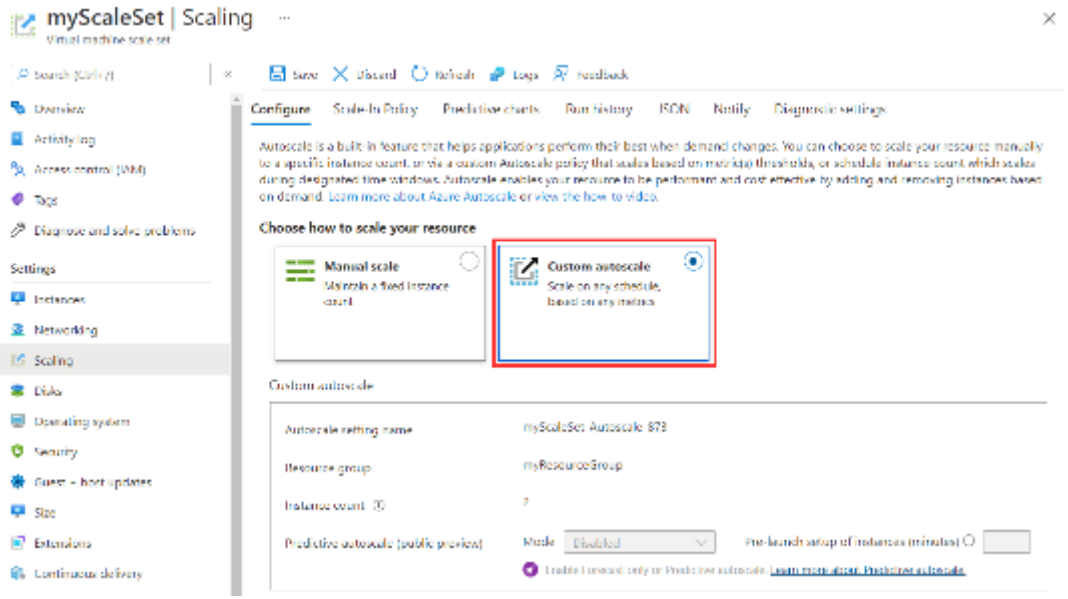


Activité 2
Implémenter les mécanismes de sécurité des VM

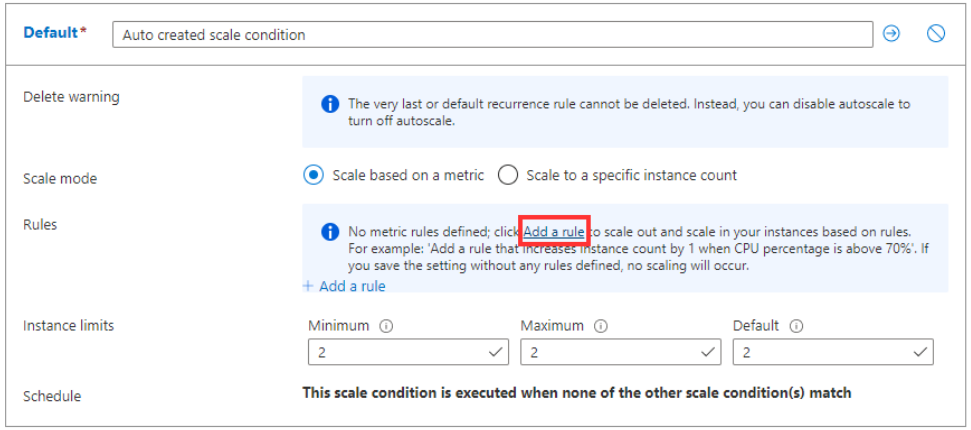
Eléments de réponse

❑ **Mise à l'échelle horizontale :**

Choisir l'une des VMs précédemment créées puis dans le menu horizontal sélectionnez « Mise à l'échelle », puis sélectionnez le bouton pour effectuer une **Mise à l'échelle automatique personnalisée.**



Sélectionnez l'option pour **Ajouter une règle**.



Chaque groupe devra argumenter le choix des limites implémentées pour la mise à l'échelle automatique des instances.

PARTIE 2

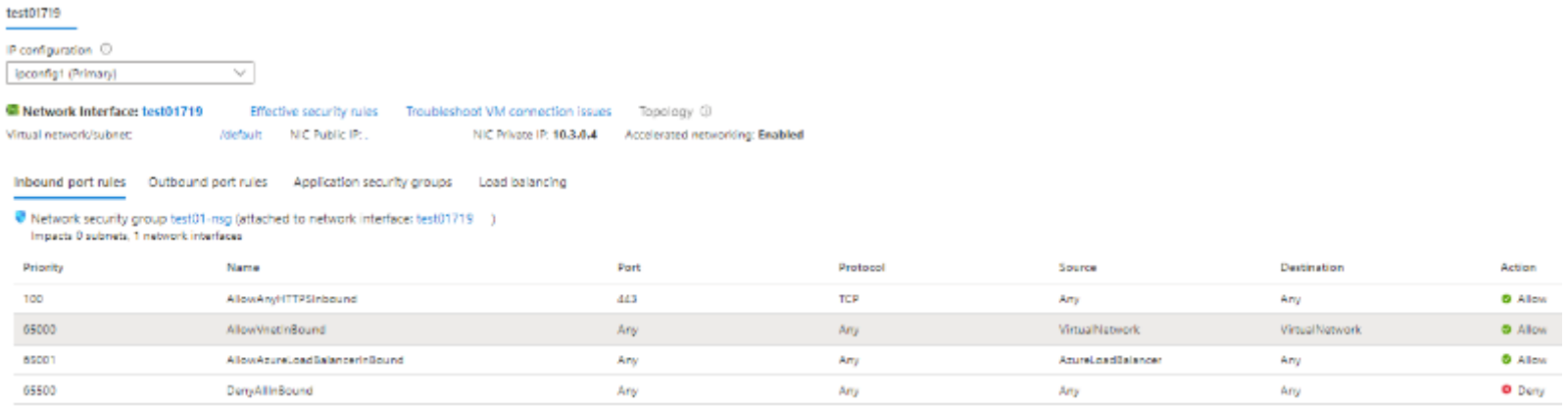
Activité 2
Implémenter les mécanismes de sécurité des VM

PARTIE 2

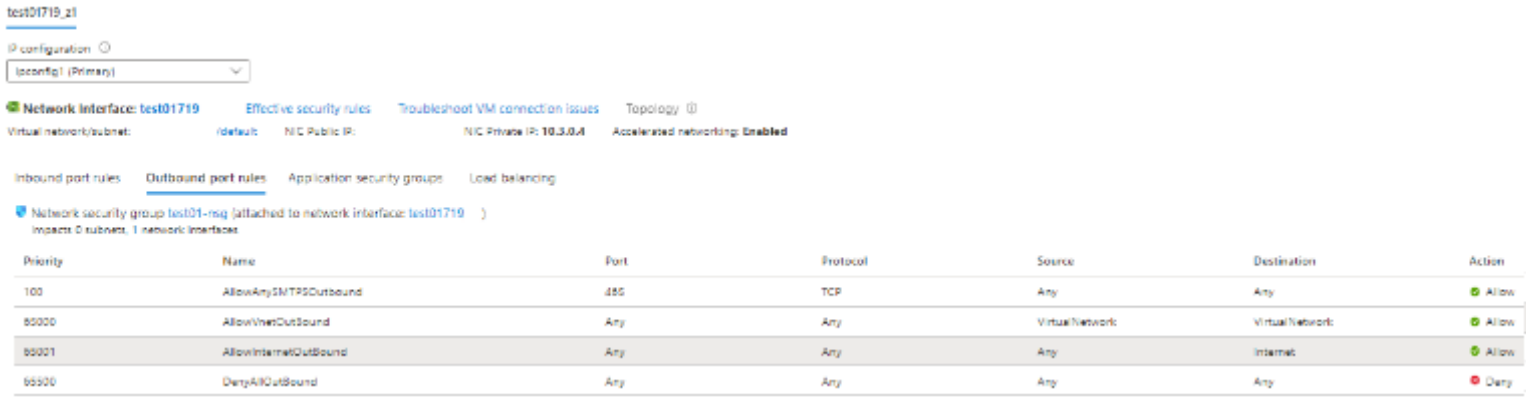
Eléments de réponse

Tâche 3 : Sachant que la solution effectue l'envoi des notifications par mail en utilisant le protocole SMTP sécurisé et expose une interface Web accessible over internet via Https. Indiquer et implémenter la matrice des flux (sortant et entrant) à adopter pour la VM applicative;

Flux entrant :



Flux sortant :



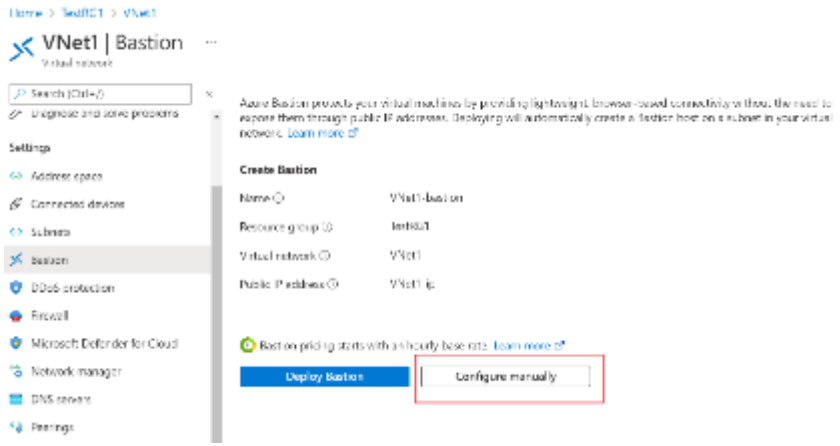
Eléments de réponse

Tâche 4 : Indiquer les mesures de sécurité qui seront déployées pour assurer une sécurité renforcée de la VM et procéder au déploiement d'un bastion pour accès aux machines.

- La désactivation des ports non utilisés, à savoir **internet, SSH et RDP et utilisation du service Bastion pour l'accès à la machine**.

Déployer Bastion

1. Connectez-vous au portail Azure.
2. Accédez à votre réseau virtuel.
3. Sur la page de votre réseau virtuel, dans le volet gauche, sélectionnez Bastion pour ouvrir la page Bastion .
4. Sur la page Bastion, sélectionnez Configurer manuellement. Cela vous permet de configurer des paramètres supplémentaires spécifiques lors du déploiement de Bastion sur votre réseau virtuel.



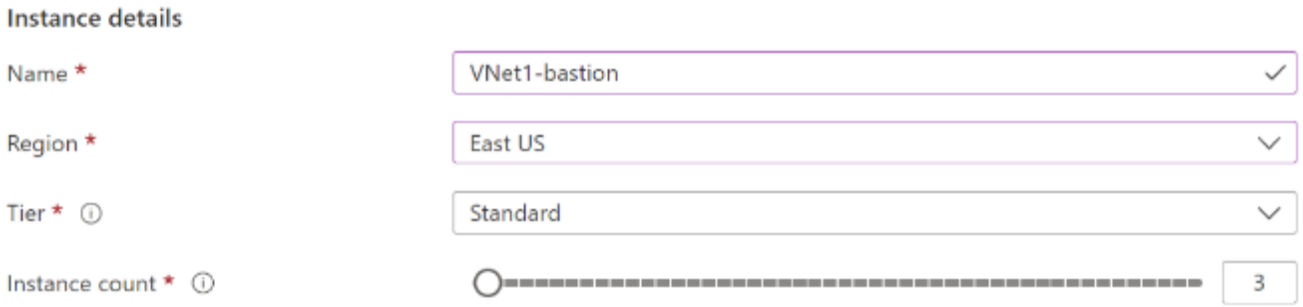
PARTIE 2

Activité 2
Implémenter les mécanismes de sécurité des VM

Eléments de réponse

Dans la page **Créer un Bastion**, configurez les paramètres de votre hôte bastion. Les détails du projet sont renseignés à partir des valeurs de votre réseau virtuel. Configurez les valeurs des **Détails de l'instance**.

- **Nom** : Tapez le nom que vous souhaitez utiliser pour votre ressource Bastion.
- **Région** : région publique Azure dans laquelle est créée la ressource. Choisissez la région dans laquelle réside votre réseau virtuel.
- **Niveau :** également appelé **Référence SKU**. Pour ce TP, sélectionnez **Standard**. Le niveau SKU standard vous permet de configurer le nombre d'instances pour la mise à l'échelle de l'hôte et d'autres fonctionnalités. Pour plus d'informations sur les fonctionnalités qui requièrent le niveau SKU standard, consultez Paramètres de configuration - Références SKU.
- **Nombre d'instances :** Il s'agit du paramètre de **mise à l'échelle de l'hôte**. Il est configuré en incréments d'unités d'échelle. Utilisez le curseur ou tapez un nombre pour configurer le nombre d'instances souhaitées. Pour ce tutoriel, vous pouvez sélectionner le nombre d'instances de votre choix. Pour plus d'informations, consultez Mise à l'échelle de l'hôte et Tarifs.



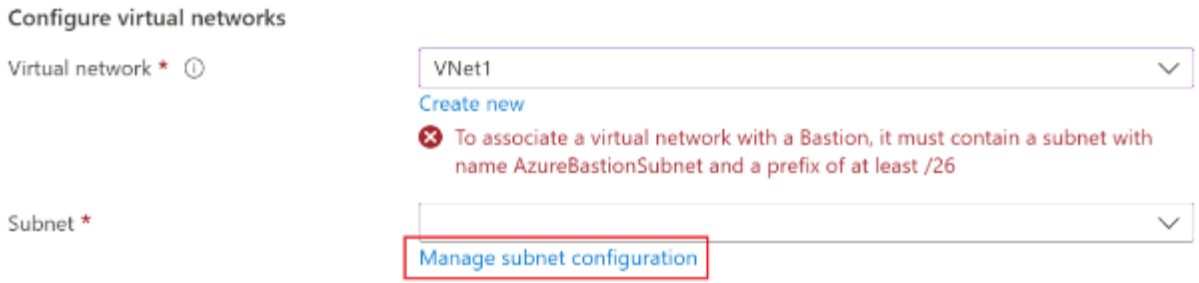
PARTIE 2

Activité 2
Implémenter les mécanismes de sécurité des VM

Eléments de réponse

Configurer les paramètres des **réseaux virtuels**. Sélectionnez votre réseau virtuel dans la liste déroulante. Si vous ne voyez pas votre réseau virtuel dans la liste déroulante, assurez-vous que vous avez sélectionné la région appropriée dans les paramètres précédents de cette page.

Pour configurer AzureBastionSubnet, sélectionnez **Gérer la configuration du sous-réseau**.



Dans la page **Sous-réseaux**, sélectionnez **+Sous-réseau** pour ouvrir la page **Ajouter un sous-réseau**.

Dans la page **Ajouter un sous-réseau**, créez le sous-réseau « AzureBastionSubnet » en utilisant les valeurs suivantes. Laissez les autres valeurs sur la valeur par défaut.

Le nom du sous-réseau doit être **AzureBastionSubnet**.

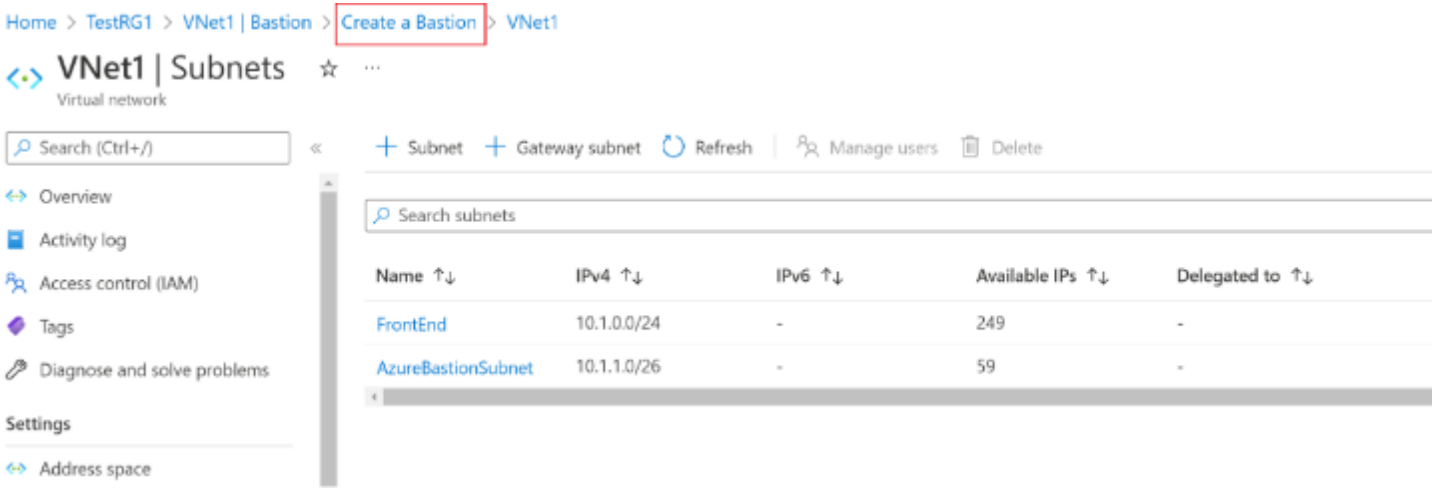
Le sous-réseau doit être au moins **/26 ou supérieur** (/26, /25, /24, etc.) pour prendre en charge les fonctionnalités disponibles avec la référence SKU Standard.

Sélectionnez **Enregistrer** au bas de la page pour enregistrer vos modifications.

PARTIE 2

Eléments de réponse

En haut de la page **Sous-réseaux**, sélectionnez **Créer un bastion** pour revenir à la page de configuration du bastion.



La section **Adresse IP publique** contient l'adresse IP publique de la ressource de l'hôte bastion sur laquelle accéder à RDP/SSH (sur le port 443). L'adresse IP publique doit être située dans la même région que la ressource Bastion que vous créez. Créez une adresse IP publique. Vous pouvez laisser la suggestion d'affectation de noms par défaut.

Quand vous avez terminé de spécifier les paramètres, sélectionnez **Vérifier + créer**. Cela valide les valeurs.

Une fois la validation réussie, vous pouvez déployer Bastion. Sélectionnez **Create** (Créer). Un message vous informe que votre déploiement est en cours de traitement. L'état s'affiche sur cette page à mesure que les ressources sont créées. Il faut environ 10 minutes pour que la ressource Bastion soit créée et déployée.

PARTIE 2

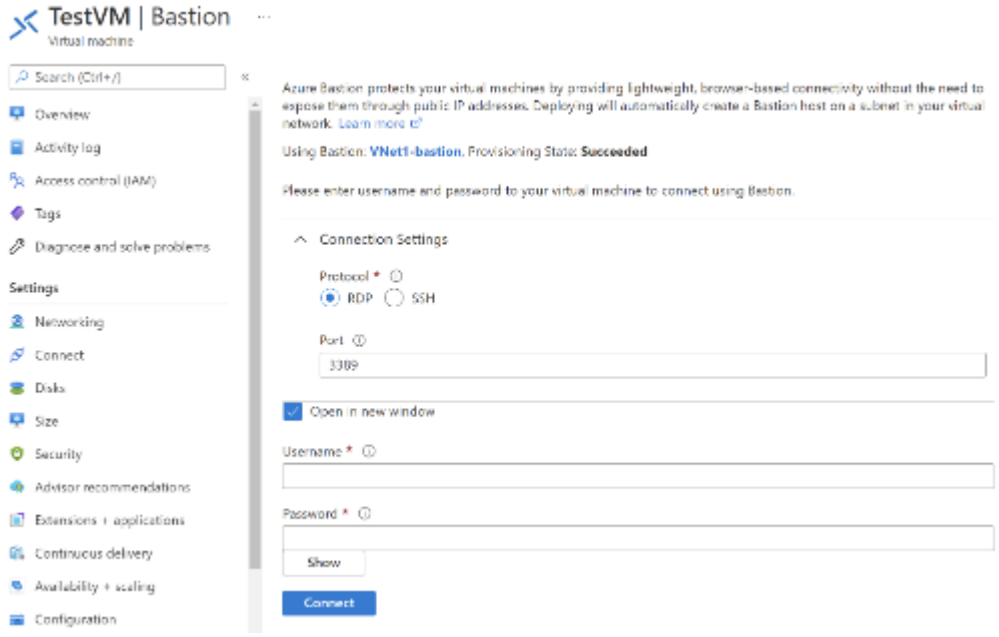
Eléments de réponse

Procédure de connexion via Bastion

Dans le portail Azure, accédez à la machine virtuelle à laquelle vous souhaitez vous connecter.

En haut de la page, sélectionnez **Connecter-Bastion** pour accéder à la page **Bastion**. Vous pouvez également accéder à la page Bastion à l'aide du menu de gauche.

Les options disponibles dans la page **Bastion** dépendent du niveau SKU Bastion. Si vous utilisez la **référence SKU De base**, vous vous connectez à un ordinateur Windows à l'aide du protocole RDP et du port 3389, et à un ordinateur Linux à l'aide de SSH et du port 22. Vous n'avez pas d'options pour modifier le numéro de port ou le protocole. Toutefois, vous pouvez modifier la langue du clavier pour RDP en développant les **paramètres de connexion**.

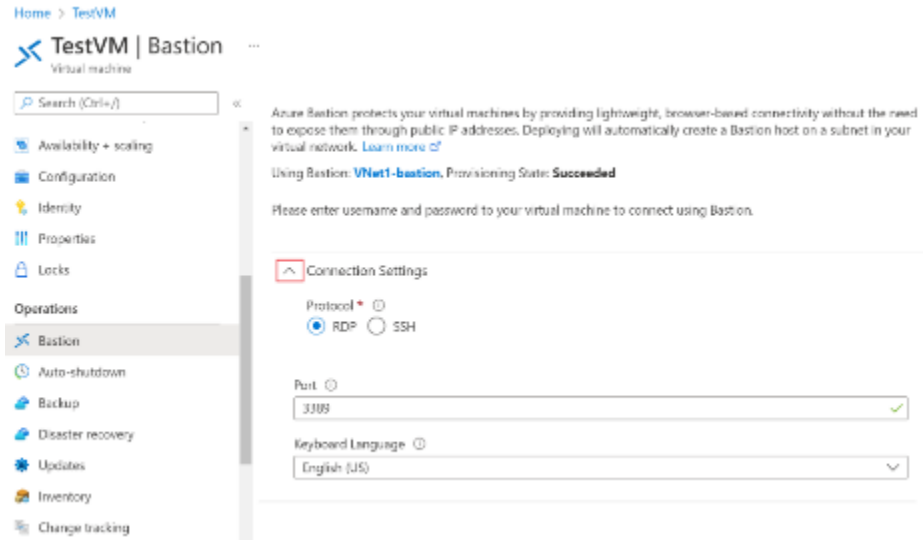


PARTIE 2

Activité 2
Implémenter les mécanismes de sécurité des VM

Eléments de réponse

Si vous utilisez la **référence SKU Standard**, vous avez plus d'options de protocole de connexion et de port disponibles. Développez **Paramètres de connexion** pour afficher les options. En règle générale, sauf si vous avez configuré des paramètres différents pour votre machine virtuelle, vous vous connectez à un ordinateur Windows à l'aide du protocole RDP et du port 3389, et à un ordinateur Linux à l'aide de SSH et du port 22.

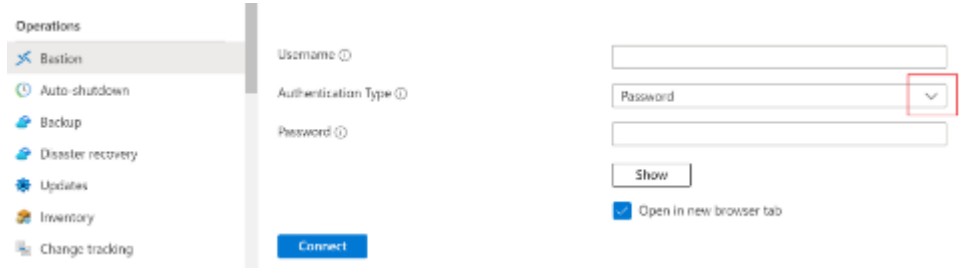


Sélectionnez le **type d'authentification** dans la liste déroulante. Le protocole détermine les types d'authentification disponibles. Complétez les valeurs d'authentification requises.

PARTIE 2

Activité 2
Implémenter les mécanismes de sécurité des VM

Eléments de réponse

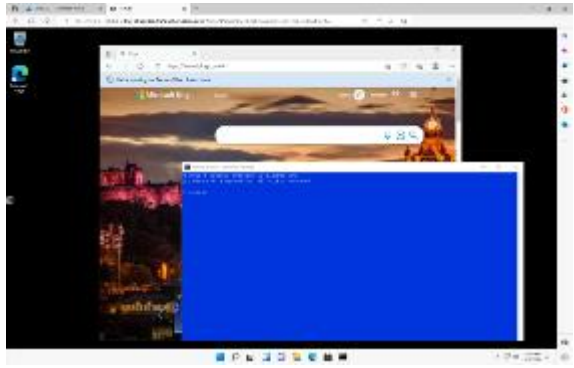


Pour ouvrir la session de machine virtuelle dans un nouvel onglet de navigateur, laissez **Ouvrir dans un nouvel onglet de navigateur** sélectionné.

Cliquez sur **Se connecter** pour vous connecter à la machine virtuelle.

La connexion à cette machine virtuelle avec Bastion s'ouvrira directement dans le portail Azure (en HTML5) via le port 443 et le service Bastion.

- Lorsque vous vous connectez, le bureau de la machine virtuelle est différent de celui présenté dans la capture d'écran.
- L'utilisation de touches de raccourci lorsque vous êtes connecté à une machine virtuelle peut ne pas s'accompagner du même comportement que les touches de raccourci sur un ordinateur local. Par exemple, lorsque vous êtes connecté à une machine virtuelle Windows à partir d'un client Windows, CTRL+ALT+FIN est le raccourci clavier pour CTRL+ALT+SUPPR sur un ordinateur local. Pour effectuer cette opération depuis un Mac alors que vous êtes connecté à une machine virtuelle Windows, le raccourci clavier est Fn+CTRL+ALT+Retour arrière.



PARTIE 2

ACTIVITÉ 3

Configuration de la MFA

Compétences visées :

- Configurer l'authentification à multiples facteurs sur Microsoft Azure.

Recommandations clés :

- Appréhender le fonctionnement du MFA au niveau de Azure.

8 heures

CONSIGNES

1. Pour le formateur

- Maitrise de la configuration du MFA Azure
- Débloquer les stagiaires en cas de difficulté
- Laisser un peu de temps aux stagiaires pour qu'ils puissent réaliser les tâches eux mêmes

2. Pour l'apprenant

- Suivre le TP étape par étape et dans l'ordre
- En cas de problème ou blocage, le faire savoir à votre formateur
- Parcourir les réponses proposées
- Comparer vos réponses à celles proposés pour évaluer votre niveau de compréhension du cours

3. Conditions de réalisation :

- Seul ou en binôme
- Des ordinateurs dotés d'une connexion internet
- Des comptes Azure pour que les stagiaires puissent réaliser le TP
- Un projecteur dans le cas d'une présentation à faire par le formateur pour montrer un use case aux stagiaires

4. Critères de réussite :

- Terminer toutes les étapes du TP avec succès
- Atteindre l'objectif global du TP

Activité 3
Configuration de la MFA

Travail demandé

Dans ce TP, vous allez effectuer les tâches suivantes:

Tâche 1 : Créer un nouveau locataire Azure AD.

Tâche 2 : Activer la version d'essai d'Azure AD Premium P2.

Tâche 3 : Créer des utilisateurs et des groupes Azure AD.

Tâche 4 : Attribuer des licences Azure AD Premium P2 aux utilisateurs Azure AD.

Tâche 5 : Configurer les paramètres Azure MFA.

Tâche 6 : Valider la configuration MFA

PARTIE 2

PARTIE 2

Eléments de réponse : tâche 1

Tâche 1 : Créer un nouveau locataire Azure AD.

Dans cette tâche, vous allez créer un nouveau locataire Azure AD.

1. 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, tapez **Azure Active Directory** et appuyez sur la touche **Entrée**.
2. Sur le panneau affichant **Overview** de votre locataire Azure AD actuel, cliquez sur **Gérer les locataires** , puis sur l'écran suivant, cliquez sur **+ Créer**.
3. Dans l'onglet **Bases** du panneau **Créer un locataire**, assurez-vous que l'option **Azure Active Directory** est sélectionnée et cliquez sur **Suivant : Configuration >** .
4. Dans l'onglet **Configuration** du panneau **Créer un locataire**, spécifiez les paramètres suivants :
   - **Nom de l'organisation** (Exp: **TP_MFA**)
   - **Nom de domaine initial**
   - **Pays ou région**
5. Cliquez sur **Réviser + Créer** , puis sur **Créer**.
6. Ajoutez le code Captcha sur **Aidez-nous à prouver que vous n'êtes pas un robot**, puis cliquez sur le bouton **Soumettre**.

Remarques

- Enregistrez le nom de domaine initial. Vous en aurez besoin plus tard dans cet atelier.
- Attendez que le nouveau locataire soit créé. Utilisez l'icône de notification pour surveiller l'état du déploiement.

Eléments de réponse : tâche 2

Tâche 2 : Activer la version d'essai d'Azure AD Premium P2.

Dans cette tâche, vous vous inscrirez à l'essai gratuit d'Azure AD Premium P2.

1. Dans le portail Azure, dans la barre d'outils, cliquez sur l' icône **Annuaire + abonnement**, située à droite de l'icône Cloud Shell.
2. Dans le panneau **Répertoire + abonnement**, cliquez sur le locataire nouvellement créé **TP_MFA** et cliquez sur le bouton **Basculer** pour le définir comme répertoire actuel.
3. 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**,** tapez **Azure Active Directory** et appuyez sur la touche **Entrée** . Sur le panneau **TP_MFA** , dans la section **Gérer**, cliquez sur **Licences**.
4. Sur les **licences | Panneau Vue d'ensemble**, dans la section **Gérer**, cliquez sur **Tous les produits**, puis cliquez sur **+ Essayer / Acheter**.
5. Sur le **panneau Activer**, dans la section Azure AD Premium P2, cliquez sur **Essai gratuit**, puis cliquez sur **Activer** .

Remarques

- Vous devrez peut-être actualiser la fenêtre du navigateur si l'entrée **TP_MFA** n'apparaît pas dans la liste Annuaire + filtre d'abonnement.

Activité 3
Configuration de la MFA

Eléments de réponse : tâche 3

Tâche 3 : Créer des utilisateurs et des groupes Azure AD**.**

Dans cette tâche, vous allez créer trois utilisateurs : **aaduser1** (Global Admin), **aaduser2** (utilisateur) et **aaduser3** (utilisateur). Vous aurez besoin du nom principal et du mot de passe de chaque utilisateur pour les tâches ultérieures.

1. Revenez au **panneau TP_MFA** Azure Active Directory et, dans la section **Gérer** , cliquez sur **Utilisateurs**.
2. Sur les **utilisateurs | panneau Tous les utilisateurs**, cliquez sur **+ Nouvel utilisateur**.
3. Dans le **panneau Nouvel utilisateur**, assurez-vous que l'option **Créer un utilisateur** est sélectionnée, et spécifiez les paramètres suivants (laissez tous les autres avec leurs valeurs par défaut) et cliquez sur **Créer** :
    - Nom d'utilisateur: **aaduser1**
    - Nom: **aaduser1**
    - Mot de passe: assurez-vous que l'option **Générer automatiquement le mot de passe** est sélectionnée et cliquez sur **Afficher le mot de passe.**
    - Groupes: **0 groupes sélectionnés**
    - Les rôles: cliquez sur **Utilisateur**, puis cliquez sur **Administrateur général**, et cliquez sur **Sélectionner.**
    - Lieu d'utilisation: un pays (Ex: Etat Unis)
4. Retour sur les **Utilisateurs | Panneau Tous les utilisateurs**, cliquez sur **+ Nouvel utilisateur**.

PARTIE 2

Activité 3
Configuration de la MFA

Eléments de réponse : tâche 3

5. Dans le **panneau Nouvel utilisateur**, assurez-vous que l'option **Créer un utilisateur** est sélectionnée et spécifiez les paramètres suivants (laissez tous les autres paramètres avec leurs valeurs par défaut) :
    - Nom d'utilisateur: **aaduser2**
    - Nom: **aaduser2**
    - Mot de passe: assurez-vous que l'option **Générer automatiquement le mot de passe** est sélectionnée et cliquez sur **Afficher le mot de passe.**
    - Groupes: **0 groupes sélectionnés**
    - Les rôles: **Utilisateur**
    - Lieu d'utilisation: un pays (Ex: Etat Unis)
6. Retour sur les **Utilisateurs | Panneau Tous les utilisateurs**, cliquez sur **+ Nouvel utilisateur**.
7. Cliquez sur **Nouvel utilisateur**, complétez les paramètres de configuration du nouvel utilisateur, puis cliquez sur **Créer**.
    - Nom d'utilisateur: **aaduser3**
    - Nom: **aaduser3**
    - Mot de passe: assurez-vous que l'option **Générer automatiquement le mot de passe** est sélectionnée et cliquez sur **Afficher le mot de passe.**
    - Groupes: **0 groupes sélectionnés**
    - Les rôles: **Utilisateur**
    - Lieu d'utilisation: un pays (Ex: Etat Unis)

PARTIE 2

Activité 3
Configuration de la MFA

Eléments de réponse : tâche 3

Remarques

- Enregistrez le nom d'utilisateur et le mot de passe de l'utilisateur. Vous en aurez besoin plus tard dans ce TP.
- À ce stade, vous devriez avoir trois nouveaux utilisateurs répertoriés sur la page **Utilisateurs.**

PARTIE 2

Eléments de réponse : tâche 4

Tâche 4 : attribuer des licences Azure AD Premium P2 aux utilisateurs Azure AD.

Dans cette tâche, vous attribuerez à chaque utilisateur la licence Azure Active Directory Premium P2.

1. Sur les **utilisateurs | Dans le panneau Tous les utilisateurs**, cliquez sur l'entrée représentant votre compte d'utilisateur.
2. Sur le panneau affichant les propriétés de votre compte utilisateur, cliquez sur **Modifier**. Vérifiez que l'emplacement d'utilisation est défini sur **États-Unis** sinon définissez l'emplacement d'utilisation et cliquez sur **Enregistrer**.
3. Revenez au **panneau TP_MFA** Azure Active Directory et, dans la section **Gérer**, cliquez sur **Licences** .
4. Sur les **licences | Dans le panneau Vue d'ensemble**, cliquez sur **Tous les produits**, cochez la case **Azure Active Directory Premium P2**, puis cliquez sur **+ Attribuer**.
5. Dans le **panneau Attribuer des licences**, cliquez sur **+ Ajouter des utilisateurs et des groupes**.
6. Dans le panneau **Utilisateurs**, sélectionnez **aaduser1**, **aaduser2**, **aaduser3** et votre compte d'utilisateur, puis cliquez sur **Sélectionner**.
7. De retour sur le **panneau Attribuer des licences**, cliquez sur **Options d'attribution**, assurez-vous que toutes les options sont activées, cliquez sur **Vérifier + attribuer**, cliquez sur **Attribuer**.
8. Déconnectez-vous du portail Azure et reconnectez-vous avec le même compte. Cette étape est nécessaire pour que l'attribution de licence prenne effet.

Remarques

- A ce stade, vous avez attribué des licences Azure Active Directory Premium P2 à tous les comptes d'utilisateurs que vous utiliserez dans cet atelier. Assurez-vous de vous déconnecter, puis de vous reconnecter.

PARTIE 2

Eléments de réponse : tâche 5

Tâche 5 : Configurer les paramètres Azure MFA.

Dans cette tâche, vous allez configurer MFA et activer MFA pour aaduser1.

1. Dans le portail Azure, revenez au panneau de locataire **TP_MFA** Azure Active Directory.
2. Sur le panneau de locataire **TP_MFA** Azure Active Directory, dans la section **Gérer**, cliquez sur **Sécurité**.
3. Sur la **sécurité | Panneau Prise en main**, dans la section **Gérer**, cliquez sur **MFA**.
4. sur l' **authentification multifacteur | Dans** le panneau **Prise en main, cliquez sur le** lien **Paramètres MFA supplémentaires basés sur le cloud.**
5. Sur la page **d'authentification** multifacteur, cliquez sur l'onglet **des paramètres de service. Passez en** revue **les options de vérification**. Notez que **Message texte au téléphone**, **Notification via l'application mobile** et **Code de vérification de l'application mobile ou du jeton matériel** sont activés. Cliquez sur **Enregistrer** puis cliquez sur **Fermer**.
6. Passez à l'onglet **utilisateurs, cliquez sur** l'entrée **aaduser1, cliquez sur le lien Activer** et, lorsque vous y êtes invité, cliquez sur **activer l'authentification multifacteur**.
7. Notez que la colonne d' **état Multi-Factor Auth** pour **aaduser1** est maintenant **Enabled**.
8. Cliquez sur **aaduser1** et notez qu'à ce stade, vous avez également l'option **Appliquer.**

Eléments de réponse : tâche 5

9. Après avoir sélectionné l'entrée **aaduser1** , cliquez sur **Gérer les paramètres utilisateur** et passez en revue les options disponibles :
    - Exiger que les utilisateurs sélectionnés fournissent à nouveau des méthodes de contact.
    - Supprimez tous les mots de passe d'application existants générés par les utilisateurs sélectionnés.
    - Restaurer l'authentification multifacteur sur tous les appareils mémorisés.
10. Cliquez sur **Annuler** et revenez à l'onglet du navigateur affichant l'**authentification multifacteur | Panneau Prise en main** dans le portail Azure.
11. Dans la section **Paramètres**, cliquez sur **Alerte à la fraude**.

sur l'**authentification multifacteur | Panneau d'alerte de fraude**, configurez les paramètres suivants :

- Autoriser les utilisateurs à soumettre des alertes de fraude
- Bloquer automatiquement les utilisateurs qui signalent une fraude
- Code pour signaler une fraude lors de l'accueil initial

12. Cliquez sur **Enregistrer**
13. Revenez au panneau de locataire **TP_MFA** Azure Active Directory, dans la section **Gérer**, cliquez sur **Propriétés**, cliquez ensuite sur le lien **Gérer les paramètres de sécurité par défaut en bas du panneau, sur le panneau Activer les paramètres de sécurité par défaut**, cliquez sur **Non**. Sélectionnez **Mon organisation utilise** l'accès conditionnel comme raison, puis cliquez sur **Enregistrer** .

Eléments de réponse : tâche 5

Tâche 5 : Configurer les paramètres Azure MFA.

Remarques

- Assurez-vous que vous êtes connecté au locataire **TP_MFA** Azure AD. Vous pouvez utiliser le filtre **Annuaire + abonnement** pour basculer entre les locataires Azure AD. Assurez-vous que vous êtes connecté en tant qu'utilisateur avec le rôle d'administrateur général dans le locataire Azure AD.

Eléments de réponse : tâche 6

Tâche 6 : Valider la configuration MFA

Dans cette tâche, vous validerez la configuration MFA en testant la connexion du compte utilisateur aaduser1.

1. Ouvrez une fenêtre de navigateur InPrivate.
2. Accédez au portail Azure et connectez-vous à l'aide du compte d'utilisateur **aaduser1**.
3. Lorsque vous y êtes invité, dans la boîte de dialogue **Plus d'informations requises**, cliquez sur **Suivant**.
4. Sur la page **Maintenir la sécurité de votre compte**, sélectionnez le lien **Je souhaite configurer une méthode différente**, dans la **section Quelle méthode souhaitez-vous utiliser ?** liste déroulante, sélectionnez **Téléphone**, puis sélectionnez **Confirmer**.
5. Sur la page **Gardez votre compte sécurisé**, sélectionnez votre pays ou votre région, saisissez votre numéro de téléphone mobile dans la zone **Entrer le numéro de téléphone**, assurez-vous que l'option **M'envoyer un code par** SMS est sélectionnée, puis cliquez sur **Suivant**.
6. Sur la page **Gardez votre compte sécurisé**, saisissez le code que vous avez reçu dans le message texte sur votre téléphone mobile, puis cliquez sur **Suivant**.
7. Sur la page **Gardez votre compte sécurisé**, assurez-vous que la vérification a réussi et cliquez sur **Suivant**.
8. Sur la page **Sécuriser votre compte**, cliquez sur **Je souhaite utiliser une autre méthode**, sélectionnez E- **mail** dans la liste déroulante, cliquez sur **Confirmer**, indiquez l'adresse e-mail que vous comptez utiliser, puis cliquez sur **Suivant**. Une fois que vous avez reçu l'e-mail correspondant, identifiez le code dans le corps de l'e-mail, fournissez-le, puis cliquez sur **Terminé**.

Activité 3
Configuration de la MFA

Eléments de réponse : tâche 6

9. Lorsque vous y êtes invité, modifiez votre mot de passe. Assurez-vous d'enregistrer le nouveau mot de passe.
10. Vérifiez que vous vous êtes bien connecté au portail Azure.
11. Déconnectez vous en tant que **aaduser1** et fermez la fenêtre du navigateur InPrivate.

Remarques

- Vous avez créé un nouveau locataire AD, configuré des utilisateurs AD, configuré MFA et testé l'expérience MFA pour un utilisateur.

PARTIE 2

ACTIVITÉ 4

Manipulation des mécanismes de protection des données

Compétences visées :

- Manipulation du masquage et démasquage des données sur une base de données SQL Server déployée sur Azure

Recommandations clés :

- Appréhender les mécanismes de protection des données sur une base de données SQL SERVER.

6 heures

CONSIGNES

1. Pour le formateur

- Connaissances solide du SQL Server
- Maitrise des aspects du masquage des données sur SQL Server
- Débloquer les stagiaires en cas de difficulté
- Laisser un peu de temps aux stagiaires pour qu'ils puissent réaliser les tâches eux mêmes

2. Pour l'apprenant

- Suivre le TP étape par étape et dans l'ordre
- En cas de problème ou blocage, le faire savoir à votre formateur
- Parcourir les réponses proposées
- Comparer vos réponses à celles proposés pour évaluer votre niveau de compréhension du cours

3. Conditions de réalisation :

- Seul ou en binôme
- Des ordinateurs dotés d'une connexion internet
- Des comptes Azure pour que les stagiaires puissent réaliser le TP
- Un projecteur dans le cas d'une présentation à faire par le formateur pour montrer un use case aux stagiaires

4. Critères de réussite :

- Terminer toutes les étapes du TP avec succès
- Atteindre l'objectif global du TP

Activité 4
Manipulation des mécanismes de protection des données

Travail demandé

Le masquage dynamique des données limite l'exposition des données sensibles en les masquant aux utilisateurs non privilégiés.

Il s'agit d'une fonctionnalité de protection des données qui masque les données sensibles dans le résultat d'une requête sur des champs de base de données intermédiaires, tandis que les données de la base de données ne sont pas modifiées. Le masquage dynamique des données est facile à utiliser avec les applications existantes, car les règles de masquage sont appliquées dans les résultats de la requête.

Dans ce TP, vous allez effectuer les tâches suivantes:

Tâche 1: Créer une base de données AdventureWorks sur une instance SQL.

Tâche 2: Configurer les règles du firewall coté base de données SQL pour autoriser l'IP Client pour s'y connecter.

Tâche 3: Configuration des règles de masquage.

PARTIE 2

Eléments de réponse : tâche 1

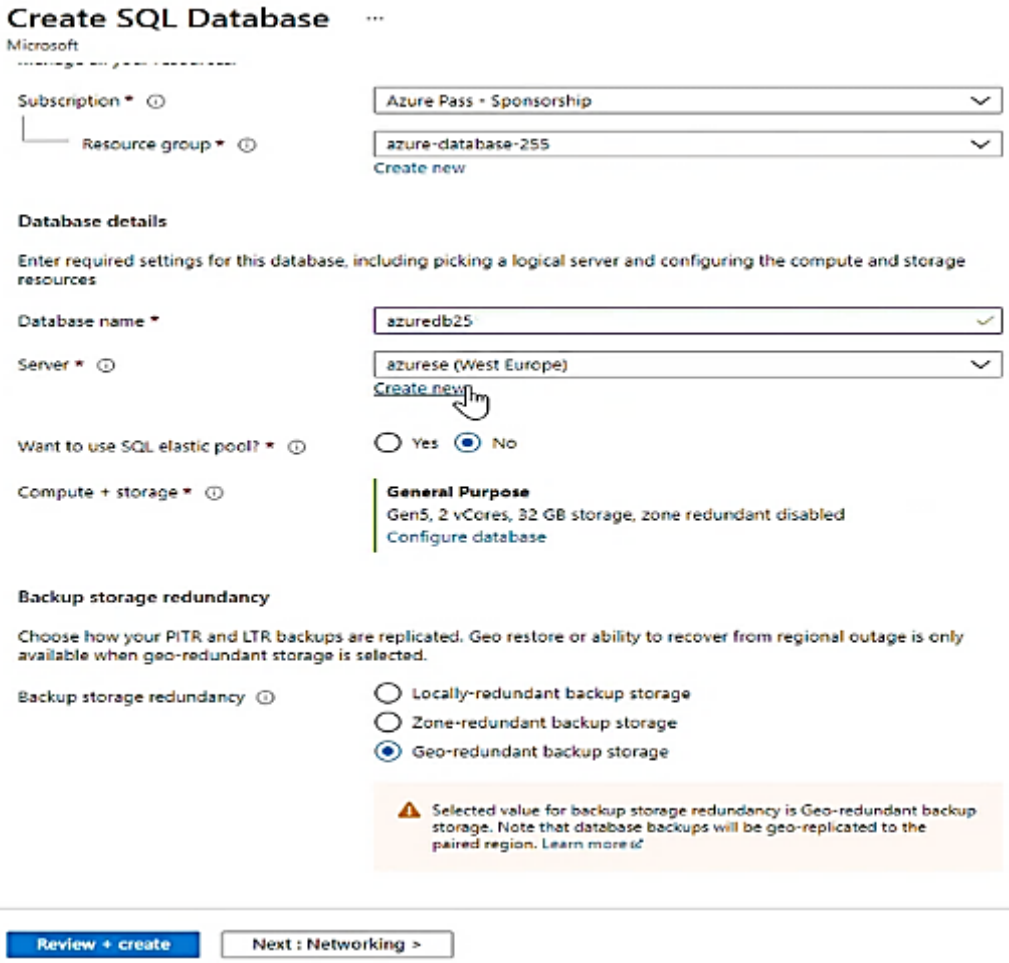
Tâche 1: Créer une base de données AdventureWorks sur une instance SQL.

1. Connectez-vous au portail Azure à l'aide de votre compte.
2. Sous la section « Services Azure », cliquez sur **+ créer une ressource**.
3. Sélectionnez ensuite **Base de données**, puis cliquez sur créer sous « **Base de données SQL** ».
4. Renseignez les champs obligatoires sur l'onglet « De base » comme décrit dans la capture ci-dessous:

Activité 4
Manipulation des mécanismes de protection des données

PARTIE 2

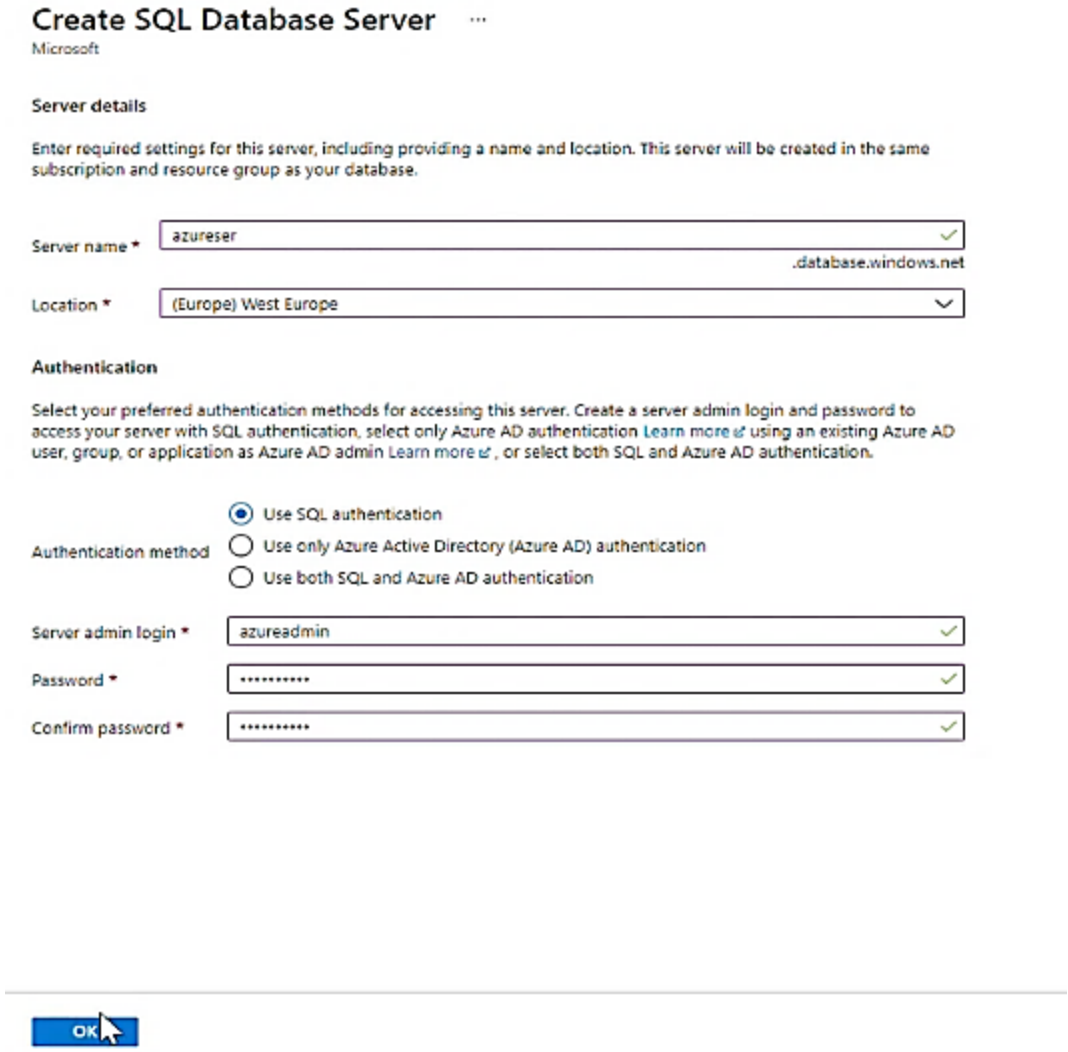
Eléments de réponse : tâche 1



Eléments de réponse : tâche 1

5. Pour le champs serveur, cliquez sur créer nouveau afin de définir les paramètres du nouveau serveur de base de données SQL:
6. Cliquez ensuite sur OK.

→ Si tout est bien, vous devrez revenir vers l'écran précédent pour continuer le paramétrage.



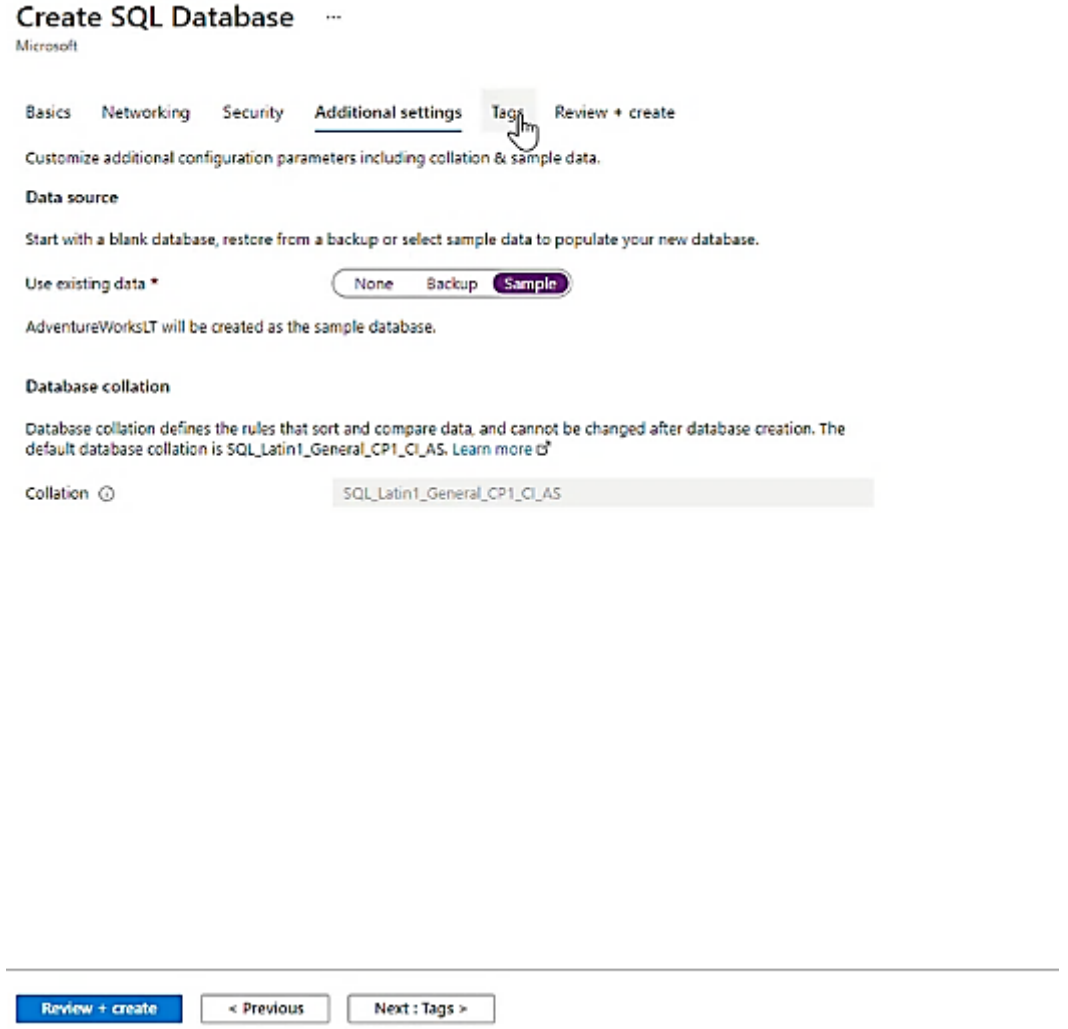
PARTIE 2

Activité 4
Manipulation des mécanismes de protection des données

Eléments de réponse : tâche 1

7. Passez à l'onglet « Aditional settings », et sélectionnez l'utilisation des données existantes « Sample ».
8. Cliquer ensuite sur « Review + create » puis « create »

→ Le déploiement de la base de données SQL commencera immédiatement. Vous devez patientez jusqu'à la fin du déploiement.

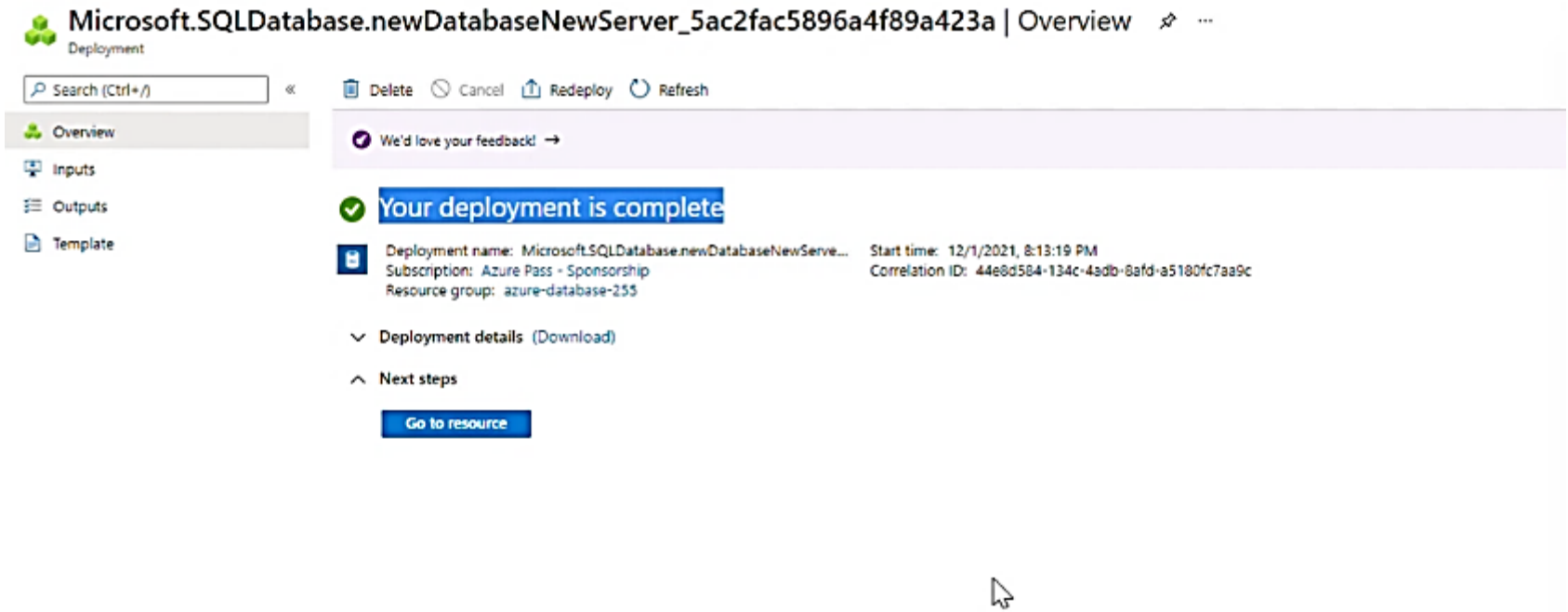


PARTIE 2

Eléments de réponse : tâche 2

Tâche 2: Configurer les règles du firewall coté base de données SQL pour autoriser l'IP Client pour s'y connecter.

Une fois le déploiement de la base de données SQL terminé, vous serez invités à accéder à la ressource créée (Cf capture ci-dessous).

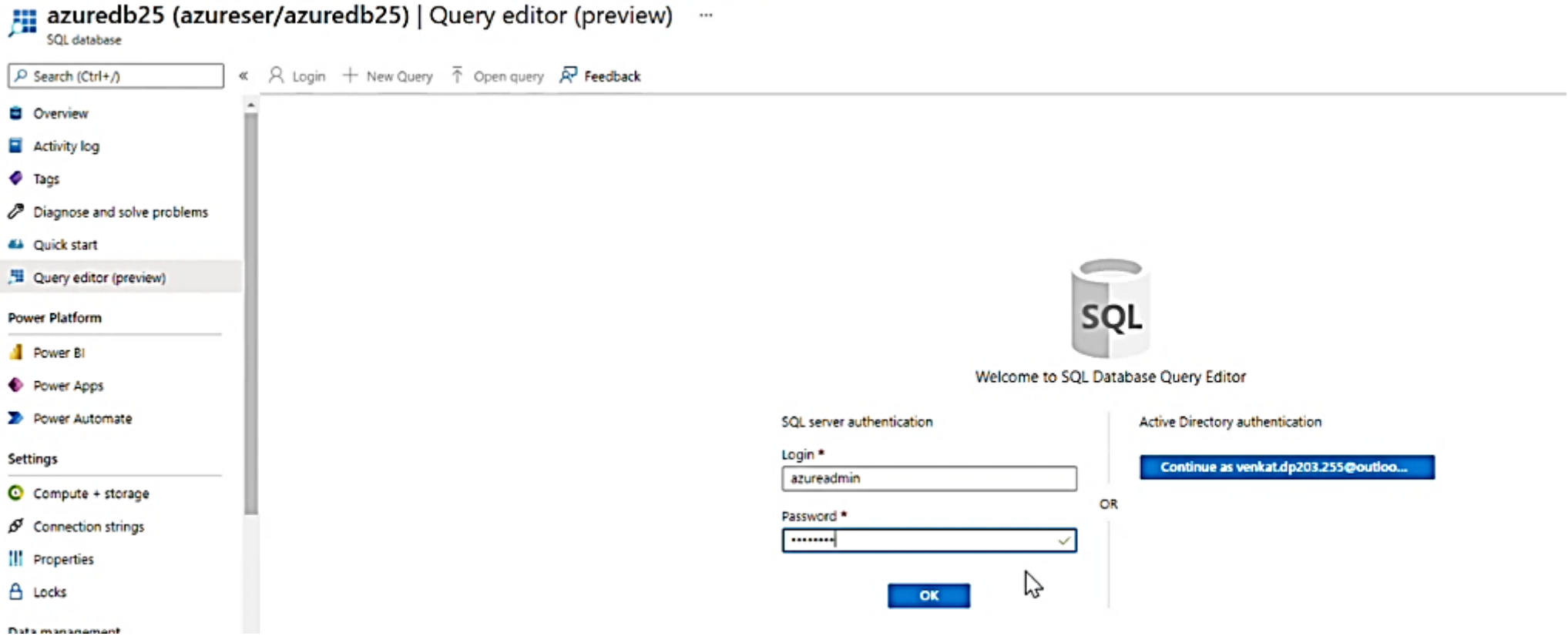


PARTIE 2

PARTIE 2

Eléments de réponse : tâche 2

1. Cliquez sur « Go to resource »
2. Sur le menu à gauche, cliquez sur « Query editor » et renseignez les champs login et mot de passe, afin de se connecter au serveur de base de données SQL:



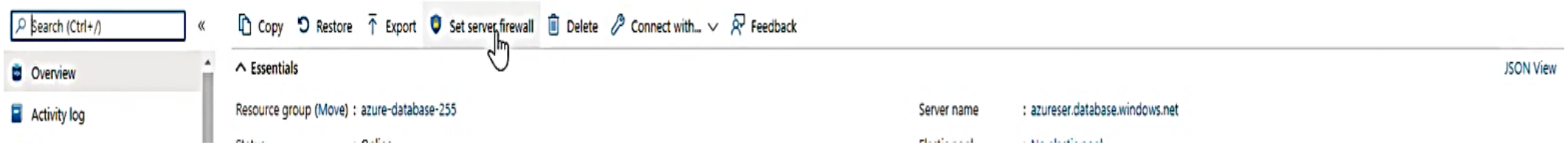
PARTIE 2

Eléments de réponse : tâche 2

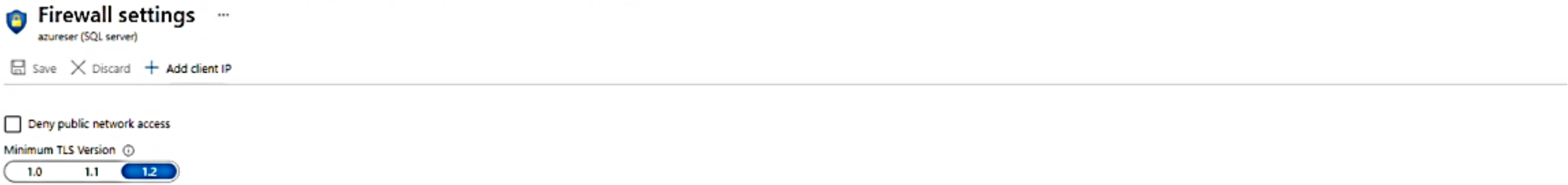
Normalement, sur l'étape précédente, vous devez voir apparaitre un message d'erreur, vous indiquant que vous n'êtes pas autorisé à vous connecter au serveur de base de données. Car vous devez d'abord configurer le firewall de cette base de données afin d'avoir la possibilité de l'exploiter.

Pour ce faire:

1. Revenez sur l'« Overview » de la ressource concernant la base de données SQL que vous avez créée, puis cliquez sur « set server firewall »



2. Cliquez en suite sur « Add Client IP » pour ajouter votre adresse IP. C'est comme ça qu'on vous autorise à exploiter la base de données SQL.



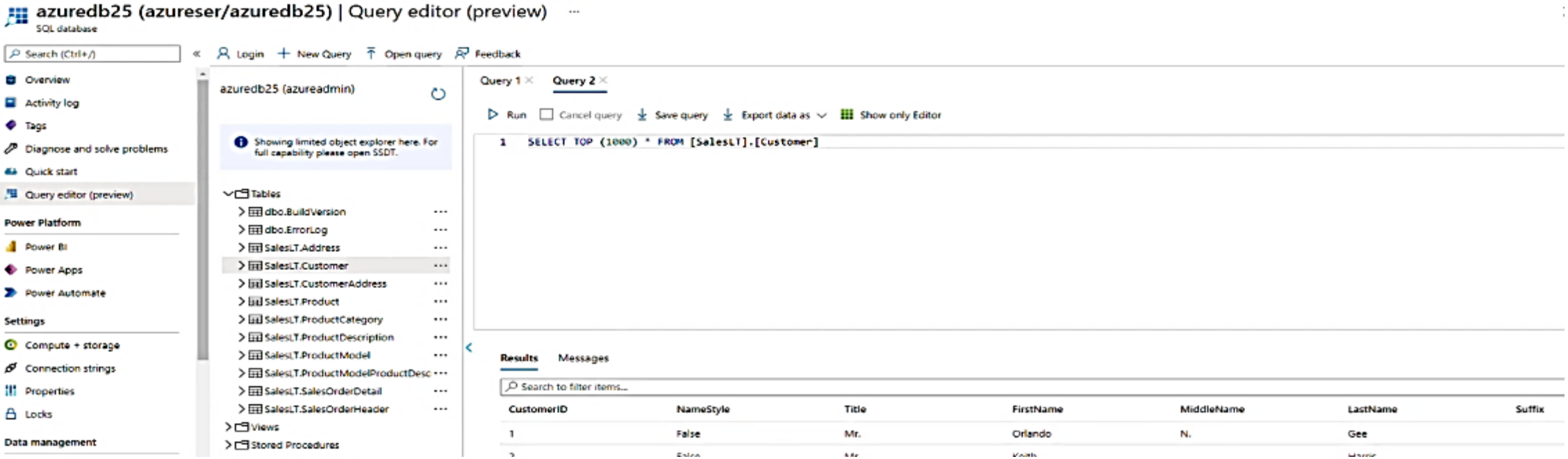
3. Cliquez sur « Save »pour enregistrer cette autorisation.

PARTIE 2

Eléments de réponse : tâche 3

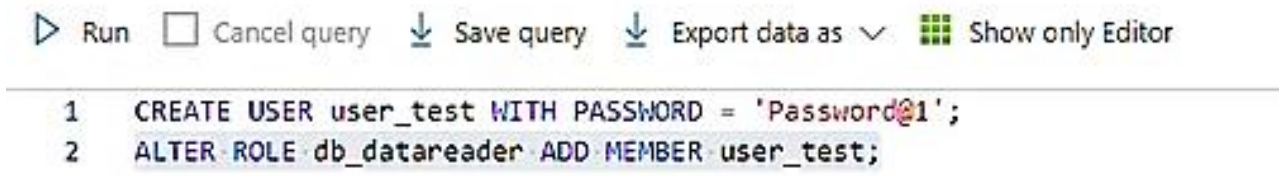
Tâche 3: Configuration des règles de masquage.

1. Revenez à la section « Overview » de la ressource.
2. Sur le menu à gauche, cliquez sur « Query editor » et renseignez les champs login et mot de passe, afin de vous connecter au serveur de base de données SQL.
3. Cette fois-ci, vous devez accéder sans problème à votre service de base de données SQL:

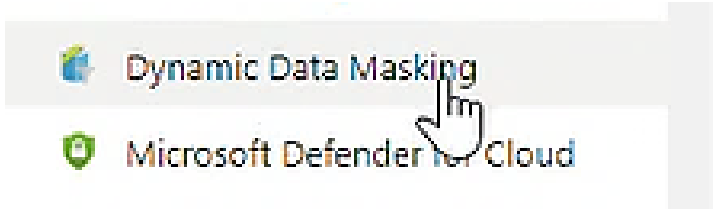


Eléments de réponse : tâche 3

4. Prenez 5 minutes afin de parcourir la structure de la base de données « AdventureWorks »
5. Sur l'éditeur de requêtes SQL, écrivez des instructions SQL pour créer un utilisateur et lui attribuer le rôle « datareader ». Exemple ci-dessous:



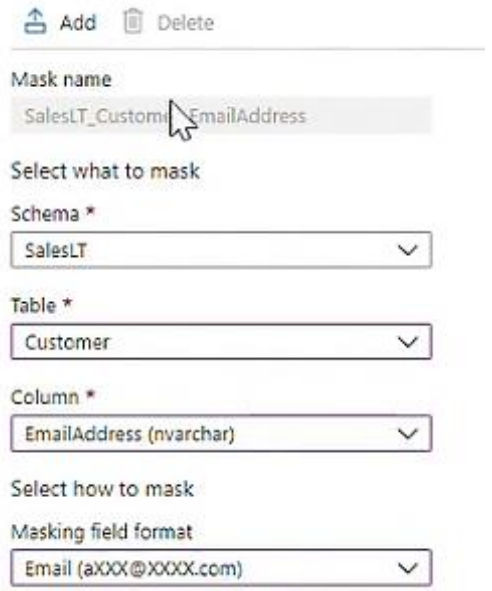
6. Sur le menu gauche, toujours au sein de la ressource de la base de données, cliquez sur « Dynamique Data Masking »



PARTIE 2

Eléments de réponse : tâche 3

6. Cliquez ensuite sur « Add mask »
7. Sur l'écran qui apparaitra, renseignez les champs comme décrit dans la capture ci-dessous:



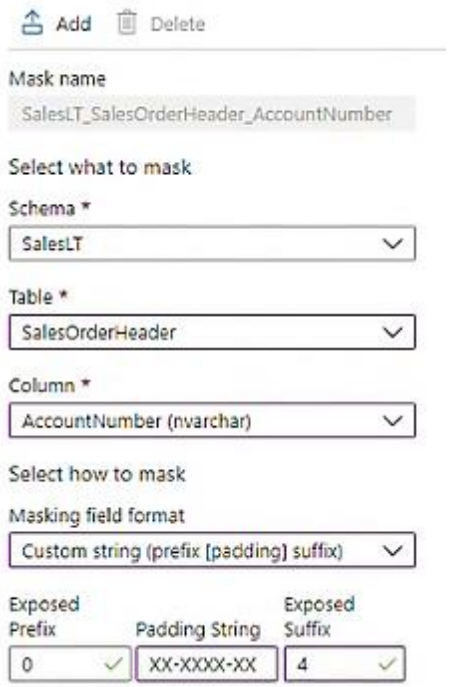
8. Cliquez sur « Add » puis sur « Save »

→ Vous venez d'ajouter une règle de masquage sur la colonne **EmailAdresse** de la table **Customer** en appliquant le format de masquage « aXXX@XXXX.com ».

PARTIE 2

Eléments de réponse : tâche 3

9. Ajouter une autre règle de masquage comme suit:



→ En faisant ainsi, vous créez une règle de masquage sur la colonne **AccountNumber** de la Table **SalesOrderHeader** qui affichera uniquement les 4 derniers chiffres.

PARTIE 2

Eléments de réponse : tâche 3

Pour pouvoir voir l'impact des deux dernières règles de masquage de données que vous avez créées, connectez vous en tant « user_test » (l'utilisateur que vous avez créé précédemment):

Une fois connecté, écrivez et exécutez sur « Query editor » la requête montrée dans la capture suivante.

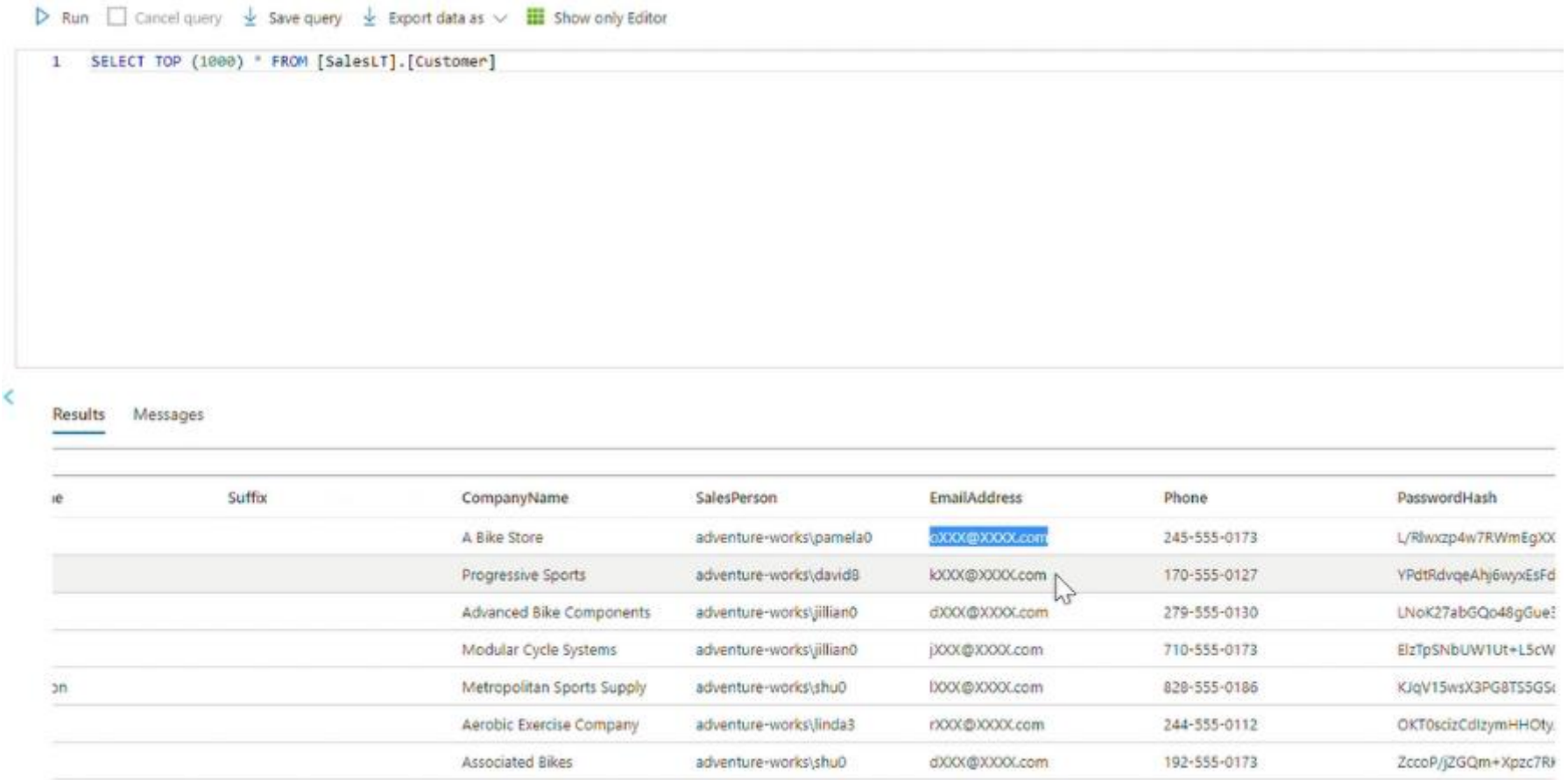
Vous allez remarquer que les données de la colonne **EmailAdresse** de la table **Customer** sont masquées conformément à la règle de masquage que vous avez défini.

PARTIE 2

Activité 4
Manipulation des mécanismes de protection des données

PARTIE 2

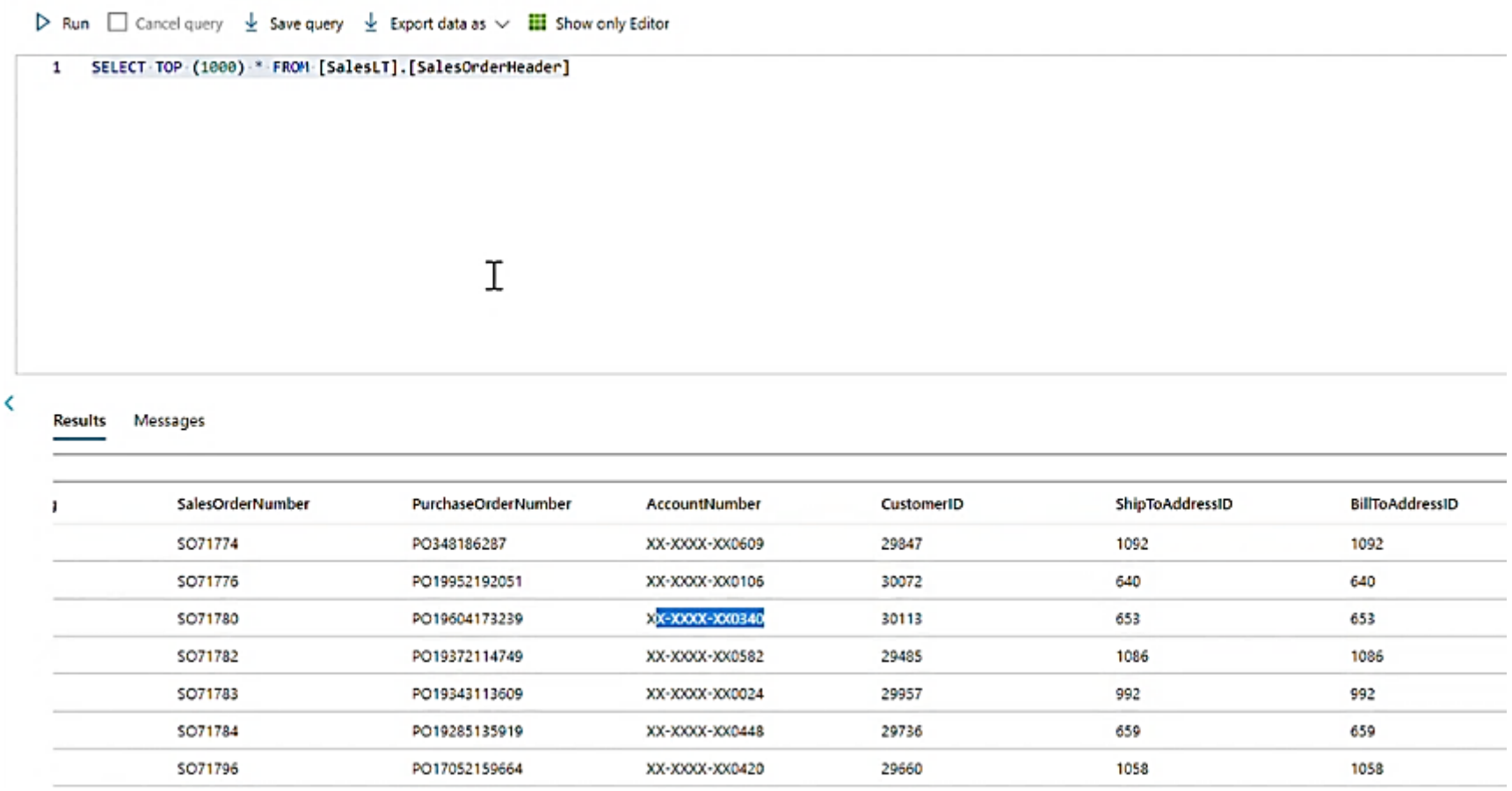
Eléments de réponse : tâche 3



ıe	Suffix	CompanyName	SalesPerson	EmailAddress	Phone	PasswordHash
		A Bike Store	adventure-works\pamela0	pXXX@XXXX.com	245-555-0173	L/Rlwxzp4w7RWmEgXX
		Progressive Sports	adventure-works\david8	kXXX@XXXX.com	170-555-0127	YPdtRdvqeAhj6wyxEsFd
		Advanced Bike Components	adventure-works\jillian0	dXXX@XXXX.com	279-555-0130	LNoK27abGQo48gGue3
		Modular Cycle Systems	adventure-works\jillian0	jXXX@XXXX.com	710-555-0173	ElzTpSNbUW1Ut+L5cW
on		Metropolitan Sports Supply	adventure-works\shu0	lXXX@XXXX.com	828-555-0186	KJqV15wsX3PG8TS5GSc
		Aerobic Exercise Company	adventure-works\linda3	rXXX@XXXX.com	244-555-0112	OKT0sclzCdIzymHHOty
		Associated Bikes	adventure-works\shu0	dXXX@XXXX.com	192-555-0173	ZccoP/jZGQm+Xpzc7R

Eléments de réponse : tâche 3

Idem pour la colonne **EmailAdresse** de la table **Customer:**



	SalesOrderNumber	PurchaseOrderNumber	AccountNumber	CustomerID	ShipToAddressID	BillToAddressID
	SO71774	PO348186287	XX-XXXX-XX0609	29847	1092	1092
	SO71776	PO19952192051	XX-XXXX-XX0106	30072	640	640
	SO71780	PO19604173239	XX-XXXX-XX0340	30113	653	653
	SO71782	PO19372114749	XX-XXXX-XX0582	29485	1086	1086
	SO71783	PO19343113609	XX-XXXX-XX0024	29957	992	992
	SO71784	PO19285135919	XX-XXXX-XX0448	29736	659	659
	SO71796	PO17052159664	XX-XXXX-XX0420	29660	1058	1058

PARTIE 2

ACTIVITÉ 5

QCM concernant la sécurité, Conformité et identité sur le Cloud Azure

Compétences visées :

- Valider et approfondir les connaissances de l'apprenant concernant les aspects de sécurité, Conformité et identité sur le Cloud Azure

Recommandations clés :

- Connaissance avancée sur les principes de sécurité, conformité et identité sur le Cloud Azure

4 heures

CONSIGNES

1. Pour le formateur

- Connaissances solides de la sécurité, Conformité et identité sur le Cloud Azure
- Débloquer les stagiaires en cas de difficulté
- Laisser un peu de temps aux stagiaires pour qu'ils puissent réaliser les tâches eux-mêmes
- Demander des explications quant aux réponses fournies

2. Pour l'apprenant

- Lire attentivement les questions
- En cas de problème ou blocage, le faire savoir à votre formateur
- Parcourir les réponses proposées
- Comparer vos réponses à celles proposées pour évaluer votre niveau de compréhension du cours

3. Conditions de réalisation :

- Seul
- Des ordinateurs dotés d'une connexion internet
- Un projecteur dans le cas d'une présentation à faire par le formateur pour présenter les réponses

4. Critères de réussite :

- +70% de réponses correctes

Activité 5

QCM concernant la sécurité, Conformité et identité sur le Cloud Azure

Travail demandé

Répondre aux questions ci-dessous concernant les aspects sécurité, confidentialité et identité sur le Cloud Azure :

1 - Dans le modèle de responsabilité partagée pour un déploiement Azure, Microsoft est responsable uniquement de la gestion de ?

A. Les appareils mobiles
B. Les autorisations pour les données utilisateur stockées dans Azure
C. La création et la gestion des comptes utilisateurs
D. La gestion du matériel physique

2 - Que pouvez-vous utiliser pour fournir à un utilisateur une fenêtre de deux heures pour effectuer une tâche administrative dans Azure ?

A. Azure Active Directory (Azure AD) Gestion des identités privilégiées (PIM)
B. Authentification multifacteur Azure (MFA)
C. Protection d'identité Azure Active Directory (Azure AD)
D. Politiques d'accès conditionnel

3 - Sélectionnez la réponse qui complète correctement la phrase.
Nécessite une vérification supplémentaire, comme un code de vérification envoyé vers un mobile :

A. Réécriture du mot de passe
B. Authentification multifacteur (MFA)
C. Authentification directe
D. Authentification unique (SSO)

4 - Pour chacune des affirmations suivantes, sélectionnez Oui si l'affirmation est vraie. Sinon, sélectionnez Non.

A. Les politiques d'accès conditionnel peuvent utiliser l'état d'un appareil comme signal (Oui – Non)
B. Les politiques d'accès conditionnel s'appliquent avant la fin de l'authentification du premier facteur (Oui – Non)
C. Les politiques d'accès conditionnel peuvent déclencher une authentification multi-facteurs (MFA) si un utilisateur tente d'accéder à une application spécifique (Oui – Non)

5 - Azure Active Directory (Azure AD) est _____ utilisé pour l'authentification et l'autorisation.

A. Un système de détection et de réponse étendues (XDR)
B. Un fournisseur d'identité
C. Un gestionnaire de groupe
D. Un système de gestion des informations et des événements de sécurité (SIEM)

Activité 5

QCM concernant la sécurité, Conformité et identité sur le Cloud Azure

Travail demandé

Répondre aux questions ci-dessous concernant les aspects sécurité, confidentialité et identité sur le Cloud Azure :

6 - Quelles sont les deux fonctionnalités de Microsoft Defender pour Endpoint ? Chaque sélection correcte présente une solution complète.

A. Investigation et correction automatisées
B. Cryptage du transport
C. Détection informatique fantôme (Shadow IT)
D. Réduction de la surface d'attaque

7 - Associez le service de mise en réseau Azure à la description appropriée. Pour répondre, faites correspondre le service approprié de la colonne de gauche vers sa description à droite. Chaque service peut être utilisé une fois, plusieurs fois ou pas du tout.

1 - Azure Bastion	A - Fournit des services de traduction d'adresses réseau (NAT)
2 - Azure Firewall	B - Fournit une connectivité de bureau à distance sécurisée et transparente aux machines virtuelles Azure
3 - Network Security Group (NSG)	C - Fournit un filtrage du trafic qui peut être appliqué à des interfaces réseau spécifiques sur un réseau virtuel

8 - Pour chacune des affirmations suivantes, sélectionnez Oui si l'affirmation est vraie. Sinon, sélectionnez Non.

A. Azure Active Directory (Azure AD) Identity Protection peut ajouter des utilisateurs à des groupes en fonction du niveau de risque de l'utilisateur. (Oui – Non)
B. Azure Active Directory (Azure AD) Identity Protection peut détecter si les informations d'identification de l'utilisateur ont été divulguées au public. (Oui – Non)
C. Azure Active Directory (Azure AD) Identity Protection peut être utilisé pour appeler l'authentification multifacteur en fonction du niveau de risque d'un utilisateur. (Oui – Non)

9 - Pour chacune des affirmations suivantes, sélectionnez Oui si l'affirmation est vraie. Sinon, sélectionnez Non.

A. L'application de mises à jour système augmente le score de sécurité d'une organisation dans Azure Security Center. (Oui – Non)
B. Le score de sécurité dans Azure Security Center peut évaluer les ressources sur plusieurs abonnements Azure. (Oui – Non)
C. L'activation de l'authentification multifacteur (MFA) augmente le score de sécurité d'une organisation dans Azure Security Center. (Oui – Non)

10 - Quel portail Microsoft fournit des informations sur la conformité des services Cloud Microsoft aux normes réglementaires, telles que l'Organisation internationale pour Normalisation (ISO) ?

A. Le centre d'administration Microsoft Endpoint Manager
B. Gestion des coûts Azure + Facturation
C. Le Portail Microsoft Service Trust
D. Le centre d'administration Azure Active Directory

Activité 5

QCM concernant la sécurité, Conformité et identité sur le Cloud Azure

Travail demandé

Répondre aux questions ci-dessous concernant les aspects sécurité, confidentialité et identité sur le Cloud Azure :

11 - Qu'utilisez-vous pour fournir une intégration en temps réel entre Azure Sentinel et une autre source de sécurité ? A. Connexion Azure AD B. Un espace de travail Log Analytics C. Protection des informations Azure D. Un connecteur
12 - Pour chacune des affirmations suivantes, sélectionnez Oui si l'affirmation est vraie. Sinon, sélectionnez Non. A. Vous pouvez créer des rôles personnalisés dans Azure Active Directory (Azure AD). (Oui – Non) B. L'administration globale est un rôle dans Azure Active Directory (Azure AD). (Oui – Non) C. Un utilisateur Azure Active Directory (Azure AD) ne peut se voir attribuer qu'un seul rôle. (Oui – Non)
13 - Azure DDoS Protection Standard peut être utilisé pour protéger A. Applications Azure AD. B. Utilisateurs Azure AD. C. Groupes de ressources. D. Réseaux virtuels.
14 - Sélectionnez la réponse qui complète correctement la phrase. _____ est une solution Cloud native de gestion des informations et des événements de sécurité (SIEM) et de réponse automatisée d'orchestration de la sécurité (SOAR) utilisée pour fournir une solution unique pour la détection des alertes, la visibilité des menaces, la recherche proactive et la réponse aux menaces. A. Azure Advisor. B. Azure Monitor. C. Azure Sentinel. D. Azure Bastion.
15 - Dans un modèle d'identité hybride, que pouvez-vous utiliser pour synchroniser les identités entre les services de domaine Active Directory (AD DS) et Azure Active Directory (Azure AD) ? A. Services de fédération Active Directory (AD FS). B. Azure Sentinel. C. Azure AD Connect. D. Azure AD Privileged Identity Management (PIM).

PARTIE 2

Activité 5

QCM concernant la sécurité, Conformité et identité sur le Cloud Azure

Travail demandé

Répondre aux questions ci-dessous concernant les aspects sécurité, confidentialité et identité sur le Cloud Azure :

16 - Sélectionnez la réponse qui complète correctement la phrase.
_____est une solution basée sur le Cloud qui exploite les signaux Active Directory sur site pour identifier, détecter et enquêter sur les menaces avancées.

A. Microsoft Cloud App Security.
B. Microsoft Defender for Endpoint.
C. Microsoft Defender for Identity.
D. Microsoft Defender for Office 365.

17 - Pour chacune des affirmations suivantes, sélectionnez Oui si l'affirmation est vraie. Sinon, sélectionnez Non.

A. Azure Defender peut détecter les vulnérabilités et les menaces pour le Azure Storage. (Oui – Non)
B. Cloud Security Posture Management (CSPM) est disponible pour tous les abonnements Azure. (Oui – Non)
C. Azure Security Center peut évaluer la sécurité des charges de travail déployées sur Azure ou sur site. (Oui – Non)

18 - Sélectionnez la réponse qui complète correctement la phrase.
_____fournit les meilleures pratiques des employés, partenaires et clients de Microsoft, y compris des outils et des conseils pour faciliter un déploiement Azure.

A. Azure Blueprint.
B. Azure Policy.
C. A ressource lock.
D. The Microsoft Cloud Adoption Framework to Azure.

19 - Sélectionnez la réponse qui complète correctement la phrase.
_____un fichier rend les données du fichier lisibles et utilisables par les utilisateurs disposant de la clé appropriée.

A. Archivage.
B. Compression.
C. Déduplication.
D. Chiffrement.

PARTIE 2

Activité 5

QCM concernant la sécurité, Conformité et identité sur le Cloud Azure

Travail demandé

Répondre aux questions ci-dessous concernant les aspects sécurité, confidentialité et identité sur le Cloud Azure :

20 - Vous avez des machines virtuelles Azure sur lesquelles Update Management est activé. Les machines virtuelles sont configurées comme indiqué dans le tableau suivant.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West US	RG1
VM3	Windows Server 2016	West US	RG2
VM4	Ubuntu Server 18.04 LTS	West US	RG2
VM5	Red Hat Enterprise Linux 7.4	East US	RG1
VM6	CentOS 7.5	East US	RG1

Vous planifiez deux déploiements de mise à jour nommés Update1 et Update2. Update1 met à jour VM3. Update2 met à jour VM6.
Quelles machines virtuelles supplémentaires peuvent être mises à jour à l'aide de Update1 et Update2 ? Pour répondre, Choisissez les options appropriées.

Update 1 :

A. VM2 uniquement.
B. VM4 uniquement.
C. VM1 et VM2 uniquement.
D. VM1, VM2, VM4, VM5 et VM6.

Update 2 :

A. VM5 uniquement.
B. VM1 et VM5 uniquement.
C. VM4 et VM5 uniquement.
D. VM1, VM2 et VM5 uniquement.
E. VM1, VM2, VM3, VM4 et VM5.

PARTIE 2

Activité 5

QCM concernant la sécurité, Conformité et identité sur le Cloud Azure

Eléments de réponse : QCM

1 - Dans le modèle de responsabilité partagée pour un déploiement Azure, Microsoft est responsable uniquement de la gestion de ?

A. Les appareils mobiles
B. Les autorisations pour les données utilisateur stockées dans Azure
C. La création et la gestion des comptes utilisateurs
D. La gestion du matériel physique

2 - Que pouvez-vous utiliser pour fournir à un utilisateur une fenêtre de deux heures pour effectuer une tâche administrative dans Azure ?

A. Azure Active Directory (Azure AD) Gestion des identités privilégiées (PIM)
B. Authentification multifacteur Azure (MFA)
C. Protection d'identité Azure Active Directory (Azure AD)
D. Politiques d'accès conditionnel

3 - Sélectionnez la réponse qui complète correctement la phrase.
Nécessite une vérification supplémentaire, comme un code de vérification envoyé vers un mobile :

A. Réécriture du mot de passe
B. Authentification multifacteur (MFA)
C. Authentification directe
D. Authentification unique (SSO)

4 - Pour chacune des affirmations suivantes, sélectionnez Oui si l'affirmation est vraie. Sinon, sélectionnez Non.

A. Les politiques d'accès conditionnel peuvent utiliser l'état d'un appareil comme signal (Oui – Non)
B. Les politiques d'accès conditionnel s'appliquent avant la fin de l'authentification du premier facteur (Oui – Non)
C. Les politiques d'accès conditionnel peuvent déclencher une authentification multi-facteurs (MFA) si un utilisateur tente d'accéder à une application spécifique (Oui – Non)

5 - Azure Active Directory (Azure AD) est _____ utilisé pour l'authentification et l'autorisation.

A. Un système de détection et de réponse étendues (XDR)
B. Un fournisseur d'identité
C. Un gestionnaire de groupe
D. Un système de gestion des informations et des événements de sécurité (SIEM)

PARTIE 2

Activité 5

QCM concernant la sécurité, Conformité et identité sur le Cloud Azure

Eléments de réponse : QCM

6 - Quelles sont les deux fonctionnalités de Microsoft Defender pour Endpoint ? Chaque sélection correcte présente une solution complète. A. Investigation et correction automatisées B. Cryptage du transport C. Détection informatique fantôme (Shadow IT) D. Réduction de la surface d'attaque
7 - Associez le service de mise en réseau Azure à la description appropriée. Pour répondre, faites correspondre le service approprié de la colonne de gauche vers sa description à droite. Chaque service peut être utilisé une fois, plusieurs fois ou pas du tout. 2 – A 1 -- B 3 -- C
8 - Pour chacune des affirmations suivantes, sélectionnez Oui si l'affirmation est vraie. Sinon, sélectionnez Non. A. Azure Active Directory (Azure AD) Identity Protection peut ajouter des utilisateurs à des groupes en fonction du niveau de risque de l'utilisateur. (Oui – Non) B. Azure Active Directory (Azure AD) Identity Protection peut détecter si les informations d'identification de l'utilisateur ont été divulguées au public. (Oui – Non) C. Azure Active Directory (Azure AD) Identity Protection peut être utilisé pour appeler l'authentification multifacteur en fonction du niveau de risque d'un utilisateur. (Oui – Non)
9 - Pour chacune des affirmations suivantes, sélectionnez Oui si l'affirmation est vraie. Sinon, sélectionnez Non. A. L'application de mises à jour système augmente le score de sécurité d'une organisation dans Azure Security Center. (Oui – Non) B. Le score de sécurité dans Azure Security Center peut évaluer les ressources sur plusieurs abonnements Azure. (Oui – Non) C. L'activation de l'authentification multifacteur (MFA) augmente le score de sécurité d'une organisation dans Azure Security Center. (Oui – Non)
10 - Quel portail Microsoft fournit des informations sur la conformité des services Cloud Microsoft aux normes réglementaires, telles que l'Organisation internationale pour Normalisation (ISO) ? A. Le centre d'administration Microsoft Endpoint Manager B. Gestion des coûts Azure + Facturation C. Le Portail Microsoft Service Trust D. Le centre d'administration Azure Active Directory

PARTIE 2

Activité 5

QCM concernant la sécurité, Conformité et identité sur le Cloud Azure

Eléments de réponse : QCM

11 - Qu'utilisez-vous pour fournir une intégration en temps réel entre Azure Sentinel et une autre source de sécurité ?

A. Connexion Azure AD
B. Un espace de travail Log Analytics
C. Protection des informations Azure
D. Un connecteur

12 - Pour chacune des affirmations suivantes, sélectionnez Oui si l'affirmation est vraie. Sinon, sélectionnez Non.

A. Vous pouvez créer des rôles personnalisés dans Azure Active Directory (Azure AD). (Oui – Non)
B. L'administration globale est un rôle dans Azure Active Directory (Azure AD). (Oui – Non)
C. Un utilisateur Azure Active Directory (Azure AD) ne peut se voir attribuer qu'un seul rôle. (Oui – Non)

13 - Azure DDoS Protection Standard peut être utilisé pour protéger

A. Applications Azure AD.
B. Utilisateurs Azure AD.
C. Groupes de ressources.
D. Réseaux virtuels.

14 - Sélectionnez la réponse qui complète correctement la phrase.

_____ est une solution Cloud native de gestion des informations et des événements de sécurité (SIEM) et de réponse automatisée d'orchestration de la sécurité (SOAR) utilisée pour fournir une solution unique pour la détection des alertes, la visibilité des menaces, la recherche proactive et la réponse aux menaces.

A. Azure Advisor.
B. Azure Monitor.
C. Azure Sentinel.
D. Azure Bastion.

15 - Dans un modèle d'identité hybride, que pouvez-vous utiliser pour synchroniser les identités entre les services de domaine Active Directory (AD DS) et Azure Active Directory (Azure AD) ?

A. Services de fédération Active Directory (AD FS).
B. Azure Sentinel.
C. Azure AD Connect.
D. Azure AD Privileged Identity Management (PIM).

PARTIE 2

Activité 5

QCM concernant la sécurité, Conformité et identité sur le Cloud Azure

Eléments de réponse : QCM

16 - Sélectionnez la réponse qui complète correctement la phrase.

_____est une solution basée sur le Cloud qui exploite les signaux Active Directory sur site pour identifier, détecter et enquêter sur les menaces avancées.

A. Microsoft Cloud App Security.
B. Microsoft Defender for Endpoint.
C. Microsoft Defender for Identity.
D. Microsoft Defender for Office 365.

17 - Pour chacune des affirmations suivantes, sélectionnez Oui si l'affirmation est vraie. Sinon, sélectionnez Non.

A. Azure Defender peut détecter les vulnérabilités et les menaces pour le Azure Storage. (Oui – Non)
B. Cloud Security Posture Management (CSPM) est disponible pour tous les abonnements Azure. (Oui – Non)
C. Azure Security Center peut évaluer la sécurité des charges de travail déployées sur Azure ou sur site. (Oui – Non)

18 - Sélectionnez la réponse qui complète correctement la phrase.

_____fournit les meilleures pratiques des employés, partenaires et clients de Microsoft, y compris des outils et des conseils pour faciliter un déploiement Azure.

A. Azure Blueprint.
B. Azure Policy.
C. A ressource lock.
D. The Microsoft Cloud Adoption Framework to Azure.

19 - Sélectionnez la réponse qui complète correctement la phrase.

_____un fichier rend les données du fichier lisibles et utilisables par les utilisateurs disposant de la clé appropriée.

A. Archivage.
B. Compression.
C. Déduplication.
D. Chiffrement.

PARTIE 2

Activité 5

QCM concernant la sécurité, Conformité et identité sur le Cloud Azure

Eléments de réponse : QCM

20 - Vous avez des machines virtuelles Azure sur lesquelles Update Management est activé. Les machines virtuelles sont configurées comme indiqué dans le tableau suivant.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West US	RG1
VM3	Windows Server 2016	West US	RG2
VM4	Ubuntu Server 18.04 LTS	West US	RG2
VM5	Red Hat Enterprise Linux 7.4	East US	RG1
VM6	CentOS 7.5	East US	RG1

Vous planifiez deux déploiements de mise à jour nommés Update1 et Update2. Update1 met à jour VM3. Update2 met à jour VM6.
Quelles machines virtuelles supplémentaires peuvent être mises à jour à l'aide de Update1 et Update2 ? Pour répondre, Choisissez les options appropriées.

Update 1 :

A. VM2 uniquement.
B. VM4 uniquement.
C. VM1 et VM2 uniquement.
D. VM1, VM2, VM4, VM5 et VM6.

Update 2 :

A. VM5 uniquement.
B. VM1 et VM5 uniquement.
C. VM4 et VM5 uniquement.
D. VM1, VM2 et VM5 uniquement.
E. VM1, VM2, VM3, VM4 et VM5.

PARTIE 2

ACTIVITÉ 6

Chiffrement de disque d’une VM avec l’utilisation d’Azure Key Vault

Compétences visées :

- Manipuler Azure Key Vault
- Comprendre comment chiffrer un disque d’une VM sur Azure

Recommandations clés :

- Consulter le support de cours afin de se rappeler du principe de base des keys vault et du chiffrement des disques sur Azure

5 heures

CONSIGNES

1. Pour le formateur

- Maitrise des aspects du chiffrement des disques au niveau de Azure avec l'utilisation des key vaults
- Débloquer les stagiaires en cas de difficulté
- Laisser un peu de temps aux stagiaires pour qu'ils puissent réaliser les tâches eux mêmes

2. Pour l'apprenant

- Suivre le TP étape par étape et dans l'ordre
- En cas de problème ou blocage, le faire savoir à votre formateur
- Parcourir les réponses proposées
- Comparer vos réponses à celles proposées pour évaluer votre niveau de compréhension du cours

3. Conditions de réalisation :

- Seul ou en binôme
- Des ordinateurs dotés d'une connexion internet
- Des comptes Azure pour que les stagiaires puissent réaliser le TP
- Un projecteur dans le cas d'une présentation à faire par le formateur pour montrer un use case aux stagiaires

4. Critères de réussite :

- Terminer toutes les étapes du TP avec succès
- Atteindre l'objectif global du TP

Activité 6

Chiffrement de disque d'une VM avec l'utilisation d'Azure Key Vault

Travail demandé

Dans ce TP, vous allez effectuer les tâches suivantes:

Tâche 1: Créer un Key Vault

Tâche 2: En utilisant Cloud Shell sur le portail Azure, vous allez effectuer quelques commandes PowerShell afin de chiffrer un disque sur une VM déjà créée.

PARTIE 2

Activité 6

Chiffrement de disque d'une VM avec l'utilisation d'Azure Key Vault

Travail demandé

Tâche 1: Créer un Key Vault

1. Se connecter au portail Azure avec vos identifiants de connexion.
2. Sur la barre de recherche, tapez le mot « key vault »:

3. Cliquez ensuite sur le service Key vault.

PARTIE 2

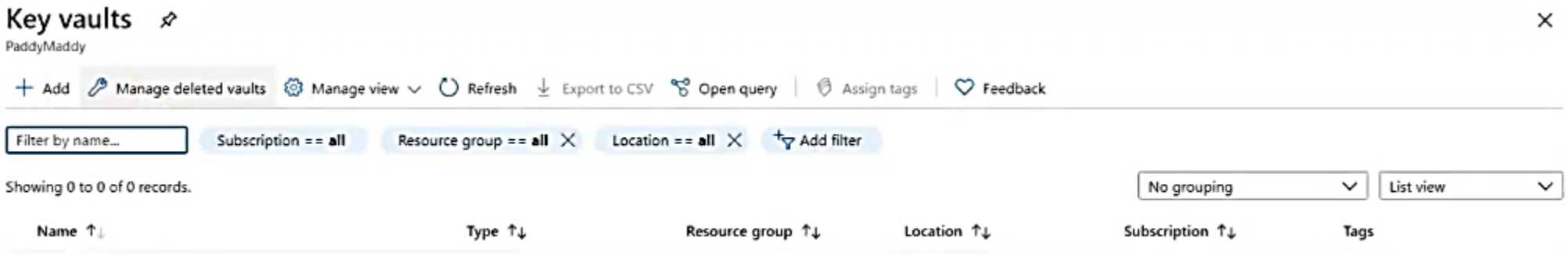
Activité 6

Chiffrement de disque d'une VM avec l'utilisation d'Azure Key Vault

Travail demandé

Une fois que vous avez cliqué sur le service « Key vault », vous allez être redirigé vers une autre page qui contient les différents key vaults déjà créés.

4. Cliquez sur « + Add » pour ajouter un nouveau Key vault:



5. Renseignez les champs obligatoires sur la première page:

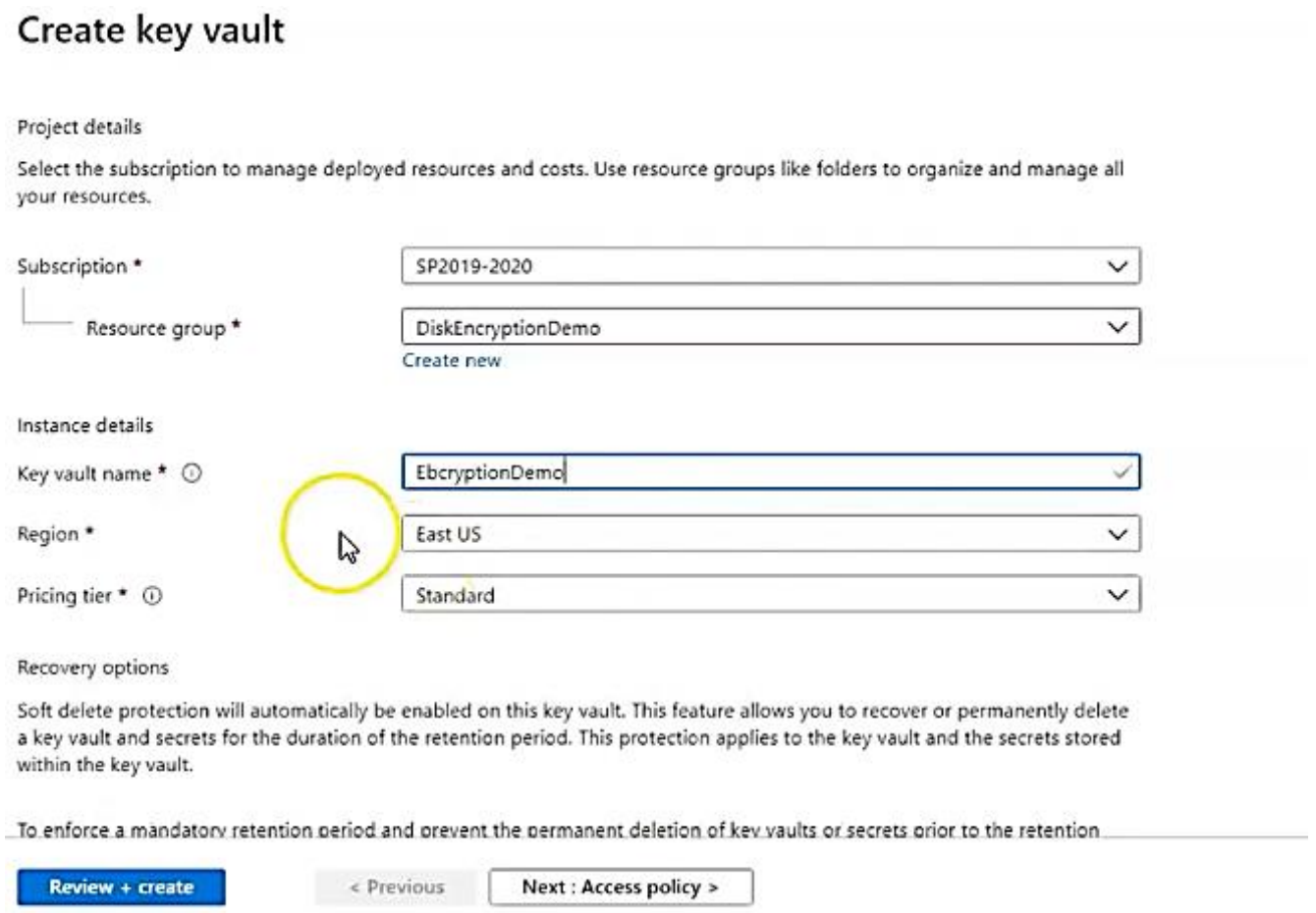
PARTIE 2

Activité 6

Chiffrement de disque d'une VM avec l'utilisation d'Azure Key Vault

PARTIE 2

Travail demandé

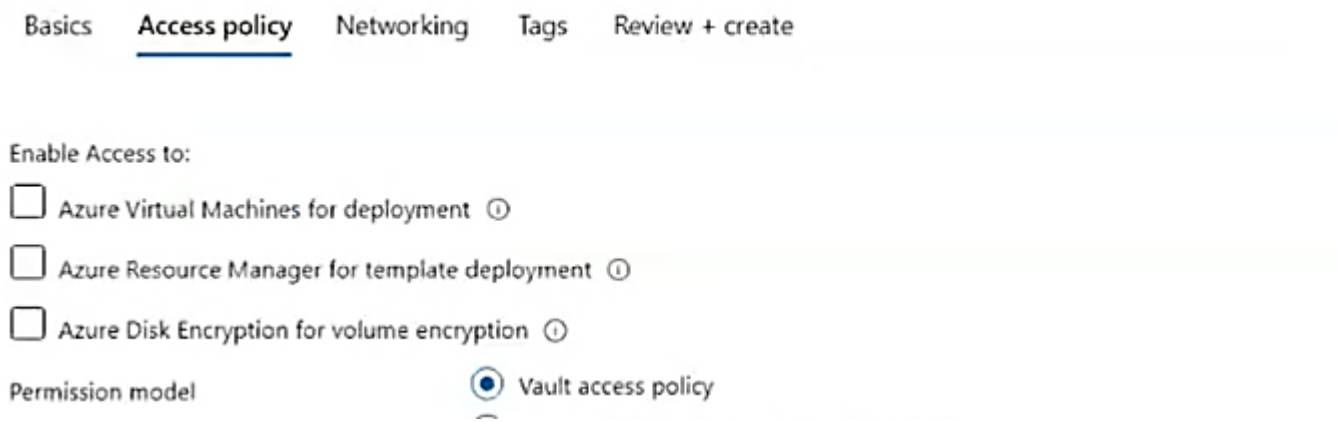


Activité 6

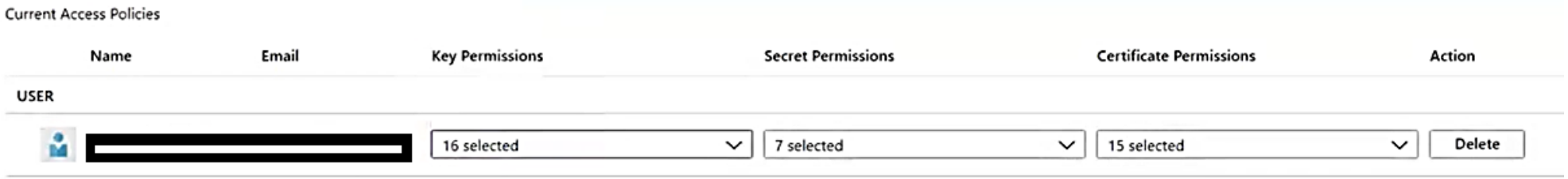
Chiffrement de disque d'une VM avec l'utilisation d'Azure Key Vault

Travail demandé

6. Cliquez sur « Next: Access Policy > » et cochez les trois cases à cocher sous « Enable Access to: »:



7. Sous « Current Access Policies », cochez toutes les cases à cocher disponibles dans: « Key permession », « Secret Permission » et « Certificate Permission ».



PARTIE 2

Activité 6

Chiffrement de disque d'une VM avec l'utilisation d'Azure Key Vault

Travail demandé

7. Cliquez sur « Review + Create » puis sur « create »

→ A ce stade, la création du nouveau Key Vault est lancée et doit être prête dans quelques seconds.

8. Une fois la création du keyvault terminée, accéder à cette nouvelle ressource. Sur la partie « Overview », repérez la propriété « Vault URI » et notez la.

PARTIE 2

Activité 6

Chiffrement de disque d'une VM avec l'utilisation d'Azure Key Vault

Travail demandé

Tâche 2: En utilisant Cloud Shell sur le portail Azure, vous allez effectuer quelques commandes PowerShell afin de chiffrer un disque sur une VM déjà créée.

1. Sur la barre en haut du portail Azure, cliquez sur l'option « Cloud Shell »

2. Tapez la commande ci-dessous:

```
$KeyVault = Get-AzKeyVault -VaultName EbcryptionDemo -ResourceGroupName DiskEncryptionDemo
```

Ceci vous permet de stocker la valeur du key vault sur une variable $KeyVault.

3. Tapez la commande ci-dessous:

```
Set-AzVMDiskEncryptionExtension -ResourceGroupName DiskEncryptionDemo -VMName VM01 -DiskEncryptionKeyVaultUrl $KeyVault.VaultUri -DiskEncryptionKeyVaultId $KeyVault.ResourceId
```

La commande ci-dessus, vous permet de chiffrer le disque de la VM01 en utilisant le kevault que vous avez créé précédemment.

Si vous exécutez cette commande, vous devrez avoir un message comme celui-ci:

PARTIE 2

Activité 6

Chiffrement de disque d'une VM avec l'utilisation d'Azure Key Vault

Travail demandé

```
Enable AzureDiskEncryption on the VM
This cmdlet prepares the VM and enables encryption which may reboot the machine and takes 10-15 minutes to finish. Please save your work on the VM before
confirming. Do you want to continue?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
```

4. Assurez-vous d'avoir sauvegardé vos travaux sur cette machine avant de procéder à la confirmation.

5. Tapez « Y » pour confirmer.

Si tout est OK, vous devez avoir le message ci-dessous:

```
RequestId IsSuccessStatusCode StatusCode ReasonPhrase
--------- ------------------- ---------- ------------
                         True         OK OK
```

Afin de vérifier si le disque sur cette machine est chiffré, déplacez vous la VM concernée, puis cliquez sur « Disks ». Normalement, vous devez observer que le disque est chiffré avec une clé de chiffrage grâce au key vault créé précédemment:

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption ⓘ	Host caching ⓘ
Vm01_disk1_3fc6059122ab4	Premium SSD	127	500	100	SSE with PMK & ADE	Read/write

PARTIE 2

PARTIE 3

Superviser les ressources Cloud

Dans ce module, vous allez :

- Découvrir la journalisation des événements dans un espace centralisé

9 heures

ACTIVITE n°1

Utiliser les outils natifs de journalisation des évènements dans le Cloud

Compétences visées :

- Déployer les mécanismes de journalisation des événements dans le Cloud

Recommandations clés :

- Se référer au cours
- Discuter en groupe les nouveaux termes liés au Cloud

4 heures

CONSIGNES

1. Pour le formateur

- Permettre au stagiaire de bien lire et comprendre seul les études de cas
- S'assurer de la bonne compréhension des cas d'étude
- Discuter les réponses des stagiaires avant de donner la solution
- Favoriser le travail en groupe concernant les activités de recherche sur internet

2. Pour l'apprenant

- Lire et bien comprendre les études de cas avant de passer aux questions
- Lire et bien comprendre les questions

3. Conditions de réalisation :

- Individuel ou par groupes (2 ou 3 maximum)
- Support de résumé théorique accompagnant
- Ordinateur portable avec un abonnement Azure payant ou gratuit actif

4. Critères de réussite :

- Répondre aux différentes questions soulevées au niveau de l'énoncé
- Travail en groupe
- Travaux pratiques opérationnels

Etude de cas n°1 : Journalisation des évènements dans le Cloud

Les journaux de ressources fournissent des insights sur le fonctionnement détaillé des ressources Azure, et sont utiles pour superviser leur intégrité et leur disponibilité. Les ressources Azure génèrent automatiquement des journaux de ressource, mais vous devez créer un paramètre de diagnostic pour les collecter. Dans ce TP vous êtes amené à créer un paramètre de diagnostic pour envoyer des journaux de ressource à un espace de travail Log Analytics dans lequel vous pouvez les analyser avec des requêtes de journal.

Tâche 1 : Créer un espace de travail Log Analytics dans Azure Monitor pour une machine virtuelle.

Tâche 2 : Créer un paramètre pour collecter les logs des ressources.

Tâche 3 : Créer une requête de journal simple pour analyser les journaux collecter.

Tâche 4 : Créer une règle d'alerte de requête de journal.

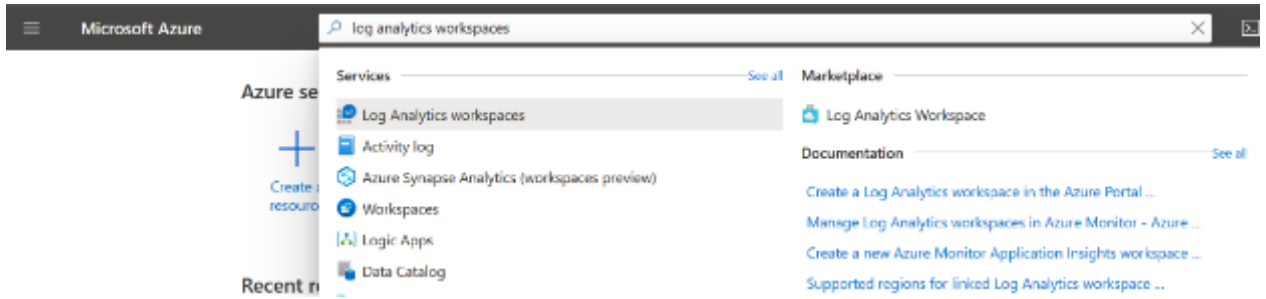
Tâche 5 : Créer un groupe d'actions pour définir les détails de la notification.

PARTIE 3

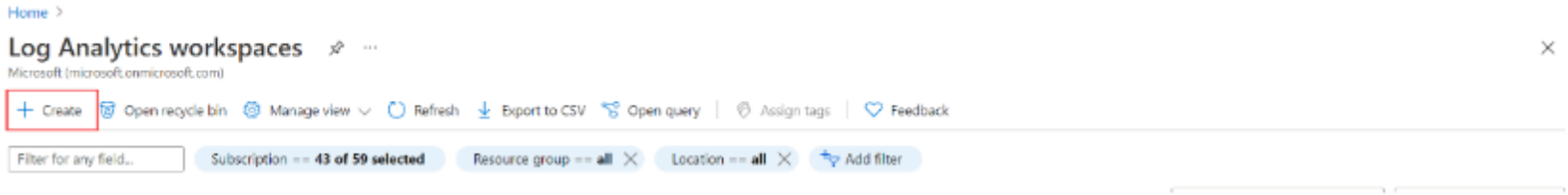
Eléments de réponse

Tâche 1 : Créer un espace de travail Log Analytics dans Azure Monitor pour une machine virtuelle.

À partir de **Tous les services** dans le portail Azure, sélectionnez **Espaces de travail Log Analytics**.



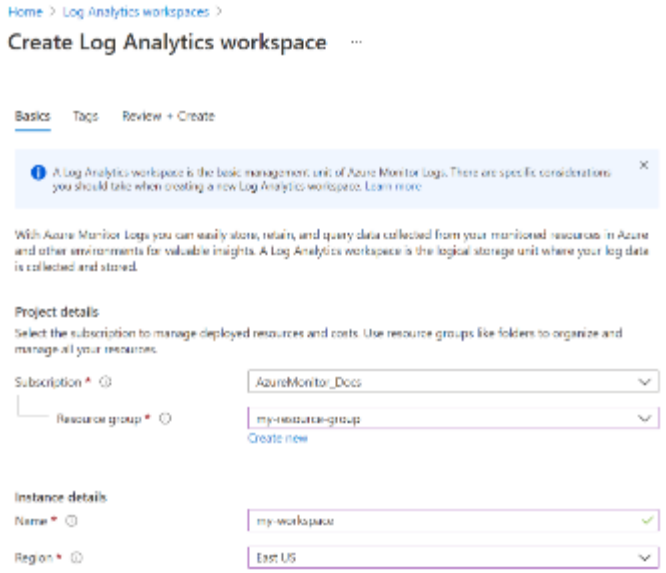
Cliquez sur **Créer** pour créer un espace de travail.



PARTIE 3

Eléments de réponse

Sous l'onglet **Informations de base**, sélectionnez un **abonnement**, un **groupe de ressources** et une **région** pour l'espace de travail. Ces derniers n'ont pas besoin d'être identiques à ceux de la ressource supervisée. Indiquez un **nom** globalement unique sur l'ensemble des abonnements Azure Monitor.



Cliquez sur **Vérifier + créer** pour créer l'espace de travail.

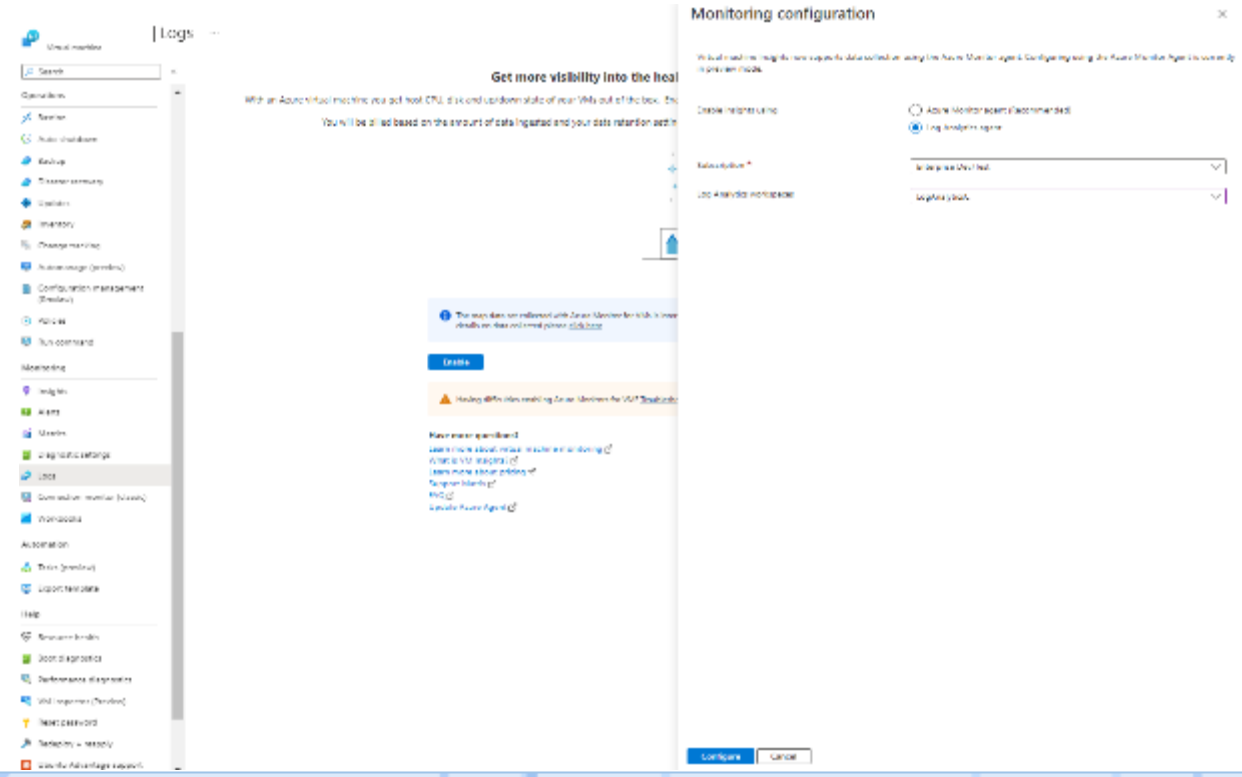
PARTIE 3

Eléments de réponse

Tâche 2 : Créer un paramètre de diagnostic pour collecter des journaux de ressources.

Les paramètres de diagnostic définissent où les journaux de ressources doivent être envoyés pour une ressource particulière. Un même paramètre de diagnostic peut avoir plusieurs destinations, mais nous n'utiliserons qu'un espace de travail Log Analytics dans ce tutoriel.

Sous la section **Monitoring** du menu de votre ressource, sélectionnez **Logs** et cliquez sur **Activer** puis sélectionnez **Log analyse agent** et choisissez le nom Log Workspace puis **Configure**.



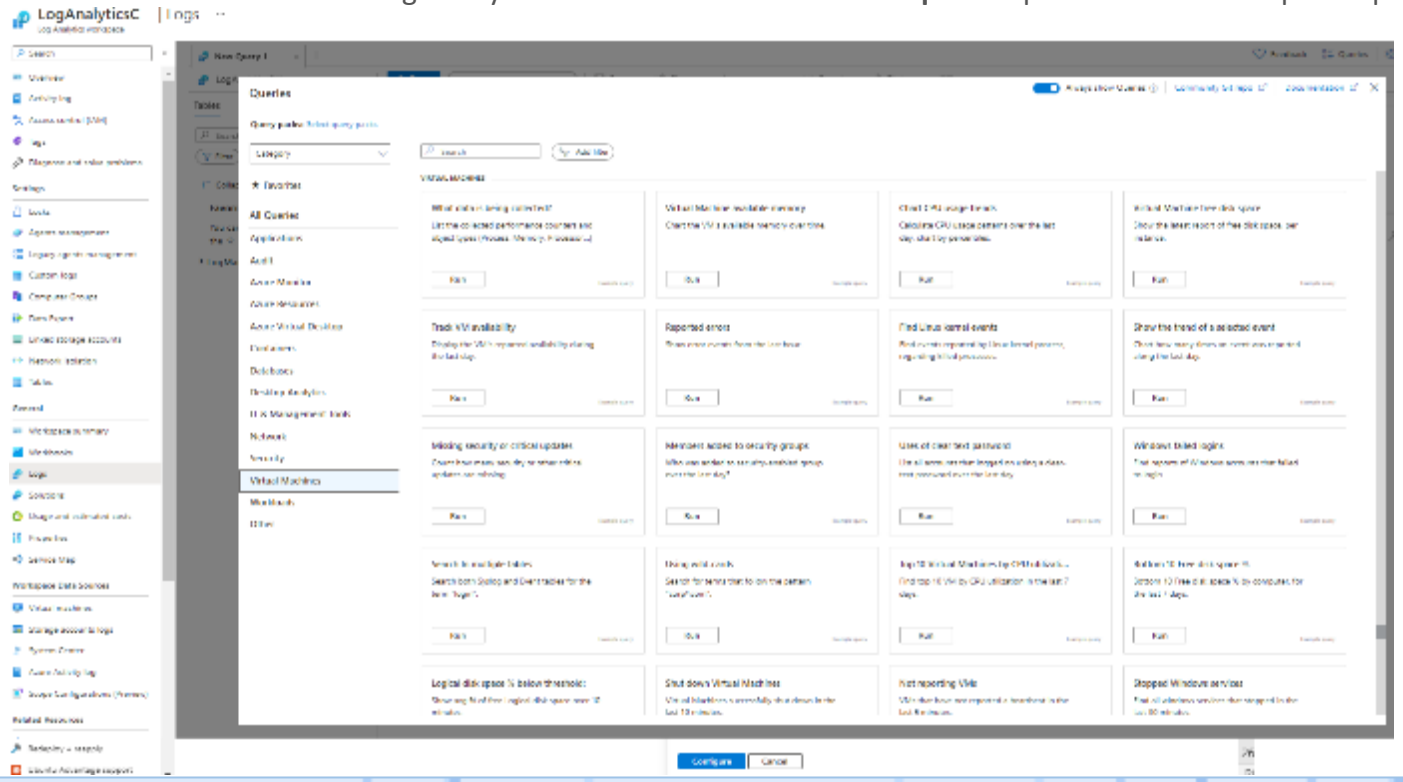
PARTIE 3

Eléments de réponse

Tâche 3 : Créer une requête de journal simple pour analyser les journaux collectés.

Les données sont récupérées à partir d'un espace de travail Log Analytics à l'aide d'une requête de journal écrite en langage KQL (Kusto Query Language). Un ensemble de requêtes précréées est disponible pour de nombreux services Azure. Vous n'avez donc pas besoin de connaître KQL pour commencer.

Sélectionnez **Journaux** dans le menu de votre ressource. Log Analytics s'ouvre avec la fenêtre **Requêtes** qui contient des requêtes prégénérées pour votre **Type de ressource**.

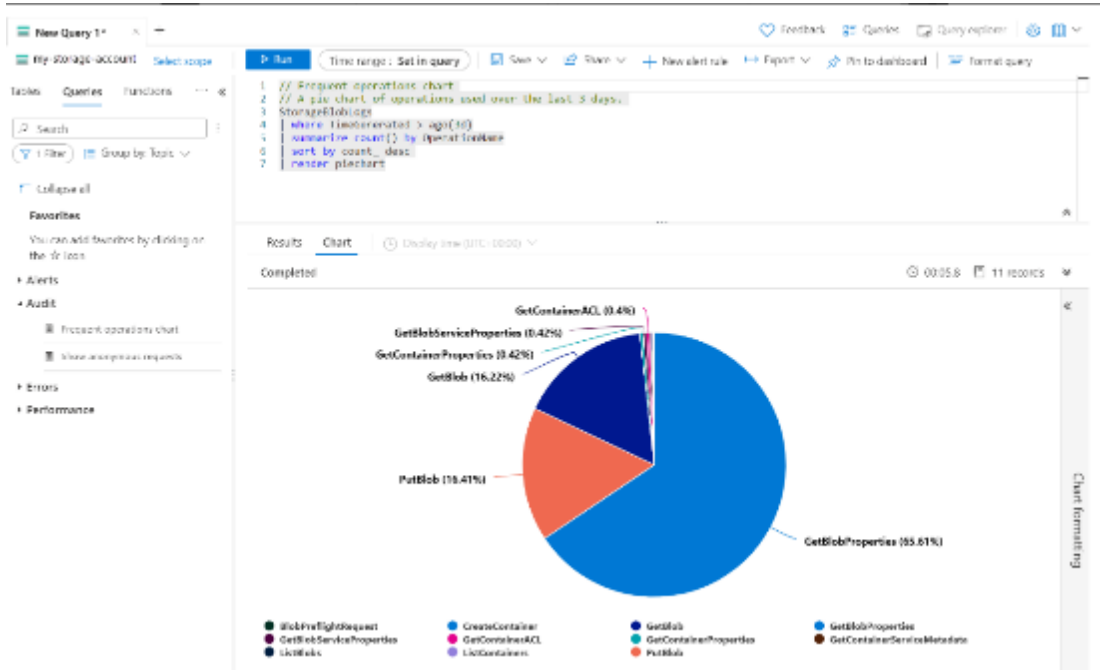


PARTIE 3

Eléments de réponse

Tâche 3 : Créer une requête de journal simple pour analyser les journaux collectés.

Parcourez les requêtes disponibles. Identifiez-en une à exécuter et cliquez sur **Exécuter**. La requête est ajoutée à la fenêtre de requête et les résultats sont retournés.



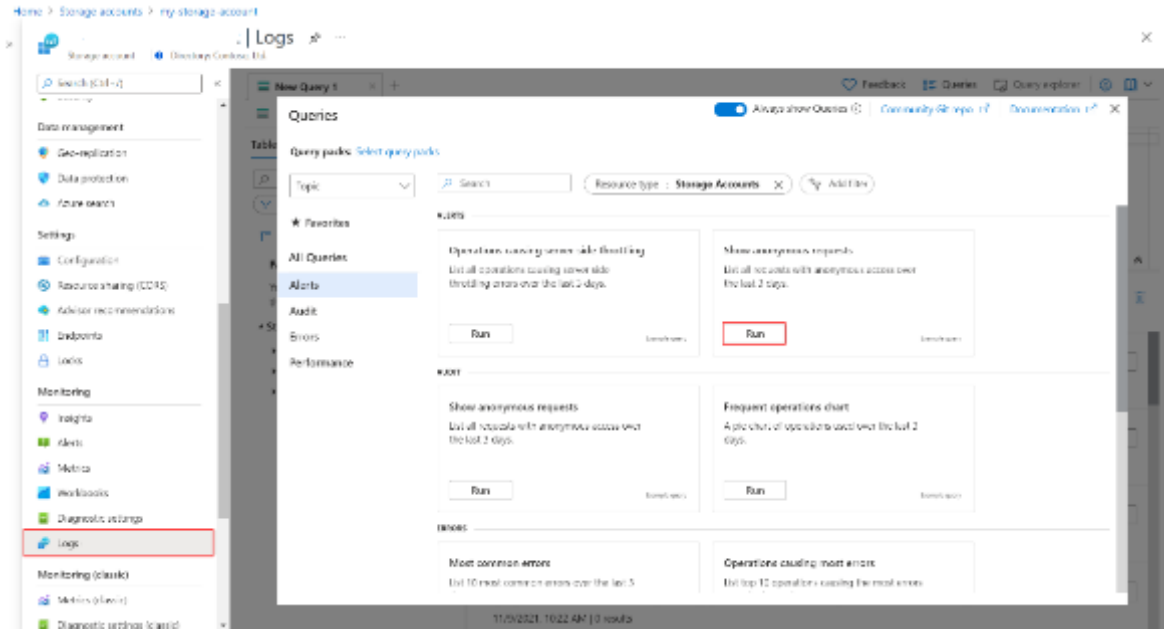
PARTIE 3

Eléments de réponse

Tâche 4 : Créer une règle d'alerte de requête de journal.

Les données sont récupérées à partir d'un espace de travail Log Analytics à l'aide d'une requête de journal écrite en langage KQL (Kusto Query Language). Les insights et solutions dans Azure Monitor fournissent des requêtes de journal afin de récupérer des données pour un service particulier, mais vous pouvez travailler directement avec des requêtes de journal et leurs résultats dans le portail Azure avec Log Analytics.

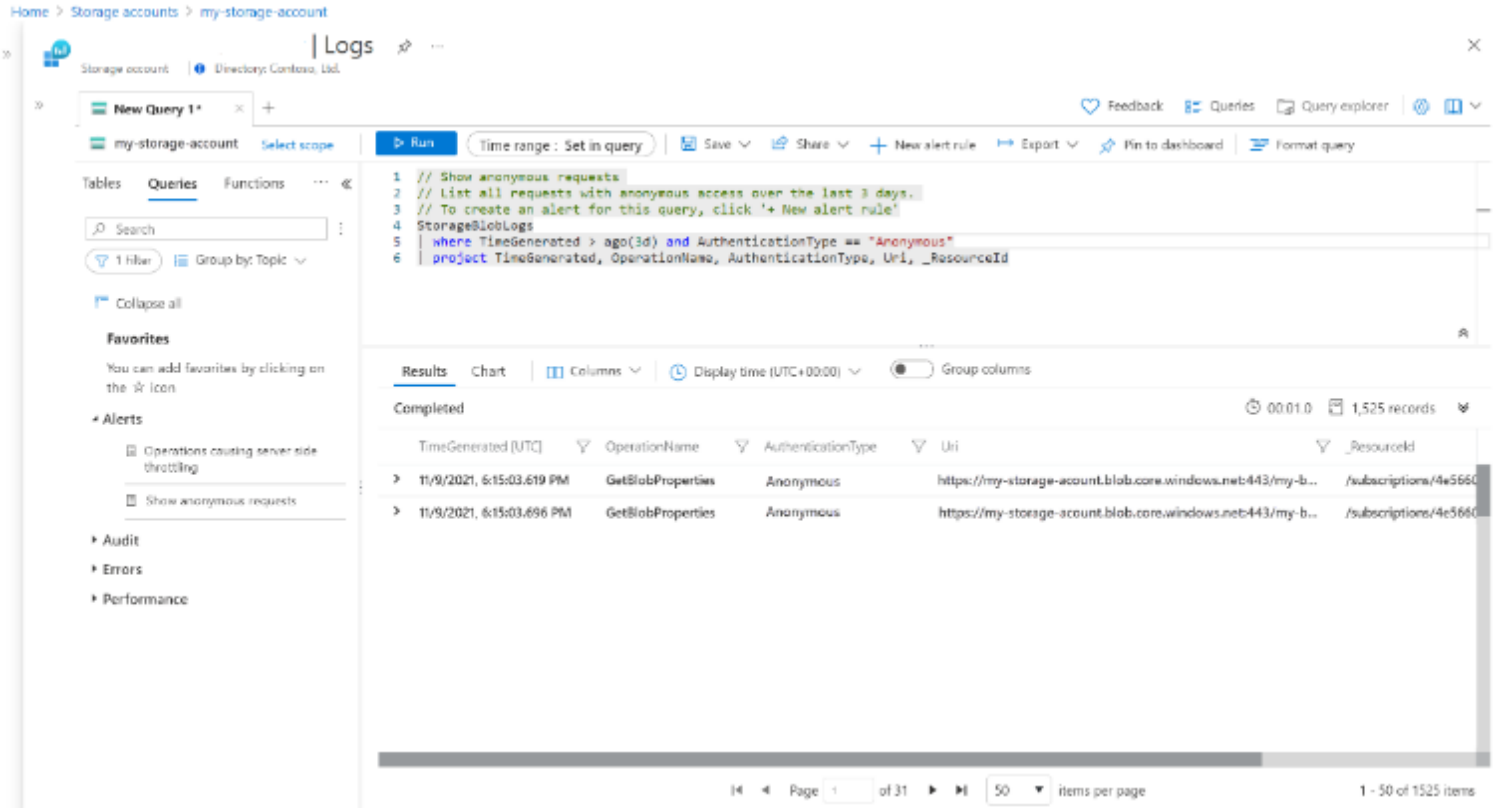
Sélectionnez **Journaux** dans le menu de votre ressource. Log Analytics s'ouvre avec la fenêtre **Requêtes** qui contient des requêtes prégénérées pour votre **type de ressource**. Sélectionnez **Alertes ou Virtual Machine** pour voir les requêtes spécifiquement conçues pour les règles d'alerte.



PARTIE 3

Eléments de réponse

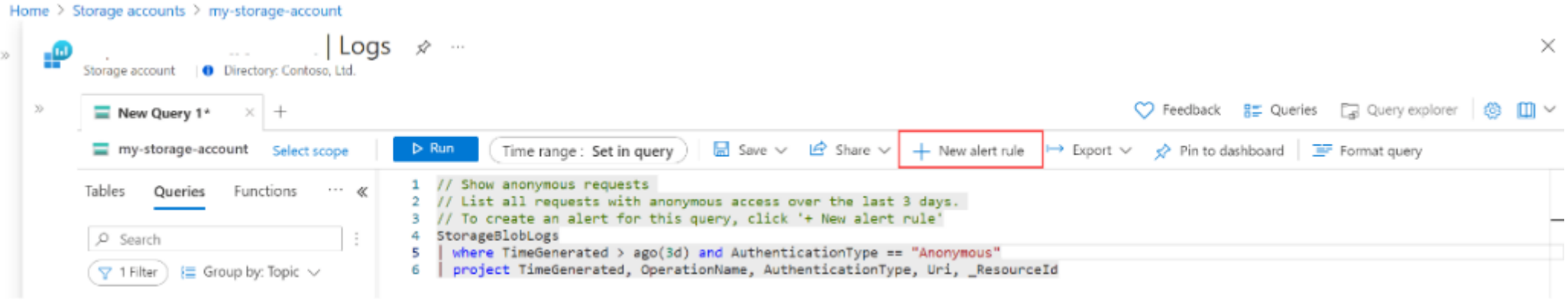
Sélectionnez une requête et cliquez sur **Exécuter** pour la charger dans l'éditeur de requête et retourner des résultats. Vous pouvez modifier la requête et la réexécuter. Par exemple, la requête **Afficher les demandes anonymes** pour les comptes de stockage est indiquée ci-dessous. Vous pouvez modifier la valeur **AuthenticationType** ou filtrer sur une autre colonne.



Eléments de réponse

Créer une règle d'alerte

Une fois que vous avez vérifié votre requête, vous pouvez créer la règle d'alerte. Sélectionnez **Nouvelle règle d'alerte** pour créer une règle d'alerte basée sur la requête de journal actuelle. L'**étendue** est déjà définie sur la ressource actuelle. Vous n'avez pas besoin de changer cette variable.



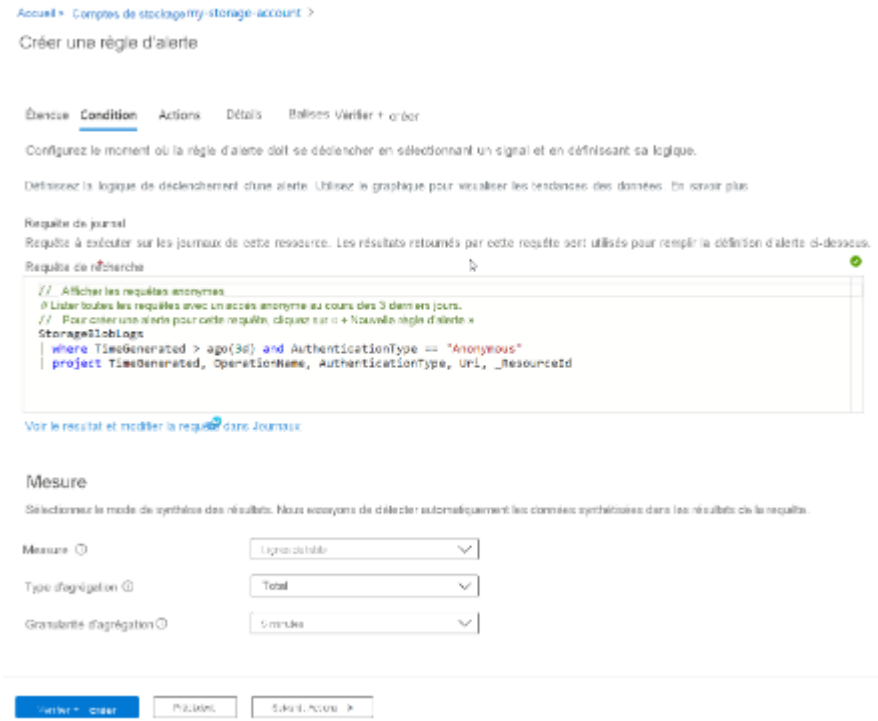
PARTIE 3

PARTIE 3

Eléments de réponse

Configurer une condition

Sous l’onglet **Condition**, la **Requête de journal** est déjà renseignée. La section **Mesure** définit la manière dont les enregistrements de la requête de journal sont mesurés. Si la requête ne calcule pas le total, la seule option est de **Compter** le nombre de **Lignes de table**. Si la requête comprend une ou plusieurs colonnes totalisées, vous pouvez utiliser le nombre de **Lignes de table** ou un calcul basé sur l’une des colonnes totalisées. La **Granularité d’agrégation** définit l’intervalle de temps sur lequel les valeurs collectées sont agrégées.



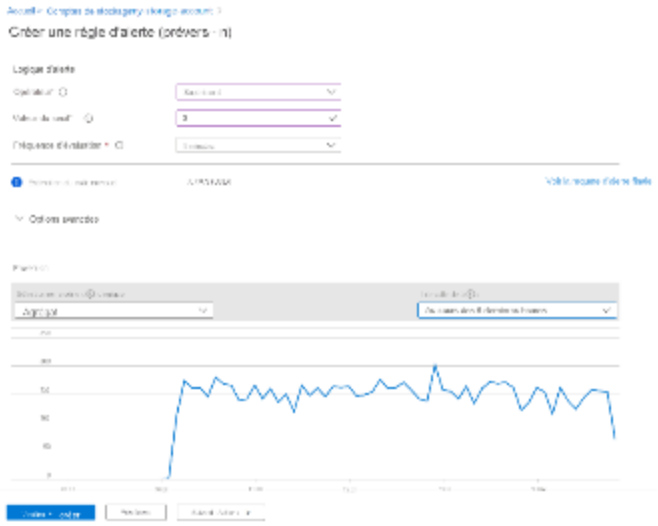
Eléments de réponse

Tâche 5 : Créer un groupe d’actions pour définir les détails de la notification.

Configurer une logique d’alerte

Dans la logique d’alerte, configurez l’**Opérateur** et la **Valeur de seuil** à comparer à la valeur retournée par la mesure. Une alerte est créée quand cette valeur est True. Sélectionnez une valeur pour la **Fréquence d’évaluation** qui définit la fréquence d’exécution et d’évaluation de la requête de journal. Le coût de la règle d’alerte augmente quand la fréquence est basse. Quand vous sélectionnez une fréquence, le coût mensuel estimé s’affiche en plus d’un aperçu des résultats de la requête sur une période donnée.

Par exemple, si la mesure est **Lignes de table**, la logique d’alerte peut être **Supérieure à 0**, ce qui indique qu’au moins un enregistrement a été retourné. Si la mesure est une valeur de colonnes, la logique doit peut-être être supérieure ou inférieure à une valeur de seuil en particulier. Dans l’exemple ci-dessous, la requête de journal recherche des demandes anonymes dans un compte de stockage. Si une demande anonyme a été effectuée, nous devons déclencher une alerte. Dans ce cas, une seule ligne retournée déclenche l’alerte et la logique d’alerte doit être **Supérieure à 0**.



PARTIE 3

PARTIE 3

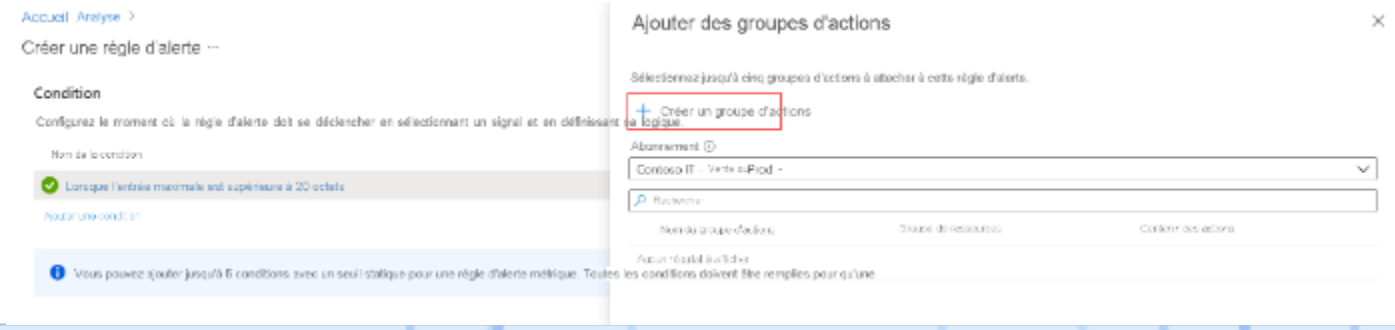
Eléments de réponse

Configurer les actions

Les groupes d'actions définissent un ensemble d'actions à entreprendre lorsqu'une alerte est déclenchée, par exemple l'envoi d'un e-mail ou d'un SMS.

Cliquez sur **Ajouter des groupes d'actions** pour en ajouter un à la règle d'alerte.

Si vous ne possédez pas encore de groupe d'actions dans votre abonnement, cliquez sur **Créer un groupe d'actions** pour en créer un.

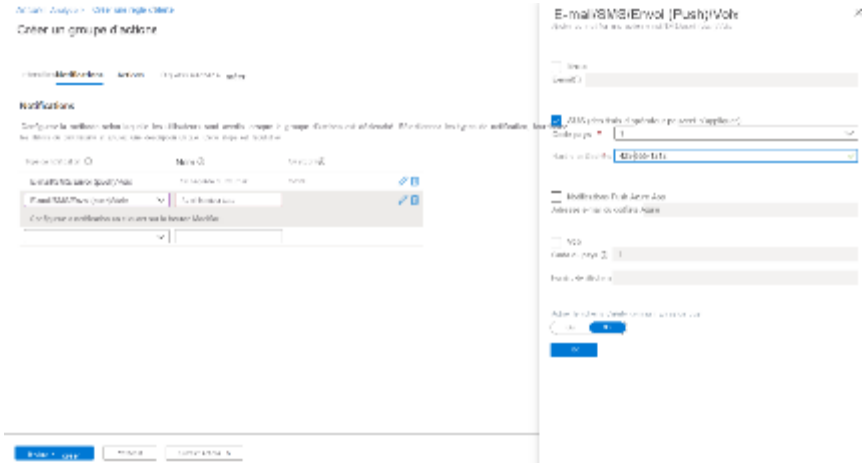


PARTIE 3

Eléments de réponse

Sélectionnez un **Abonnement** et un **Groupe de ressources** pour le groupe d’actions. Ensuite, donnez-lui un **Nom de groupe d'actions** qui s’affichera sur le portail et un **Nom d'affichage** qui apparaîtra dans les notifications par e-mail.

Sélectionnez l’onglet **Notifications** et ajoutez une ou plusieurs méthodes de notification des personnes concernées lorsque l’alerte est déclenchée.



PARTIE 3

Eléments de réponse

Configuration des détails

Configurez des paramètres différents pour la règle d’alerte dans la section **Détails de la règle d’alerte**.

Nom de la règle d’alerte qui doit être descriptif, car il s’affiche lorsque l’alerte est déclenchée.

Vous pouvez également fournir une **description** qui est incluse dans les détails de l’alerte.

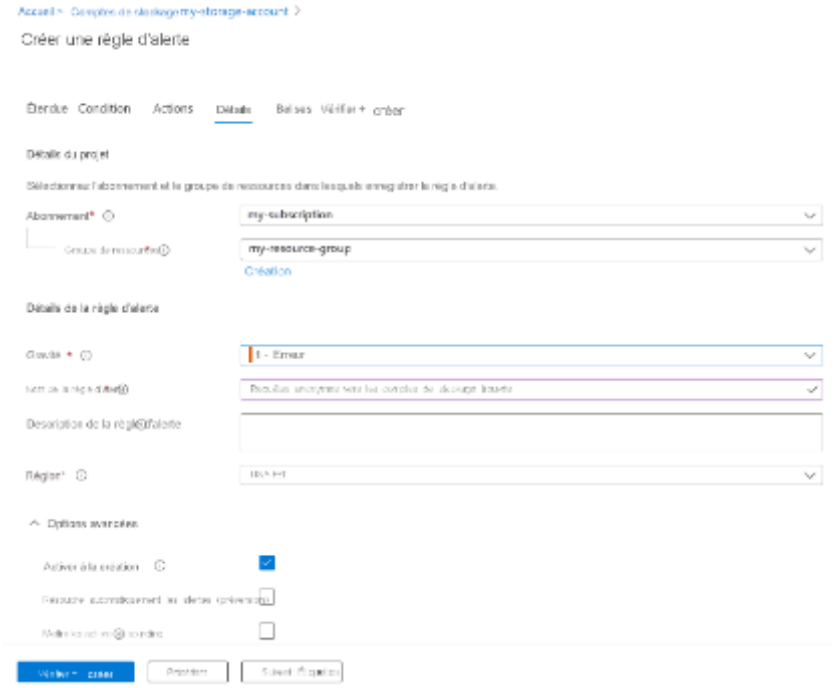
Abonnement et **groupe de ressources** dans lesquels la règle d’alerte sera stockée. Il ne doit pas nécessairement s’agir du même groupe de ressources que celui de la ressource en cours de monitoring.

Configurez la **Gravité** de l’alerte. Elle permet de regrouper les alertes présentant une importance relative similaire. Une gravité de niveau **Erreur** est appropriée pour une machine virtuelle qui ne répond pas.

Maintenez la case **Activer l’alerte dès la création** cochée.

Maintenez la case **Résoudre automatiquement les alertes** cochée. Cela change l’alerte en alerte avec état, ce qui signifie que l’alerte est résolue lorsque la condition n’est plus remplie.

Cliquez sur **Créer une règle d’alerte** pour créer la règle d’alerte.



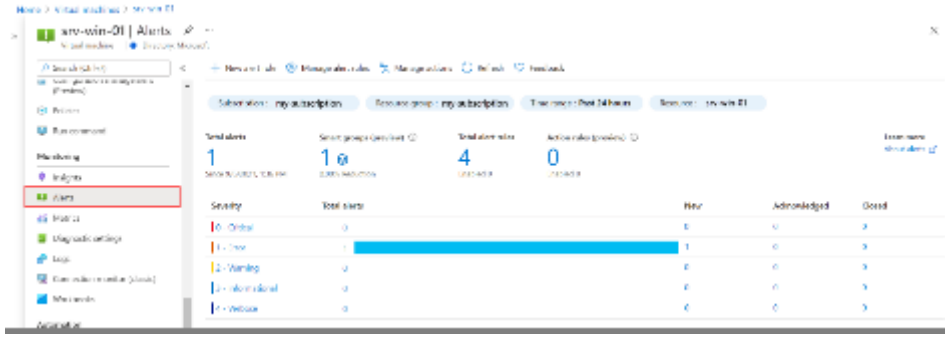
PARTIE 3

Eléments de réponse

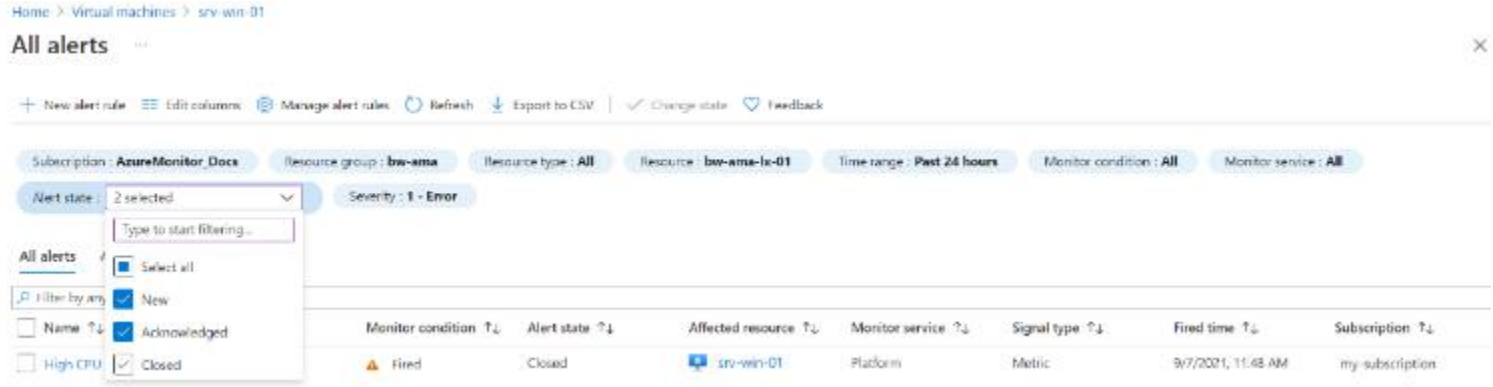
Voir l'alerte

Quand une alerte se déclenche, elle envoie des notifications dans ses groupes d'actions. Vous pouvez également afficher l'alerte dans le portail Azure.

Sélectionnez **Alertes** dans le menu de la ressource. S'il existe des alertes ouvertes pour les ressources, elles sont incluses dans l'affichage.

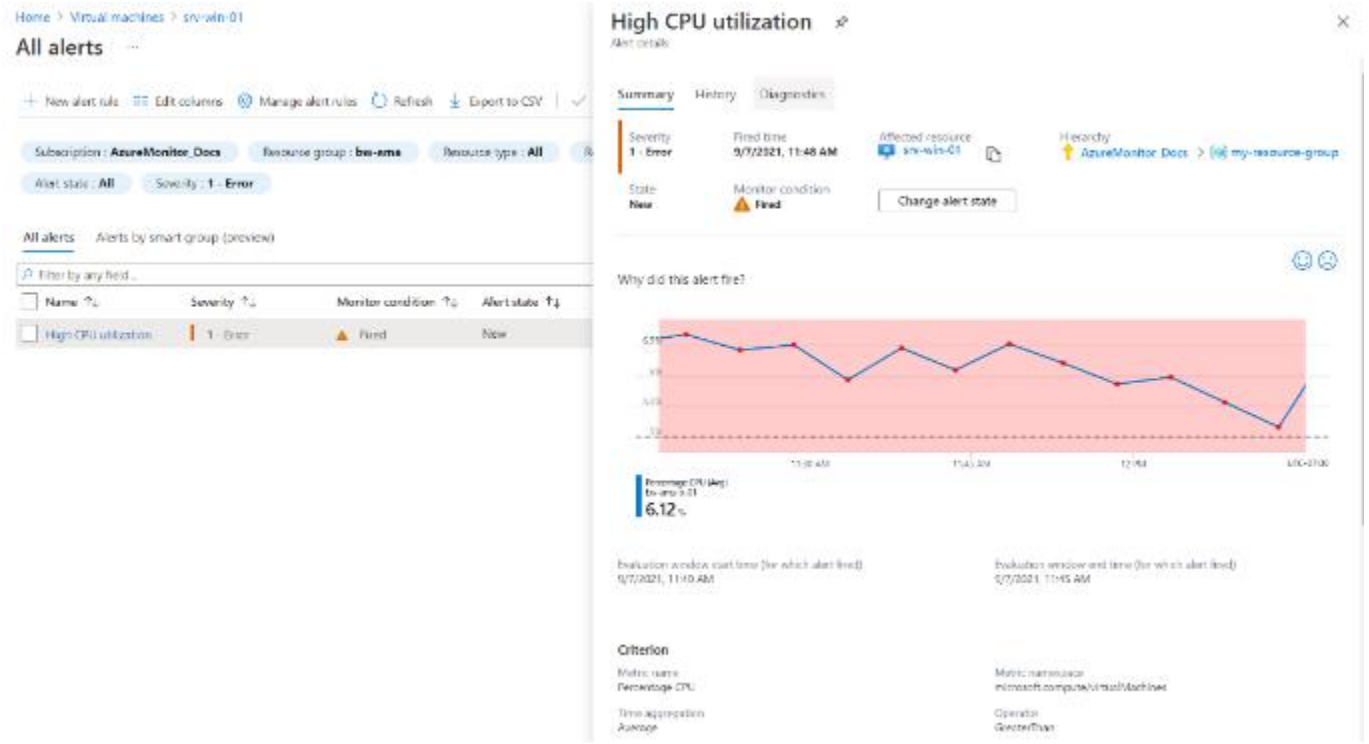


Cliquez sur une gravité pour voir les alertes correspondantes. Cochez **État de l'alerte** et décochez **Fermé** pour afficher uniquement les alertes ouvertes.



Eléments de réponse

Cliquez sur le nom d’une alerte pour voir ses détails.



PARTIE 3

ACTIVITE n°2

Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

Compétences visées :

- Automatiser à l'aide des playbooks la remontée des notifications d'incident par email depuis Microsoft Sentinel

Recommandations clés :

- Se référer au cours ainsi qu'à la documentation officielle Microsoft Sentinel
- Discuter en groupe les nouveaux termes liés au Cloud

5 heures

CONSIGNES

1. Pour le formateur

- Permettre au stagiaire de se familiariser avec les fonctionnalités avancées Microsoft Sentinel
- S'assurer de la bonne compréhension des travaux
- Discuter les réponses des stagiaires avant de donner la solution
- Favoriser le travail en groupe

2. Pour l'apprenant

- Lire et bien comprendre les études de cas avant de passer aux questions
- Lire et bien comprendre les questions

3. Conditions de réalisation :

- Par groupes (2 ou 3 maximum)
- Ordinateur portable avec un abonnement Azure payant ou gratuit actif
- Recherche sur Internet

4. Critères de réussite :

- Travail en groupe
- Travaux pratiques opérationnels

Etude de cas n°1 : Utiliser des playbooks pour notification par email des incidents au niveau Microsoft Sentinel

Microsoft Sentinel est un outil natif du Cloud Azure qui permet une analyse de sécurité intelligente et permet de remonter des renseignements sur les menaces à l'échelle de l'entreprise. Avec Microsoft Sentinel, vous disposez d'une solution unique pour la détection des attaques, la visibilité des menaces, la chasse proactive et la réponse aux menaces. Dans ce sens, à travers ce TP vous allez utiliser des playbooks avec des règles d'automatisation pour automatiser votre réponse aux incidents et corriger les menaces de sécurité détectées par ladite solution.

Tâche 1 : Fournir une définition des règles d'automatisation et playbook pour Microsoft Sentinel

Tâche 2 : Créer un playbook avec un déclencheur d'incident

Tâche 3 : Activer l'identité attribuée par système et attribuer le rôle de contributeur Microsoft Sentinel à la ressource

Tâche 4 : Modifier le playbook créé précédemment pour permettre l'envoi des emails

Tâche 5 : Linker le playbook avec les alertes

Tâche 6 : Vérifier la réception d'alerte par email et au niveau Microsoft Sentinel

Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

Etude de cas n°1

Eléments de réponse

Tâche 1 : Fournir une définition des règles d'automatisation et playbook pour Microsoft Sentinel

Les règles d'automatisation vous aident à trier les incidents dans Microsoft Sentinel. Vous pouvez les utiliser pour attribuer automatiquement des incidents aux personnes appropriées, fermer des incidents indésirables ou des faux positifs connus, modifier leur gravité et ajouter des balises. Ils sont également le mécanisme par lequel vous pouvez exécuter des règles en réponse aux incidents.

Un playbook est une collection de procédures qui peut être exécutée à partir de Microsoft Sentinel en réponse à une alerte ou à un incident. Un playbook peut vous aider à automatiser et à orchestrer votre réponse, et peut être configuré pour s'exécuter automatiquement lorsque des alertes ou des incidents spécifiques sont générés, en les joignant à une règle d'analyse ou à une règle d'automatisation. Il peut également être exécuté manuellement à la demande.

Les playbooks dans Microsoft Sentinel reposent sur des workflows conçus dans Azure Logic Apps. Cela signifie que vous bénéficiez de la puissance, des possibilités de personnalisation et des modèles intégrés de Logic Apps. Chaque playbook est créé pour l'abonnement spécifique auquel il appartient, mais l'affichage des **règles** reprend toutes les règles disponibles dans les abonnements sélectionnés.

PARTIE 3

Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

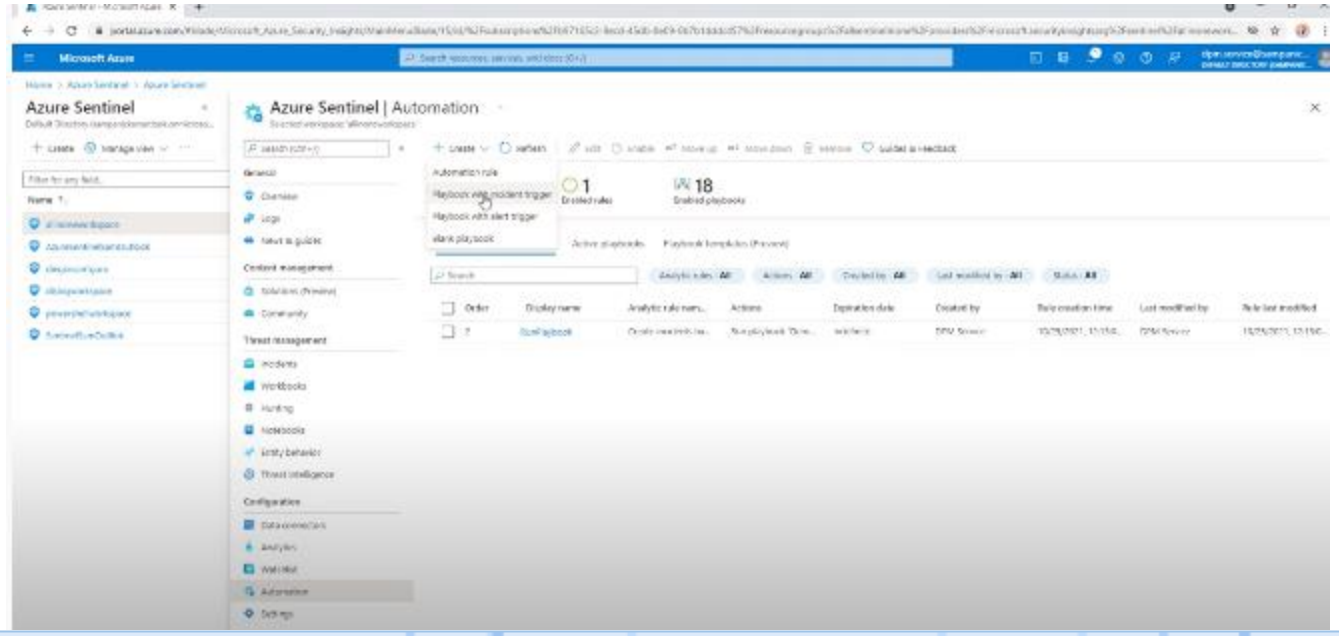
Etude de cas n°1

PARTIE 3

Eléments de réponse

Tâche 2 : Créer un playbook avec un déclencheur d'incident

- Se connecter au **Portail Azure (https://portal.azure.com)**
- Sélectionner dans la barre de recherche **Microsoft Sentinel**
- Puis procéder à la création d'un espace de travail (Workspace) au niveau Microsoft Sentinel qu'on va nommée « **allinoneworkspace** »
- Sélectionner le workspace créé « **allinoneworkspace** » puis dans le menu vertical à gauche choisir **Automatisation ou (Automation)**
- Au niveau du Menu horizontal choisir « **créer (Create) »** puis cliquer sur **«** playbook avec un déclencheur d'incident (Playbook with incident trigger) »



Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

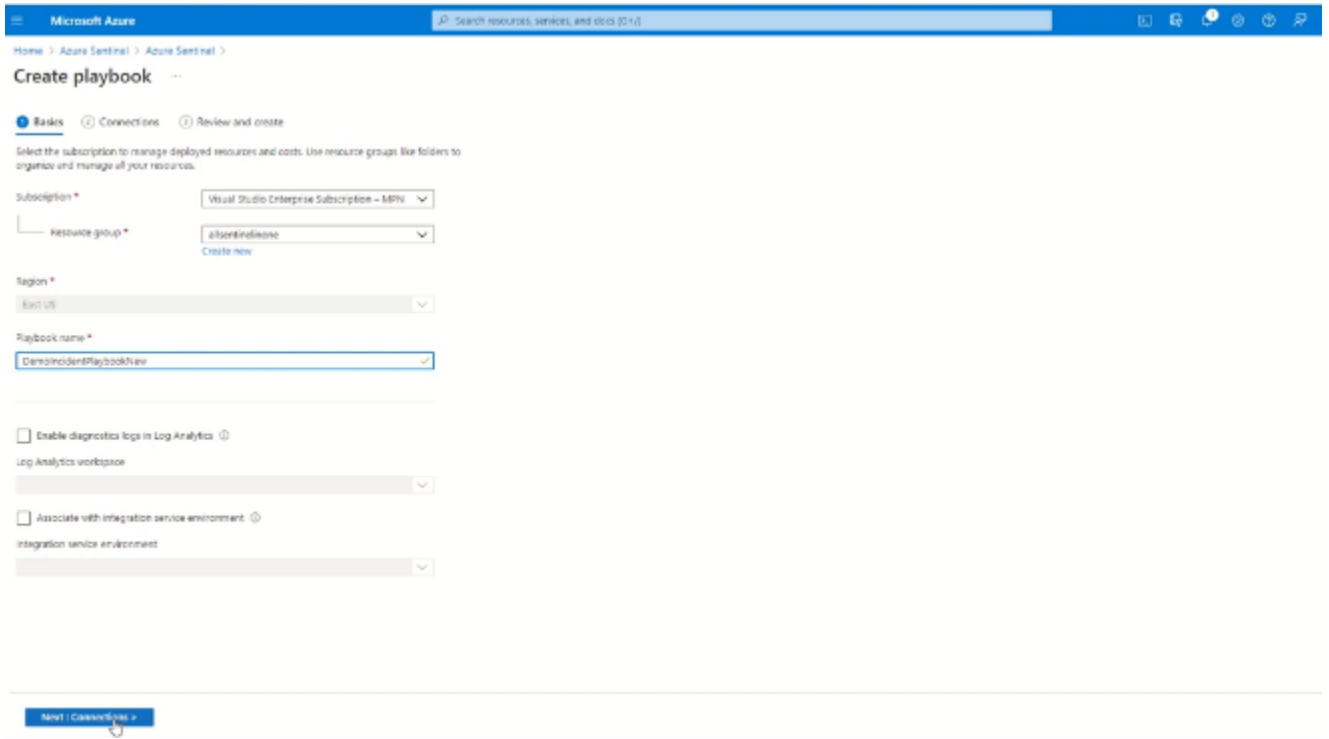
Etude de cas n°1

PARTIE 3

Eléments de réponse

Tâche 2 : Créer un playbook avec un déclencheur d'incident

- Renseigner le nom du playbook « **DemoincidentPlaybookNew** » et choisir « **suivant** »

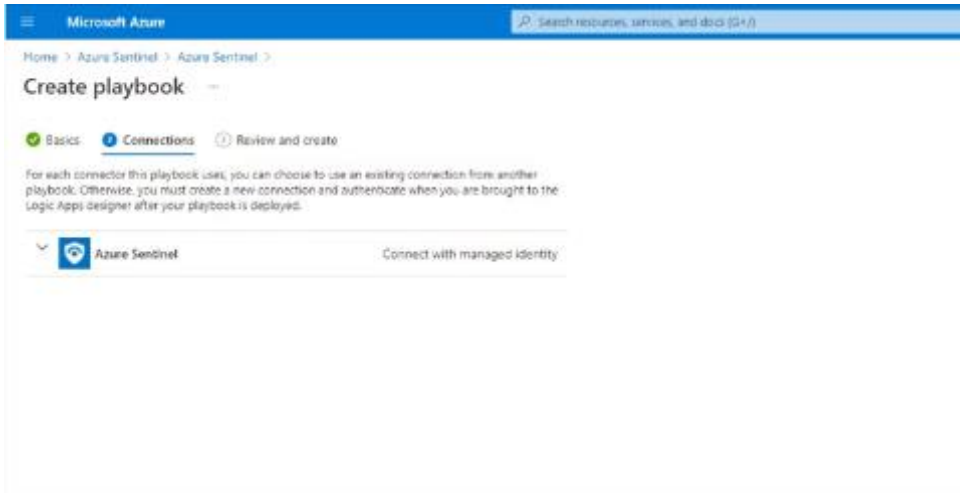


Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

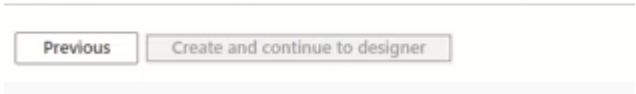
Etude de cas n°1

Eléments de réponse

- Au niveau de l'onglet « **Connexions** » sélectionner « **Azure Sentinel** » pour lui attribuer les droits de connexion avec les entités managées.



- Choisir créer pour démarrer la phase de désigne du workflow. Et attendre la fin de la création du playbook



PARTIE 3

Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

Etude de cas n°1

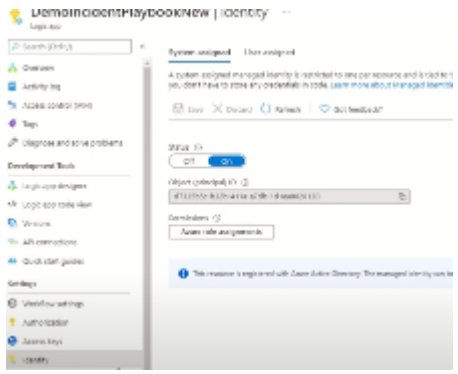
PARTIE 3

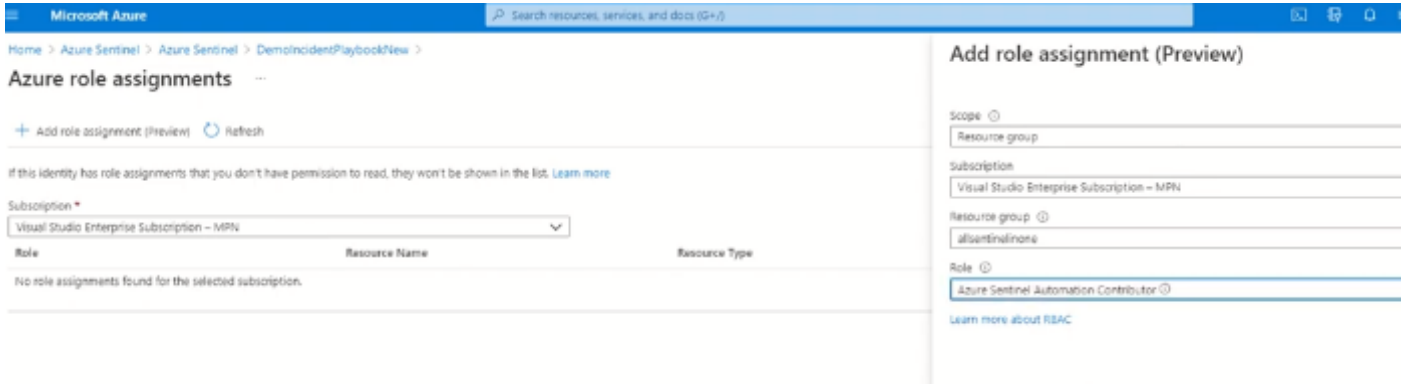
Eléments de réponse

Tâche 3 : Activer l'identité attribuée par le système et attribuer le rôle de contributeur Microsoft Sentinel à la ressource

- Sélectionner le playbook « **DemoincidentPlaybookNew** » puis au niveau du menu vertical choisir « **Logic App designer** ». Vous remarquerez qu'un trigger par défaut est déjà créé.

- Au niveau du menu vertical choisir « **Identity** » pour gérer l'identité. Ceci va nous permettre d'éviter d'utiliser le login/password à chaque fois que le déclencheur playbook est déclenché.
- Puis choisir « **Azure role assignements** » puis choisir « **add role assignement** » puis renseigner **« scope = Ressouce groupe » et « Role=Azure Sentinel Automation Contributor »** et valider la création.





Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

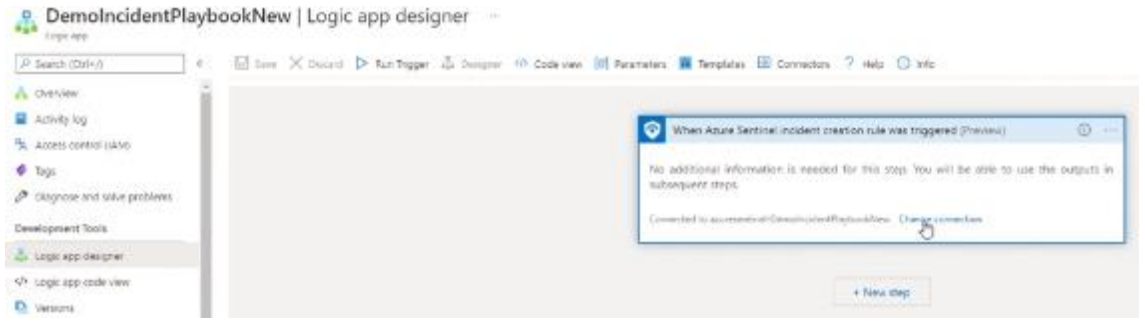
Etude de cas n°1

PARTIE 3

Eléments de réponse

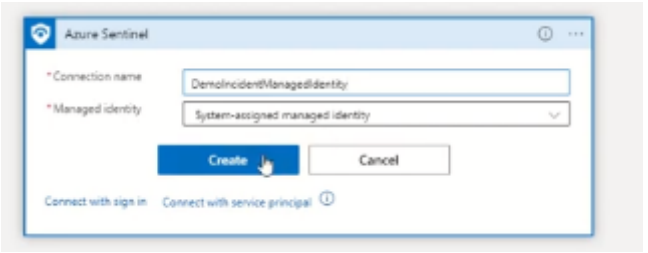
Tâche 3 : Activer l'identité attribuée par le système et attribuer le rôle de contributeur Microsoft Sentinel à la ressource

- Au niveau du menu vertical choisir « **Logic App designer** ». Sélectionner le déclencheur (Trigger) puis choisir « **Change Connection** »



- Puis choisir « **ajouter nouveau** » :

- Sélectionner **« Connect with managed identity »** et renseigner le nom de la connexion **« DemoincidentManagedIdentity »** puis sélectionner **« créer »**



Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

Etude de cas n°1

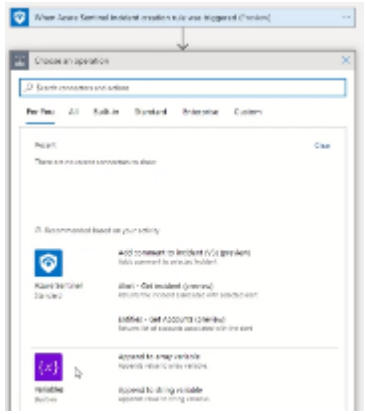
PARTIE 3

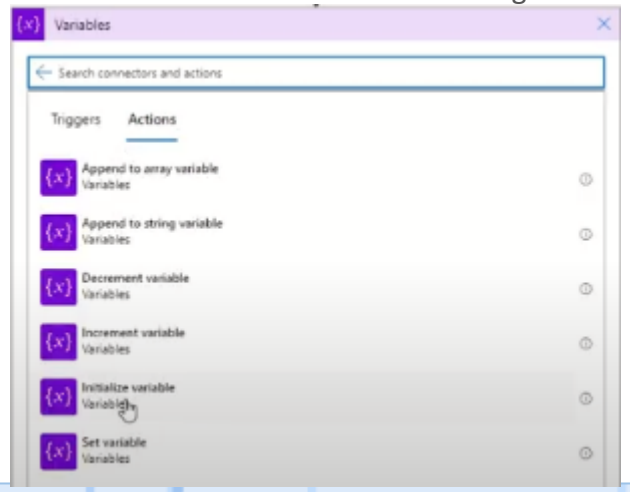
Eléments de réponse

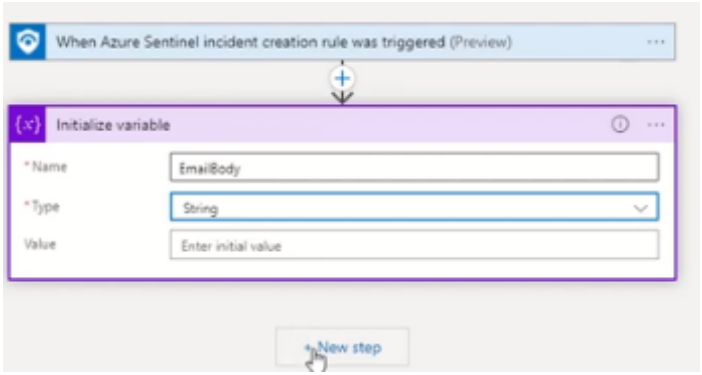
Tâche 4 : Modifier le playbook créé précédemment pour permettre l'envoi des emails

- Au niveau du menu vertical choisir « **Logic App designer** ». Sélectionner « **Next Step** » sous le trigger afin d'ajouter une variable pour le formatage du contenu de l'email en HTML.

- Choisir **« Variable »,** puis choisir le type de variable **« Initialisation de variable »** et renseigner le nom **« EmailBody »** et le **« type =String »:**







Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

Etude de cas n°1

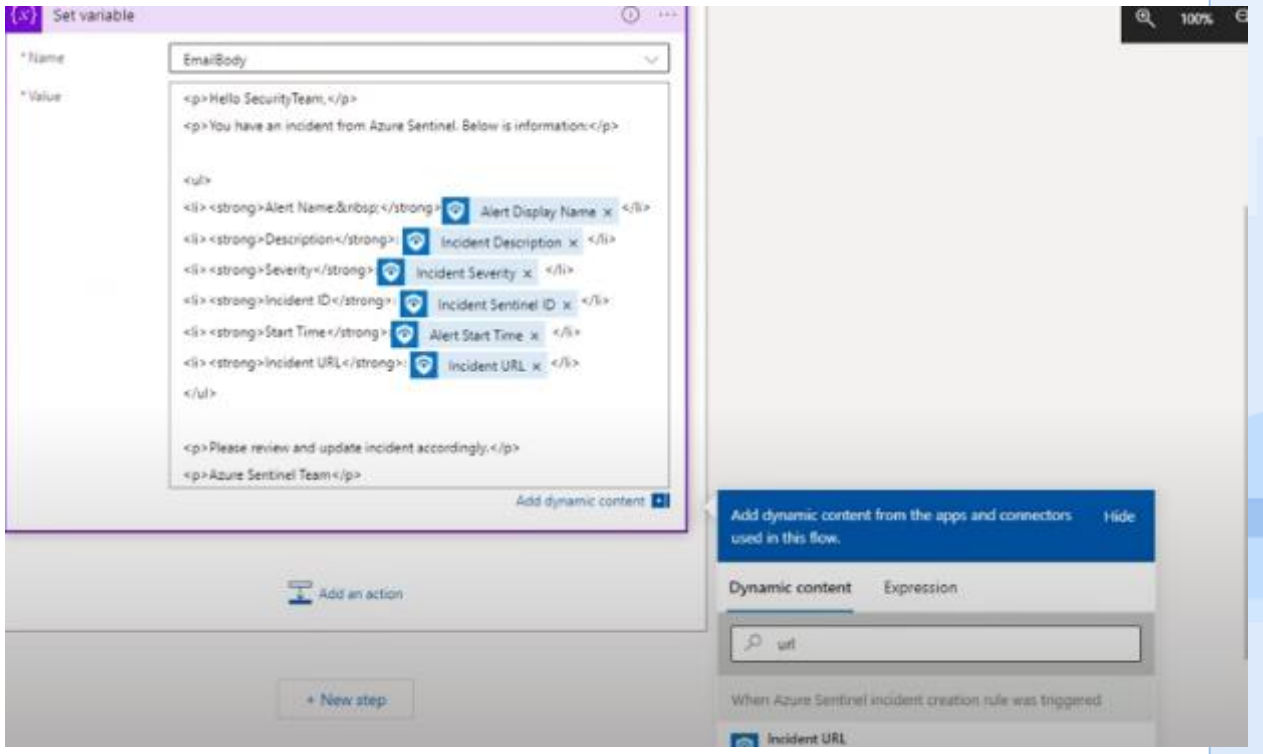
PARTIE 3

Eléments de réponse

Tâche 4 : Modifier le playbook créé précédemment pour permettre l'envoi des emails

- Sélectionner à nouveau « **Next Step** » sous l'étape « initialisation de variable » puis choisir « **Set variable** » et choisir au niveau du nom = **EmailBody (créer precedemment)** puis dans valeur coller le contenu de l'alerte sous format HTML.
- Vous pouvez ajouter des variables dynamiques à base du trigger en choisissant en bas **« ajouter contenu dynamique ». Les champs en rouge** doivent être modifiés comme indiqué ci-dessous :

```
<p>Bonjour Equipe de sécurité </p>
<p>Vous avez un incident depuis Azure Sentinel. Ci-dessous le detail :</p>
 <ul>
 <li><strong>Nom Alerte :&amp;nbsp;</strong> AlertDisplayName</li>
<li><strong>Déscription</strong>: IncidentDescription</li>
<li><strong>Gravité</strong>: Incident Severiity</li>
 <li><strong>ID Incident</strong>: IncidentSentinelID</li>
<li><strong>Heure début</strong>: AlertStartTime</li>
 <li><strong>URL de l'Incident</strong>: IncidentURL</li>
 </ul>
 <p>Merci de faire les mises à jour necessaires.</p>
<p>L'équipe Azure Sentinel </p>
```



Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

Etude de cas n°1

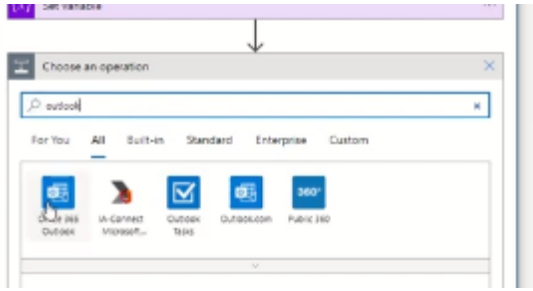
PARTIE 3

Eléments de réponse

Tâche 4 : Modifier le playbook créé précédemment pour permettre l'envoi des emails

- Sélectionner « **ajouter action** » en bas de l'étape « **Set Variable** » pour ajouter la dernière action pour l'envoi des emails via Microsoft 365.

- Puis renseigner dans la barre de recherche « **Outlook** » puis sélectionner « **Office 365 Outlook** »



- Au niveau de l'onglet action rechercher « **envoi email** » et choisir « **Send an email (V2)** »

Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

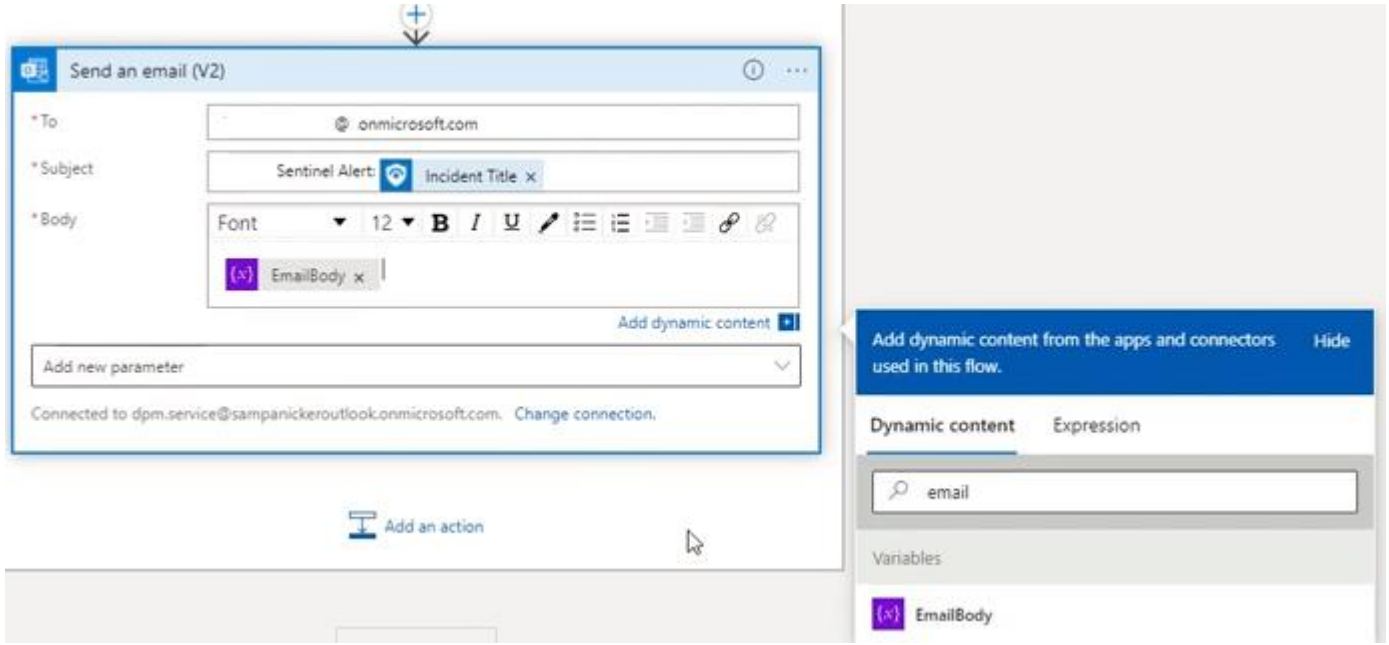
Etude de cas n°1

PARTIE 3

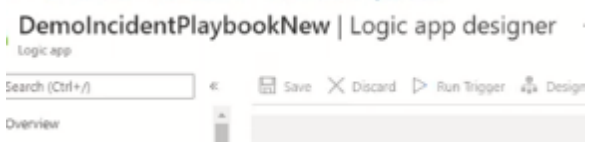
Eléments de réponse

Tâche 4 : Modifier le playbook créé précédemment pour permettre l'envoi des emails

- Renseigner l'adresse email qui recevra les notifications, l'objet du mail ainsi que le contenu (body) qui doit comprendre le contenu dynamique « **EmailBody** ».



- Valider les changements en cliquant sur sauvegarder (Menu horizontal)



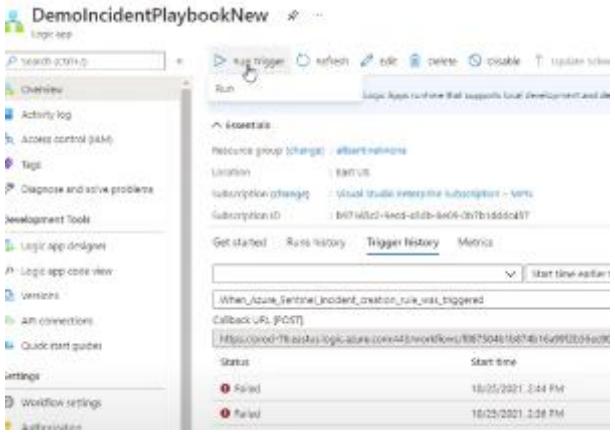
Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

Etude de cas n°1

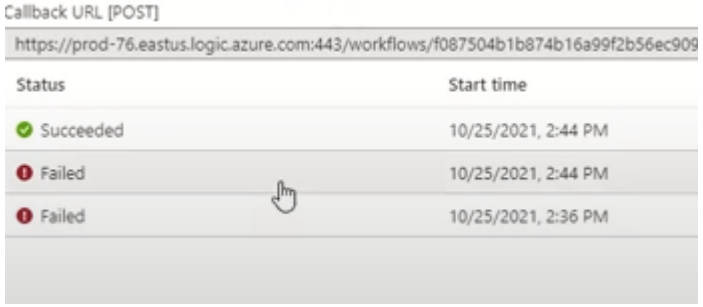
Eléments de réponse

Tâche 4 : Modifier le playbook créé précédemment pour permettre l'envoi des emails

- Pour vérifier le fonctionnement du déclencheur (Trigger), sélectionner le playbook puis choisir « Run trigger puis Run »



- Une nouvelle ligne s'affichera indiquant que le lancement s'est bien déroulé :



PARTIE 3

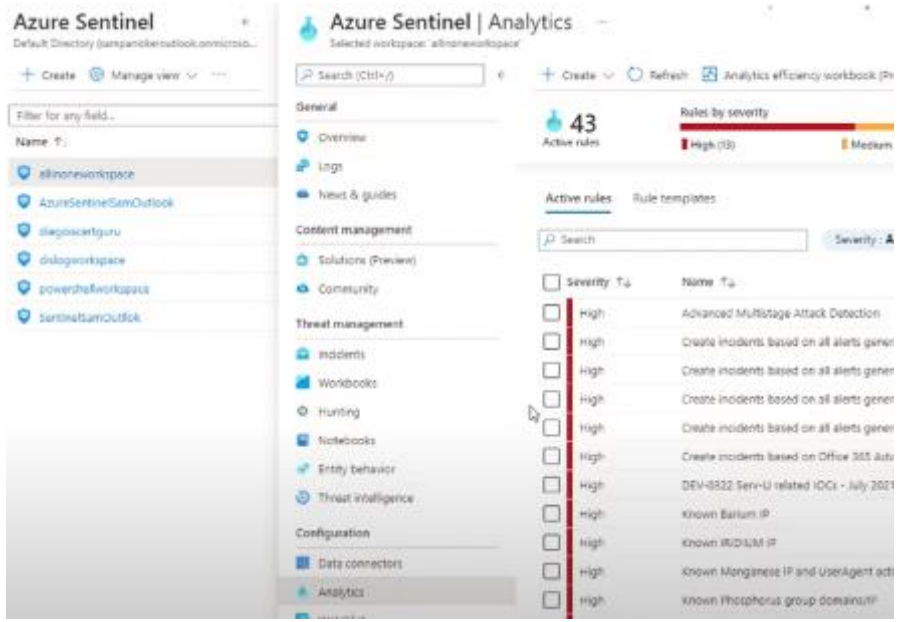
Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

Etude de cas n°1

Eléments de réponse

Tâche 5 : Linker le playbook avec les alertes

- Maintenant que nous avons créé le déclencheur pour l'envoi d'email nous allons lier les incidents pour permettre de lancer l'envoi :
- Sélectionner « Azure sentinel » puis l'espace de travail « **allinoneworkspace** » au niveau du menu vertical choisir « **Analytics** »



PARTIE 3

PARTIE 3

Eléments de réponse

Tâche 5 : Linker le playbook avec les alertes

- Choisir une des alertes déjà disponibles au niveau du worskpace (si aucune alerte disponible, il faudra configurer les alertes du VMs par exemple pour remonter au niveau d'Azure Sentinel pour le workspace que nous avons créé).

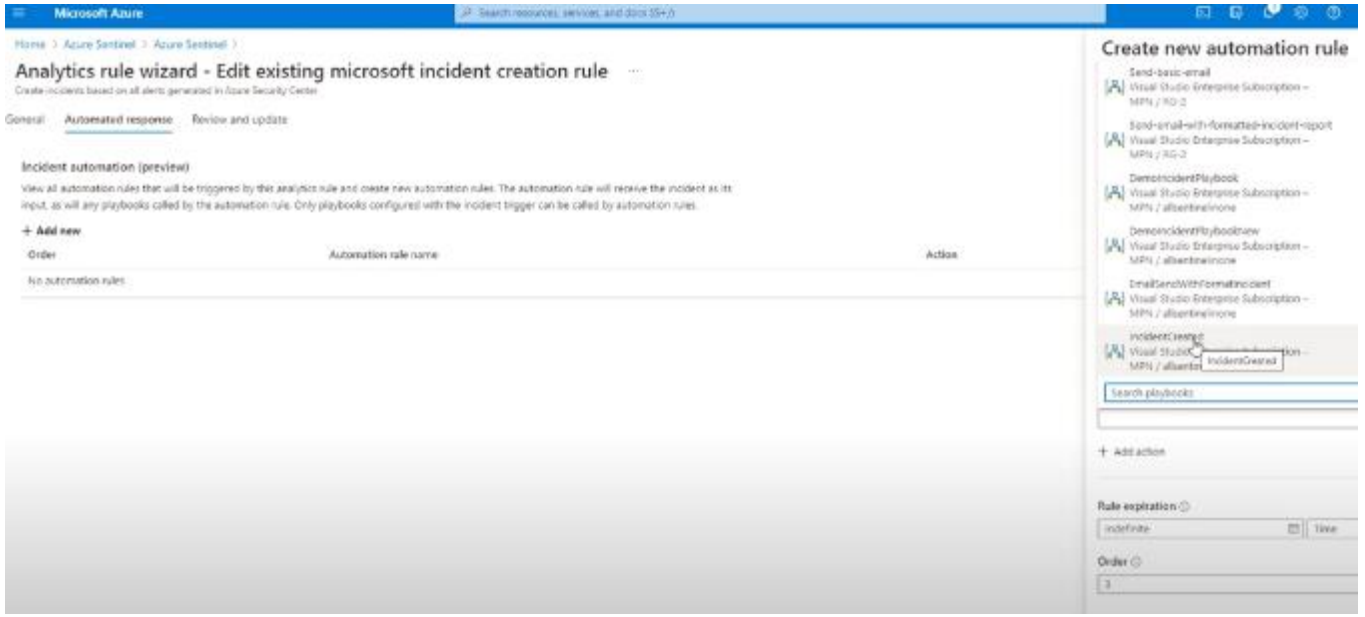
Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

Etude de cas n°1

Eléments de réponse

Tâche 5 : Linker le playbook avec les alertes

- Choisir le 2ème onglet « **Automated response** » puis sélectionner le playbook que nous avons créé précédemment :



- Puis valider la création en choisissant « **sauvegarder** »

PARTIE 3

Configuration automatique des remontées d'incident via email sur Microsoft Sentinel

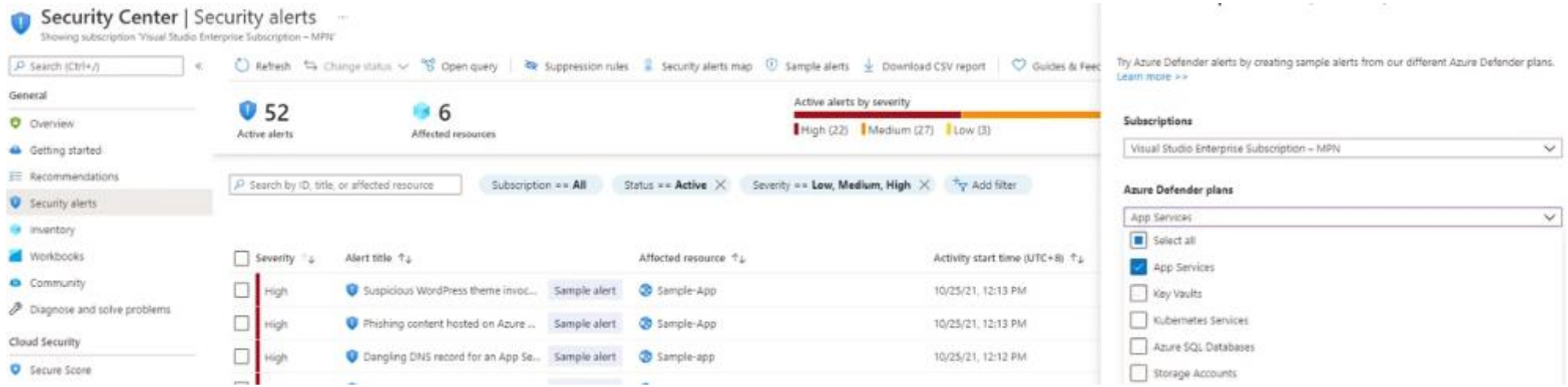
Etude de cas n°1

PARTIE 3

Eléments de réponse

Tâche 6 : Vérifier la réception d'alerte par email

- Une fois une alerte détectée (vous pouvez simuler la création d'une alerte à travers « **Security Center** »)
- Choisir au niveau du menu horizontal « **sample alerts** » puis cocher « App services » et valider la création.



- Vérifier la réception d'email d'alerte au niveau de la boite renseignée précédemment dans l'étape 4.