Université Cadi Ayyad Ecole
Nationale des Sciences Appliquées de Safi

Département Génie Informatique, Réseau et

Télécoms Filière de génie Télécommunications &

Réseaux 3ème année

Rapport de Projet Sécurité Cloud

"La mise en place d'Azure Sentinel SIEM "

Réalisé par :

Abdelmalek Ali

Encadré par :

M. Dalli Anouar

Sommaire

Contents

1 – Introduction

À l'ère de la transformation numérique, l'informatique en nuage a émergé comme le pivot central autour duquel gravitent les opérations informatiques des organisations. Cette migration massive vers le Cloud offre une agilité et une efficacité accrues, mais elle expose également les entreprises à des défis de sécurité sans précédent. Dans ce contexte, la présente étude se concentre sur l'intégration et l'utilisation stratégique d'Azure Sentinel, une solution de pointe développée par Microsoft, pour détecter, analyser et contrer les menaces évoluées et les attaques sophistiquées qui peuvent compromettre l'intégrité des données et la confidentialité des informations.

L'objectif principal de ce projet est d'explorer en profondeur les fonctionnalités avancées d'Azure Sentinel, en mettant particulièrement l'accent sur sa capacité à surveiller en temps réel les activités dans le Cloud, à analyser les schémas de comportement suspects, et à déclencher des réponses automatisées pour neutraliser les menaces potentielles. Nous aborderons également les différents scénarios d'attaque auxquels les entreprises peuvent être confrontées, allant des attaques par force brute aux tentatives d'infiltration plus sophistiquées, tout en mettant en lumière la manière dont Azure Sentinel peut s'avérer être une ligne de défense cruciale dans ces situations.

Cette analyse approfondie ne se limitera pas seulement à la technologie sous-jacente, mais abordera également les meilleures pratiques en matière de configuration, de surveillance continue et de collaboration entre les équipes de sécurité et les opérations Cloud. En fin de compte, ce rapport aspire à offrir une compréhension holistique de l'utilisation d'Azure Sentinel dans le contexte de la sécurité Cloud, avec l'objectif ultime de renforcer la résilience des organisations face aux menaces numériques de plus en plus sophistiquées.

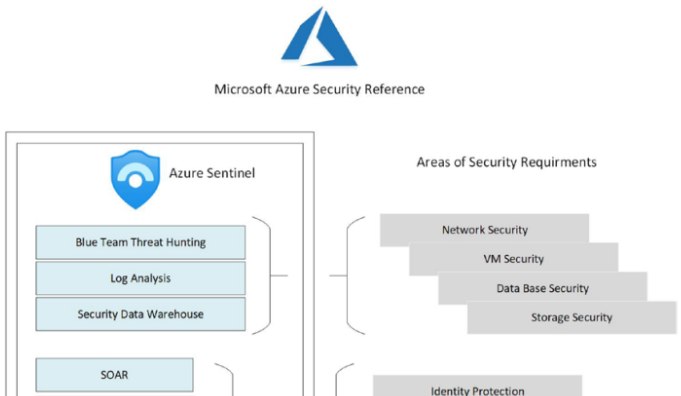
2 – Azure Sentinel

a – Définition

Azure Sentinel est un service en nuage qui répond aux besoins des équipes de sécurité en matière de plateforme de gestion des informations et des événements de sécurité (SIEM). Azure Sentinel accumule de nombreux flux de données (métriques et journaux) provenant des services Azure, tels que les activités des utilisateurs, des ordinateurs, des applications, des machines virtuelles (VM) et d'autres appareils. Les données peuvent être corrélées à partir du nuage Azure, d'un autre nuage (AWS, Google, IBM, etc.) et d'un centre de données sur site. Il comprend des connecteurs logiciels permettant d'intégrer de nombreuses solutions de sécurité tierces telles que Amazon Web Services, Barracuda Web Application Firewall, Palo Alto Networks et VMware ESXi. En outre, SOAR et l'intelligence artificielle (AI) permettent d'analyser de grands volumes de données dans le cadre d'un déploiement à l'échelle de l'entreprise.

L'avantage de cette solution SIEM en tant que service de sécurité ne doit pas être négligé : elle permet aux membres de l'équipe de se recentrer sur le déploiement dans une ou plusieurs régions géographiques d'Azur et de devenir un expert en la matière (SME) de Sentinel. L'intégration de l'IA et de l'automatisation améliore l'efficacité de la réduction des alertes de sécurité. Pour être vraiment efficace, il faut disposer de suffisamment de ressources de calcul (CPU et mémoire) et de grandes quantités de données pour l'analyse. Azure Sentinel accélère en augmentant les ressources de base au fur et à mesure que l'ingestion de données augmente afin de prendre en charge au mieux la vitesse des données fournies par Azure et les services sur site.

La facilité de déploiement pour un locataire unique nécessite des considérations de planification qui affectent le processus de collecte de métriques et de journaux. Le processus commence souvent par la collecte des données des machines virtuelles dans une infrastructure en tant que service (IaaS). Les données sont écrites dans un espace de travail Azure Log Analytics utilisé par Azure Monitor, Azure Security Center et Azure Sentinel. D'autres services Azure sont présentés au chapitre 2. Lorsque le déploiement de l'entreprise s'étend à plusieurs régions géographiques et sur site, les considérations de conception nécessitent davantage de temps de planification. Toutefois, le service Sentinel facilite la connexion des données provenant de nombreux autres produits par l'intermédiaire d'un proxy. Vous pouvez examiner une architecture simplifiée dans la figure



b – SIEM

- Définition

SIEM, qui signifie Security Information and Event Management (gestion des informations et des événements de sécurité), est une solution de sécurité complète qui combine des fonctionnalités de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Elle permet aux organisations d'avoir une vue d'ensemble de leur situation en matière de sécurité en collectant, analysant et mettant en corrélation des données provenant de diverses sources, notamment des dispositifs de réseau, des serveurs, des applications et des appareils de sécurité. Le diagramme ci-dessous vous aidera à comprendre comment vous pouvez mettre en œuvre le SIEM dans votre organisation.

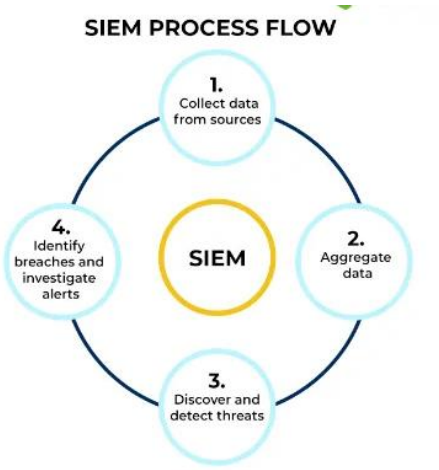


Figure 0-2 Processus de SIEM

- Principales caractéristiques et avantages du SIEM

Gestion centralisée des journaux

Le SIEM sert de référentiel central pour la collecte et l'analyse des journaux provenant de systèmes et d'appareils disparates sur le réseau. En regroupant les journaux, il permet aux équipes de sécurité d'avoir une vue unifiée des événements de sécurité, ce qui simplifie la détection des menaces et la réponse aux incidents.

Surveillance des événements en temps réel

Le SIEM surveille en permanence les événements et les alertes de sécurité en temps réel, ce qui permet une détection et une réponse précoces aux menaces potentielles. Il s'appuie sur des capacités de corrélation et d'analyse avancées pour identifier les modèles, les anomalies et les indicateurs de compromission, ce qui permet aux équipes de sécurité de prendre des mesures proactives.

Intégration des renseignements sur les menaces

Les solutions SIEM s'intègrent aux flux de renseignements externes sur les menaces, ce qui permet aux organisations de se tenir au courant des derniers acteurs de la menace, des techniques d'attaque et des vulnérabilités. Cette intégration améliore la précision de la détection des menaces et aide les organisations à répondre efficacement aux menaces émergentes.

Réponse aux incidents

Le SIEM soutient les efforts de réponse aux incidents en fournissant des informations détaillées sur les événements de sécurité, facilitant ainsi l'investigation et l'analyse médico-légale. Il permet aux équipes de sécurité de remonter à la cause première des incidents, d'identifier les systèmes compromis et de recueillir des preuves en vue d'une analyse plus approfondie ou à des fins juridiques.

c – Azure Sentinel Architecture

L'un des points forts d'Azure Sentinel par rapport à d'autres solutions SIEM est son intégration transparente avec d'autres services Azure, tels qu'Azure Active Directory (AD), Azure Monitor et Azure Security Center. Les entreprises peuvent ainsi gérer la sécurité de l'ensemble de leur environnement à partir d'une plateforme unique, ce qui réduit la complexité et améliore l'efficacité.

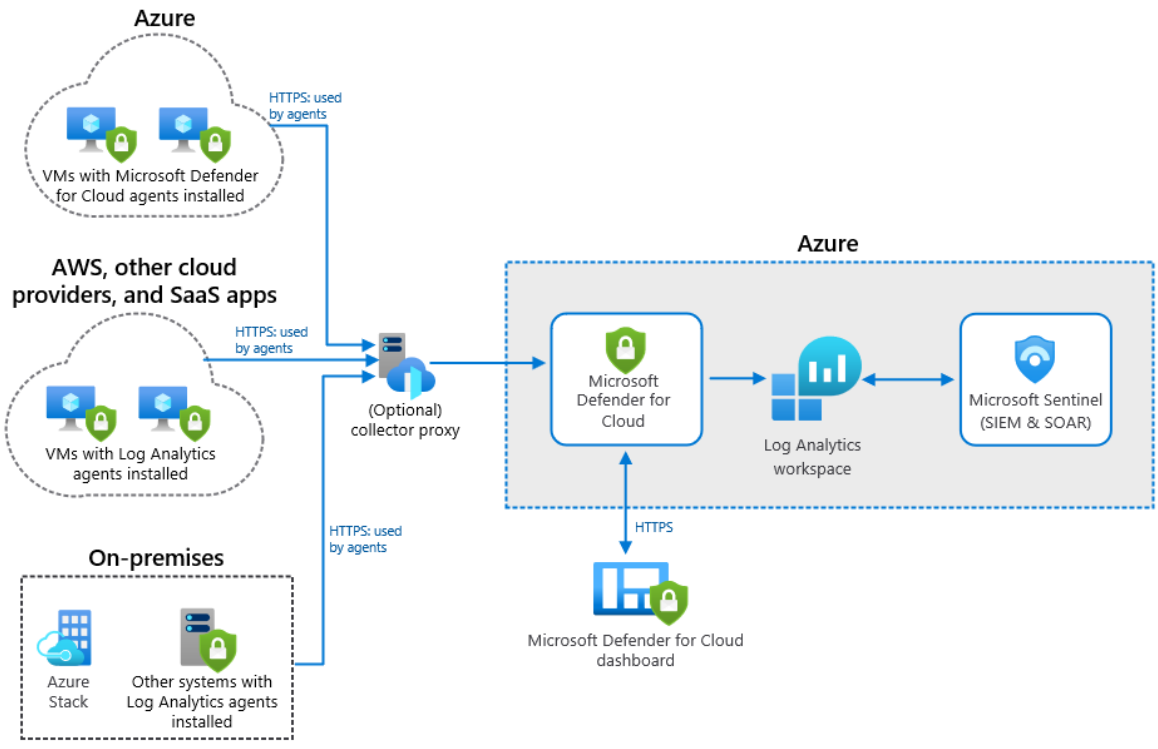


Figure 0-3 Architecture d'Azure Sentinel

Collecte des données : Azure Sentinel collecte des données de sécurité à partir de diverses sources, notamment les services Azure, les systèmes sur site, les services en nuage et les solutions de sécurité tierces. Les données collectées sont stockées dans un référentiel centralisé dans Azure.

Renseignements sur les menaces : Azure Sentinel s'intègre à une série de sources tierces de renseignements sur les menaces afin de fournir une vue d'ensemble des menaces auxquelles votre entreprise est confrontée.

Espace de travail pour l'analyse des logs : Les données de sécurité collectées sont stockées dans un espace de travail Log Analytics, qui est utilisé pour stocker, rechercher et analyser les données de sécurité.

Machine Learning: Azure Sentinel utilise des algorithmes d'apprentissage automatique et d'intelligence artificielle (IA) pour détecter et alerter les menaces en temps réel.

Workbooks : Les classeurs sont utilisés pour créer des tableaux de bord interactifs et personnalisables afin d'afficher les données de sécurité, ce qui permet aux équipes de sécurité de trouver et d'analyser rapidement les données pertinentes.

Alertes : Azure Sentinel permet aux organisations de créer des alertes personnalisées qui peuvent être déclenchées en fonction d'événements de sécurité spécifiques.

API : Azure Sentinel fournit un riche ensemble d'API qui peuvent être utilisées pour automatiser les tâches et les flux de travail courants, s'intégrer à d'autres services Azure et personnaliser les classeurs afin de répondre à des exigences et à des besoins spécifiques.

L'architecture d'Azure Sentinel est conçue pour fournir aux organisations une plateforme centralisée et évolutive pour collecter, analyser et répondre aux incidents de sécurité. Grâce à son intégration avec d'autres services Azure, à la détection des menaces en temps réel et à un riche ensemble d'API, Azure Sentinel est un outil puissant pour les organisations qui cherchent à améliorer leur posture de sécurité.

d – Conclusion :

Dans ce chapitre, nous avons découvert les avantages d'Azure Sentinel pour l'entreprise et la manière d'activer Sentinel dans votre abonnement. Enfin, nous avons appris à quel point il est facile d'activer les connexions de données et de stocker les données dans le même espace de travail Log Analytics qu'Azure Monitor.

Dans le prochain chapitre, nous commencerons à construire notre projet et à mettre en œuvre Azure Sentinel.

3 – Réalisation de projet

Dans ce chapitre, nous allons découvrir comment déployer Azure Sentenel pour collecter les logs et défendre une machine virtuelle ubuntu Server déployée, et nous allons installer rsyslog, un paquet qui nous aidera à collecter les logs d'ubuntu et à transférer les logs vers l'espace de travail d'Azure Log Analytics, puis à le connecter à Azure Sentenel.

a - L'architecture de projet

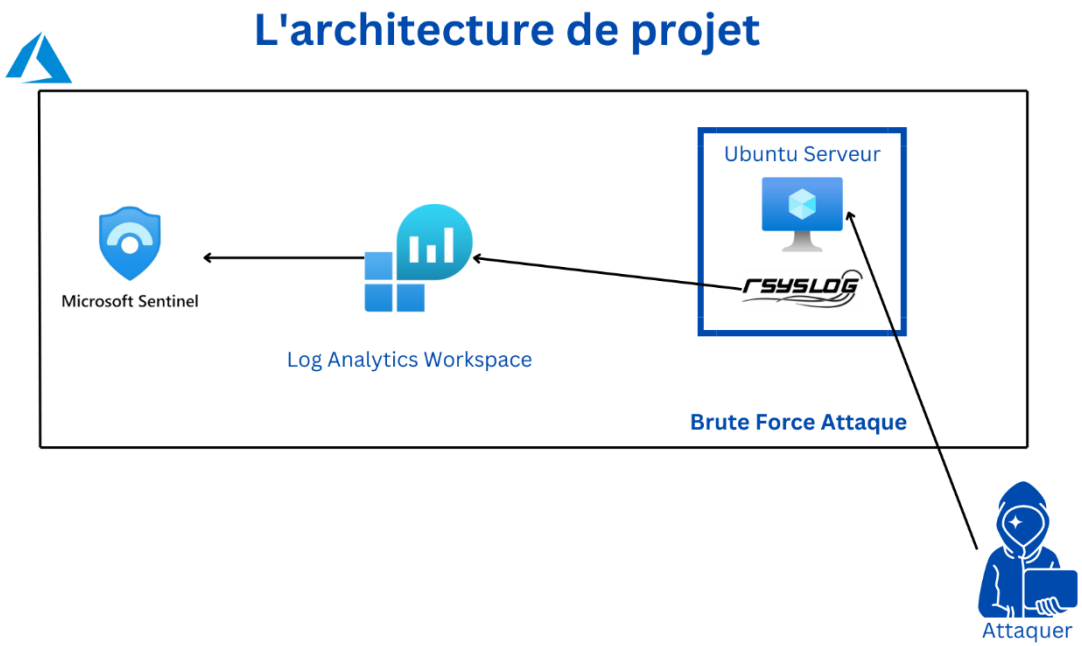


Figure 0-1 L'architecture de projet

Comme nous pouvons le voir dans la figure ci-dessus nous allons construire un archi basé sur un serveur ubuntu simulant une cible pour l'attaquant, après nous allons installer rsyslog comme le collecteur de log principal pour notre serveur c'est celui qui est responsable de la collecte des logs pour azure Log Analystics Workspaces, et le dernier aidera Sentenel à collecter ses logs pour les analyses futures et dans le prochain chapitre nous allons simuler une attaque de force sur SSH.

b – Déploiement d'un Serveur Ubuntu

Dans cette partie on lancer notre serveur qu'on va le nommer webserveur qui fait partie de « Project sécurité « ressource group.

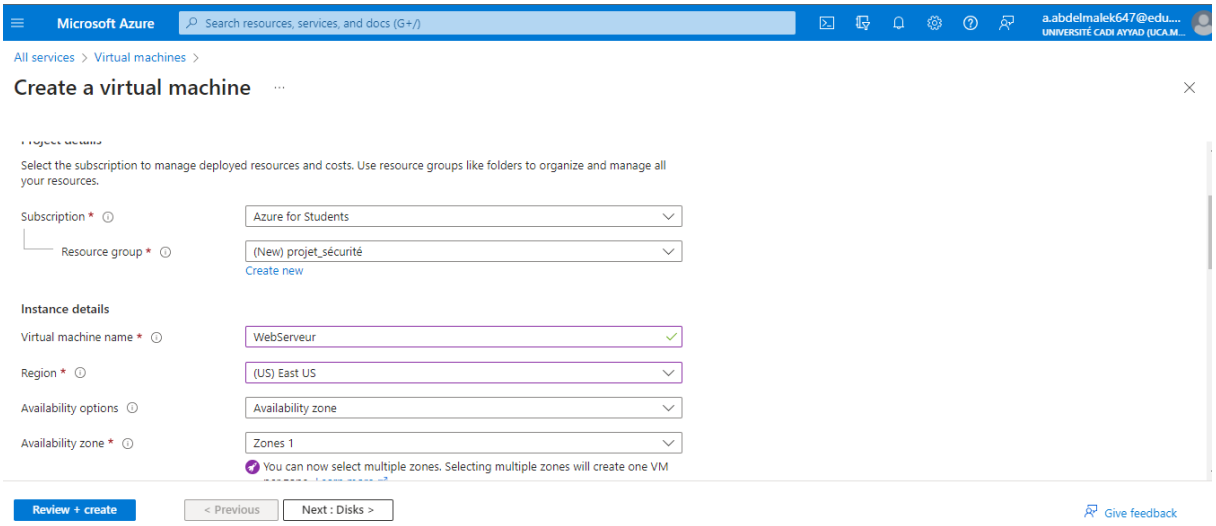


Figure 0-2 création d'un VM

Après on va spécifie les configurations et les ressources pour notre serveur.

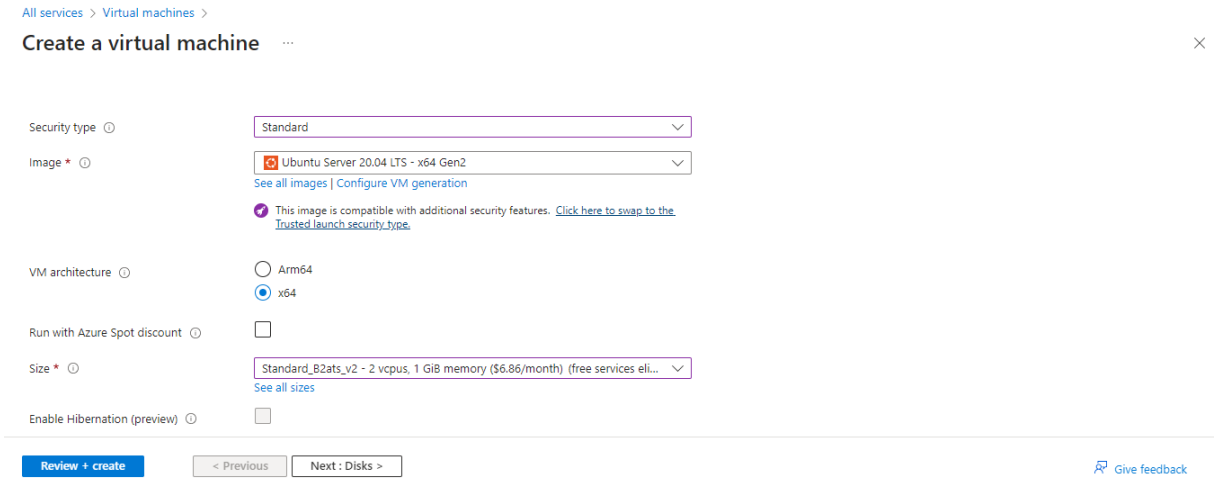


Figure 0-3 configurations de VM

Après la configuration de SSH pour l'Access à distance et pour les configurations pour le moment on va utiliser une clé publique pour se connecter mais après on va utiliser une pour mot de passe.

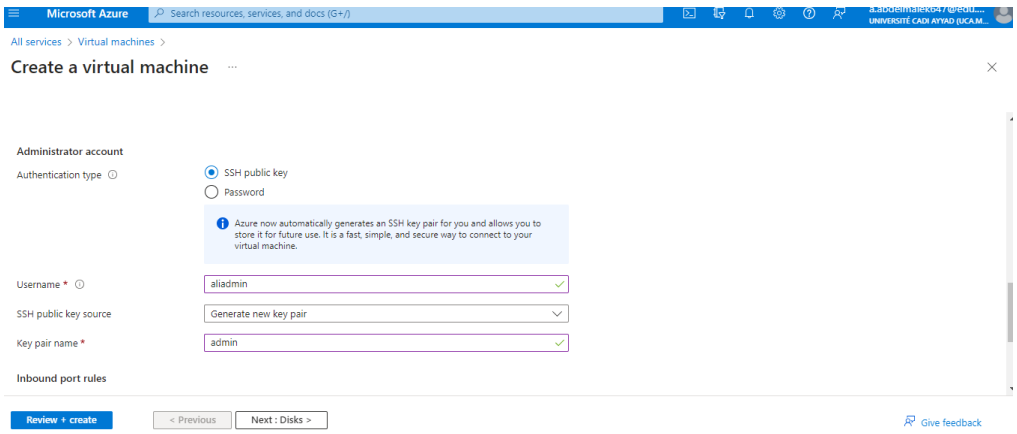


Figure 0-4 configuration de ssh

Maintenant la configuration de la ACL pour donner l'accès a l'utilisateur externes d'avoir l'accès à notre serveur via Ssh, http et https.

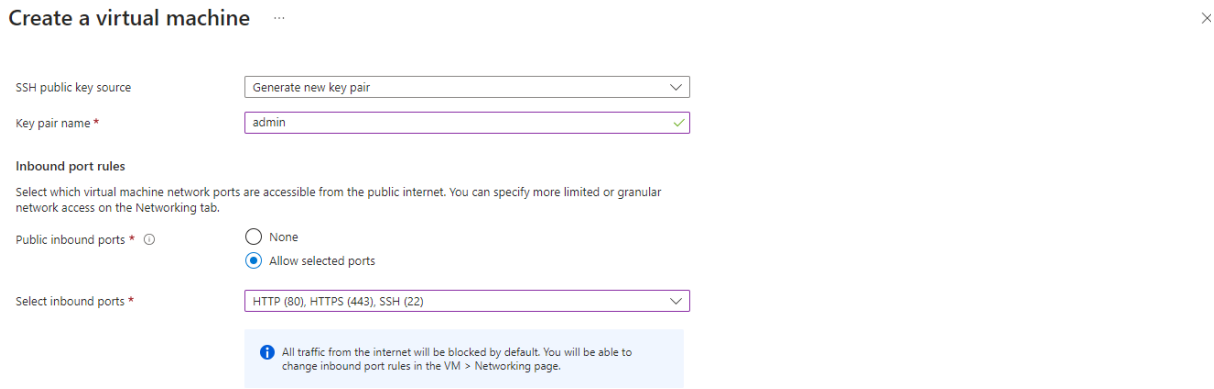


Figure 0-5 Configuration de l'ACL

Donc finalement notre serveur a été créé et maintenant on va passer vers la configuration rsyslog pour collecter les logs.

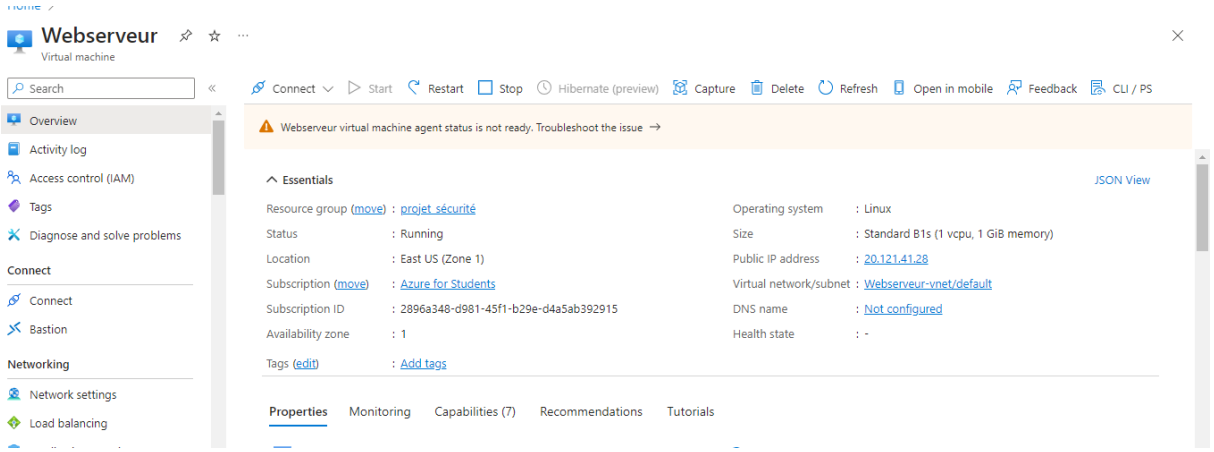


Figure 0-6 résume de serveur

c – Configuration de Rsyslog

Rsyslog est un système open source pour le traitement des logs à haute performance. Plus qu'un simple enregistreur de système, il s'agit d'un outil polyvalent qui peut recevoir des données de nombreuses sources et les envoyer vers de nombreuses destinations.

Rsyslog prend en charge le transfert des messages de journalisation sur un réseau IP, vers des bases de données, des courriers électroniques, etc. et étend le protocole syslog de base avec de puissantes capacités de filtrage. Il offre de puissantes options de configuration pour s'adapter à des besoins spécifiques.

Donc dans cette partie de ce chapitre on va configurer le rsyslog pour transférer les donnes vers azure. Premièrement on va se connecter via notre serveur en utilisant ssh. Et on va installer le paquet de rsyslog.

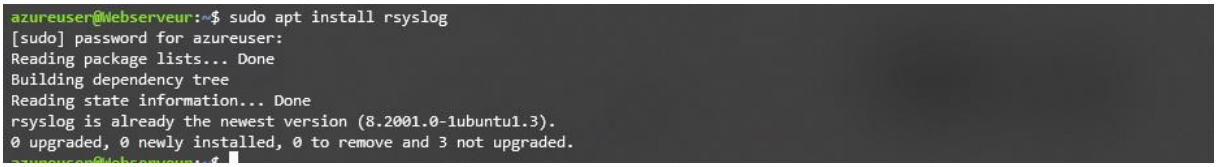


Figure 0-7 installation de rsyslog

Après on faires des configurations et éditer le ficher sur « /etc/rsyslog.conf » pour donner l'accès à rsyslog d'être accessible à l'extérieur via UDP et TCP sur le port 514.

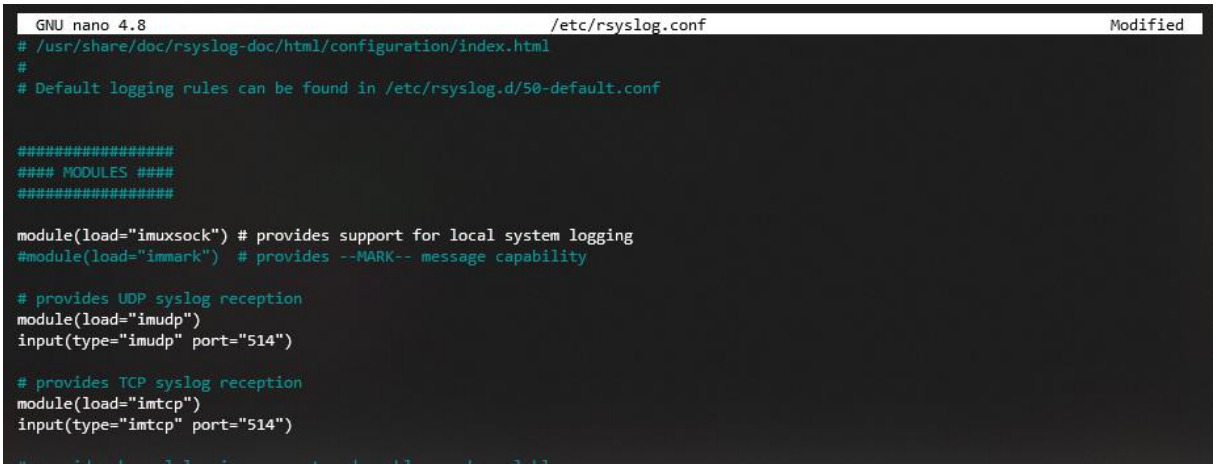


Figure 0-8 configuration de rsyslog 2

On va redémarrer rsyslog en utilisant la commande systemctl restart.

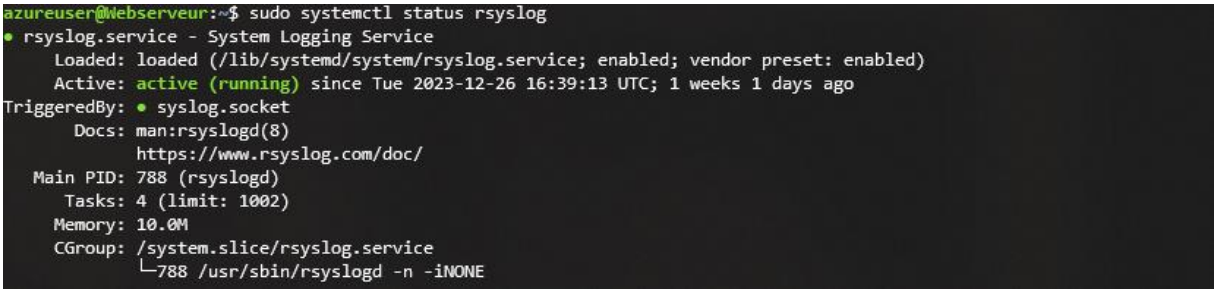


Figure 0-9 rsyslog statues

d – Connecter rsyslog avec Azure Log Analytics Workspaces

Dans cette partie de ce chapitre on va construire la première liaison entre notre serveur et Sentenel, cette étape la connexion entre rsyslog et Log analytics workspaces.

Premièrement on va commander une Log analytics workspace qui prend le nom de rsyslog.

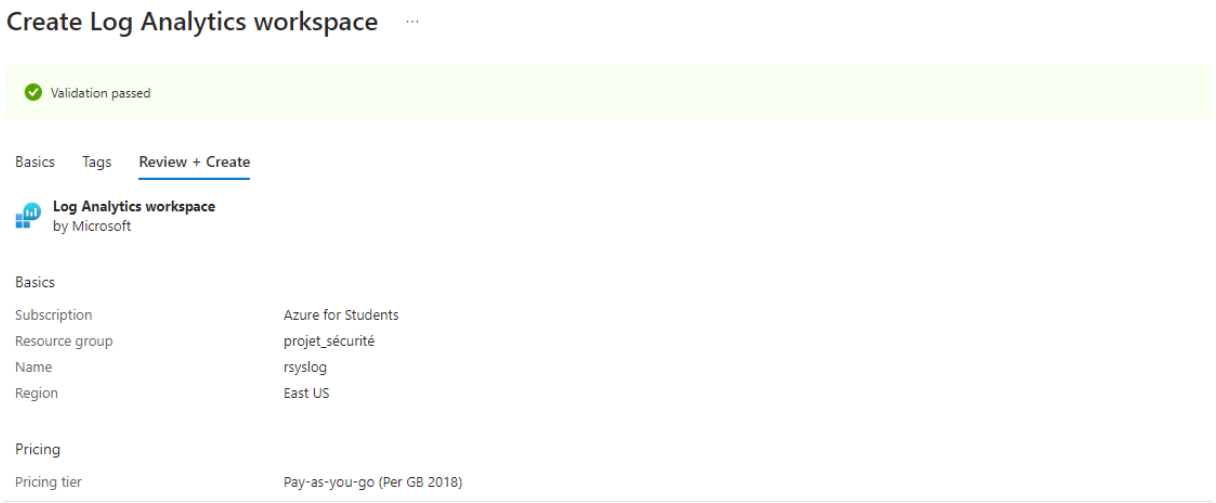


Figure 0-10 Log analytics workspace

Et maintenant on a besoin de le connecter avec notre serveur ubuntu.

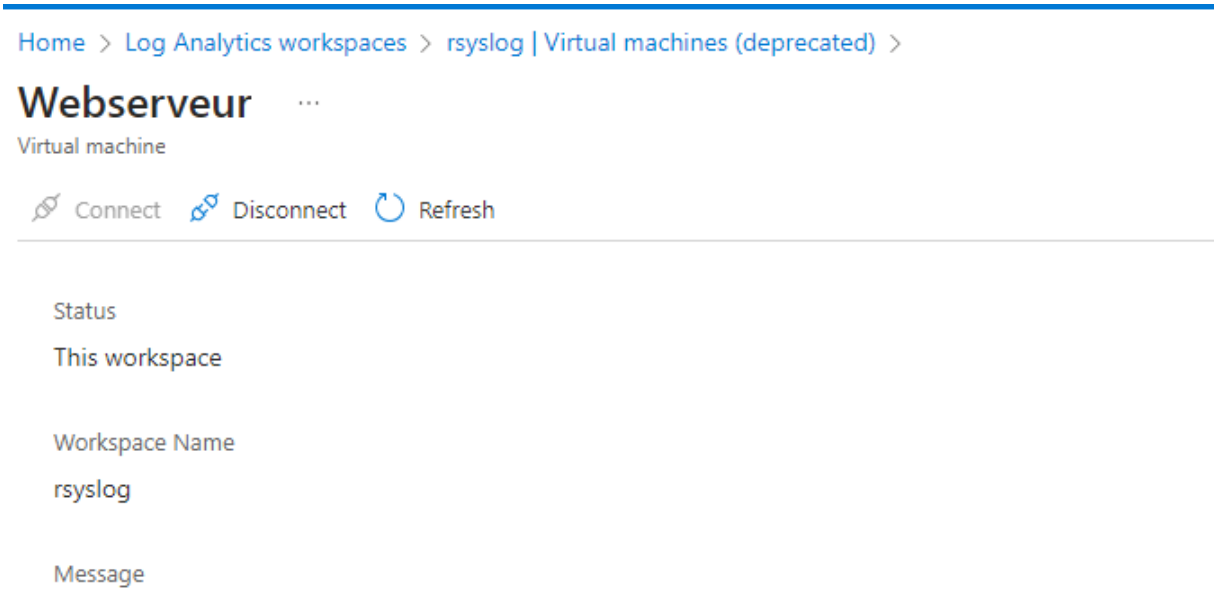


Figure 0-11 Log workspace avec le serveur

Après lorsqu'il a connecté, la workspace nous donnera une script ou un code pour l'exécuter dans notre serveur pour compléter la liaison.

```
azureuser@Webserveur:~$ wget https://raw.githubusercontent.com/Microsoft/OMS-Agent-for-Linux/master/installer/scripts/onboard_agent.sh && sh onboard_agent.sh -w 2db13a43-8671-4934-9911-9978e1f9f907 -s KeLmc/L3c6R0iXiGRAg/CIDY8G3+MJrV9xp/duxBWPQd+bxN6Yopp7KUo8AdiX3Y6nl/mInMGNBW5qjGCJNe+g== -d opinsights.azure.com
```

Figure 0-12 exécution de script

Maintenant c'est le temps de savoir est ce que on a connecté avec le serveur avec notre rsyslog workspace.

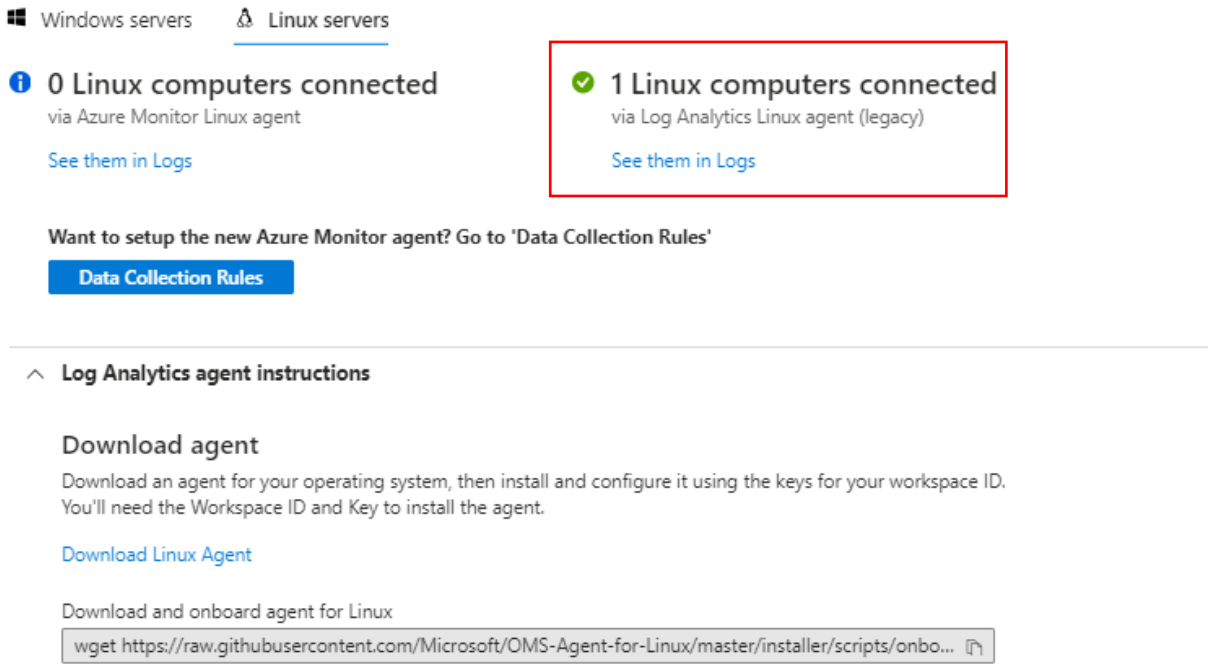


Figure 0-13 liaison complète

Si on clique sur la bouton » see them in logs » il va nous rediriger vers les logs de notre serveur.

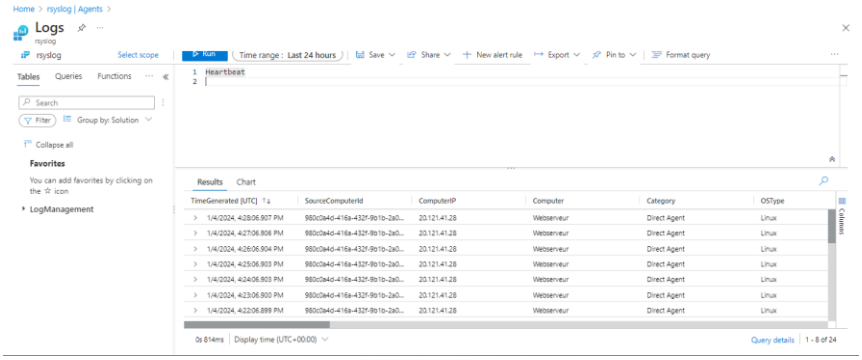


Figure 0-14 linux logs

Mais on a un problème ce que on remarque que on ne voie pas les logs de rsyslog, on va les configurer dans notre workspace.

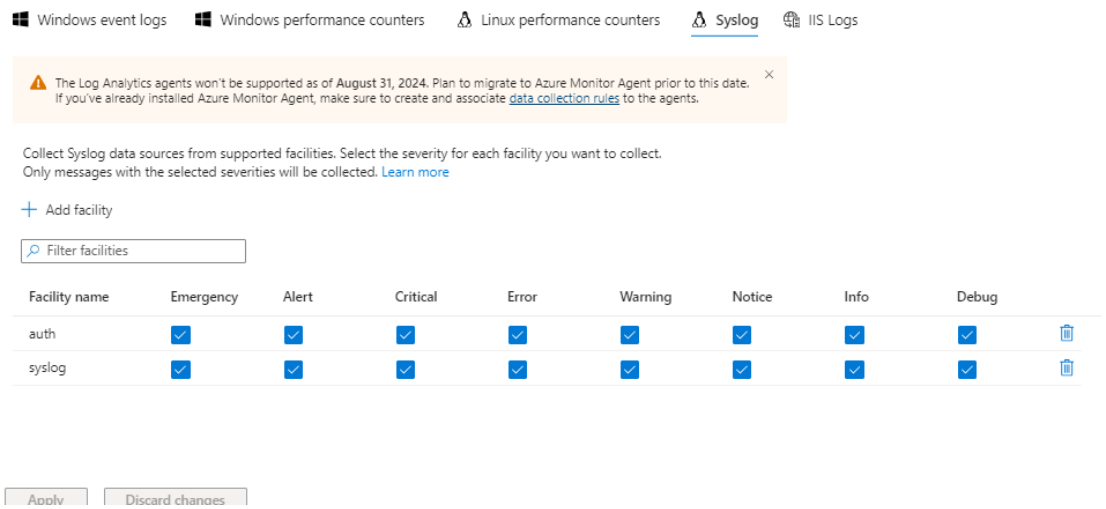


Figure 0-15 ajoutant rsyslog sur le workspace

Ans ajouter les deux facilitées « auth » et « syslog « pour collecter les logs basiques de syslog et les logs d'authentification.

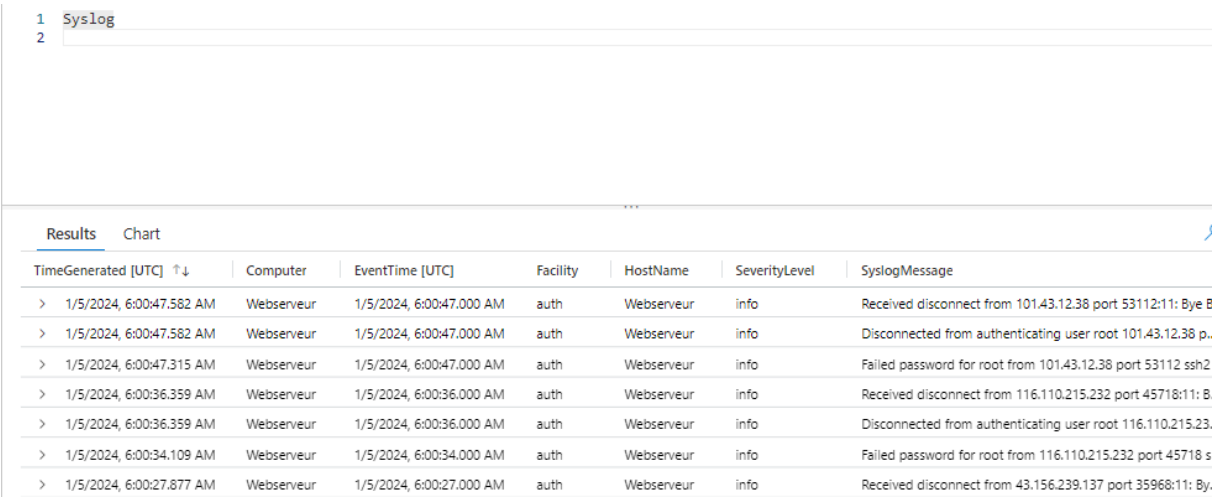


Figure 0-16 les logs de rsyslog

e – configuration de Azure Sentenel

Pour configurer sentenel, on a besoin juste de l'écrire dans Microsoft sentenel choisir le cout parfait pour vous pour nous on a choisi un mois gratuit pour le tester et lorsque on a le crée on connecter sentenel avec note log workspace qu'on a construit.

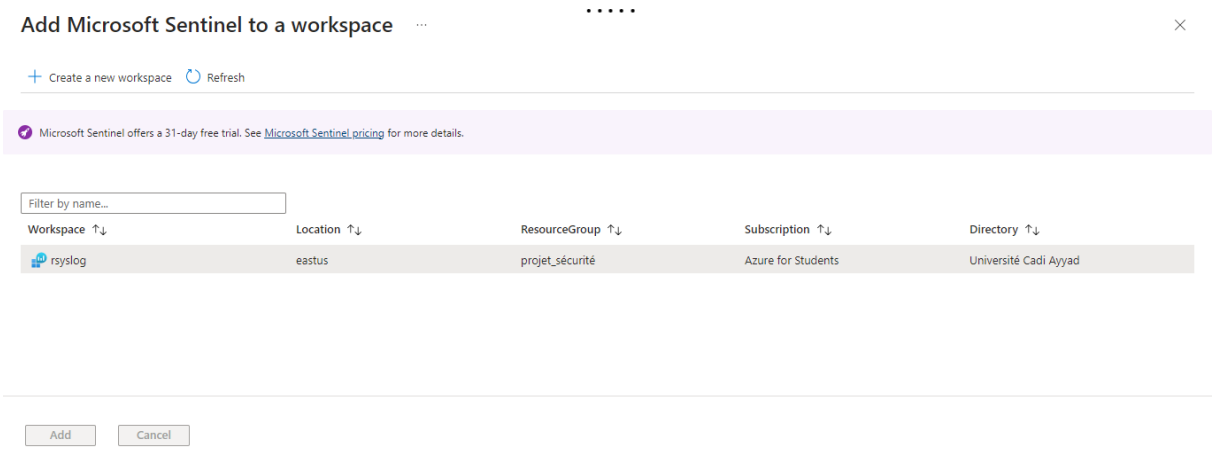


Figure 0-17 configuration de Sentenel

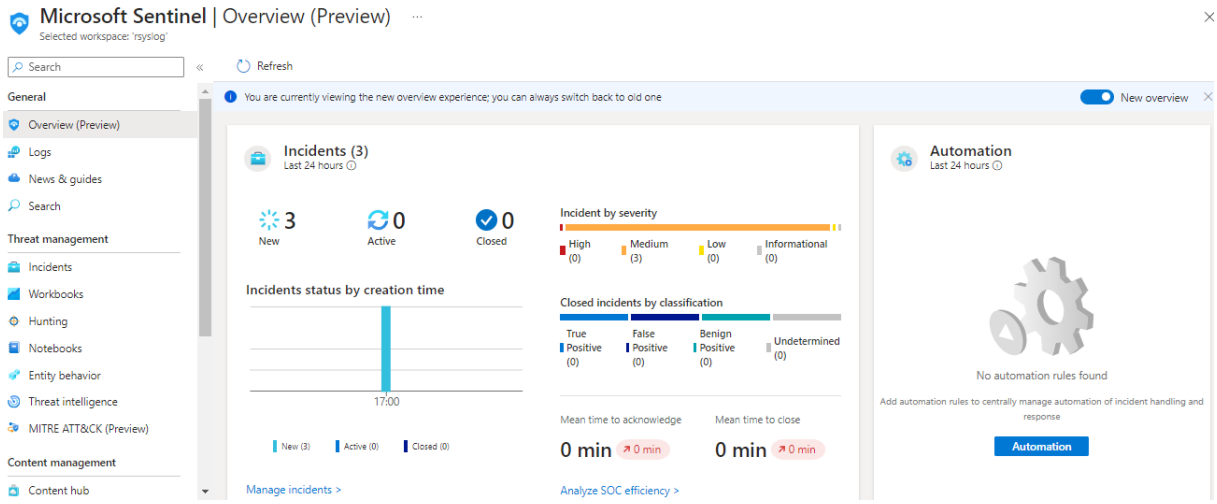


Figure 0-18 sentenel Dashboard

Voici notre tableau de bord Sentenel, nous allons passer la plupart de notre temps à analyser les logs et à créer des règles, dans ce tableau de bord nous allons remarquer beaucoup de composants et de fonctionnalités de Sentenel, par exemple il nous affiche déjà quelques incidents qui se sont déjà produits et aussi l'onglet qui nous importe beaucoup est l'onglet Analytique qui nous aidera à créer nos règles c'est ce que nous allons faire dans le prochain chapitre.

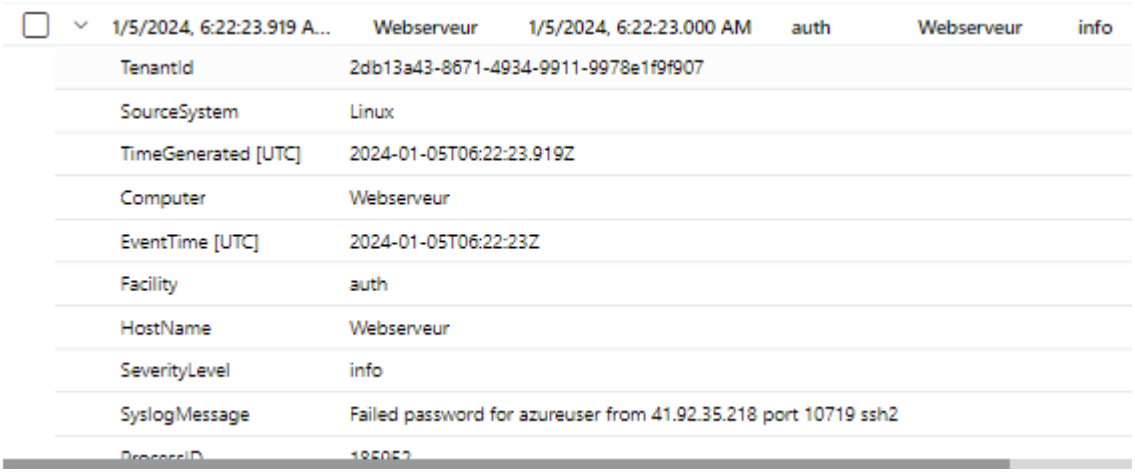
4 – Création des Rules et Simulation d’un Attaque

Dans ce chapitre, nous allons prendre un moment pour comprendre les journaux qui nous parviennent de rsyslog, puis nous allons créer une règle personnalisée pour supprimer l'attaque par force brute sur ssh, après quoi nous allons attaquer le serveur en utilisant la machine Kali et l'outil Hydra pour nous aider à simuler l'attaque.

a – création des rules

Dans cette partie du chapitre, nous allons comprendre comment syslog réagit lorsqu'un utilisateur saisit un mauvais mot de passe lorsqu'il se connecte à ssh. Et sur cette base, nous allons créer une règle qui déclenche une alerte si l'utilisateur saisit un mauvais mot de passe 10 fois.

Donc dans ces command on se connecter avec ssh mais on a saisi le mauvais mot de passe, maintenant on va remarque command sentenel va réagir.



Donc le log de l’authentification échoue on remarque 3 chose premièrement la facilité qu’il est la responsable de lancer cette log est « auth » donc il comprend que cette log est pour l’authentification, et deuxième c’est le nom et adresse ip de serveur pour que nous les analystes savoir quelle est la ou les machines affectées, et troisièmes c’est la source qui est responsable de l’authentification avec leur adresse ip. Et aussi il contient un message.

Tous ces éléments qu’on a remarqués ils vont nous aider à construire notre rule pour détecter les attaques de brute force.

Pour créer une rule on va accéder vers analystes dans sentinel.

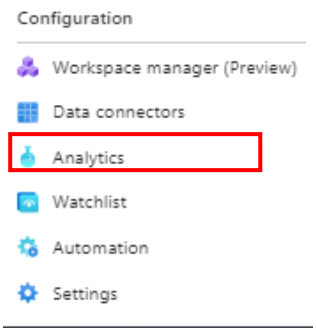


Figure 0-1 analystics

Pour construite une nouvelle rule on va cliquer sur Create > Scheduled query rule.

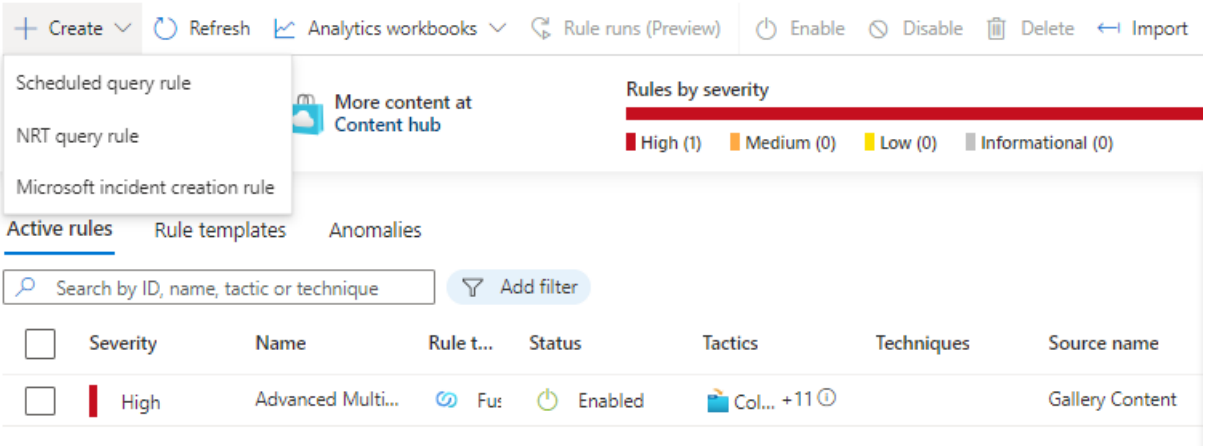


Figure 0-2 création des rule

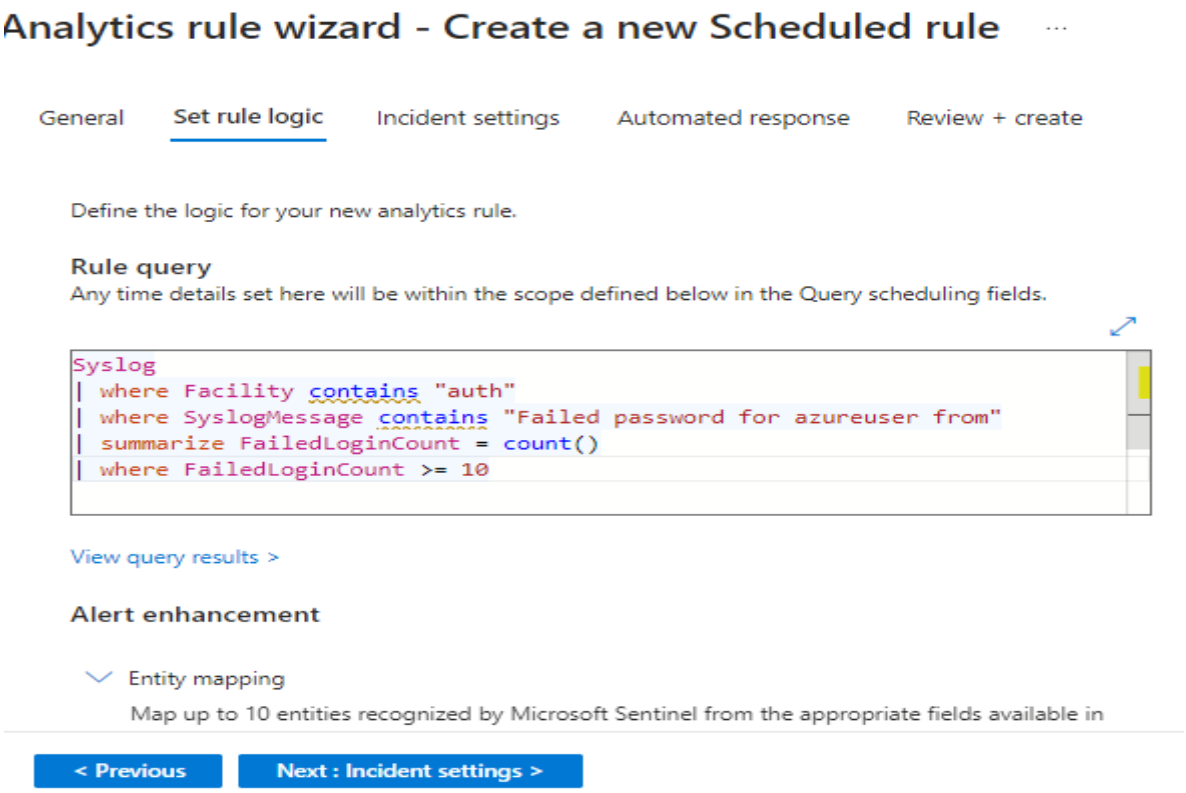


Figure 0-3 Rule de brute force

Donc on va détailler la règle pour la comprendre premièrement on sélecter syslog pour dire au sentinel que nous avons besoin des logs de rsyslog et on a choisi la facility « auth » après on va chercher les le message que contient « failed password for azure user from » et on va compter 10 fois, En résumé, si quelqu'un essaie de se connecter avec un mauvais mot de passe 10 fois via ssh, nous allons créer une alerte.

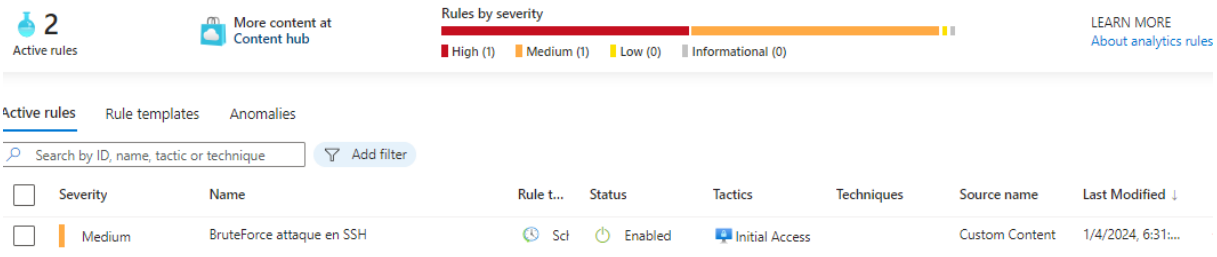


Figure 0-4 rule

Donc notre rules a été créé, on a le donné le nom « bruteforce attaque en ssh ».

b – simulation de bruteforce attaque

Dans cette partie on va utiliser une outil appelé Hydra dans Kali pour simuler l'attaque.

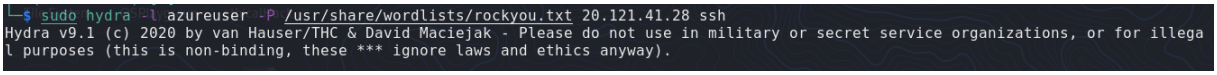
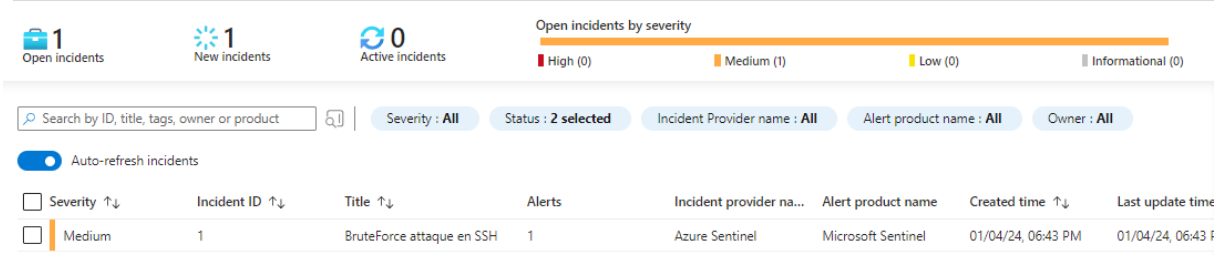


Figure 0-5 simulation de l'attaque

Donc comprendre comment ça marche on va détailler le command
Sudo : pour l'exécuter en mode administrateur
l : pour choisir une nome d'utilisateur dans notre cas 'azureuser'
P : choisir un fichier des mots de passes, on a choisi rouckyou.txt que contient des millions des mots de passes
Adresse Ip publique de notre serveur et finalement le protocole ssh

Donc on a lancer l'attaque sure la machine on va attendre pour que sentinel détecte l'attaque.



Et finalement Azure sentinel a fait son travail de détection de la menace.

c- conclusion

Nous créons ainsi notre première règle qui détecte les attaques par force brute ssh après avoir lancé notre attaque.

5 – Conclusion

En conclusion, notre exploration approfondie de l'intégration d'Azure Sentinel dans le paysage de la sécurité du Cloud révèle une perspective prometteuse pour renforcer la posture de sécurité des organisations modernes. La complexité croissante des menaces numériques et des attaques sophistiquées nécessite des solutions agiles et proactives, et Azure Sentinel émerge comme une réponse robuste à ces défis.

L'efficacité de la plateforme repose sur sa capacité à agréger et à analyser en temps réel des volumes massifs de données de sécurité, détectant ainsi les schémas de comportement anormaux et les signaux d'alerte précurseurs. L'automatisation des réponses aux incidents renforce la réactivité, permettant aux équipes de sécurité de contrer rapidement les menaces émergentes avant qu'elles ne compromettent la confidentialité des données et l'intégrité des systèmes.

Cependant, l'implémentation réussie d'Azure Sentinel ne se limite pas à la technologie seule. Une approche holistique englobe également des processus de surveillance continue, des ajustements réguliers des configurations et une collaboration étroite entre les équipes de sécurité et les opérations Cloud. Les meilleures pratiques dans ces domaines sont cruciales pour maintenir une défense proactive et adaptative.

En définitive, l'adoption d'Azure Sentinel dans le cadre de la sécurité du Cloud offre aux organisations une solution puissante et évolutive pour faire face aux menaces numériques en constante évolution. En intégrant cette technologie de manière stratégique, les entreprises peuvent renforcer leur résilience face aux attaques, protégeant ainsi leurs actifs numériques et préservant la confiance de leurs utilisateurs. L'investissement dans des solutions de sécurité avancées telles qu'Azure Sentinel représente un pas significatif vers la création d'un environnement informatique sécurisé et fiable à l'ère du Cloud.