INTRODUCTION

Ce rapport a pour objectif de documenter le processus complet de création et d'évaluation de la sécurité d'une machine virtuelle nommée Ubuntu-Pro-24.04 sur la plateforme Microsoft Azure, tout en répondant à des questions liées à l'évaluation de la sécurité.

Dans la première partie, nous explorons les informations à collecter pour une évaluation de la sécurité de la VM, même avec un accès administrateur sur Azure. Nous répondrons à la question cruciale : quelles données supplémentaires demander au client pour garantir une évaluation complète de la sécurité de la VM ?

La seconde partie traitera de l'évaluation de la sécurité de la machine virtuelle elle-même, en analysant ses différents aspects pour déterminer si elle peut être considérée comme « sécuritaire ».

Dans la troisième partie, des captures d'écran illustrent les étapes clés du processus de création de la VM sur Microsoft Azure. Ces images incluent des informations sur :

- Le tableau de bord Azure avec votre compte étudiant (Partie 2 – Étape 1),
- Les détails de votre abonnement (Partie 2 – Étape 6),
- Les propriétés de la VM créée (Partie 3 – Étape 13),
- L'adresse IP de la VM pour la connexion SSH (Partie 3 – Étape 15),
- La liste des ressources créées pendant le processus (Partie 3 – Étape 20).

Chaque capture sera accompagnée d'une brève explication, décrivant les informations essentielles contenues dans l'image et leur importance dans le contexte de la gestion et de la sécurité de la machine virtuelle.

PARTIE 1

Si vous étiez chargé d'évaluer la sécurité de la machine virtuelle que vous venez de créer (Ubuntu-Pro-24.04), en supposant que vous disposez déjà d'un accès administrateur à cette VM, quelles informations demanderiez-vous au client pour mener à bien votre évaluation ? En d'autres termes, même avec un accès administrateur à Azure, quelles informations vous manqueraient pour réaliser une évaluation de sécurité complète ?

Pour répondre à cette question, je me suis basé sur le cours, les étapes du laboratoire et les références de sécurité disponibles sur le site de Microsoft : *Azure Virtual Machines Security Baseline.*

Pour évaluer la sécurité de la machine virtuelle, je demanderais au client les informations suivantes :

- **Politique de sécurité en place :** Quelle politique de sécurité est appliquée à la VM (CIS, ISO 27001, etc.) ?
- **Authentification :** Le client a-t-il activé l'authentification multifacteur sur la VM ou utilise-t-il des clés SSH pour la connexion ?
- **Scan de vulnérabilités externes :** Le client utilise-t-il d'autres outils externes de gestion des vulnérabilités en plus d'Azure Security Center ?
- **Exigences de sécurité spécifiques :** Le client pourrait avoir des critères spécifiques liés à son organisation ou des obligations de conformité réglementaire.

En plus de ces quatre points, en tant qu'administrateur, je pourrais demander d'autres informations au client, mais il est possible que je puisse les obtenir moi-même. Par exemple :

- **Configuration réseau :** Vérifiez les groupes de sécurité réseau (règles de filtrage, restrictions IP, etc.).
- **Contrôles d'accès :** Quels types de contrôles d'accès sont en place ?
- **Chiffrement des disques :** Le chiffrement des disques est-il activé ?
- **Sécurité des connexions SSH :** Vérifiez si les connexions SSH sont bien sécurisées.
- **Analyse des journaux :** Examiner les fichiers logs pour détecter d'éventuelles activités suspectes.

PARTIE 2

Selon vous, est-ce que votre machine virtuelle peut être considérée comme "sécuritaire" ? Expliquez votre réponse.

Pour répondre à cette question, je me suis basé sur les propriétés de la machine

virtuelle (Ubuntu-Pro-24.04) créée lors du laboratoire 1, en les comparant aux références et recommandations pour sécuriser une VM. À partir de cette analyse, je peux affirmer que la machine virtuelle **Ubuntu-Pro-24.04** n'est pas entièrement sécurisée, bien qu'elle comporte certaines mesures de sécurité comme l'utilisation des clés SSH et la restriction des ports au seul port SSH (22). Cependant, il reste plusieurs aspects à renforcer pour garantir une sécurité complète, tels que la gestion des vulnérabilités, la détection des menaces et une meilleure restriction des accès via la configuration de pare-feu.

PARTIE 3

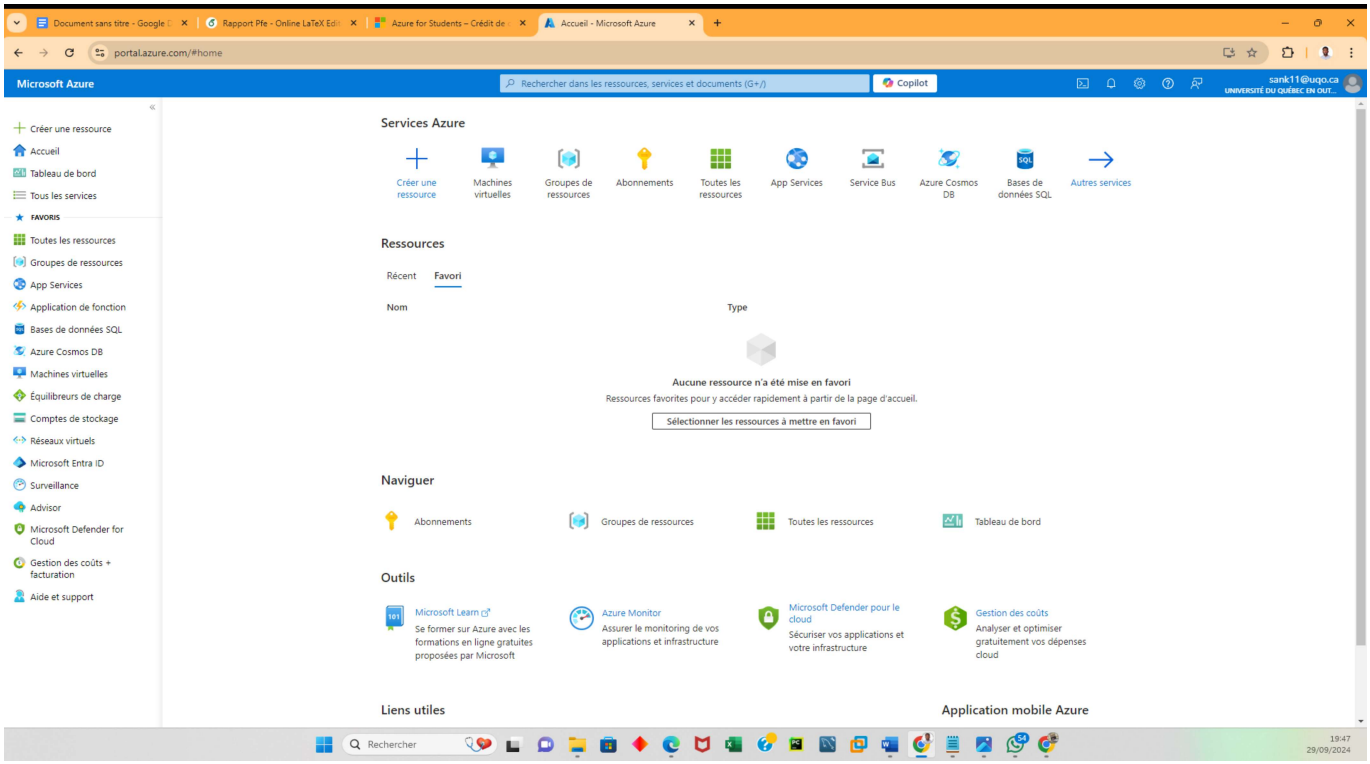
Dans cette dernière partie, nous allons présenter les différentes étapes de la création d'un compte Microsoft Azure pour étudiants, depuis la configuration jusqu'à la création de la machine virtuelle mentionnée plus haut.

A) Tableau de bord dans Microsoft Azure (Partie 2 – Étape 1)

Après avoir rempli le formulaire d'inscription à Microsoft Azure (saisie des informations personnelles et celles de l'établissement), nous accédons à la page d'accueil d'Azure. Cette page regroupe les principales fonctionnalités du système.

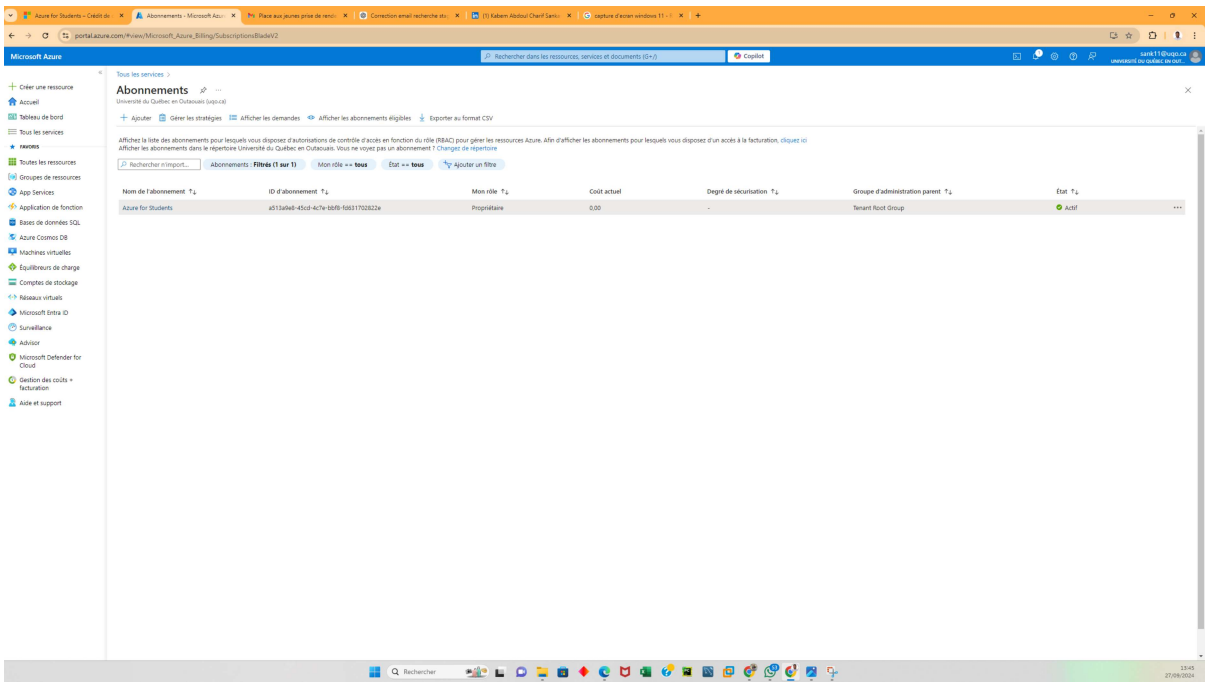
En haut à droite, une option permet d'afficher notre profil ainsi que le nom de l'établissement (Université du Québec en Outaouais), confirmant ainsi que notre compte est bien un compte étudiant.

La page d'accueil, décrite précédemment, est accessible via la barre latérale gauche.



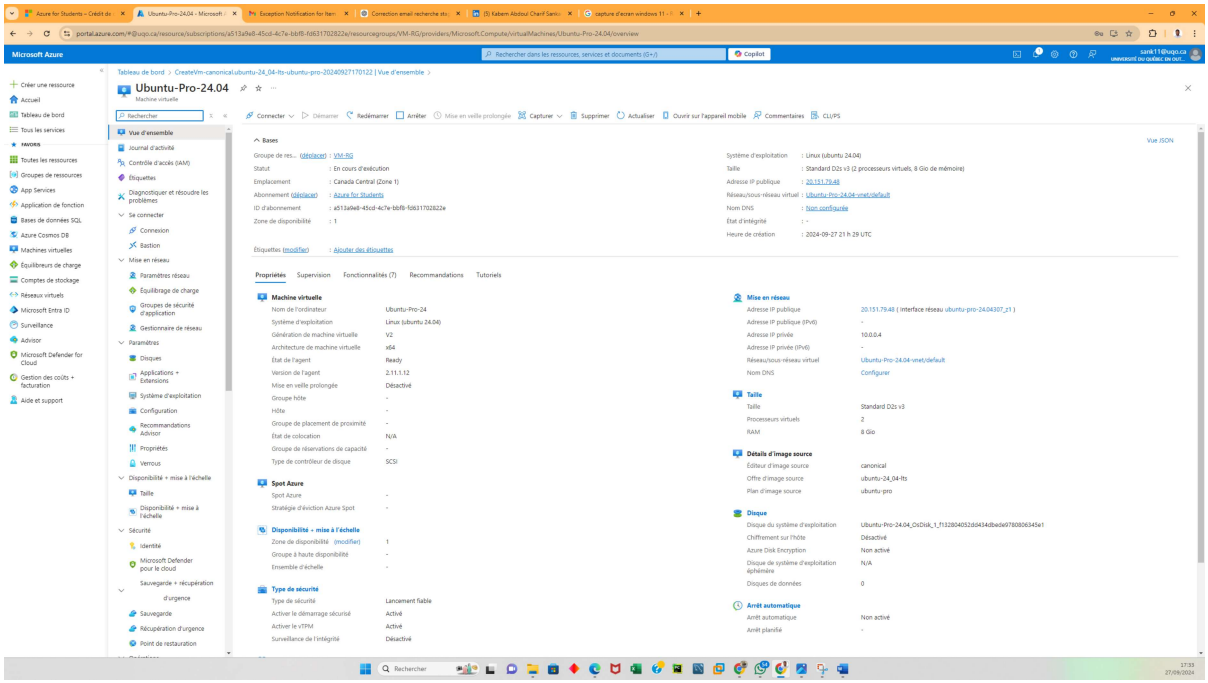
B) Votre abonnement (Partie 2 – Étape 6)

Dans cette partie, nous pouvons voir sur la capture d'écran notre abonnement. Un abonnement dans Microsoft Azure est comme un compte qui permet d'utiliser les services du cloud. Dans notre cas, nous utilisons l'abonnement *Azure for Students*, qui est activé grâce à notre compte étudiant.



C) Propriétés de votre VM (Partie 3 – Étape 13)

Après avoir terminé la configuration d'*Azure for Students*, nous passons à la création de notre machine virtuelle. Avant cela, nous avons créé un groupe de ressources, qui permet de gérer et de classer les différentes ressources associées à notre machine virtuelle.

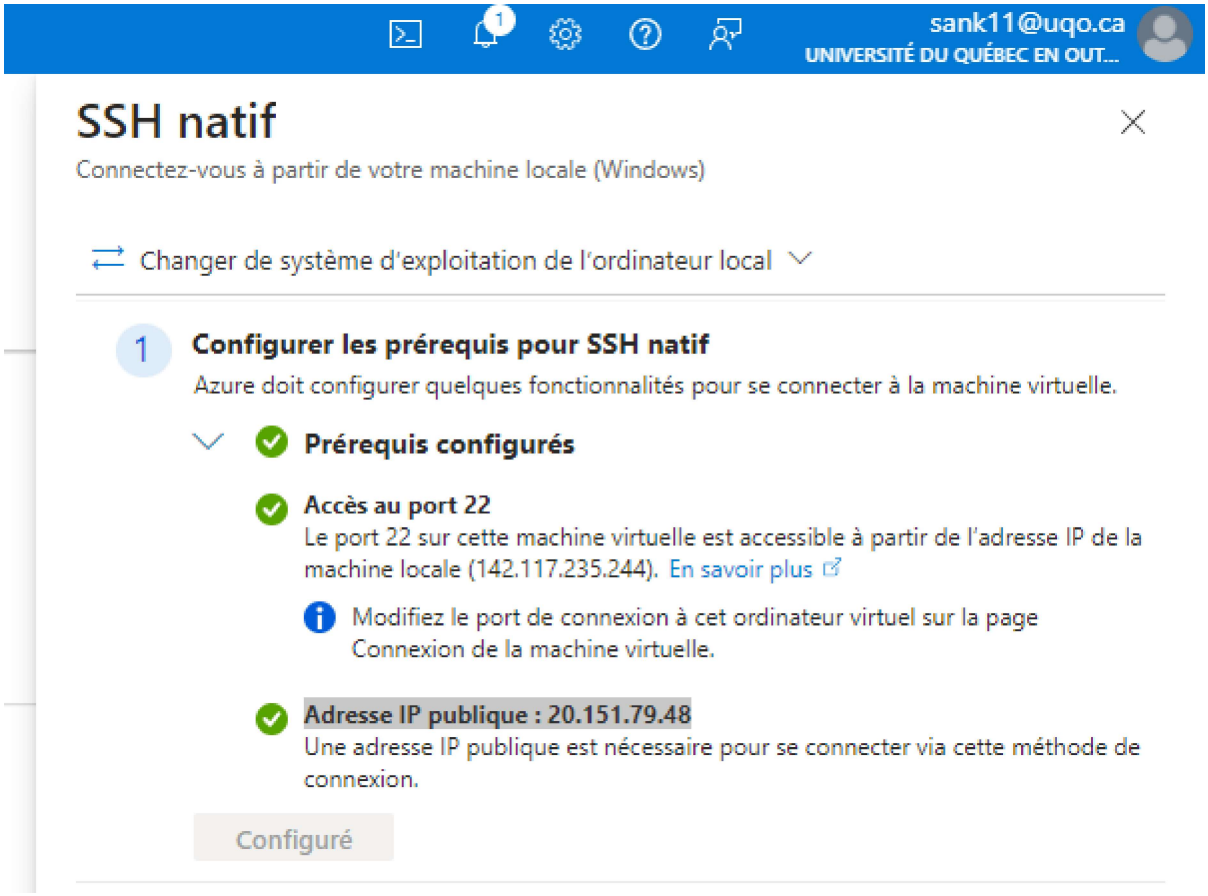


Voici maintenant la création de notre machine virtuelle. Nous pouvons voir toutes les caractéristiques de notre machine dans les propriétés, que ce soit le groupe de ressources utilisé, la zone d'emplacement, le nom de la machine, le système d'exploitation utilisé, l'adresse IP, la taille de la RAM, etc.

D) L'adresse IP de votre machine virtuelle pour la connection Native SSH (Partie 3 – Étape 15)

Après la création de la machine, nous générons l'adresse IP publique afin de retrouver la machine et de nous connecter à elle à distance. Cela nous permet de transférer des fichiers et d'avoir accès aux services, etc.

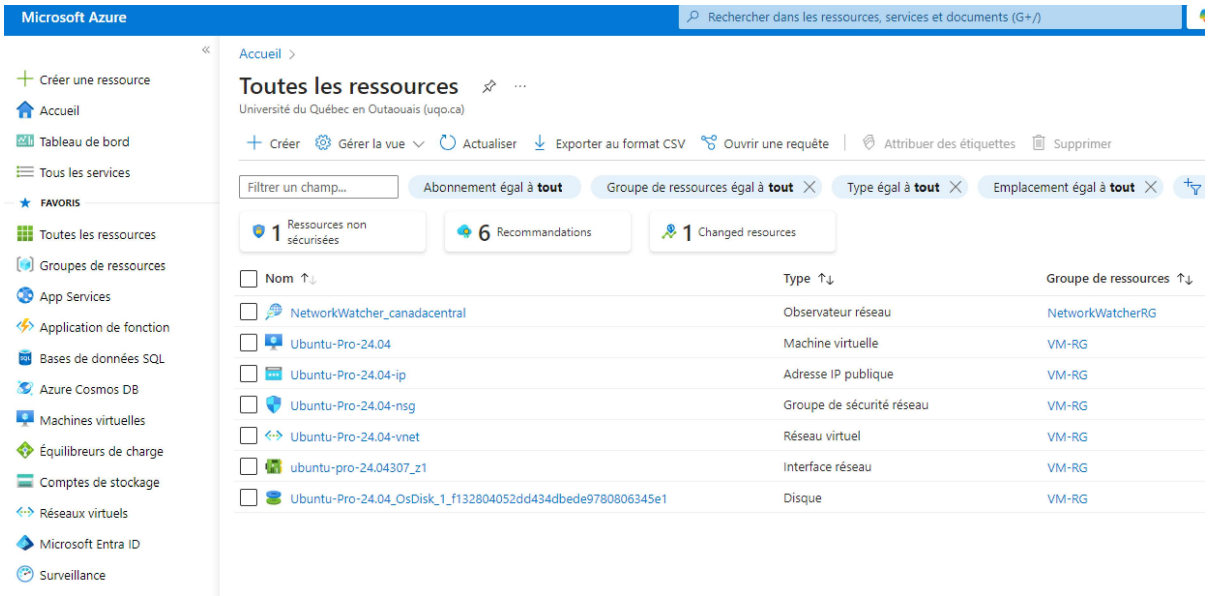
Dans notre cas, l'adresse IP est : `20.151.79.48`



E) Liste des ressources créées (Partie 3 – Étape 20)

l'onglet contenant l'ensemble des fonctionnalités, nous avons la section "Ressources", qui affiche les ressources créées en même temps que notre machine virtuelle.

Nous pouvons constater ici que toutes nos ressources appartiennent à un même groupe de ressources, qui est nommé `VM-RG`.



Conclusion

Ce rapport a présenté le processus de création et d'évaluation de la sécurité d'une machine virtuelle appelée Ubuntu-Pro-24.04 sur Microsoft Azure.

Dans la première partie, nous avons discuté des informations nécessaires pour évaluer la sécurité de la machine virtuelle, même avec un accès administrateur. Nous avons souligné l'importance de demander des données supplémentaires au client pour une évaluation complète.

La seconde partie a analysé la sécurité de la machine virtuelle. Bien qu'elle ait certaines mesures de sécurité en place, nous avons identifié des points à améliorer pour garantir une protection adéquate.

Enfin, la troisième partie a montré les étapes de création de la machine virtuelle, illustrées par des captures d'écran. Ces images ont aidé à visualiser le tableau de bord, les détails de l'abonnement, les propriétés de la machine, l'adresse IP pour la connexion SSH, et la liste des ressources créées.

En résumé, ce rapport nous a aidés à comprendre comment créer et gérer une machine virtuelle dans le cloud, tout en prenant en compte la sécurité.