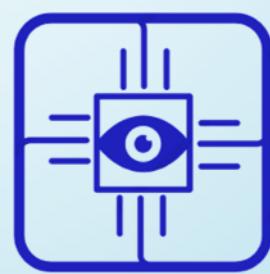


Proposition infrastructure

Partie Gouvernance



**NET
STACK**

Sommaire

Table des matières

Introduction.....	3
Infrastructure as Code.....	3
Introduction.....	3
Présentation détaillée de la solution <i>GitHub</i>	4
Détails des tests à effectuer	6
Gestion du parc	13
Introduction.....	13
Intégration de l'outil <i>ITSM Servicenow</i> avec Azure	13
Intégration de l'outil <i>ITAM Servicenow</i> avec Azure	19
Tarification de la solution.....	23
Gestion des logs	23
Introduction.....	23
Justification du choix de l'outil	24
Solution de gestion des logs système de l'infrastructure MALO	24
Présentation détaillée de la solution <i>Azure Monitor Logs</i>	24
Exportation des logs Azure AD vers l'espace de travail Analytics	26
Création d'une Data Collection Rules pour les logs	28
Paramètres de diagnostic (<i>Diagnostic Settings</i>).....	31
Logs Query.....	31
Stratégie de rétention des logs	33
Solution de gestion des logs sécurité de l'infrastructure MALO	33
Présentation détaillée de la solution <i>Azure Sentinel</i>	33
Configuration du SIEM.....	34
Rétention des logs	39
Solution de gestion des logs des équipements réseaux On-Premise.....	40
Choix du modèle.....	40
Coût de l'outil.....	41
Installation dans l'environnement réseau de l'entreprise MALO	41
Tarification pour la gestion des logs.....	49
Supervision	52
Introduction.....	52
Présentation détaillée de la solution <i>Azure Monitor</i>	52

Création d'une Règle de Collecte des Données	53
Activation de la fonctionnalité <i>Insights</i>	54
Création d'alertes sur les serveurs virtuels	56
Tarification pour la supervision.....	57
Coût d'intégration et de migration	58
Coût de la main d'œuvre pour la solution <i>Infrastructure as Code</i>	58
Coût de la main d'œuvre pour la solution <i>Servicenow</i>	58
Coût de la main d'œuvre pour les solutions de gestion des logs <i>Azure Monitor Logs</i>	59
Coût de la main d'œuvre pour la solution de supervision <i>Azure Monitor</i>	59
Coût de la main d'œuvre pour la solution de gestion des logs de l'infrastructure On-Premise.....	60
Planning de la migration.....	60
Modalités pour rendre autonome l'équipe IT de la société MALO.....	61
Schéma récapitulatif.....	63
Schéma global	64

Introduction

La partie Gouvernance de la nouvelle infrastructure de la société MALO se découpe de la manière suivante :

- La supervision : l'infrastructure de la société MALO va être migrée sur le cloud Azure, et une solution de supervision sera proposée pour permettre au service informatique de la société de mieux gérer son infrastructure et prendre les décisions nécessaires avec le plus d'éléments possibles.
- La gestion des logs : qu'une infrastructure soit On-Premise ou sur Cloud, les logs sont une pièce centrale dans la bonne gestion d'une infrastructure et de sa sécurité. Nous allons expliquer la solution retenue pour la gestion des logs système et de sécurité (On-Premise et sur cloud), qui jouent un rôle majeur dans les décisions de gestion de l'infrastructure.
- La gestion du parc : la société MALO n'ayant aucune solution de ticketing et de gestion du matériel, nous allons expliquer la solution retenue pour chacune de ces fonctionnalités, et en quoi ces solutions sont pertinentes et efficaces dans le cadre de la migration vers le cloud Azure.
- L'Infrastructure as Code : C'est un modèle de gestion de l'infrastructure qui se développe de plus en plus dans les entreprises, du fait de son efficacité et de sa scalabilité. Nous allons décrire dans la partie qui lui sera dédiée la solution retenue et pourquoi cette solution sera efficace dans l'environnement cloud de la société MALO.

Infrastructure as Code

Introduction

Pour gérer l'Infrastructure as Code de l'entreprise MALO, nous avons fait le choix de passer par la plateforme de gestion de déploiement et du stockage de code GitHub, qui est un service web d'hébergement et de gestion de développement de logiciels, utilisant le logiciel de gestion de versions Git¹. Pour écrire le code qui automatisera la gestion de l'infrastructure MALO, nous avons fait le choix d'utiliser les formats JSON² et YAML³.

Une version GitHub Entreprise est disponible, mais elle ne sera pas pertinente compte tenu du besoin actuel.

Compte tenu de ces informations, et de l'infrastructure retenue, il n'est pas nécessaire de prendre un abonnement à GitHub Entreprise. Une utilisation de GitHub gratuite sera suffisante pour les besoins de la société MALO.

Puisqu'il n'y a pas d'outil de gestion et de déploiement du code pour gérer l'infrastructure actuelle, cette solution est la plus adaptée car elle est relativement simple d'utilisation, possède une documentation exhaustive et une large communauté. Beaucoup d'exemples de modèles ARM et de

¹ Explication du fonctionnement de GitHub : [GitHub — Wikipédia \(wikipedia.org\)](https://fr.wikipedia.org/wiki/GitHub)

² Explication du format JSON : [JSON](https://fr.wikipedia.org/wiki/JSON)

³ Explication du format YAML : [YAML Syntax — Ansible Documentation](https://fr.wikipedia.org/wiki/YAML)

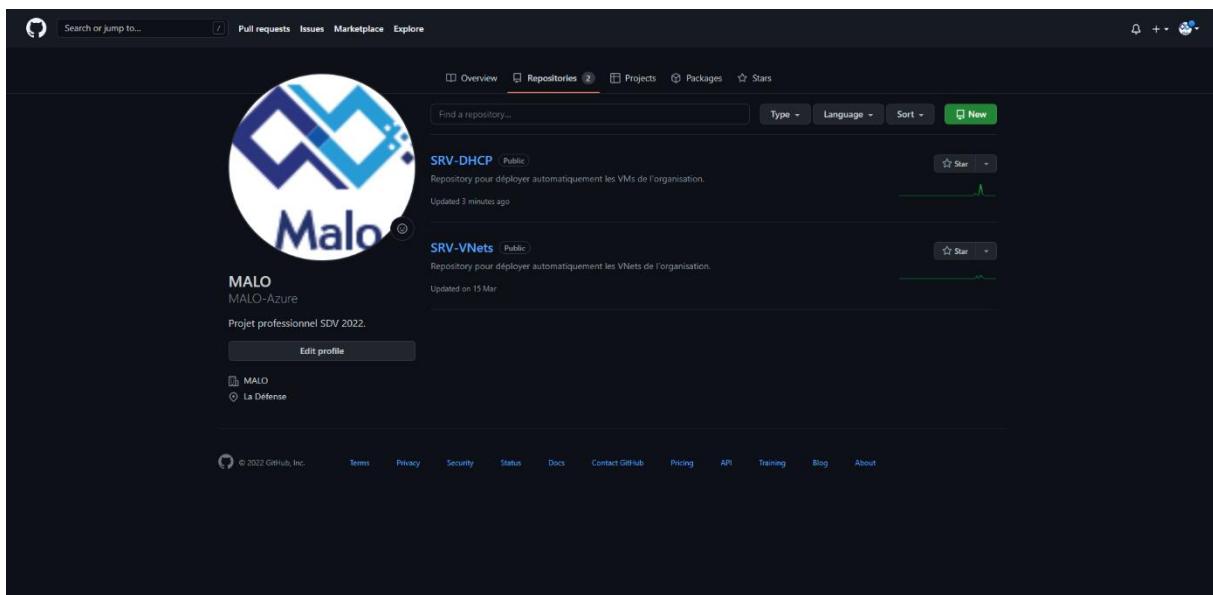


déploiement via *Github Actions* sont disponibles en ligne gratuitement⁴. La documentation GitHub est également disponible et fournit une liste exhaustive de ce qu'il est possible de faire avec les modèles de déploiement⁵.

Présentation détaillée de la solution *Github*

Le déploiement des serveurs virtuels se fera de la manière suivante :

1. L'hébergement du code se fera sur le compte GitHub de l'entreprise. Chaque fonction du code sera stockée dans un *repository* dédié. Pour le déploiement des machines virtuelles, un repository appelé *SRV-X* sera créé pour y héberger le code. Chaque serveur virtuel aura son répertoire afin d'y déployer le code plus facilement par fonction (voir la partie *Infrastructure* de ce document pour voir les différents serveurs virtuels). Plusieurs fichiers avec une nomenclature définie suivant la nature de l'image et sa fonction seront stockés dans ce *repository*. L'arborescence pourra prendre la forme suivante :



A l'intérieur de ces *repository*, plusieurs fichiers seront présents pour déployer la ressource voulue (2 fichiers sous format JSON & un sous format YAML). A noter qu'il y aura deux types de format utilisés pour déployer les ressources sur Azure : un format JSON (pour renseigner les informations nécessaires à la création de la ressource, comme la région ou la nature de l'image) ; et un format YAML (pour déployer le code via *Github Actions*⁶).

Le détail du déploiement d'une ressource sera expliqué dans le point 3 ci-après.

2. L'édition du code se fera par deux outils : *Github Desktop* et *VS Code*. *Github Desktop* sera installé sur la machine des développeurs ou administrateurs qui auront besoin de travailler sur le code, afin notamment de cloner en local un répertoire ou fichier présent sur le compte

⁴ Exemples de modèles de déploiement sur le compte GitHub suivant : [Azure-quickstart-templates/quickstarts at master · Azure/azure-quickstart-templates \(github.com\)](https://github.com/Azure/azure-quickstart-templates/tree/master)

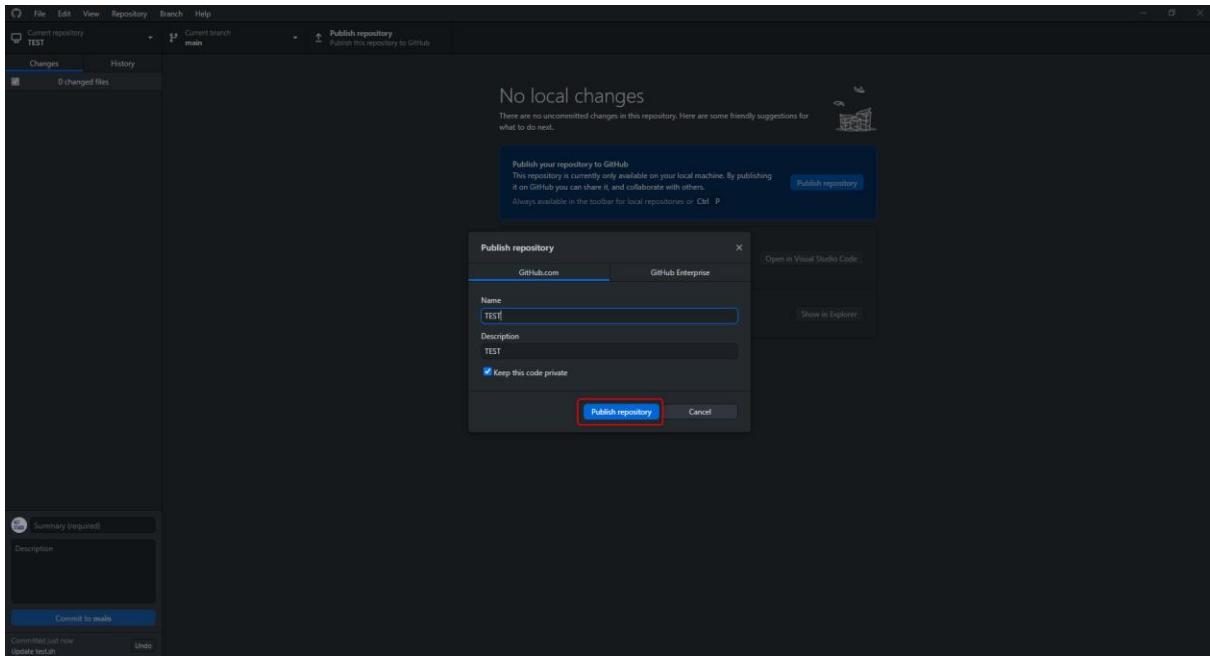
⁵ Documentation GitHub Actions : <https://docs.github.com/en/actions>

⁶ Explication de la fonctionnalité *Actions* dans GitHub : [Features • GitHub Actions](https://github.com/features/actions)



GitHub de l'entreprise en ligne, et/ou de créer un dossier/fichier en local et de le pousser plus tard sur le compte GitHub de l'entreprise en ligne.

3. Une fois le fichier édité en local via *VS Code*, nous pouvons le pousser sur le compte GitHub de l'entreprise dans le bon *repository* via *GitHub Desktop* de la manière suivante :



Ainsi, il est possible de travailler en local sur notre propre machine, d'éditer le code nécessaire via *VS Code*, et de le pousser ensuite sur le compte GitHub de l'entreprise via *GitHub Desktop*.

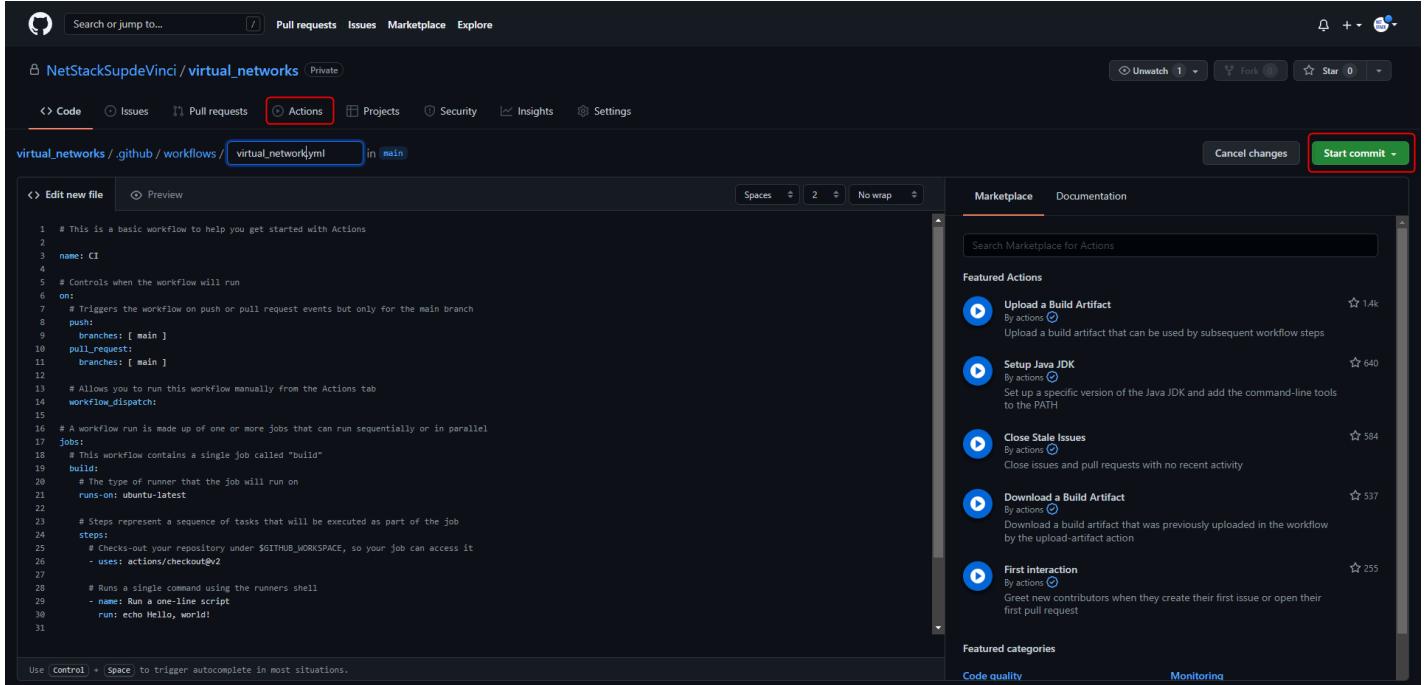
Il est également possible de modifier et créer directement le code via le compte GitHub en ligne. Mais l'environnement *VS Code* offre des outils de vérification du code pour chaque langage, ce qui améliore la mise en production du code, en réduisant le temps de relecture de ce dernier.

4. Nous allons maintenant détailler la mise en production sur Azure :

- On débutera la procédure par la création d'un *ARM Template* qui va contenir les informations nécessaires à la construction de l'objet ou de la ressource (dans cet exemple, le serveur virtuel SRV-DHCP). On stockera ce modèle à la racine du *repository* SRV-DHCP. A noter que l'on aura deux fichiers sous format JSON, comme nous le verrons plus tard dans le cadre d'un déploiement de machine virtuelle.
- On renseignera ensuite les *Secrets Azure* sur GitHub (Tenant ID, Application ID, Subscription ID...) générés avec des lignes de code sur Azure CLI⁷. Cela permettra de mieux renforcer la sécurité du code et de permettre à GitHub d'apporter des modifications à l'environnement Azure.

⁷ Détails de la procédure pour créer un *service principal* : [Créer un principal de service Azure – Azure CLI | Microsoft Docs](#)

- Une fois les *Secrets* renseignés dans GitHub, nous commencerons le déploiement de la ressource virtuelle via *Github Actions*. Quand le *Workflow* (première étape lorsque l'on se rend sur *Actions*) sera créé, GitHub nous proposera un modèle de démarrage au format YAML (format utilisé pour *Github Actions*). Ce modèle sera l'unique script nécessaire pour déployer le serveur DHCP. Le modèle prendra la forme suivante :



```

1 # This is a basic workflow to help you get started with Actions
2
3 name: CI
4
5 # Controls when the workflow will run
6 on:
7   # Triggers the workflow on push or pull request events but only for the main branch
8   push:
9     branches: [ main ]
10    pull_request:
11      branches: [ main ]
12
13 # Allows you to run this workflow manually from the Actions tab
14 workflow_dispatch:
15
16 # A workflow run is made up of one or more jobs that can run sequentially or in parallel
17 jobs:
18   # This workflow contains a single job called "build"
19   build:
20     # The type of runner that the job will run on
21     runs-on: ubuntu-latest
22
23   # Steps represent a sequence of tasks that will be executed as part of the job
24   steps:
25     # Checks-out your repository under $GITHUB_WORKSPACE, so your job can access it
26     - uses: actions/checkout@v2
27
28     # Runs a single command using the runners shell
29     - name: Run a one-line script
30       run: echo Hello, world!
31

```

C'est dans ce fichier au format YAML que nous mettrons le chemin de notre modèle au format JSON, contenant les informations nécessaires à la création de la ressource⁸.

- Comme on peut le remarquer dans la documentation, plusieurs types de déclencheurs sont disponibles afin de mieux préciser quand le *Workflow* devra se déployer sur Azure⁹.

Nous pouvons nous référer à la documentation de Azure pour voir plus en détail comment déployer une ressource avec le lien suivant : [Exercise - Deploy ARM templates as part of your CI/CD efforts with GitHub Actions - Learn | Microsoft Docs.](#)

Détails des tests à effectuer

Au sujet des tests à effectuer, nous procéderons à plusieurs d'entre eux à chaque étape clé du processus de déploiement :

- La création des *Secrets* Azure de la société MALO avec la commande PowerShell suivante :

⁸ Comment spécifier le chemin de notre code au format JSON dans notre fichier YAML : [Deploy Resource Manager templates by using GitHub Actions - Azure Resource Manager | Microsoft Docs](#)

⁹ Déclencheurs GitHub que l'on peut utiliser dans le cadre d'un déploiement :

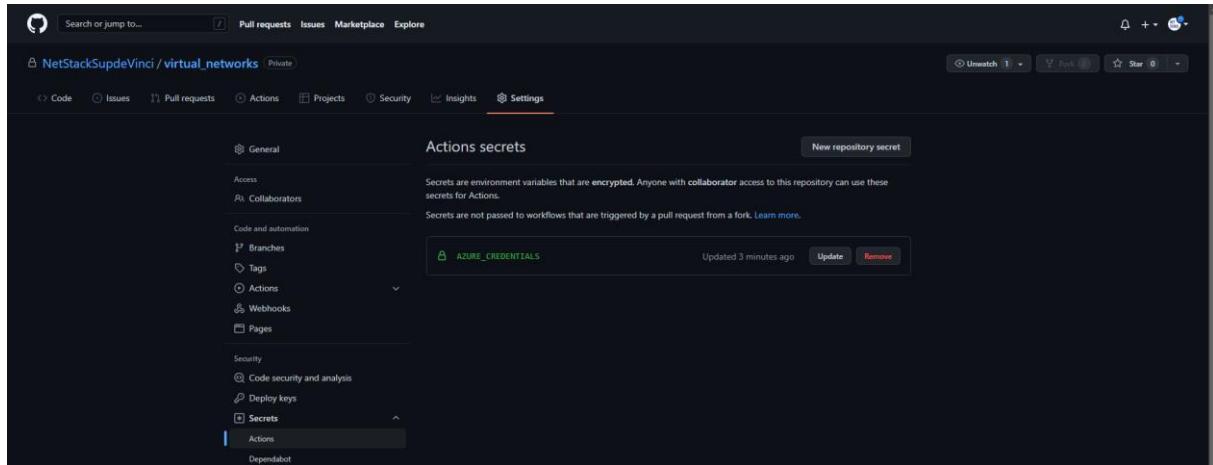
<https://docs.github.com/en/actions/using-workflows/events-that-trigger-workflows>

```

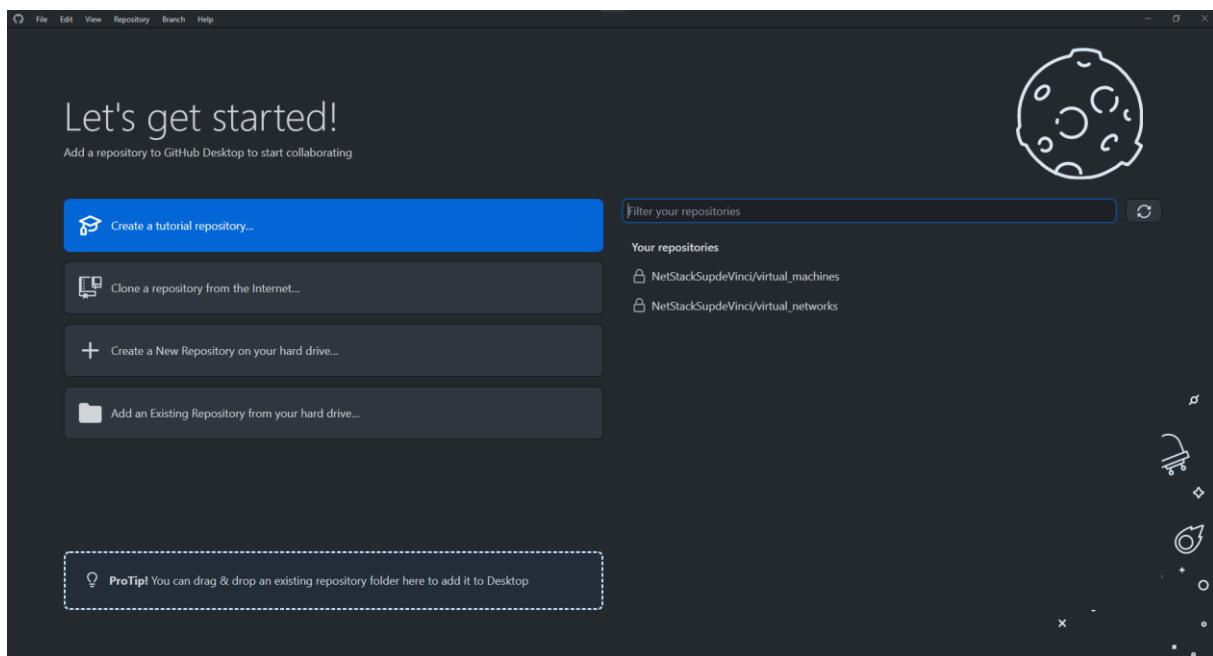
PowerShell | ? ? ... x
Home > Resource groups > ...
CRA SUP DE VINCI (supdevvcl)
PS /home/asix> az ad sp create-for-rbac --name "vmsa" --role contributor --scope "/subscriptions/50219ffe-7246-47fd-8826-0384581c0a9/resourceGroups/Netstack --ad-auth"
The underlying Active Directory Graph API will be replaced by Microsoft Graph API in a future version of Azure CLI. Please carefully review all breaking changes introduced during this migration: https://docs.microsoft.com/azure/microsoft-graph-migration
Option '--ad-auth' has been deprecated and will be removed in a future release.
Creating 'vmsa' contributor role under scope '/subscriptions/50219ffe-7246-47fd-8826-0384581c0a9/resourceGroups/Netstack'
The output includes credentials that you must protect. Be sure that you do not include these credentials in your code or check the credentials into your source control. For more information, see https://aka.ms/adsp-clt
{
  "client_id": "06edf0f-70ba-4ac-0391-c0349e08cf0",
  "client_secret": "8.We6TxeD0d0uhXK9YdRc-t.K7-RQ_2D2",
  "subscription_id": "50219ffe-7246-47fd-8826-0384581c0a9",
  "tenant_id": "b76023b0-7c2-4c02-92a6-8cdad1d189",
  "active_directory_graph_resource_id": "https://graph.windows.net",
  "active_directory_graph_endpoint_url": "https://management.azure.com/",
  "active_directory_graph_source_id": "https://graph.windows.net",
  "gallery_endpoint_url": "https://gallery.azure.com",
  "management_endpoint_url": "https://management.core.windows.net/"
}
PS /home/asix>

```

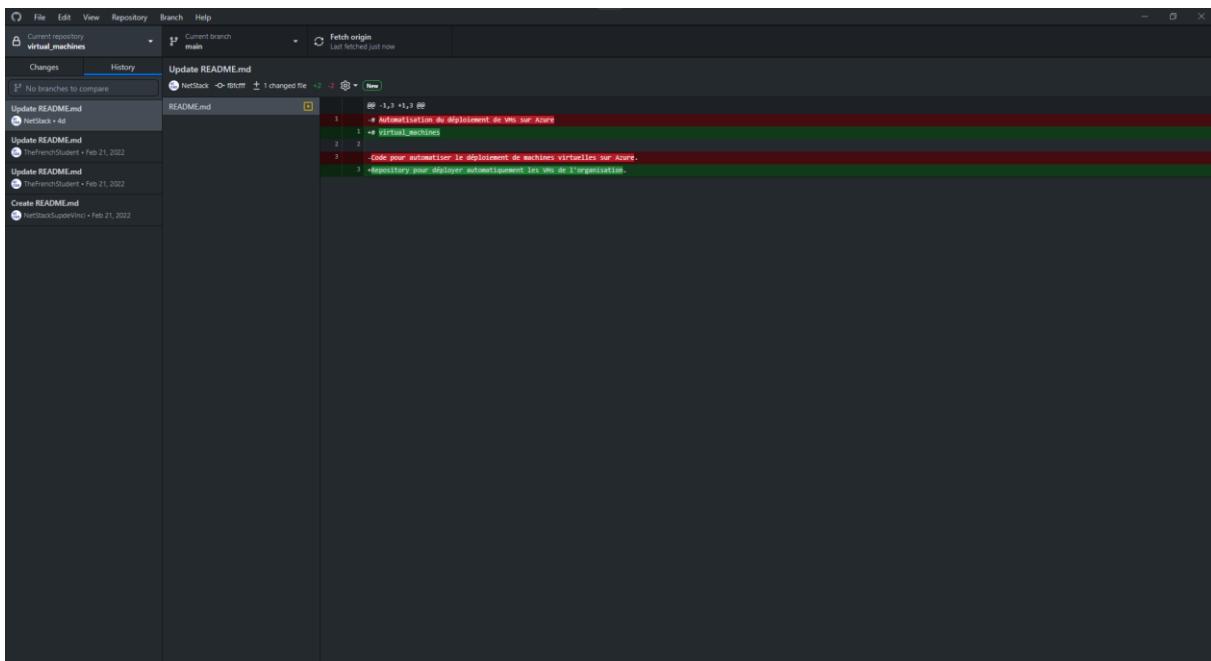
- La saisie de ces informations dans l'onglet *Secrets* du compte GitHub de la société MALO :



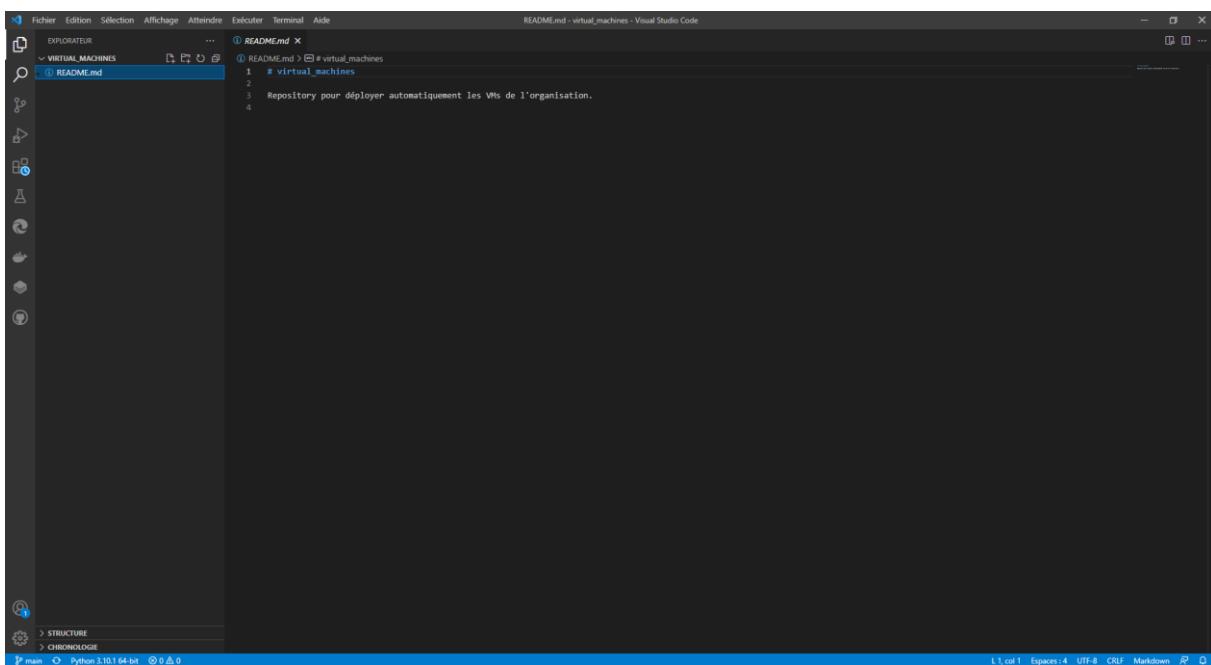
- Une première étape de connexion à *GitHub Desktop* via l'identifiant GitHub de l'entreprise.
- La page d'accueil de *GitHub Desktop* sera la suivante :



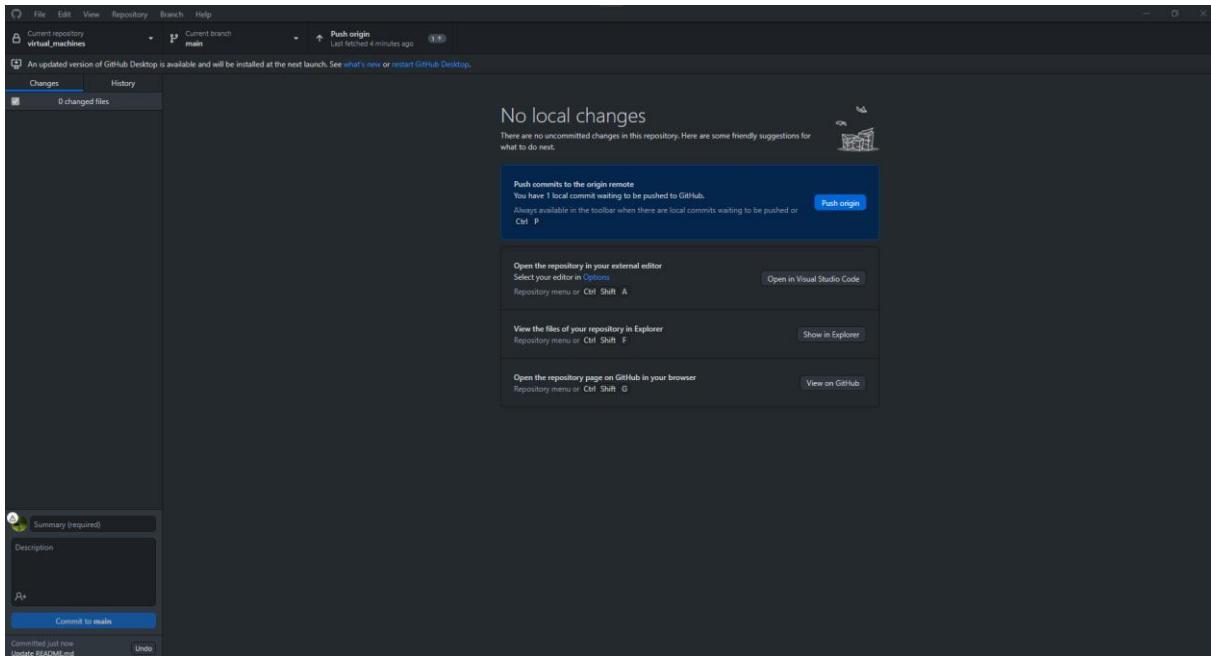
- La seconde étape consistera à cloner sur la machine locale un répertoire du compte GitHub de l'entreprise afin de mieux l'édition sur l'éditeur de code *VS Code* :



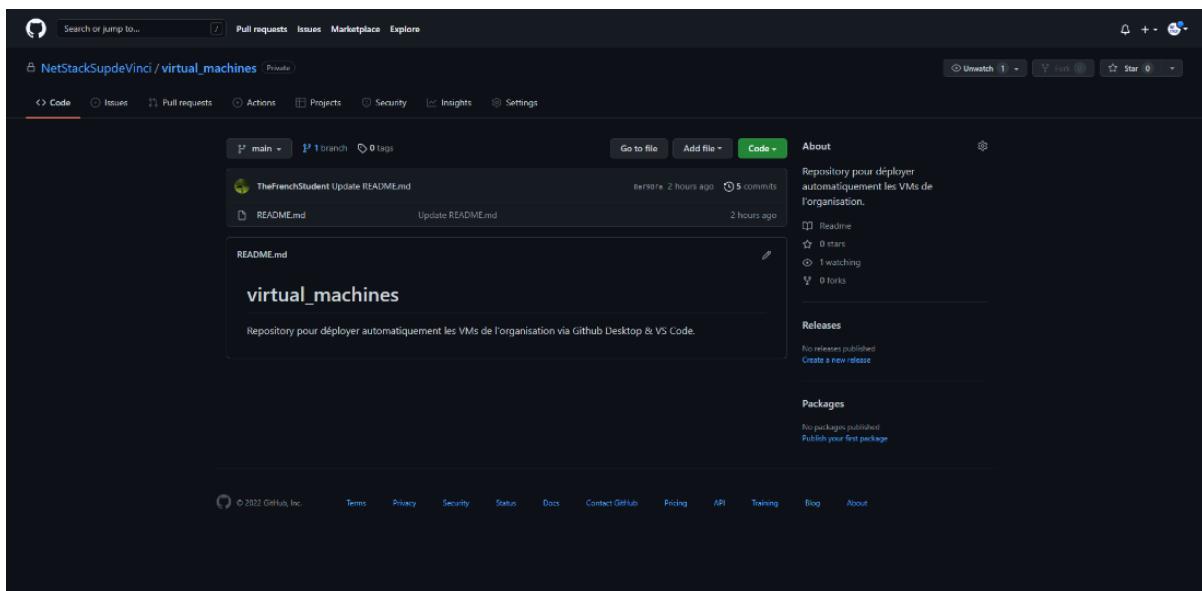
Une fois cloné et ouvert dans *GitHub Desktop*, il est possible d'ouvrir le dossier dans *VS Code* pour profiter des plugins de l'éditeur de code suivant le langage utilisé :



- Une fois le code modifié, il faudra ensuite pousser les changements faits sur le fichier local vers le compte GitHub en ligne :



- Nous vérifierons ensuite que les changements ont bien été poussés sur le compte GitHub de l'entreprise :



Les changements ont bien été effectués. La solution est bien fonctionnelle.

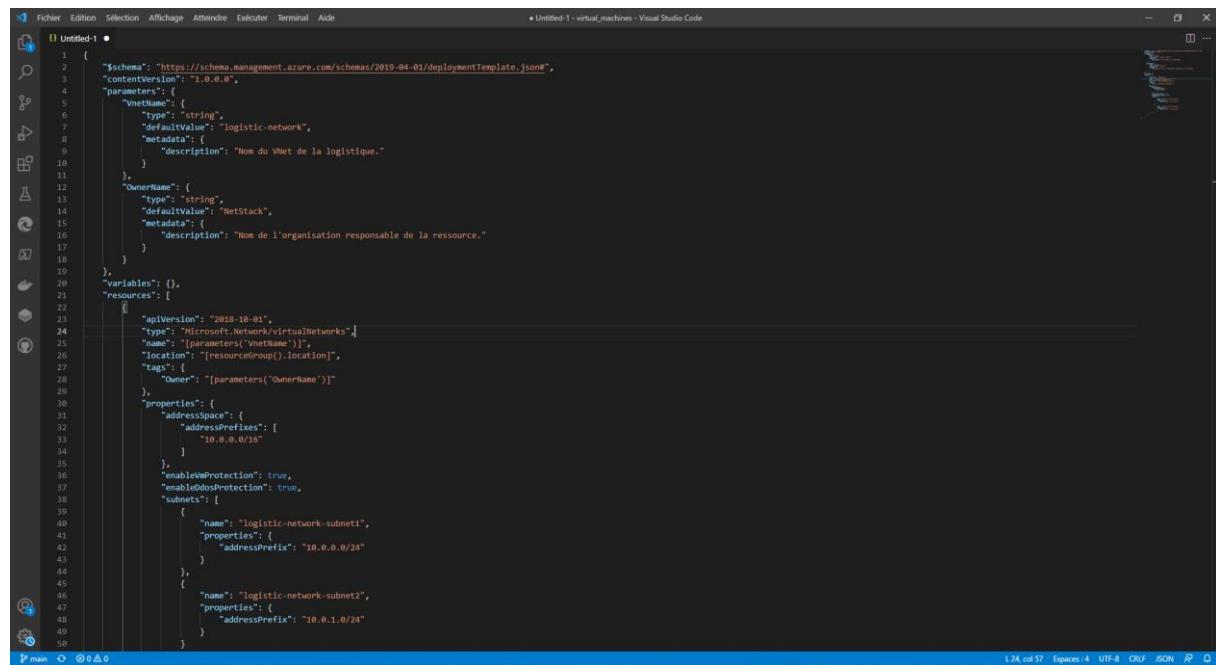
Il reste cependant une étape cruciale pour vérifier le bon fonctionnement de la solution : implémenter un exemple concret de déploiement. Nous configurerons le script suivant sous format YAML qui permettra de déployer un réseau virtuel et 2 sous-réseaux sur le compte Azure de l'organisation :

```

1 name: Deploy ARM Template
2
3 # TEST
4
5 on:
6   push:
7     branches:
8       - main
9   env:
10    AZURE_SUBSCRIPTION_ID: 50219ffe-7246-47fd-8826-0384581c80a9 # set this to your Azure Subscription Id
11    AZURE_RESOURCE_GROUP: NetStack # set this to your target resource group
12
13 jobs:
14   deploy-virtual-network-template:
15     runs-on: ubuntu-latest
16     steps:
17       - name: Checkout source code
18         uses: actions/checkout@main
19
20       - name: Login to Azure
21         uses: azure/login@v1
22         with:
23           creds: ${{ secrets.AZURE_CREDENTIALS }}
24
25       - name: Deploy ARM Template
26         uses: azure/arm-deploy@v1
27         with:
28           scope: resourcegroup
29           subscriptionId: ${{ env.AZURE_SUBSCRIPTION_ID }}
30           resourceGroupName: ${{ env.AZURE_RESOURCE_GROUP }}
31           template: ./VNet.json

```

Nous écrirons un autre script sous format JSON qui contiendra toutes les informations nécessaires à la création du réseau virtuel et de ses sous-réseaux :



```

1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "vnetName": {
6       "type": "string",
7       "defaultValue": "logistic-network",
8       "metadata": {
9         "description": "Nom du VNet de la logistique."
10      }
11    },
12    "OwnerName": {
13      "type": "string",
14      "defaultValue": "NetStack",
15      "metadata": {
16        "description": "Nom de l'organisation responsable de la ressource."
17      }
18    }
19  },
20  "variables": {},
21  "resources": [
22    {
23      "apiVersion": "2018-10-01",
24      "type": "Microsoft.Network/virtualNetworks",
25      "name": "[parameters('vnetName')]",
26      "location": "[resourceGroup().location]",
27      "tags": {
28        "Owner": "[parameters('OwnerName')]"
29      },
30      "properties": {
31        "addressSpace": {
32          "addressPrefixes": [
33            "10.0.0.0/16"
34          ]
35        },
36        "enableIpProtection": true,
37        "enableDdosProtection": true,
38        "subnets": [
39          {
40            "name": "logistic-network-subnet1",
41            "properties": {
42              "addressPrefix": "10.0.0.0/24"
43            }
44          },
45          {
46            "name": "logistic-network-subnet2",
47            "properties": {
48              "addressPrefix": "10.0.1.0/24"
49            }
50          }
51        }
52      }
53    }
54  ]
55 }

```

Une fois les *Secrets* du compte générés par Azure et renseignés sur GitHub, nous pourrons lancer notre *Workflow* et suivre sa progression :

The screenshot shows the GitHub Actions interface for a repository named 'NetStackSupdeVinci/virtual_networks'. The 'All workflows' tab is selected, displaying three workflow runs. The first run, 'Update VNet.json', was triggered by a commit and succeeded 8 minutes ago. The second run, 'Update network-deployment.yml', was triggered by a commit and succeeded 12 minutes ago. The third run, 'Create network-deployment.yml', was triggered by a commit and succeeded 27 minutes ago. Each run includes a link to the commit and the specific ARM template deployed.

La dernière étape de notre vérification consistera à se rendre sur Azure et vérifier que la ressource a bien été créée :

The screenshot shows the Microsoft Azure portal with the search bar set to 'Search resources, services, and docs (G+/-)'. The main view is the 'Virtual networks' blade for a resource group named 'NetStack'. It displays one record: a virtual network named 'logistic-network' located in 'West Europe'. The 'Essentials' section shows the subscription information ('Azure for Students'), deployment status ('1 Succeeded'), and location ('West Europe'). The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Deployments, Security, Policies, Properties, Looks, Cost Management, Monitoring, and Insights (preview).

Un message d'erreur nous indiquera d'enregistrer un fournisseur de ressource pour permettre à GitHub d'apporter des modifications à la ressource Azure que vous souhaitez déployer. Ce message sera différent suivant le type de ressource déployé via GitHub. Dans notre cas, il faut se rendre dans l'onglet *Resource Providers* de l'abonnement et enregistrer le fournisseur manquant de la manière suivante :

Enfin, une fois les 6 serveurs virtuels de la société MALO créés, nous sauvegarderons les scripts sous le format JSON dans le OneDrive de l'équipe IT. Cela permettra de créer les serveurs virtuels plus rapidement si jamais un besoin urgent apparaît.

Pour enregistrer le code sous le format JSON de la ressource, nous allons nous rendre dans la ressource virtuelle SRV-DHCP puis dans l'onglet *Automation* et cliquer sur *Export template* puis *Download* :

```

1  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
2  "contentVersion": "1.0.0.0",
3  "parameters": {
4      "extensions_Microsoft_Insights_VMDiagnosticsSettings_xmlCfg": {
5          "type": "SecureString"
6      },
7      "extensions_Microsoft_Insights_VMDiagnosticsSettings_storageAccountName": {
8          "type": "SecureString"
9      },
10     "extensions_Microsoft_Insights_VMDiagnosticsSettings_storageAccountKey": {
11         "type": "SecureString"
12     },
13     "extensions_Microsoft_Insights_VMDiagnosticsSettings_storageEndPoint": {
14         "type": "SecureString"
15     },
16     "virtualMachines_SRV_DHCP_name": {
17         "defaultValue": "SRV-DHCP",
18         "type": "String"
19     },
20     "disks_SRV_DHCP_OsDisk_1_61d26f00fc64a45b318a1ff9f59e0bd_externalId": {
21         "defaultValue": "subscriptions/50219ffe-7246-47fd-8826-0384581c00a9/resourceGroups/NETSTACK/providers/Microsoft.Compute/disks/
22 SRV-DHCP_OsDisk_1_61d26f00fc64a45b318a1ff9f59e0bd",
23         "type": "String"
24     },
25     "networkInterfaces_srv_dhcp100_externalId": {
26         "defaultValue": "subscriptions/50219ffe-7246-47fd-8826-0384581c00a9/resourceGroups/NetStack/providers/Microsoft.Network/networkInterfaces/srv-dhcp100",
27         "type": "String"
28     }
}

```

Gestion du parc

Introduction

Pour la gestion du parc informatique de la société MALO, nous avons choisi de partir avec l'outil payant Servicenow. Nous aurons besoin de deux licences, une pour l'outil de gestion des tickets et une autre pour la gestion du matériel et des logiciels de la société. Cet outil présente plusieurs avantages comparés aux autres outils présents sur le marché :

- Il est personnalisable à souhait. On peut créer des filtres de notre choix et personnaliser notre tableau bord.
- La base de connaissances est très large et facile à appréhender.
- Le support technique Servicenow est très réactif et efficace.
- Il s'intègre très facilement aux fournisseurs de cloud public, ce qui est un avantage considérant le fait que nous partons sur une infrastructure cloud Azure.
- Il a plusieurs options et licences qui conviennent à tout type d'entreprise.
- Le prix se fera en fonction du nombre d'employés dans l'entreprise et la nature de l'industrie. Cela permet d'obtenir un devis personnalisé et adapté au besoin de l'entreprise.

Concernant le prix de cet outil, il dépend beaucoup de la nature de l'entreprise, le nombre d'employés, sa localisation... Il existe plusieurs types de licences pour la gestion des tickets, à savoir ITSM, ITSM Professional & ITSM Entreprise¹⁰. Nous allons partir sur une solution ITSM classique, car nous avons besoin des fonctionnalités suivantes : gestion des incidents, des requêtes, des problèmes, reporting, base de connaissance interne, gestion du matériel et gestion des contrats et fournisseurs.

Pour la gestion du matériel, nous n'avons qu'une seule licence à choisir, l'ITAM¹¹, qui complètera notre outil ITSM pour former un outil global de gestion de parc avec la fonctionnalité suivante : processus de découverte Servicenow du matériel et des logiciels (*MID Server*, que l'on verra un peu plus loin dans cette partie).

Nous allons maintenant voir dans les deux prochaines sections comment intégrer Servicenow avec l'environnement Azure de la société MALO via le SSO, et comment intégrer le processus de découverte du matériel et des logiciels à la nouvelle infrastructure.

Intégration de l'outil *ITSM Servicenow* avec Azure

Pour que les utilisateurs puissent se connecter avec leur compte Microsoft sur le nouvel outil de ticket Servicenow, nous devrons configurer un SSO avec Azure AD. Etablir un SSO va permettre d'accroître la sécurité de l'infrastructure, et simplifier le processus de connexion dans le même temps. Cela réduit également les situations d'oubli de mot de passe et les pratiques peu sécurisées

¹⁰ Détails des licences pour la gestion de tickets de Servicenow : [IT Service Management \(ITSM\) - ServiceNow](#)

¹¹ Détail de l'outil ITAM pour gérer le matériel : [ITAM – IT Asset Management – ServiceNow](#)

de gestion des mots de passe, puisque les utilisateurs n'auront qu'un seul mot de passe pour plusieurs services, à savoir leur mot de passe de Microsoft¹².

Le processus d'établissement du SSO entre Azure et Servicenow se passera de la manière suivante¹³ :

1. Nous nous rendrons sur le service *Azure Active Directory*, puis dans l'onglet *Enterprise Applications* (ou *SaaS*) et nous ajouterons le service *Servicenow*, disponible dans la galerie des applications de Microsoft Azure. Cette opération durera quelques minutes au maximum, car le service s'ajoute au *tenant ID* de la société MALO.

The screenshot shows two main windows from the Microsoft Azure portal.

Left Window: Browse Azure AD Gallery

- Header: Microsoft Azure, Home > CFA SUP DE VINCI > Enterprise applications >
- Search bar: Search resources, services, and docs (G+ /)
- Section: ServiceNow
- Details: Name: ServiceNow, Publisher: ServiceNow, Provisioning: Automatic provisioning supported, Single Sign-On Mode: SAML-based Sign-on, URL: http://www.servicenow.com/
- Bottom: Read our step-by-step ServiceNow integration tutorial

Right Window: Configure sign-on

Section: Automatically Configure ServiceNow

Description: Azure AD can automatically configure ServiceNow for single sign-on. Simply provide the information below and click "Configure Now". Or, check "Manually configure single sign-on" to learn how to perform the configuration manually.

Fields (filled in):

- * ServiceNow Instance Name: contoso
- * Admin Username: (empty)
- * Admin Password: (empty)
- Make this the default identity provider for ServiceNow

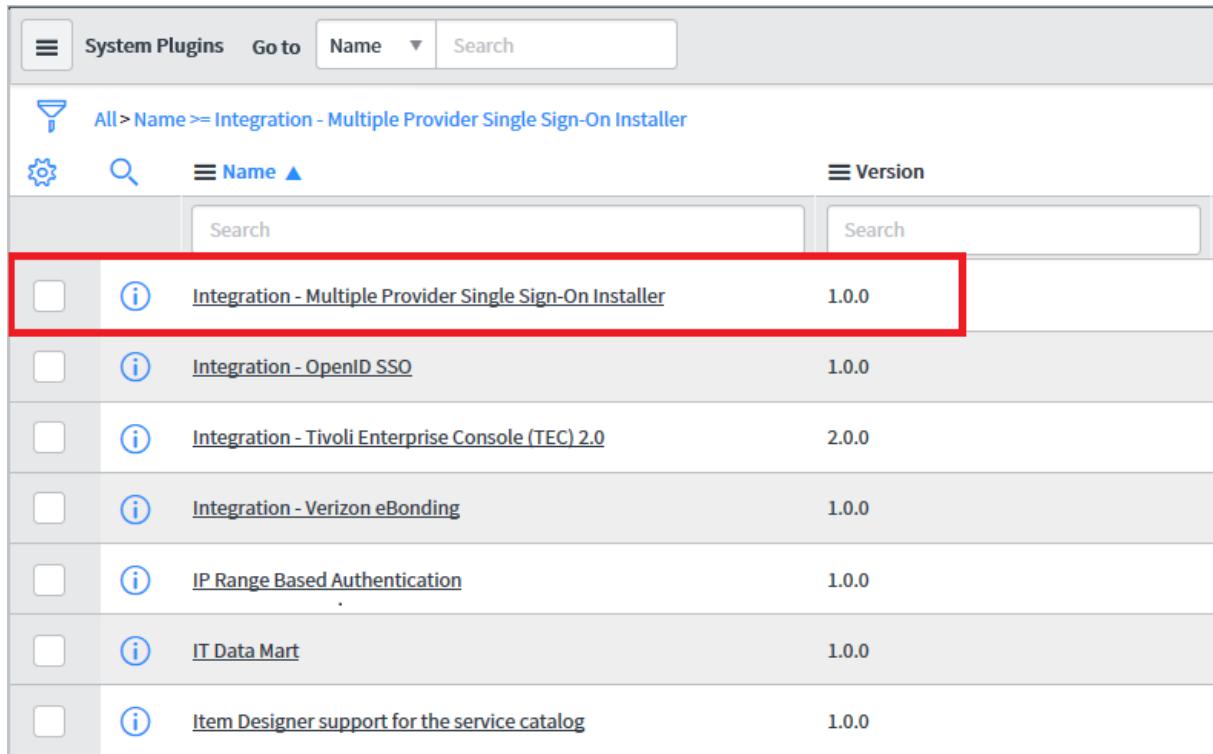
Buttons:

- Configure Now** (button highlighted with a red border)
- Manually configure single sign-on

¹² Explication du SSO et de ses avantages : [Top Benefits of SSO and Why It's Important for Your Business \(pingidentity.com\)](https://pingidentity.com/top-benefits-of-single-sign-on/)

¹³ Comment établir un SSO entre Azure et Servicenow : [Tutorial: Azure Active Directory single sign-on \(SSO\) integration with ServiceNow | Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-sso-service-now-tutorial)

2. Une fois l'application ajoutée, nous irons dans l'onglet SSO de cette dernière et choisisrons l'option *SSO SAML*. En parallèle, nous ajouterons le plugin *SSO Integration* du côté du compte administrateur Servicenow pour que l'Azure AD fasse le lien.



System Plugins		
	Name	Search
	All > Name >= Integration - Multiple Provider Single Sign-On Installer	
	Search	Search
<input type="checkbox"/>	Integration - Multiple Provider Single Sign-On Installer	1.0.0
<input type="checkbox"/>	Integration - OpenID SSO	1.0.0
<input type="checkbox"/>	Integration - Tivoli Enterprise Console (TEC) 2.0	2.0.0
<input type="checkbox"/>	Integration - Verizon eBonding	1.0.0
<input type="checkbox"/>	IP Range Based Authentication	1.0.0
<input type="checkbox"/>	IT Data Mart	1.0.0
<input type="checkbox"/>	Item Designer support for the service catalog	1.0.0

3. L'étape suivante consistera à renseigner l'URL de ce qu'on appelle l'instance Servicenow. La forme que prend cette URL est la suivante : <https://malo.servicenow>. Nous renseignerons également le nom du compte administrateur et son mot de passe durant cette étape.

Identity Provider

Name: Microsoft Azure Federated Single Sign-on

Default:

Identity Provider URL:

Identity Provider's AuthnRequest:

Identity Provider's SingleLogoutRequest:

ServiceNow Homepage:

Entity ID / Issuer: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Audience URI:

NameID Policy:

External logout redirect: external_logout_complete.do

Failed Requirement Redirect:

Encryption And Signing **User Provisioning** **Advanced**

User Field:

NameID Attribute:

Create AuthnContextClass:

AuthnContextClassRef Method:

Force AuthnRequest:

Is Passive AuthnRequest?

Single Sign-On Script: MultiSSOv2_SAML2_custom

Clock Skew: 60

Protocol Binding for the IDP's AuthnRequest:

Protocol Binding for the IDP's SingleLogoutRequest:

IDP Metadata URL:

- Une fois l'étape précédente complétée, le SSO se lancera automatiquement. Une fois le processus fini, nous irons dans les propriétés du SSO de Servicenow et vérifier si tous les paramètres sont bien établis. Nous importerons ensuite le certificat de l'Azure AD de la société MALO dans Servicenow pour ajouter une couche de sécurité supplémentaire.

SSO Login Test Results

- ✓ SAML Login response received
- ✓ SAML Assertion retrieved
- ✓ Signature Validated
- ✓ Certificate Validated
- ✓ AudienceRestriction/Condition Validated
- ✓ Certificate Issuer Validated
- ✓ Subject Confirmation Validated

SSO Logout Test Results

- ✗ Cannot logout of IDP's session
IDP's logout URL not set. So, cannot logout the IDP session.

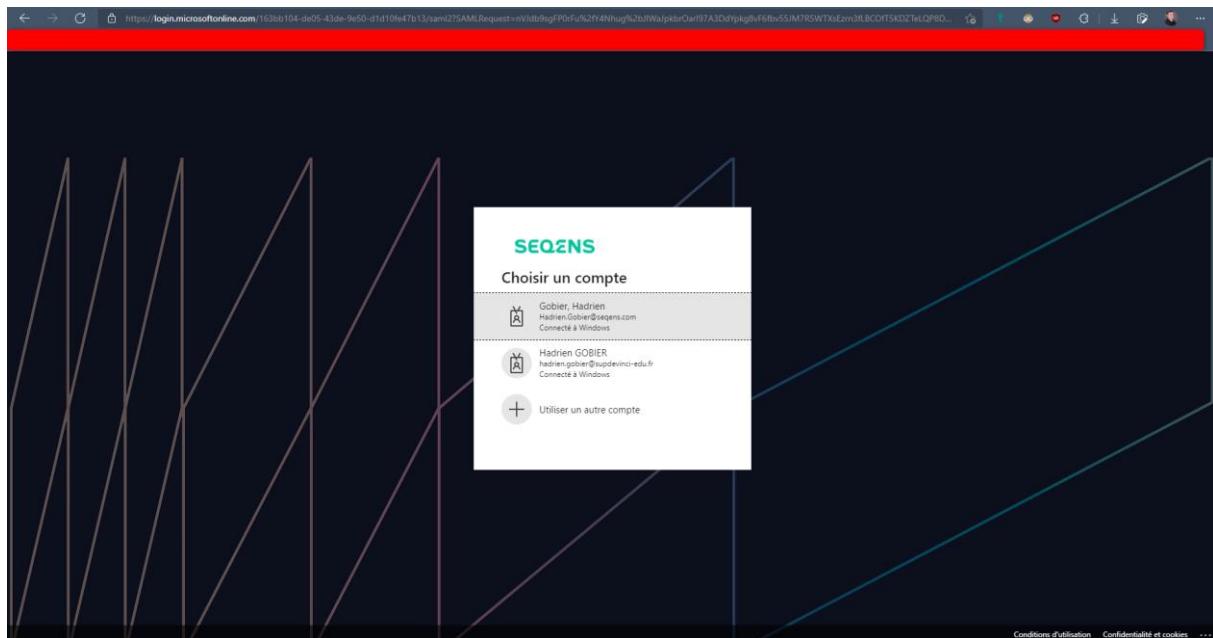
SSO Test Connection Summary

- ✓ SSO Login tests succeeded. SSO Logout tests failed. IDP Configuration can be activated by clicking 'Activate' button. Users will be able to login and logout of the instance, but will not be logged out of the IDP. Please refer to the logs for test details.

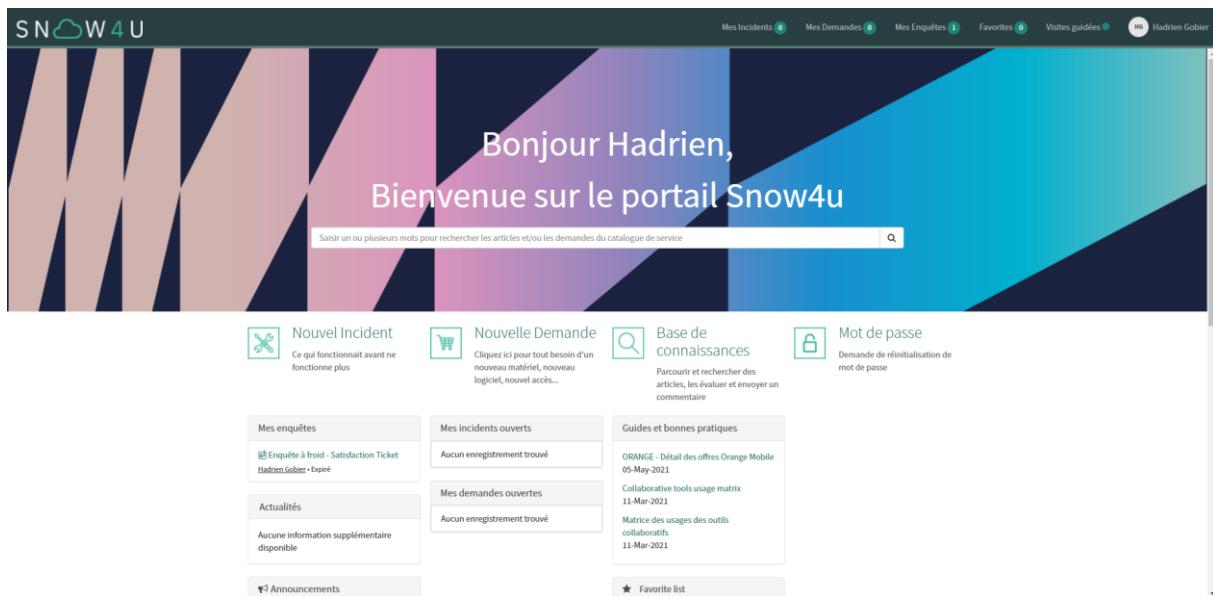
Click the "Activate" button to save and activate this configuration. Click the "Close" button to close this window and continue editing the SSO configuration.

5. Enfin, nous ajouterons les utilisateurs de l’organisation dans l’application Servicenow afin que le SSO s’applique à tous les utilisateurs actuels et futurs de l’entreprise MALO. Nous configurerons également l’auto-redirection sur le compte administrateur Servicenow, dans la section SSO afin que tous les utilisateurs précédemment renseignés soient automatiquement redirigés vers la page de connexion Microsoft.

Le résultat final nous donnera la page de connexion suivante (personnalisée avec le logo de l’entreprise) :



Etant donné que le SSO a été configuré avec l’adresse électronique de l’organisation, il n’est possible de se connecter à Servicenow qu’avec cette dernière. L’utilisateur arrivera ainsi sur la page suivante :



Nous pourrons ainsi voir le tableau de bord de l'utilisateur, qui aura la possibilité de créer une demande d'incident, une nouvelle requête (matériel ou licence de logiciel, par exemple), une demande de réinitialisation de mot de passe ou accéder à une base de connaissance (personnalisée et dont le contenu pourra être modifié par l'équipe informatique).

Une page pour les administrateurs sera configurée, différente de la page des utilisateurs. Cette page prendra la forme suivante (personnalisation possible suivant les besoins de l'entreprise) :

Cette page permettra de mieux suivre l'évolution des tickets de la société MALO et leur traitement. Des filtres permettront de personnaliser la page de traitement des tickets, ce qui est très utile si l'entreprise MALO s'étend à l'étranger (en dehors de sa filiale à Bruxelles) :

Enfin, la page Dev, qui est l'interface principale pour configurer les différents modules internes de Servicenow, prendra la forme suivante :

C'est à partir de cette interface que les administrateurs responsables du déploiement de Servicenow chez MALO pourront apporter des modifications aux interfaces des utilisateurs et y pousser des changements.

Intégration de l'outil ITAM Servicenow avec Azure

Concernant le matériel, l'outil sera le même. Pour rappel, il nous faudra obtenir deux licences : IT Service Management Standard & IT Asset Management.

L'entreprise ayant déjà des équipements existants, il nous faudra renseigner tous ces équipements dans Servicenow via un processus de découverte *agentless* fourni par Servicenow. Ce processus de découverte du matériel permet à Servicenow via un *MID Server* d'interagir avec le matériel de

manière fréquente et de renseigner les informations trouvées dans l’outil de gestion du matériel Servicenow.

Le *MID Server*¹⁴ est une application Java qui peut tourner sur un serveur Windows ou Linux/UNIX permettant la découverte du matériel. Ce serveur initie toutes les communications de découverte du matériel et les sécurise. Le *MID Server* sera installé sur les machines virtuelles SRV-VB365 & SRV-PRINT, qui respectent les prérequis d’installation¹⁵. Deux machines virtuelles seront requises pour assurer une tolérance de panne.

Même si le serveur sera à l’intérieur du réseau local de la société MALO, nous lui donnerons les droits suivants :

- Accès aux deux appliances Fortinet physiques (autorisation de connexion pour scanner le réseau).
- Autorisation du port 443 sur le réseau des machines virtuelles où le *MID Server* est hébergé pour accéder à l’instance MALO Servicenow.

Le processus de découverte se déroulera de la manière suivante¹⁶¹⁷ :

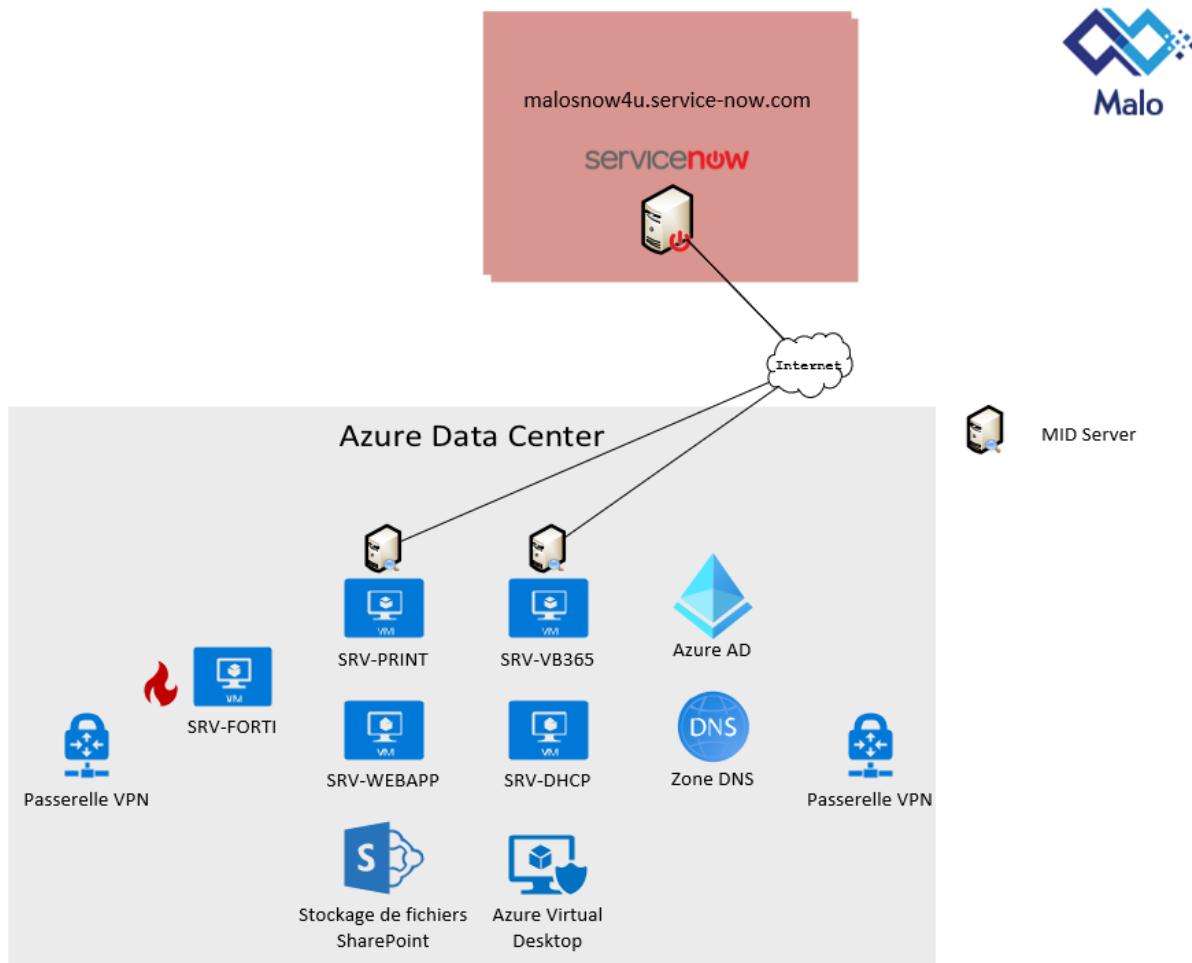
1. Servicenow Discovery scannera d’abord le réseau de la société MALO en envoyant des *queries* sur les ports fréquemment utilisés via le *MID Server*. Une fois la réponse obtenue d’un port en particulier sur une plage d’adresses IP définie, l’agent Servicenow saura d’emblée quel type de matériel se trouve derrière ce port (par exemple, réponse du port 135 qui est un serveur Windows).
2. A l’étape suivante, Servicenow Discovery trouvera des ordinateurs ou serveurs derrière un port scanné et enverra des *queries* supplémentaires d’un type bien particulier pour obtenir plus d’information sur l’OS du matériel, son modèle, sa marque, le numéro de série...
3. Si l’agent voit que le matériel est déjà renseigné dans Servicenow avec des informations anciennes, il remplacera ces informations par les nouvelles qu’il a obtenues via ce scan périodique, ou en ajoutera pour mieux compléter la fiche du matériel sur Servicenow.

¹⁴ Explication du *MID Server* et son rôle dans la découverte du matériel de l’entreprise : [MID Server | ServiceNow Docs](#)

¹⁵ Prérequis d’installation de l’outil : [MID Server system requirements | ServiceNow Docs](#)

¹⁶ Détails du processus de Discovery de Servicenow : [Discovery basics | ServiceNow Docs](#)

¹⁷ Détails du processus de découverte du matériel et logiciel de l’entreprise via Servicenow Discovery : [ITOM_NowForum Melbourne_Final_211016 \(servicenow.fr\)](#)



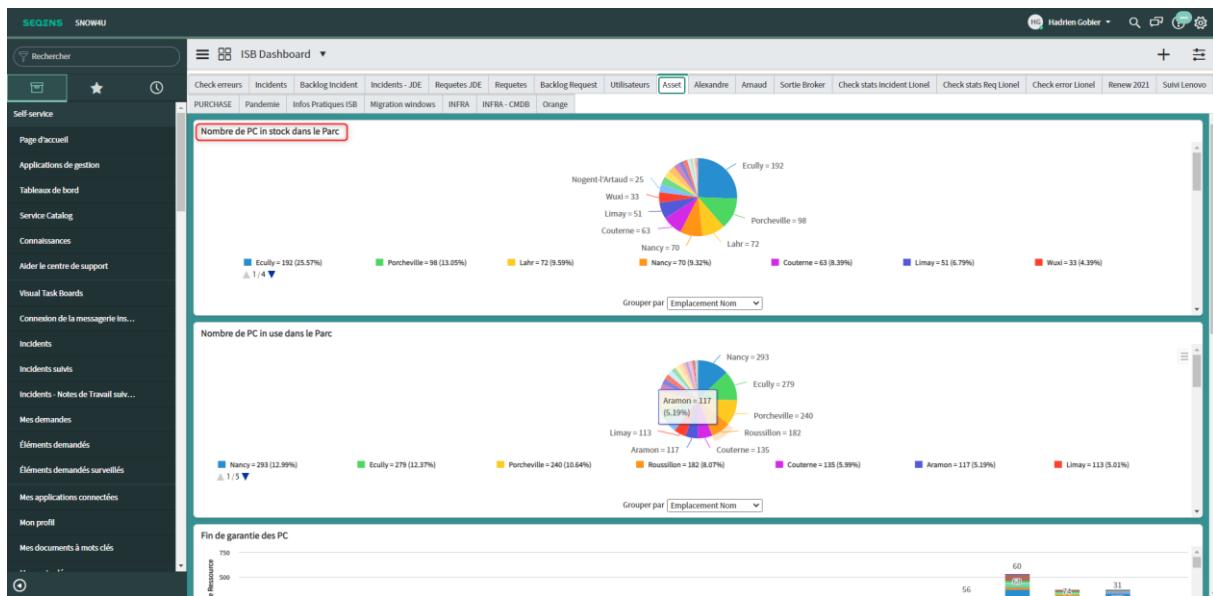
4. Comme mentionné précédemment, le *MID Server* possède plusieurs types de *queries* qui permettent de découvrir la nature du matériel scanné :

Type	Description
Network discovery	Run this type of discovery to find the internal IP networks within your organization. If you already know the IP address ranges in your network, it is not necessary to run network discovery.
CI discovery	Run this type of discovery to find the devices, computers, and applications on your network. This is essentially the standard type of discovery that you run most often.
Cloud discovery	Run this type of discovery to find AWS and Azure resources in your organization's cloud.
Serverless discovery	Run this type of discovery to find applications on host machines without the need to discover the host first. Serverless discovery relies on patterns to explore CIs on a host.

Nous configurerons également ce processus de découverte pour qu'il puisse scanner les logiciels utilisés par la société MALO afin de les renseigner sur ServiceNow¹⁸.

Ainsi, les matériels et logiciels scannés seront recensés dans la page du Tableau de Bord de la société MALO :

¹⁸ Possibilité de découvrir des applications installées sur des machines via le *MID Server* : [Software discovery | ServiceNow Docs](#)



Ce Tableau de Bord sera très utile pour visualiser les équipements disponibles par site (pour le site de Bruxelles par exemple). Nous créerons et personnaliserons des onglets pour mettre en avant les données de choix concernant le matériel des deux sites de la société MALO, comme les ordinateurs fixes et portables utilisés. On peut enfin obtenir une liste plus exhaustive du matériel suivant différents filtres. Cette liste prendra la forme suivante pour les équipements du site français de la société MALO :

Pour ce qui est du cas particulier des clients légers, nous changerons la règle d'identification du process de découverte pour que Servicenow classe les sessions Azure Virtual Desktop comme des ordinateurs virtuels. Si nous ne modifions pas cette règle, le processus Servicenow va catégoriser ces clients légers comme des serveurs ou machines virtuelles.

Tarification de la solution

L'outil Servicenow est basé sur plusieurs modules, qui détermineront le prix avec d'autres variables comme le nombre d'employés, le secteur d'entreprise et le type d'engagement (1 ans, 3 ans ou plus). Comme nous avons pu le voir précédemment, dans le cadre de la nouvelle infrastructure MALO, nous allons prendre les modules suivants :

- Gestion des tickets
- Gestion du matériel
- Gestion des incidents et des problèmes
- Requête (demande de changement)
- Gestion des logiciels
- Gestion de l'infrastructure
- *Servicenow Discovery*
- Base de connaissance
- Gestion des contrats et fournisseurs

Tous ces modules seront personnalisables via l'interface Dev. Au total, pour la société MALO, ces modules coûteront 60 000 € sur 3 ans (contrats négociés sur 3 ans), en sachant que ce prix a été établi pour la société MALO uniquement en tenant compte de ses besoins, de son effectif (et future évolution) ainsi que de son secteur d'activité.

Gestion des logs

Introduction

Puisque l'infrastructure de l'entreprise MALO va être migrée sur le cloud Azure, nous avons choisi une gestion des logs système qui se fera via le service *Azure Monitor*¹⁹. Ce service va nous permettre de superviser les logs générés par la nouvelle infrastructure de la société MALO. Cette solution sera couplée à *Microsoft Azure Sentinel*, qui est un autre service de type SIEM s'occupant de gérer la partie des événements sécurité dans l'environnement cloud. Enfin, la solution *FortiAnalyzer* s'occupera quant à elle de gérer les logs de nos équipements réseaux On-Premise.

Azure Monitor est le nom marketing du service qui exploite les *logs* et *metrics* de l'infrastructure Azure. Derrière ce service repose les fonctionnalités *Azure Monitor Logs* (anciennement *Azure Monitor Log Analytics*) et *Azure Monitor Metrics Explorer* (anciennement *Azure Monitor Metrics Analytics*). Nous avons établi un schéma récapitulatif en fin de partie pour permettre de mieux comprendre comment l'architecture globale de la gestion des logs va fonctionner.

¹⁹ Présentation de Azure Monitor : [Vue d'ensemble d'Azure Monitor - Azure Monitor | Microsoft Docs](#)

Justification du choix de l'outil

Nous avons fait le choix de l'outil Azure pour plusieurs raisons :

- Puisque nous avons décidé de partir sur une infrastructure à majorité cloud, opter pour le service *Azure Monitor* permet d'utiliser le plein potentiel du cloud Azure et de ses solutions natives. Il permet de superviser toutes les ressources de l'entreprise et ses différentes données depuis un seul endroit.
- Le cloud permet une meilleure scalabilité et sécurité qu'une infrastructure On-Premise (vieillissante, dans le cadre de l'infrastructure actuelle de la société MALO). De plus, il est très adaptable et permet d'intégrer différentes applications de manière simple et efficace comme Servicenow.
- L'outil est puissant et très complet. Il permet de trier et personnaliser les données sensibles et critiques que nous souhaitons voir dans un environnement cloud, ce dernier pouvant rapidement devenir compliqué et complexe à gérer.
- *Azure Monitor* est *agentless* et tourne de manière invisible dans le fond sans besoin de ressources supplémentaires.
- L'outil fournit un système d'alerte et de remédiation très performant et rapide, ce qui est une condition importante à remplir lorsque l'on gère un parc informatique.

Pour ce qui est de l'outil *FortiAnalyzer*, il est plus intéressant de choisir une solution proposée par le fournisseur leader des pares-feux pour des raisons de simplicité et de gestion. La solution s'intégrera plus facilement à l'environnement Fortinet de nos firewalls.

Nous allons d'abord présenter la solution pour la gestion des logs système, puis nous détaillerons le choix de l'outil SIEM et son fonctionnement. Enfin, nous expliquerons le fonctionnement de l'outil d'analyse et de gestion des logs de nos équipements réseaux On-Premise.

Solution de gestion des logs système de l'infrastructure MALO

Présentation détaillée de la solution *Azure Monitor Logs*

Dès la création d'une ressource (machine virtuelle, réseau virtuel, adresse IP publique...), des *logs* et *metrics* sont générés et vont permettre de faire différentes actions, comme analyser des données, créer des alertes et des scénarios qui sont déclenchés quand un certain type de donnée est reçu dans l'espace de travail *Logs Analytics*²⁰ (qui stocke les logs de l'infrastructure Azure). Les *logs* et *metrics* sont donc deux types de données différentes²¹, générées par tout type de ressource Azure²² (que ce soit une ressource ou un abonnement).

²⁰ Présentation de *Log Analytics Workspace* : [Designing your Azure Monitor Logs deployment - Azure Monitor | Microsoft Docs](#)

²¹ Différences entre les deux types de données récoltées par Azure : [Logs and Metrics: What are they, and how do they help me? | Sumo Logic](#)

²² Vue d'ensemble des logs sur Azure : [Overview of Azure platform logs - Azure Monitor | Microsoft Docs](#)



Le tableau suivant récapitule le processus et les fonctionnalités des services Azure Monitor & Sentinel

:



Les logs peuvent être collectés de manière automatique dès la création de ressources. On peut cependant configurer certains éléments en plus pour obtenir une vision plus détaillée via les éléments suivants (que nous verrons plus loin dans cette partie) :

- Azure Activity Log : Collecte des logs au niveau de l'abonnement²³.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
> ➊ Validate Deployment	Succeeded	5 minutes ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➋ Validate Deployment	Succeeded	14 minutes ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➌ Deallocate Virtual Machine	Succeeded	44 minutes ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
➍ Health Event Updated	Updated	45 minutes ago	Fri May 06 2023	Azure for Students	
> ➎ Create or Update Public Ip Address	Succeeded	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➏ Create or Update Virtual Machine Extension	Succeeded	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➐ Create Workspace	Succeeded	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➑ Create or Update Virtual Machine	Succeeded	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➒ Get DNS alias target dependencies	Succeeded	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➓ Get DNS alias target dependencies	Succeeded	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➔ Get Network Interface Effective Security Groups	Succeeded	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➕ Get Network Interface Effective Security Groups	Accepted	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➖ Validate Deployment	Succeeded	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➗ List Workspace Shared Keys	Succeeded	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➘ Validate Deployment	Succeeded	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...
> ➙ Validate Deployment	Succeeded	an hour ago	Fri May 06 2023	Azure for Students	asi-pp-netstack2-sra@sup...

- Data Collection Rules : Azure donne la possibilité de choisir quels types de données nous souhaitons collecter sur les machines virtuelles et les envoyer vers l'espace de travail.

²³ Définition de Azure Activity Log : [Azure Activity log - Azure Monitor | Microsoft Docs](#)

- *Diagnostic Settings* : Ils permettent d'obtenir des informations plus détaillées sur les problèmes rencontrés par les ressources virtuelles²⁴. Nous n'allons pas le configurer pour les machines virtuelles de la société MALO, car la règle de collecte des données ainsi que la fonctionnalité *Insights* (que nous verrons plus loin dans la partie *Supervision*) vont déjà nous fournir les éléments nécessaires à leur bonne supervision.
Configurer les paramètres de diagnostic sur les ressources pour envoyer les logs sur l'espace de travail *Analytics* est indispensable pour une gestion efficace des logs.

Exportation des logs Azure AD vers l'espace de travail Analytics

Pour ce qui est des logs de l'Azure AD de l'entreprise MALO, nous allons les configurer pour qu'ils soient envoyés directement dans l'espace de travail *Analytics*²⁵, créé à cet effet, de la manière suivante :

- Nous allons nous rendre dans l'onglet *Diagnostic Settings* de l'Azure AD et activer ces paramètres de diagnostic.
- Puis nous choisissons l'espace de travail de la société MALO où envoyer les données choisies. Ici nous choisirons les logs d'Audit et de connexion :

Diagnostic setting ...

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name * SendToLogAnalytics

Category details

log

AuditLogs
 SignInLogs

In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, start a free trial.

NonInteractiveUserSignInLogs
 ServicePrincipalSignInLogs
 ManagedIdentitySignInLogs
 ProvisioningLogs
 ADFSSignInLogs

Destination details

Send to Log Analytics workspace

Subscription Visual Studio Enterprise Subscription

Log Analytics workspace NewLogsAnalyticsWorkspace (westus2)

Archive to a storage account
 Stream to an event hub
 Send to partner solution

²⁴ Vue d'ensemble de *Diagnostic Settings* = [Création de paramètres de diagnostic pour envoyer des métriques et journaux de plateforme Azure Monitor vers différentes destinations - Azure Monitor | Microsoft Docs](#)

²⁵ Tutoriel pour exporter les logs de Azure AD vers notre espace de stockage de logs : [azure-docs/how-to-integrate-activity-logs-with-log-analytics.md at main · MicrosoftDocs/azure-docs \(github.com\)](#)

Microsoft propose des filtres personnalisés pour exploiter les logs de la ressource via l'outil *Log Analytics* au mieux²⁶. Nous allons également configurer ce filtre pour la société MALO et donner un exemple d'alerte basée sur ce nouveau filtre :

- Nous allons télécharger les fichiers nécessaires via le lien suivant : [Deployment-Plans/Log Analytics Views at master · AzureAD/Deployment-Plans · GitHub](#)
- Nous nous rendons dans l'espace de travail de l'entreprise et dans l'onglet *View Designer*, puis nous choisissons l'option *Import the views from your local computer*.
- Nous sélectionnons les fichiers précédemment téléchargés et les importons. Ainsi, nous obtenons un filtre personnalisé et efficace pour superviser et gérer les logs AD de la société MALO.
- Nous allons répéter l'opération pour les vues *Azure AD Account Provisioning Events* et *Sign-ins*.
- Une fois ces opérations faites, nous pouvons ensuite nous rendre dans l'onglet *Workspace Summary* et sélectionner un des deux filtres (ou *view*) suivant : *Azure AD Account Provisioning Events* ou *Sign-ins Events*.
- Nous allons ensuite paramétrier une alerte qui nous préviendra lorsqu'une erreur d'authentification aura lieu de la façon suivante :
 - Nous nous rendons dans la vue *Sign-ins Events* puis nous sélectionnons le rapport *Sign-in errors over time* et nous allons dans *Analytics* pour ouvrir la page avec les détails des requêtes contenus dans le rapport choisi :

The screenshot shows the Microsoft Log Analytics workspace interface. At the top, there is a search bar with the text "signinLogs" and a "Run" button. To the right of the search bar are buttons for "Save", "Copy link", "Export", and a red-bordered "Set alert" button. Below the search bar is a code editor window containing a Log Search query:

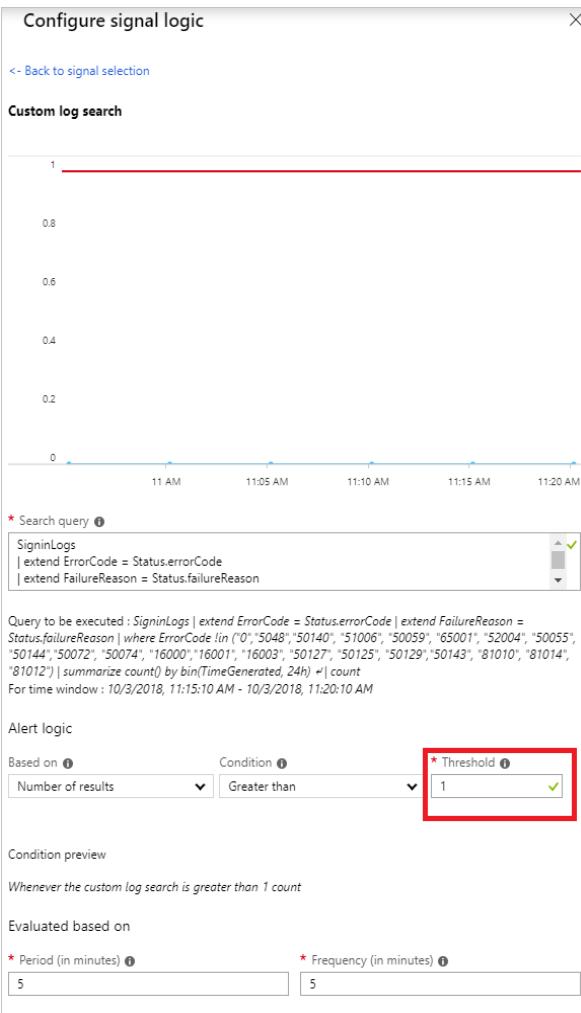
```
$ signinLogs
| extend ErrorCode = Status.errorCode
| extend FailureReason = Status.failureReason
| where ErrorCode in ("0", "50048", "50140", "51006", "50059", "65001", "52004", "50055", "50144", "50072", "50074", "16000", "16001", "16003", "50127", "50125", "50129", "50143", "81010", "81014", "81012")
| summarize count() by bin(TimeGenerated, 24h)
```

Below the code editor, a message states "Completed. Showing results from the custom time range." and "00:00:01.410 1 records". A table view is displayed with the following data:

TimeGenerated [UTC]	count_
2018-10-03T00:00:00.000	2

- Nous cliquons ensuite sur *Set Alert* et sélectionnons *Whenever the Custom log search is <logic undefined>* sous la section *Alert Criteria*. Nous plaçons le seuil d'alerte minimum à 1 (pour activer l'alerte quand il y a au minimum une erreur d'authentification) :

²⁶ Tutoriel sur comment installer les filtres personnalisés de Microsoft pour la gestion des logs de Azure AD : [How to install and use the log analytics views | Microsoft Docs](#)



The screenshot shows the 'Create rule' interface under 'Rules management'. In the 'Define alert condition' section, the alert criteria is set to 'Whenever the Custom log search is <logic undefined>'. In the 'Define alert details' section, the alert rule name is 'Alert on sign-in error', the description is 'Alert whenever there's a sign-in error', and the severity is 'Warning (Sev 1)'.

- Nous choisissons ensuite l'action à effectuer dans cette alerte est déclenchée. Nous allons configurer l'envoi d'un email à l'équipe informatique de la société MALO.

Une fois l'alerte créée, l'équipe informatique de la société MALO recevra donc un email dès qu'une erreur d'authentification d'un utilisateur sera détectée.

Création d'une Data Collection Rules pour les logs

Nous créerons une règle de collecte des données pour les serveurs virtuels & clients légers de la société MALO afin que cette dernière puisse monitorer depuis son espace de travail les logs générés par sa nouvelle infrastructure. Nous procéderons comme suit :

- Une fois dans le service *Azure Monitor*, nous cliquerons sur l'onglet *Data Collection Rule* puis *Création d'une Règle de Collecte des Données*. Nous sélectionnerons ensuite le type d'OS que nous souhaitons utiliser (en l'occurrence Windows, puisque les serveurs virtuels de l'entreprise sont tous sous cet OS) :

Home > Monitor >

Create Data Collection Rule ...

Data collection rule management

Basics Resources Collect and deliver Review + create

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources.

Rule details

Rule Name * Logs

Subscription * Azure for Students

Resource Group * NetStack

Create new

Region * North Europe

Platform Type * Windows

Linux

Custom

Review + create < Previous Next : Resources >

• Nous ajouterons les machines virtuelles sur lesquelles nous souhaitons collecter les logs (ici SRV-DHCP) :

Home > Monitor >

Create Data Collection Rule ...

Data collection rule management

Resources Basics Collect and deliver Review + create

Pick a set of machines to collect data from. The Azure Monitor Agent will be automatically installed on virtual machines, scale sets, and Arc-enabled servers. For Windows 10 and 11 devices, download the client installer [\(overview\)](#) and follow the [guidance here](#).

This will also enable System Assigned Managed Identity on these machines, in addition to existing User Assigned Identities (if any). Note: Unless specified in the request, the machine will default to using System Assigned Identity for all other apps. [Learn More](#)

Currently, only resources in certain region(s) are supported. [Learn More](#)

+ Add resources + Create endpoint

Enable Data Collection Endpoints

Only virtual machines in the same region can be assigned to the same endpoint. [Learn More](#)

Name	Type	Location
No resources added		

Select a scope

Browse Recent

Resource group All resource groups

Resource types All resource types

Locations All locations

Search to filter items...

Scope	Resource type	Location
<input type="checkbox"/> Azure for Students	Subscription	-
<input type="checkbox"/> netStack	Resource group	-
<input checked="" type="checkbox"/> SRV-DHCP	Virtual machine	North Europe

Review + create < Previous Next : Collect and deliver > Apply Cancel Clear all selections

- Puis nous choisirons les types de logs que nous souhaitons (ici tous les types proposés) :

The screenshot shows the 'Create Data Collection Rule' wizard. In the 'Add data source' step, the 'Event logs' section is selected under 'Data source type'. The 'Basic' collection type is chosen. Under 'Configure the event logs and levels to collect', log levels for Application (Critical, Error, Warning, Information, Verbose), Security (Audit success, Audit failure), and System (Critical, Error, Warning, Information, Verbose) are checked. A note at the bottom states: '⚠️ Update the basic configuration will remove any custom event logs that have been configured.'

- Nous sélectionnerons l'espace de travail Log Analytics qui stockera tous les logs générés par les serveurs virtuels. Enfin, nous créerons la règle suivante :

The screenshot shows the 'Monitor | Data Collection Rules' page in the Azure portal. It lists a single rule named 'Logs', which is associated with the 'Logs' resource group in the 'Azure for Students' subscription and located in 'North Europe'. The data source is set to 'Windows event logs' and the destination is 'Azure Monitor Logs'. The 'Data Collection Rules' option is highlighted in the left sidebar.

Pour le cas particulier des clients légers (*Azure Virtual Desktop*), le processus est similaire à celui des machines virtuelles. Nous allons configurer cette collecte des données depuis le service *Azure Virtual Desktop*²⁷.

²⁷ Configuration de l'envoi des logs des clients légers vers l'espace Analytics : [How to enable Azure Monitor for Windows Virtual Desktop – Robin Hobo](#)

Paramètres de diagnostic (*Diagnostic Settings*)

Nous configurerons les paramètres de diagnostic sur les ressources (autres que les serveurs virtuels) de la société MALO, tels que la passerelle VPN et les VNets notamment, de la façon suivante :

- Une fois dans la ressource en question, nous irons dans la section *Monitoring*, puis nous choisirons l'onglet *Paramètres de diagnostic* :

- Nous sélectionnerons ensuite les logs qui nous intéressent, ici la catégorie *allLogs*, qui regroupe plusieurs types de logs liés à la ressource choisie. Puis nous les enverrons sur l'espace de travail de la société MALO et nous enregistrerons les changements :

Nous répéterons le même procédé pour les autres ressources éligibles à ce service, dont les logs seront envoyés vers l'espace de travail de la société MALO.

Les espaces de travail *Analytics* jouent un rôle majeur, car c'est eux qui stockent les données générées par Azure.

Logs Query

Si nous souhaitons obtenir des logs spécifiques d'une machine virtuelle de la société MALO, comme le SRV-DHCP, en particulier depuis la plateforme centrale *Azure Monitor*, nous allons nous rendre

dans l'onglet *Logs* afin de créer une requête de données pour cette machine virtuelle²⁸. La requête va alors rechercher les logs demandés dans l'espace de travail que nous lui aurons fourni, pour ensuite nous mettre en avant les logs de la machine virtuelle ou ressource en question.

Par exemple, si nous souhaitons obtenir les logs du serveur virtuel SRV-DHCP, nous procéderons de la manière suivante :

- Nous nous rendrons dans le service *Monitor* puis dans l'onglet *Logs* de la section *Overview* :

- Nous choisirons ensuite la catégorie *Machines Virtuelles*. Dans cette catégorie, nous pourrons choisir une des nombreuses requêtes proposées par Microsoft. Nous pourrons observer la dernière fois qu'un serveur a été actif en cas d'interruption de services :

TimeGenerated (UTC)	Computer	SourceComputerId	ComputerIP	Category	OSType	OSMajorVersion
5/6/2022, 11:51:01.987	SRV-DHCP	Beb34218-4e84-4d11-9e56-0d...	20.107.203.109	Direct Agent	Windows	10

- Une fois la requête effectuée, nous la sauvegarderons afin que la société MALO puisse la lancer plus rapidement lorsque ce sera nécessaire.

Concernant la gestion des logs des postes légers, ils seront visibles et exploitables depuis *Azure Monitor*.

²⁸ Détail de la fonctionnalité *Log Analytics* : [Tutoriel Log Analytics - Azure Monitor | Microsoft Docs](#)

Stratégie de rétention des logs

La stratégie Azure définit une rétention par défaut à 31 jours gratuits, et 90 jours gratuits si un abonnement à *Azure Sentinel* est actif pour le stockage des logs système.

Dans notre cas, si nous souhaitons appliquer une stratégie de rétention des logs système sur 6 mois glissants, le montant estimé dépendra de la quantité de logs générés par l'infrastructure. Il est possible de configurer cette rétention dans l'espace *Azure Monitor*, et de modifier la stratégie de rétention par défaut. Nous pouvons établir un minimum de 30 jours, et un maximum de 730 jours.

Il est également possible de passer par l'espace *Analytics* où seront stockés les logs système pour modifier cette stratégie de rétention :

The screenshot shows two windows side-by-side. On the left is the 'Usage and estimated costs' page for the 'NetStack-Workspace'. It displays various metrics like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main content area shows a table of estimated monthly costs for different pricing tiers: Pay-as-you-go, 100 GB/day Commitment Tier, 200 GB/day Commitment Tier, 300 GB/day Commitment Tier, and 400 GB/day Commitment Tier. The 'Pay-as-you-go' tier is selected. On the right is a 'Data Retention' configuration dialog. It includes a note about 31 days of retention being included with the pricing plan, a slider for 'Data Retention (Days)' set to 180, and a note about Application Insights data types defaulting to 90 days. Below these are sections for 'Usage Charts' (showing billable data ingestion per solution over 31 days) and 'Data ingested per solution (last 90 days)' (showing no data).

Nous verrons dans la partie *Tarification pour la gestion des logs* le montant estimé de la solution pour une rétention de logs à 6 & 12 mois glissants suivant la nature des logs.

Solution de gestion des logs sécurité de l'infrastructure MALO

Présentation détaillée de la solution *Azure Sentinel*

Pour les logs sécurité, le principe sera le même, mais via une interface différente, celle de *Microsoft Sentinel*²⁹. *Sentinel* est un SIEM³⁰ qui analyse les événements sécurité de l'infrastructure cloud Azure. Il permet les fonctionnalités suivantes :

- Collecte des données de l'infrastructure cloud, des ressources et des utilisateurs.
- Détection des menaces et faux-positifs.

²⁹ Description de *Microsoft Sentinel* et son installation : [Démarrage rapide : Intégration dans Microsoft Sentinel | Microsoft Docs](#)

³⁰ Définition d'un SIEM par Oracle : [Qu'est-ce qu'un SIEM ? | Oracle France](#)

- Protection automatisée avec l'intelligence artificielle et réponse automatique à des événements donnés.

Puisque l'infrastructure système est basée en totalité sur le cloud Azure, il est logique et avantageux d'utiliser l'outil *Sentinel*, qui pourra traiter les logs de sécurité de l'infrastructure cloud MALO rapidement, efficacement et de manière native. Il est important de rappeler que *Sentinel* n'est pas un antivirus, contrairement à *Microsoft Defender for Cloud*³¹, qui est une solution de sécurité pour l'environnement Azure (cloud & hybride).

La stratégie de rétention pour les logs est également définie à 31 jours par défaut, mais nous allons la mettre à 90 jours pour bénéficier des fonctionnalités complètes du SIEM.

Configuration du SIEM

Pour utiliser *Sentinel*, il nous sera demandé de créer ou d'utiliser un espace de travail (dans notre cas, l'espace de travail de la société MALO), puisque *Azure Monitor* est la plateforme centrale de Azure qui collecte les logs. Créer un espace de travail est donc nécessaire pour permettre la collecte des logs par *Sentinel*³². Nous le lierons à la solution SIEM :

The screenshot shows the Microsoft Sentinel interface for adding a workspace. At the top, it says "Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace". Below that is a search bar labeled "Filter by name...". A note says "Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details." The main area lists existing workspaces:

Workspace	Location	ResourceGroup	Subscription	Directory
NetStack-Sentinel-Workspace	northeurope	netstack	Azure for Students	CFA SUP DE VINCI
NetStack-Workspace	northeurope	netstack	Azure for Students	CFA SUP DE VINCI

At the bottom, there are "Add" and "Cancel" buttons.

L'étape suivante consistera à connecter les sources de données, à savoir les données émises par les ressources virtuelles de la société MALO. Par défaut, *Azure Sentinel* contient plusieurs types de connecteurs prêts à l'emploi et disponibles dans l'onglet *Data Connectors*³³. Nous configurerons l'envoi des logs sécurité de l'infrastructure Azure MALO vers *Sentinel* via le connecteur *Azure Active Directory*³⁴ :

- Une fois dans le service *Sentinel*, nous irons dans la section Configuration puis nous sélectionnerons *Azure Active Directory* dans la liste Data connectors :

³¹ Solution antivirus de Azure : [Microsoft Defender for Cloud - an introduction | Microsoft Docs](#)

³² Détails des configurations nécessaires pour mettre en place *Microsoft Sentinel* : [Présentation de Microsoft Sentinel | Microsoft Docs](#)

³³ Détails des types de connecteurs de données : [Connecteurs de données Microsoft Sentinel | Microsoft Docs](#)

³⁴ Connexion des données de l'Azure AD à *Sentinel* : [Connect Azure Active Directory data to Microsoft Sentinel | Microsoft Docs](#)

The screenshot shows the Microsoft Sentinel Data connectors page. On the left, there's a navigation sidebar with options like Overview, Logs, Threat management, Content management, Configuration, and Data connectors (which is selected). The main area displays a list of 123 connectors, each with a small icon and its name. The connectors include various cloud services and on-premises systems. On the right, there's a detailed view of the Azure Active Directory connector, showing its status as 'Not connected' and being a 'Microsoft Provider'. It includes sections for Description, Related content (7 workbooks, 2 queries, 67 Analytics rules templates), and a chart showing 'Data received' over time.

- Une fois dans la page du connecteur, nous pourrons commencer la configuration pour l'infrastructure de la société MALO :

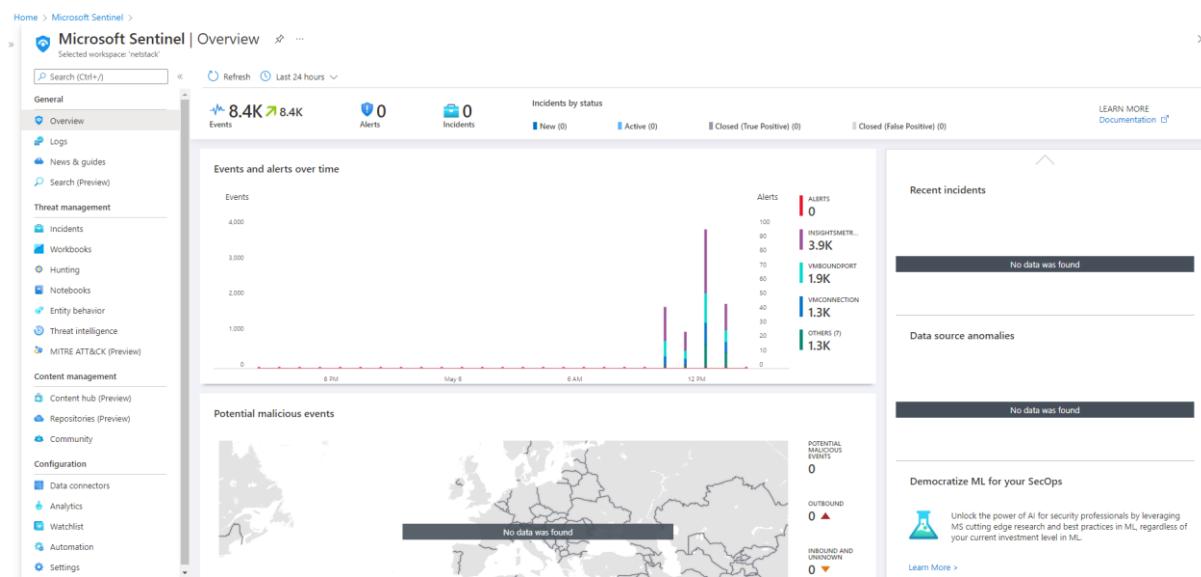
This screenshot shows the configuration page for the Azure Active Directory connector. It has two main sections: 'Instructions' and 'Next steps'. Under 'Prerequisites', it lists three items: 'Workspace' (checked), 'Diagnostic Settings' (unchecked), and 'Tenant Permissions' (checked). Under 'Configuration', it says 'Connect Azure Active Directory logs to Microsoft Sentinel' and 'Select Azure Active Directory log types:'. There are several checkboxes for different log types, with 'Sign-In Logs' being the only one checked. Below this, there's a note about needing an AD P1 or P2 license for sign-in data. The right side of the screen shows a 'Log Analytics' chart with a Y-axis for 'Data received' (0 to 100) and an X-axis for dates from May 27 to May 31. The chart shows values of 0 for most days, with a small peak around May 29.

- Nous cliquerons sur le bouton *Connect* après avoir coché toutes les cases. Cela permettra à *Sentinel* de collecter les données de l'AD et de pouvoir lancer des requêtes.

Microsoft apporte également plus de détails sur ces connecteurs³⁵.

³⁵ Explication détaillée sur la connexion aux sources de données pour Azure Sentinel : [Find your Microsoft Sentinel data connector | Microsoft Docs](#)

Une fois *Sentinel* configuré avec ces étapes, nous pourrons gérer les logs et événements de sécurité sur la plateforme Azure *Sentinel* suivante :



Une fois dans le tableau de bord de *Sentinel*, nous pourrons nous aider de plusieurs outils pour mieux gérer les logs de sécurité de l'infrastructure MALO.

C'est le cas des *playbooks*, qui permettront d'automatiser et d'orchestrer la sécurité de l'infrastructure³⁶. Cet outil utilise *Azure Logic Apps*, qui est un autre service de Microsoft Azure. Ces *playbooks* permettront par exemple de générer un ticket dans Servicenow si un événement de sécurité donné apparaît. Ou encore, il permettra de modifier automatiquement la gravité d'un faux-positif connu dans la base de données Microsoft.

Il existe déjà plusieurs centaines de modèles de *playbooks* avec lesquels nous pouvons démarrer si nous souhaitons créer une tâche d'automatisation en réponse à un événement donné. Nous commencerons par créer une tâche d'automatisation pour la société MALO qui consistera à créer un événement de sécurité majeur (high) dans l'outil Servicenow de la façon suivante :

- Une fois dans la section *Configuration*, nous nous rendrons dans *Automation* puis *Playbook templates (Preview)* afin de choisir la tâche en question :

³⁶ Détails de l'outil : [Utiliser des playbooks avec des règles d'automatisation dans Microsoft Sentinel | Microsoft Docs](#)

The screenshot shows the Microsoft Sentinel Automation blade. On the left, there's a navigation sidebar with various options like Overview, Logs, Threat management, Content management, Configuration, and Automation (which is currently selected). The main area displays a list of 'Playbook templates (Preview)'. One template, 'Create SNOW record', is highlighted. Its details pane on the right shows the trigger is 'Microsoft Sentinel Incident' and it connects to 'ServiceNow'. There are also sections for 'Prerequisites' (existing SNOW instance and credentials), 'Connectors in use' (Microsoft Sentinel and ServiceNow), and a preview of the logic app flow.

- Pour cette tâche, nous utiliserons l’instance Servicenow MALO active et les identifiants de l’administrateur Servicenow :

The screenshot shows the 'Create playbook' wizard. It's on the 'Connections' step, which is the second of two steps. It lists two connectors: 'Microsoft Sentinel' (which is selected and has a green checkmark) and 'ServiceNow' (which is new and has a red exclamation mark). Below each connector, there are buttons to 'Connect with managed identity' or 'New connection will be configured'.

- Une fois le playbook créé, nous serons redirigés vers la tâche *Logic app*, qui va nous permettre de rentrer les actions que nous souhaitons effectuer quand un incident de sécurité survient :

The screenshot shows the Logic app designer for the 'CreateSNOWRecord' logic app. The workflow starts with a 'Microsoft Sentinel incident (Preview)' trigger. This is followed by an 'Initialize variable' step, where a variable 'Severity' is set to 'String' type with value '3'. Next is a 'Switch' step, and finally a 'Connections' step. The logic app designer interface includes a toolbar at the top and a sidebar on the left with various development tools and settings.

Ainsi, une fois la tâche créée et l’instance Servicenow connectée, si un incident majeur survient sur l’infrastructure de la société MALO, un ticket sera créé dans Servicenow, alertant ainsi l’équipe IT.

D’autres outils permettent aussi de détecter et de prévenir de manière proactive les menaces potentielles comme l’outil *Threat-Hunting*³⁷ de *Sentinel*. Cet outil permettra d’améliorer la sécurité de l’infrastructure en exécutant des requêtes de sécurité qui permettent une meilleure proactivité

³⁷ Explication de la fonctionnalité *Threat-Hunting* de Azure Sentinel : [Hunting capabilities in Microsoft Sentinel | Microsoft Docs](#)

dans l'anticipation, la détection et la remédiation de menaces de sécurité. Nous configurerons plusieurs requêtes pour la société MALO.

La première requête permettra d'alerter l'équipe IT de la société MALO lorsqu'un seuil anormal de requêtes de type DNS lookup a été atteint depuis une IP cliente ou externe. Cela permettra de détecter une potentielle fuite de données de l'entreprise vers l'extérieur, ou un début d'activité type scan du réseau important :

Query	Provider	Data source	Results	Results delta	Results delta per...	Tactics
Changes made to AWS IAM policy	Microsoft	AWSCloudTrail	--	--	--	
Consent to Application discovery	Microsoft	AuditLogs	--	--	--	
Rare Audit activity initiated by App	Microsoft	AuditLogs	--	--	--	
Rare Audit activity initiated by User	Microsoft	AuditLogs	--	--	--	
Azure storage key enumeration	Microsoft	AzureActivity	--	--	--	
DNS lookups for commonly abused TLD	Microsoft	DnsEvents	N/A	--	--	
DNS - domain anomalous lookup increase	Microsoft	DnsEvents	N/A	--	--	
DNS Full Name anomalous lookup increase	Microsoft	DnsEvents	N/A	--	--	
High reverse DNS count by host	Microsoft	DnsEvents	N/A	--	--	
Abnormally long DNS URI queries	Microsoft	DnsEvents	N/A	--	--	
DNS Domains linked to WannaCry ransomware	Microsoft	DnsEvents	N/A	--	--	
Cobalt Strike DNS Beaconing	Microsoft	DnsEvents +1	N/A	--	--	

Nous ajouterons auparavant le connecteur DNS pour Sentinel afin d'obtenir ce type de logs directement dans l'espace de travail :

La deuxième requête que nous configurerons pour la société MALO permettra de détecter des comptes utilisateurs qui se sont connectés depuis différents pays dans un intervalle de temps court (défini à 10 minutes). Le but de cette requête est d'identifier des utilisateurs passant par plusieurs VPNs pour tenter de voler des données ou d'accéder à l'infrastructure MALO :

The screenshot shows the Microsoft Sentinel Hunting interface. On the left, a navigation sidebar includes options like General, Threat management, Configuration, and Hunting. The Hunting section is selected. The main area displays a summary: 155/211 Active / total queries, 0/0 Result count / queries run, 0 Livestream Results, and 0 My bookmarks. Below this is a table of search queries, with one entry highlighted: "User Login IP Address Teleportation". The right side of the interface shows a detailed view of this query, including its description, provider (Microsoft), data source (SigninLogs), and a code snippet for the query:

```
let windowTime = 2 * min / 2; //Window to lookup
and excludeIpInLog = dynamic(["127.0.0.1", ".0.0.0"]);
let excludedIpIn = SigninLogs
| where ConditionalAccessStatus == "success"
| where ip != excludedIpIn
```

Buttons for "Run Query" and "View Results" are visible at the bottom right.

La dernière requête permettra d'anticiper et de prévenir une potentielle utilisation de la faille Log4j CVE-2021-44228³⁸, qui est une vulnérabilité très grave et récente :

This screenshot shows the same Microsoft Sentinel Hunting interface as the previous one, but with a different query selected: "Azure WAF Log4j CVE-2021-44228 hunting". The right panel displays the query details, including its description, provider (Microsoft), data source (AzureDiagnostics), and a complex query script involving log4jString and log4jRegex variables. The interface remains consistent with the first screenshot, showing the same navigation sidebar and overall layout.

Rétention des logs

La méthode pour modifier la date de rétention des logs est la même que pour les logs système sur Azure Monitor : on peut la modifier directement dans le service *Sentinel* ou alors passer par l'espace de travail.

³⁸ Faille de sécurité Log4j : [Log4j – Apache Log4j 2](#)

Solution de gestion des logs des équipements réseaux On-Premise

Les cyber-attaques via les équipements réseaux étant de plus en plus fréquentes depuis la COVID-19, il est devenu nécessaire d'avoir des outils de protection et d'analyse des logs sécurité des équipements réseaux³⁹. Faire le choix d'un outil de gestion et d'analyse des logs réseaux permettra à la société MALO de mieux se protéger des attaques et de prendre de meilleures décisions à la lumière des données mises en avant par l'outil que nous allons voir ci-après.

Puisque nous allons implémenter trois pare-feux Fortinet pour protéger le réseau interne physique de la société MALO, nous avons fait le choix de la solution *FortiAnalyzer* pour analyser et gérer les logs sécurité de l'infrastructure réseau de l'entreprise. Fortinet étant le leader des solutions de firewall, il devient intéressant de choisir sa solution d'analyse et de gestion des logs réseaux pour une meilleure sécurité et performance de l'infrastructure⁴⁰.

Choix du modèle

Nous avons fait le choix du modèle *FortiAnalyzer 300F*⁴¹ pour plusieurs raisons :

- Le coût de la solution est plus avantageux que de passer par Azure Sentinel, qui nécessiterait une VM Linux, un agent particulier tournant dessus afin de transférer les logs On-Premise vers Azure, ainsi qu'un coût de stockage supplémentaire en plus des logs de l'infrastructure cloud⁴²⁴³.
- Possibilité de transférer les logs de l'outil dans un outil externe type SIEM. Cela peut être utile si jamais, à l'avenir, la société MALO décide de passer par l'outil *Sentinel* pour les logs sécurité de son infrastructure physique.
- Il conviendra parfaitement au volume des logs générés par la société MALO (capacité de 150 Go journaliers).
- Sa capacité de stockage sera suffisante pour la rétention des logs, établies à 12 mois glissants, tout comme le SIEM de la société MALO. L'outil doté de 4TB de stockage (après RAID) permettra une rétention des logs sur 12 mois compte tenu de l'activité prévisionnelle des logs. De plus, il est configuré avec un système RAID 1, qui assure la redondance des données en cas d'indisponibilité du premier disque dur (2 x 4TB).
- Il possède un tableau de bord interactif personnalisable qui aidera la société MALO à identifier rapidement les problèmes, à partir de représentations intuitives du trafic réseau, des menaces et des applications.
- Génération de rapports personnalisables qui aident à la prise de décision.
- Configuration d'alertes pour des événements donnés.

³⁹ Statistiques sur les cyber-attaques depuis la crise sanitaire : [2022 Must-Know Cyber Attack Statistics and Trends | Embroker](#)

⁴⁰ Fortinet nommé leader des solutions de pare-feu par Gartner : [Fortinet est de nouveau nommé en tant que Leader dans le Magic Quadrant 2020 de Gartner dédié aux pare-feux réseau](#)

⁴¹ Concepts et fonctionnalités clés de l'outil : [FortiAnalyzer Data Sheet \(fortinet.com\)](#)

⁴² Procédure pour transférer des logs On-Prem vers Azure Sentinel : [Transférer les journaux au format CEF de votre appareil ou dispositif dans Microsoft Sentinel | Microsoft Docs](#)

⁴³ Procédure pour envoyer les logs Fortinet vers Azure Sentinel : [Rechercher votre connecteur de données Microsoft Sentinel | Microsoft Docs](#)

- Centre d'exploitation du réseau (NOC) et Centre d'exploitation de la sécurité (SOC) intégrés dans un tableau de bord pour mieux sécuriser le réseau interne de l'entreprise MALO.

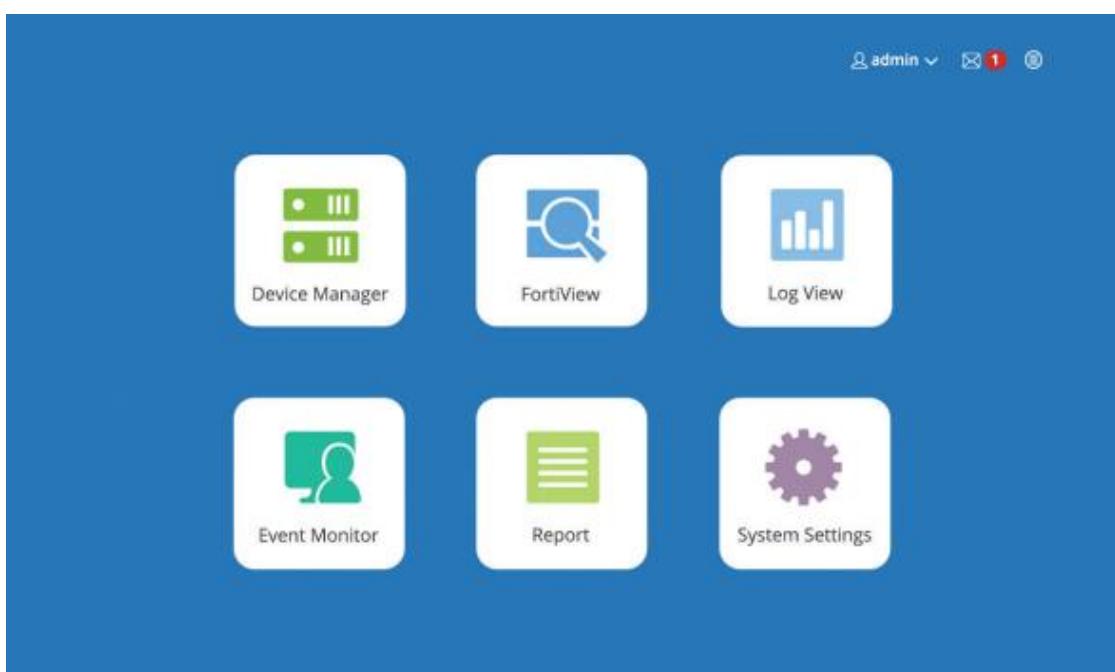
Coût de l'outil

L'outil *FortiAnalyzer 300F* avec l'option RAID 1 (2 x 4TB) a un coût de 7300€ à l'achat, incluant une protection entreprise et un support d'un an (la protection entreprise et le support peuvent être renouvelés pour un coût de 1 500€ annuel). La configuration de l'outil pour l'infrastructure MALO sera expliquée dans la partie des coûts d'intégration.

Installation dans l'environnement réseau de l'entreprise MALO

Nous allons maintenant détailler l'intégration de cet outil dans l'environnement réseau de l'organisation MALO. Un schéma d'infrastructure global incluant le *FortiAnalyzer* est disponible en fin de document pour mieux rendre compte de l'intégration de cet outil dans l'infrastructure finale. Puisque *FortiAnalyzer* est une appliance physique, il faudra procéder de la manière suivante⁴⁴ :

1. Avant de brancher l'appareil aux deux Fortinet des locaux parisiens de la société MALO, nous configurerons l'appareil via un ordinateur portable. La première étape consistera à brancher un câble internet du PC vers le port management (ou console) de l'appareil.
2. Nous modifierons l'adresse IP de l'ordinateur pour être sur le même sous-réseau que celui de l'appareil par défaut (qui est 192.168.1.99). Une fois cette modification faite, nous nous rendrons sur l'adresse IP de l'appareil via un navigateur, qui sera l'interface de management de l'appareil.
3. Nous nous connecterons avec les identifiants par défaut (admin et aucun mot de passe) :



⁴⁴ Mise en place de l'outil : [QuickStart Guide | Fortinet Documentation Library](#)

4. Nous irons ensuite dans les paramètres du système pour changer l'adresse IP de l'interface en 172.10.210.20, puisqu'il sera dans le sous-réseau des équipements réseaux (VLAN 10) :

The screenshot shows the 'System Network Management Interface' configuration page. The 'Name' field is set to 'port1'. The 'IP Address/Netmask' field contains '10.3.112.95/255.255.0.0'. The 'Default Gateway' field contains '172.16.96.1'. The 'Primary DNS Server' and 'Secondary DNS Server' fields both contain '172.16.100.100'. The 'Administrative Access' and 'IPv6 Administrative Access' sections show various checkboxes for protocols like HTTPS, HTTP, PING, SSH, TELNET, SNMP, Web Service, Aggregator, and FortiManager. At the bottom, there are tabs for 'All Interfaces', 'Routing Table', and 'IPv6 Routing Table', followed by an 'Apply' button.

Nous changerons la passerelle par défaut pour mettre celle du cluster firewall Fortinet de la société MALO. Nous décocherons également les accès administratifs TELNET.

5. L'étape suivante consistera à changer les identifiants par défaut et mettre les nouveaux identifiants de l'administrateur local de la société MALO dans le chemin suivant : *System Settings > Admin > Administrator > Create New* :

The screenshot shows the 'New Administrator' dialog box. It includes fields for 'User Name' (set to 'admin_John'), 'Comments' (empty), 'Admin Type' (set to 'LOCAL'), 'New Password' (a series of asterisks), 'Confirm Password' (also a series of asterisks), 'Admin Profile' (set to 'Super_User'), and 'Administrative Domain' (set to 'All ADOMs'). At the bottom are 'OK' and 'Cancel' buttons.

6. Nous configurerons la politique de stockage de la société MALO pour les logs sécurité de ses équipements réseaux. Toujours dans les paramètres du système, nous nous rendrons dans le *Tableau de Bord* puis *Information Système* (sous *Stratégie de Stockage des Logs*) et sélectionner *Modifier la Stratégie de Stockage des Logs*.
Dans la partie *Data Policy*, nous conserverons les logs pendant 365 jours, conformément aux attentes de la société MALO :

Edit Log Storage Policy - ADOM : root

Data Policy

Keep Logs for Analytics	60	Days
Keep Logs for Archive	365	Days

Disk Utilization

Maximum Allowed	1000	MB	Out of Available: 63.6 GB
Analytics : Archive	70%	30%	<input type="checkbox"/> Modify
Alert and Delete When Usage Reaches	90%		

*If analytic or archive log usages exceed the configured disk quota before the retention period expires, the oldest logs will be deleted.

OK **Cancel**

- La prochaine étape consistera à connecter les firewalls Fortinet au *FortiAnalyzer*. Pour se faire, nous nous connecterons aux firewalls Fortinet via un ordinateur portable pour se rendre sur l'interface web des firewalls. Nous nous rendrons dans la partie *Log & Report* puis *Log Settings* et nous cocherons la case *Envoyer les logs au FortiAnalyzer*. Nous entrerons ensuite l'adresse IP du *FortiAnalyzer* et enregistrerons les modifications :

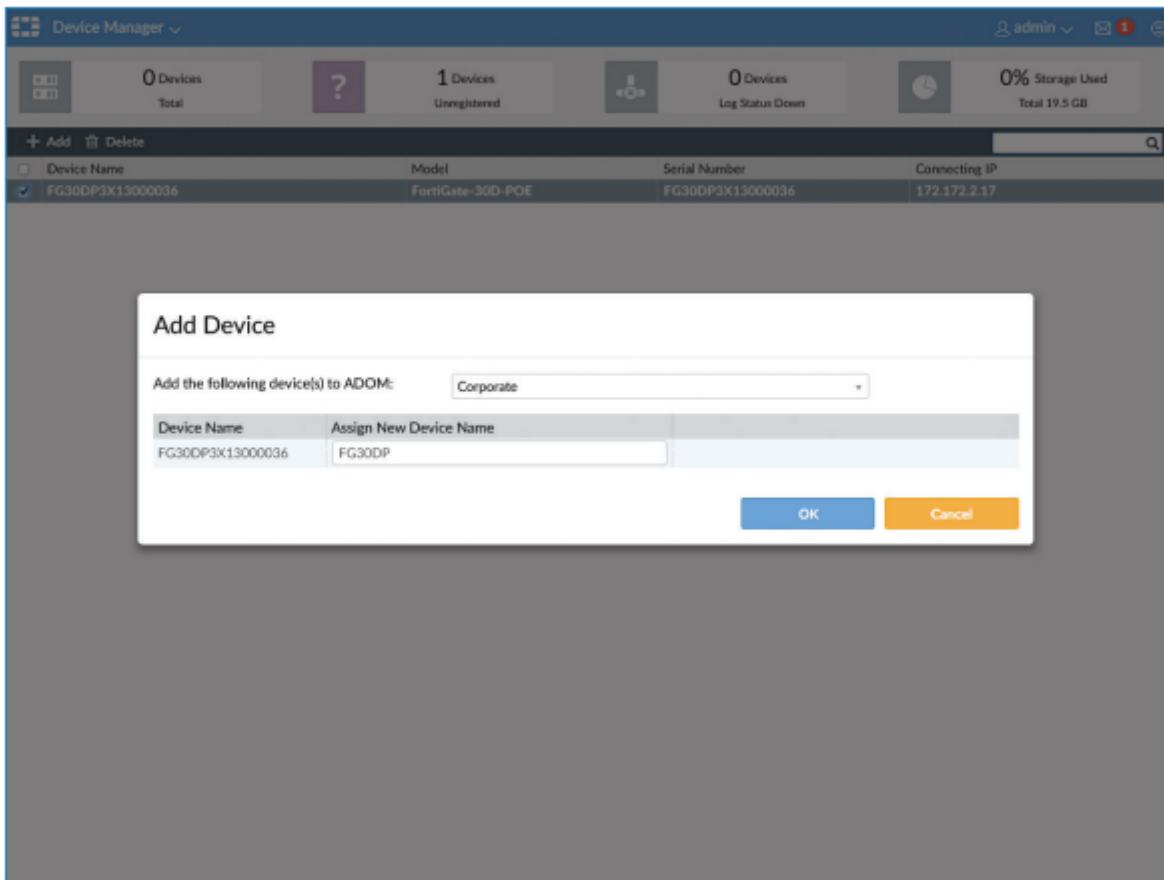
Log Settings

Remote Logging and Archiving

Send Logs to FortiAnalyzer/FortiManager	<input checked="" type="checkbox"/>	
Use FortiManager	<input type="checkbox"/>	
IP Address	172.16.96.5	Test Connectivity
Upload Option	Store & Upload Logs Realtime	

- Nous retournerons ensuite sur l'interface du *FortiAnalyzer* et dans l'onglet *Device Manager*. Nous cliquerons ensuite sur l'onglet *Unregistered Devices* et sélectionnerons l'adresse IP virtuel du cluster firewall FortiGate ainsi que leur numéro de série.

Device Name	Model	Serial Number	Connecting IP
FG300DP3X13000036	FortiGate-30D-POE	FG300DP3X13000036	172.172.2.17



9. Nous choisissons ensuite le FortiGate *Master* (172.10.210.10). Nous cliquons sur *Edit*. Dans l'onglet *Edit Device*, nous sélectionnons *HA Cluster*.

Depuis la liste *Add Existing Device*, nous sélectionnons l'autre FortiGate puis nous cliquons sur *Add*⁴⁵.

Name	FG149						
Description							
IP Address	10.10.10.10						
Serial Number	FGVM0000000000 (FortiGate-VM64)						
Firmware Version	FortiGate 5.6, build1534						
Admin User	admin						
Password	*****						
HA Cluster	<input checked="" type="checkbox"/>						
Add Existing Device	<input style="width: 20px; height: 20px;" type="button" value="+"/>						
Add Other Device	<input style="width: 20px; height: 20px;" type="button" value="+"/>						
HA Cluster List	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>#</th> <th>Device Name</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>FG149 (FGVM0000000000)</td> <td></td> </tr> </tbody> </table>	#	Device Name	Action	1	FG149 (FGVM0000000000)	
#	Device Name	Action					
1	FG149 (FGVM0000000000)						

⁴⁵ Comment créer un *HA Cluster* dans FortiAnalyzer : [Administration Guide | FortiAnalyzer 6.4.0 | Fortinet Documentation Library](#)

10. Nous retournerons ensuite dans l'onglet *Paramètres des Logs* du point 7 (évoqué plus haut) pour tester la connectivité des Fortinet et vérifier que nous recevons bien les logs générés par l'activité réseau :



11. Une fois ce test de connectivité effectué, nous irons dans *Log View* du *FortiAnalyzer* pour vérifier la liste des logs reçus :

Log View										
Traffic		Add Filter		Search		FG10003G00000291		Last 5 Minutes		GO
Event		#	Date/Time	Device ID	Action	Source	Destination IP	Service	Sent/Received	User
Event		#	Date/Time	Device ID	Action	Source	Destination IP	Service	Sent/Received	User
Security		1	14:27:26	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.3 KB	Web Management
VoIP		2	14:27:25	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 KB	Web Management
Custom View		3	14:27:25	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	2.3 KB/2.9 KB	Web Management
Storage Statistics		4	14:27:20	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	4.3 KB/4.5 KB	Web Management
Log Browse		5	14:27:20	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 KB	Web Management
Log Group		6	14:27:16	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.6 KB	Web Management
		7	14:27:14	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 KB	Web Management
		8	14:27:11	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.3 KB/1.2 KB	Web Management
		9	14:27:07	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 KB	Web Management
		10	14:27:06	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.3 KB/1.2 KB	Web Management
		11	14:27:04	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.6 KB	Web Management
		12	14:27:01	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 KB	Web Management
		13	14:27:00	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.3 KB/1.3 KB	Web Management
		14	14:27:00	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.3 KB/3.0 KB	Web Management
		15	14:26:56	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	2.9 KB/2.9 KB	Web Management
		16	14:26:55	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 KB	Web Management
		17	14:26:51	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.3 KB/1.3 KB	Web Management
		18	14:26:49	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	3.4 KB/2.7 KB	Web Management
		19	14:26:46	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/768.0 KB	Web Management
		20	14:26:46	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.6 KB	Web Management
		21	14:26:39	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	15.7 KB/33.8 ...	Web Management
		22	14:26:39	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	2.2 KB/4.6 KB	Web Management
		23	14:26:31	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	3.0 KB/6.9 KB	Web Management
		24	14:26:31	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	4.3 KB/10.0 KB	Web Management
		25	14:26:31	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	4.2 KB/11.2 KB	Web Management
		26	14:26:29	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	5.4 KB/26.2 KB	Web Management
		27	14:26:26	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.2 KB	Web Management
		28	14:26:19	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.0 KB	Web Management
		29	14:26:16	FG10003G00000291	✓	160.20c.29f.rebd:61fe	1602:16	icmp6/143/0	876.0 B/0.0 KB	icmp6/143/0
		30	14:26:16	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.0 KB	Web Management
		31	14:26:16	FG10003G00000291	✓	172.18.27.180	172.18.27.206	HTTP	1.2 KB/1.0 KB	Web Management
		32	14:26:09	FG10003G00000291	✓	-	1602:16	icmp6/143/0	3.0 KB/0.0 KB	icmp6/143/0
		33	14:26:01	FG10003G00000291	✓	160.20c.29f.rebd:61fe/7	1602:16	icmp6/143/0	579.6 KB/0.0 KB	icmp6/143/0

12. Le *FortiAnalyzer* sera opérationnel une fois ces étapes complétées. On peut se rendre dans l'onglet *FortiView* de l'accueil et commencer à avoir une vue graphique des logs générés par l'infrastructure réseau de MALO :

Fortiview Summary

Source IP 172.16.100.80 used the most bandwidth.

EICAR is the top threat to your network.

Torrent used the most bandwidth.



Voici un exemple de vue détaillée d'une menace détectée :

[Drill Down and View Log Details](#)

Here is the drill-down view of threat ow.ly at log level.

The screenshot shows the FortiView interface with the following details:

- Left Sidebar:** Summary, Threats, Threat Map, IOC, Traffic, Top Sources, Top Destinations, Top Countries, Policy Hits, Applications & Websites, VPN, WiFi, System, EndPoints.
- Top Center:** Threat Score: Blocked/ Allowed (Blocked).
- Threat Details:** Threat ID: ow.ly, Category: Malicious Websites, Threat Level: Red.
- Log Details:** Double-click a row to open the log detail pane in tree view.
- Right Side:** View UTM Logs, Click the UTM log icon to open the UTM log view window.
- Bottom:** Threat Log table with columns: Date/Time, Device ID, Action, Source, Destination IP, Service, Sent/Received, User, Application, Security Event List.

Nous générerons un rapport de l'activité de l'infrastructure réseau de la société MALO en allant dans *Reports > Report Definitions > All Reports*. Quand nous double-cliquons sur *Application Risk & Control*, nous pouvons générer ce rapport et le voir/télécharger au format souhaité :

The screenshot shows the FortiView Reports interface with the following details:

- Left Sidebar:** Report Definitions, All Reports, Templates, Chart Library, Macro Library, Datasets, Advanced, Output Profile, Language, Report Calendar.
- Top Right:** ADOM: root, admin, Edit: Application Risk and Control.
- Center:** Run Report, Delete, Report Name: Application Risk and Control-2016-09-14-1140, Format: HTML PDF XML CSV, Time Range: 2016/09/07 00:00-2016/09/13 23:59, Status: 0s.
- Bottom:** Return button.

Enfin, nous configurerons aussi une action quand une alerte sur un type de log est déclenchée. Dans le cadre de la nouvelle migration de l'infrastructure MALO, nous paramétrrons une action qui empêchera l'attaques de botnets si l'outil *FortiAnalyzer* en détecte. Pour se faire, ironsons dans *Event Management > Event Handler Lists* puis sélectionnerons l'agent par défaut *UTM App Ctrl Event* et cliquerons sur *Clone*. Nous remplirons ensuite les champs comme suit :

Clone Handler: UTM App Ctrl Event

Status	<input checked="" type="button"/> ON	
Name	Botnet App Ctrl Event	
Description	Botnet Application Control event handler	
Devices	<input checked="" type="radio"/> All Devices <input type="radio"/> Specify <input type="radio"/> Local Device	
Severity	Critical	
Filters		
Log Type	Application Control	
Group By	Application Name	
Logs match	<input type="radio"/> All <input checked="" type="radio"/> Any of the following conditions	
Log Field	Match Criteria	Value
Application Category	Equal To	Botnet
<input type="button"/> + <input type="button"/>		
Generic Text Filter 		
<input type="text"/>		
Notifications		
Generate alert when at least <input type="text"/> 1 matches occurred over a period of <input type="text"/> 30 minutes		
<input checked="" type="checkbox"/> Send Alert Email		
To	security@company.com	
From	admin@company.com	
Subject	Corporate_FGT	
Email Server	Corporate: smtp.company.com	
<input type="checkbox"/> Send SNMP(v1/v2) Trap		
<input checked="" type="checkbox"/> Send SNMP(v3) Trap <input type="text"/> Please select... <input type="button"/> +		
<input type="button"/> Factory Reset <input style="background-color: #0072bc; color: white; font-weight: bold; border-radius: 5px; padding: 2px 10px;" type="button"/> OK <input style="background-color: #fca82e; color: black; font-weight: bold; border-radius: 5px; padding: 2px 10px;" type="button"/> Cancel		

Nous pourrons ensuite voir tous les événements déclenchés de l'infrastructure MALO dans l'emplacement suivant : *Event Management > All Events* :



Tarification pour la gestion des logs

Puisque nous avons choisi de partir sur un paiement à l'utilisation, dans le cadre des logs infrastructure MALO, la tarification se basera principalement sur la quantité de données ingérées et analysées par le service *Azure Monitor*⁴⁶ & *Sentinel*⁴⁷.

Il est important de rappeler que les deux services cités ci-dessus sont liés. *Sentinel* utilise et passe par la plateforme *Monitor*, qui centralise et gère les logs système & sécurité via un stockage sur un espace de travail *Log Analytics*.

Pour calculer le coût de ces deux services dans une optique de paiement à l'utilisation, nous allons utiliser la calculette de prix de Azure. Tout d'abord, puisque le prix final dépendra de la volumétrie des logs générés, nous allons commencer par une estimation de 1 Go de logs sécurité et 1 Go de logs

⁴⁶ Tarification : [Tarification - Azure Monitor | Microsoft Azure](#)

⁴⁷ Tarification : [Prix d'Azure Sentinel | Microsoft Azure](#)

système journaliers ingérés par l'infrastructure Azure de la société MALO. Ce qui nous donnera un volume d'environ 30 Go de logs sur 30 jours pour chaque type de log. Commençons par le coût des logs système puis celui des logs sécurité :

Azure Monitor

RÉGION: West Europe

Log Analytics 77,87 €

Les données de journal quotidiennes ingérées dépendent de ce que vous supervisez avec Log Analytics. [En savoir plus](#) sur l'estimation des volumes de données.

Ingestion des données

1	x	30	x	2,69 €	=	67,33 €
Journaux quotidiens ingérés (Go/jour)		Jours		Par Go		

Cette estimation est calculée à l'aide du niveau tarifaire le plus optimal pour l'ingestion de données. Ce calcul utilise **Niveau Paiement à l'utilisation**. [En savoir plus](#) sur les niveaux tarifaires

Azure Sentinel

RÉGION: West Europe

Journaux ingérés

TYPE D'ESTIMATION DE LA TAILLE D'INGESTION: Journaux quotidiens ingérés

Journaux d'activité basiques

1	Par jour (Go)
---	---------------

Journaux d'activité analytiques

1	Par jour (Go)
---	---------------

Microsoft Sentinel est facturé en fonction du volume de données stockées dans Microsoft Sentinel et Azure Monitor Log Analytics. Cette estimation est calculée à l'aide des niveaux d'engagement les plus optimaux pour l'ingestion de données attendue. Ce calcul utilise un niveau d'engagement de Niveau Paiement à l'utilisation Go/jour sur Log Analytics et un niveau d'engagement de 0 Go/jour sur Microsoft Sentinel. L'utilisation d'Azure Logic Apps et de ressources supplémentaires pour les modèles BYOML (Bring Your Own Machine Learning) n'est pas incluse. L'utilisation des journaux de base et des archives de données peut entraîner des frais de requête et de recherche supplémentaires. Consultez la page de tarification de Azure Monitor pour plus de détails sur les frais de requête.

Azure Monitor – Ingestion des données

Journaux d'activité basiques

1	x	30	x	0,59 €	=	17,56 €
Par jour (Go)		Jours		Par Go		

Journaux d'activité analytiques

1	x	30	x	2,69 €	=	67,33 €
Par jour (Go)		Jours		Par Go/jour		

Microsoft Sentinel

Journaux d'activité basiques

1	x	30	x	0,45 €	=	13,51 €
Par jour (Go)		Jours		Par Go		

Journaux d'activité analytiques

1	x	30	x	2,34 €	=	70,25 €
Par jour (Go)		Jours		Par 0 Go/jour		

La prochaine étape sera de définir la stratégie de rétention des logs, en sachant que la société MALO aura 3 mois de rétention gratuite puisque nous avons souscrit à l'offre *Sentinel*. Et puisque nous

souhaitons une stratégie de rétention des logs système sur 6 mois, et 12 mois pour les logs sécurité, la tarification va être la suivante pour 1 Go journaliers :

Logs système :

Conservation des données 

30	x	6	x	0,12 €	=	10,68 €
Ingestion mensuelle totale en Go		Conservation totale (mois)		Par Go		

Logs sécurité :

Conservation des données 

30	x	12	x	0,12 €	=	32,05 €
Ingestion mensuelle totale en Go		Conservation totale (mois)		Par Go		

Nous arrivons donc à un total de 292,019 € par mois pour la gestion des logs sécurité et système avec une volumétrie de 1 Go journaliers générés par l'infrastructure MALO. Nous ajoutons à cela un quota de 100 SMS mensuels nécessaires aux alertes configurés pour la société MALO, dont les coûts sont les suivants :

Appel vocal et notifications SMS

 10 appels vocaux et 100 notifications SMS sont incluses gratuitement avec le code pays États-Unis (+1).

Code pays:

0	x	0,11709 €	=	0,00 €
Appels vocaux		Par appel		
100	x	0,04864 €	=	4,86 €
SMS		Par SMS		

Nous ajoutons également le coût de l'utilisation du service Azure Logic Apps pour les événements de sécurité majeurs. Puisque nous avons configuré une règle d'automatisation, le coût s'élèvera à 0,119€ par mois⁴⁸.

Pour rappel, ce coût total mensuel est une estimation qui va dépendre de la localisation, du type d'accord conclu avec Microsoft, la date d'achat et le taux de change en vigueur. La tarification est dégressive quand le volume de logs augmente. Nous conseillons donc à la société MALO de se rendre en fin de mois dans la rubrique *Utilisation et estimation des coûts* du service *Log Analytics* afin de mieux comprendre le détail de l'usage de chacune des ressources dont les logs sont ingérés sur la plateforme *Log Analytics*⁴⁹ :

⁴⁸ Détail des coûts du service Azure Logic Apps : [Tarification – Logic Apps | Microsoft Azure](#)

⁴⁹ Détail des coûts des logs ingérés dans *Log Analytics* : [Gérer l'utilisation et les coûts à l'aide des journaux d'activité Azure Monitor - Azure Monitor | Microsoft Docs](#)

Usage and estimated costs

[Usage details](#) [Daily cap](#) [Data Retention](#) [Help](#)

Your Log Analytics cost depends on your choice of pricing tier, data retention and which solutions are used. Here you can see the estimated monthly cost for each of the available pricing tiers, based on your last 31-days of Log Analytics data ingested. These cost estimates can be used to help you select the best pricing tier based on your data ingestion patterns. These estimates include the 500MB/VM/day data allowances if you are using Azure Security Center. If you have questions about using this page, contact us. Learn more about Log Analytics pricing.

Pricing Tiers

Pay-as-you-go Per GB

The Per GB 2018 pricing tier is a pay-as-you-go tier offering flexible consumption pricing in which you are charged per GB of data ingested. There are additional charges if you increase the data retention above the 31 day included retention (or 90 day included retention if using Sentinel on this workspace). Learn more about [Log Analytics pricing](#).

Estimated costs

Item type	Price	Monthly usage (last 31 days)	Estimated monthly cost
Log data ingestion	<price>	16.92 GB	<price>
Log data retention (beyond 31 days)	<price>	0.00 GB	<price>
Total			<total>

This is the current pricing tier.

Select

- 100 GB/day Commitment Tier**
15% discount over Pay-as-you-go
- 200 GB/day Commitment Tier**
20% discount over Pay-as-you-go
- 300 GB/day Commitment Tier**
22% discount over Pay-as-you-go
- 400 GB/day Commitment Tier**
23% discount over Pay-as-you-go

Usage Charts

Billable data ingestion per solution (last 31 days)

Data ingested per solution (last 90 days)

LogManagement: 58.76 GB
ContainerInsights/InfrastructureInsights/ServiceMap/VMInsights/LogManagement: 1.57 GB

Supervision

Introduction

Pour superviser l'infrastructure de la société MALO, nous allons également utiliser *Azure Monitor*, qui est la plateforme de gestion des logs et de monitoring de l'infrastructure native du cloud Azure. Puisque *Monitor* est natif de l'environnement Azure, il permet de mieux récolter les *metrics* de nos ressources Azure et de les mettre en forme, sans passer par un logiciel externe. De plus, comme nous avons pu le préciser pour la gestion des logs, l'outil d'Azure est complet et très personnalisable suivant les types de données que la société veut mettre en avant.

Cette personnalisation peut permettre de réduire les coûts, puisque nous pouvons choisir les données que nous souhaitons surveiller, et donc les données qui nous seront facturées

Présentation détaillée de la solution *Azure Monitor*

Comme nous avons pu le mentionner précédemment, *Azur Monitor* est la solution choisie pour la société MALO afin de traiter les différentes données de métriques générées par sa nouvelle infrastructure Azure. Chaque machine virtuelle, réseau virtuel, pare-feu et tout autre ressource génère des données qui peuvent être rassemblées et utilisées pour tirer des conclusions sur le fonctionnement de l'infrastructure.

Par exemple, il peut permettre à la société MALO de collecter des données d'utilisation du CPU de son serveur WEBAPP afin de mieux décider le nombre de Go à allouer à la RAM de la ressource virtuelle.

Création d'une Règle de Collecte des Données

Le fonctionnement de la collecte des données et de l'exploitation sont les mêmes que pour les logs, à savoir :

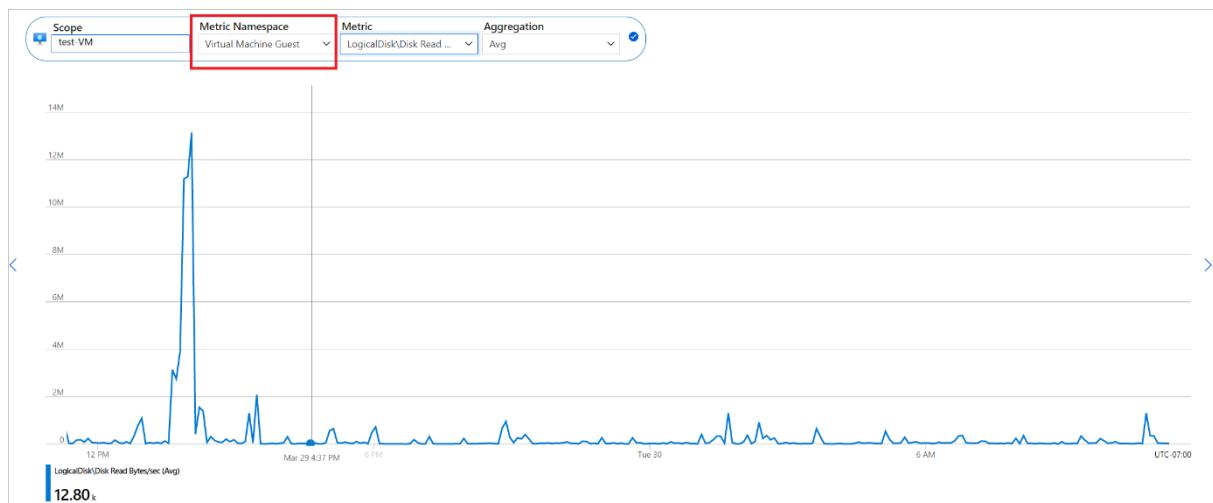
- Dans la création de la règle de collecte des données pour les logs des machines virtuelles montrées dans la précédente partie, nous ajouterons la collecte des données de type métrique sur les serveurs & sessions virtuelles Windows de la société MALO, à destination de son espace de travail *Log Analytics*.

- Il est important de noter que la collecte des *metrics* d'une machine virtuelle se fait automatiquement et peut être visualisée dans l'onglet *Metrics* de cette dernière. Cependant,

la création d'une règle de collecte des données permettra de rassembler en plus les métriques du système d'exploitation invité d'une machine virtuelle. Cela permettra donc d'obtenir plus de données pour une meilleure supervision des serveurs de la société MALO. Nous créerons cette règle et stockerons les données de supervision dans l'espace de travail déjà existant. La stratégie de rétention par défaut sera de 31 jours pour les données de supervision.

- Lors de la création de cette règle, l'agent *Azure Monitor* s'installera sur les ressources sélectionnées.
- Une fois ces étapes finalisées, nous nous rendrons dans l'onglet *Metrics* et commencerons à configurer la supervision en créant des alertes pour une ressource donnée⁵⁰ (ce que nous verrons après dans cette partie).

Azure Monitor Metrics Explorer a également la possibilité de créer des graphiques pour mettre en valeur les données choisies par la société MALO⁵¹. Une fois les quelques paramètres configurés, nous pourrons visualiser les données graphiquement et les importer sous un format Excel :



Activation de la fonctionnalité *Insights*

La fonction *Insights* permet également d'obtenir des informations détaillées et des conseils sur l'utilisation des ressources, ainsi que des prévisions en fonction de leur usage actuel⁵². Nous allons dans un premier temps activer la fonctionnalité sur les serveurs virtuels de la société MALO afin qu'elle puisse pleinement utiliser cet outil via l'interface *Azure Monitor*⁵³. Pour utiliser cette

⁵⁰ Tutoriel pour créer une alerte de type *Metrics* pour une ressource donnée : [Tutorial - Create a metric alert for an Azure resource - Azure Monitor | Microsoft Docs](#)

⁵¹ Comment utiliser *Metrics Explorer* pour mieux superviser son infrastructure : [Getting started with Azure metrics explorer - Azure Monitor | Microsoft Docs](#)

⁵² Explication de la fonctionnalité *Azure VM Insights* : [Qu'est-ce que VM Insights ? - Azure Monitor | Microsoft Docs](#)

⁵³ Comment activer la fonctionnalité *Insights* sur les machines virtuelles : [Activer la vue d'ensemble de VM Insights - Azure Monitor | Microsoft Docs](#)

fonctionnalité, nous allons la lier à l'espace de travail *Log Analytics*, qui est nécessaire afin de stocker les données générées par l'analyse de l'outil.

Logical Disk Performance

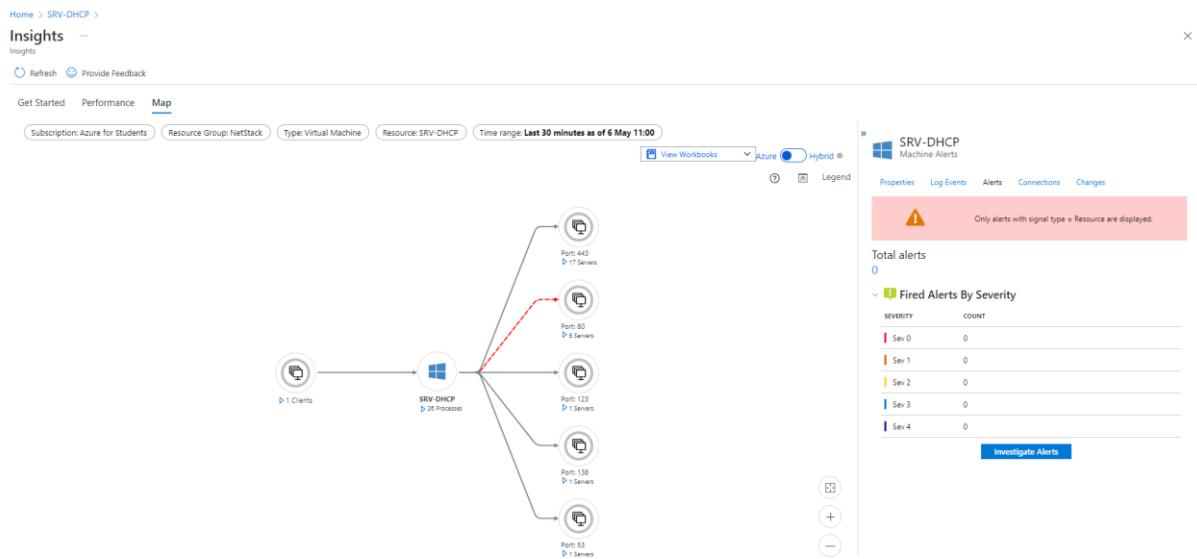
DISK	CURRENT SIZE (GB)	CURRENT USED (%)	P95 IOPS READ	P95 IOPS WRITE	P95 IOPS TOTAL	P95 MB/s READ	P95 MB/s WRITE	P95 LATENCY READ (ms)	P95 LATENCY WRITE (ms)	P95 LATENCY TOTAL (ms)	
C:	126.45	8%	352.08	53.83	394.87	16.39	1.39	17.78	8.55	34.2	13.63
D:	16	12%	0	0.29	0.29	0	0	0	0	0.18	0.18
Total	142.45	8%	352.08	53.86	394.87	16.39	1.39	17.79	8.55	34.32	13.75

Performance Metrics

- CPU Utilization %: 1m granularity. Average: 131%, 95th: 131%.
- Available Memory: 1m granularity. Average: 6.5GB, 95th: 6.1GB.
- Logical Disk IOPS: 1m granularity. Average: 6.5 IOPS, 95th: 6.1 IOPS.
- Logical Disk MB/s: 1m granularity. Average: 6.5 MB/s, 95th: 6.1 MB/s.

Nous pourrons ainsi voir tous les éléments essentiels au monitoring du serveur DHCP de la société MALO, tels que la taille du disque, l'utilisation du CPU, la mémoire disponible, les latences du disque et son utilisation.

Nous pourrons également obtenir la vue schématique de nos ressources et ses alertes comme suit :



Création d'alertes sur les serveurs virtuels

Comme nous avons pu le mentionner avant, il est possible de créer des alertes pour nos ressources, tout comme nous avons pu le faire pour les logs. Microsoft Azure nous propose déjà des règles d'alertes prédéfinies pour chaque serveur virtuel. Le processus est le suivant depuis la ressource virtuelle :

- Nous nous rendrons dans le serveur virtuel pour lequel nous voulons créer l'alerte, puis dans l'onglet *Overview*. Nous ironsons ensuite dans *Monitoring* puis cliquerons sur *Enable* :

- Nous allons laisser par défaut les alertes définies par Microsoft Azure et sélectionner la case *Email* :

SRV-DHCP

Alerts

Key Metrics

Notify me by

More alerting options

- Les alertes sont bien créées. L'équipe IT de la société MALO recevra bien des emails d'alerte si jamais un des paramètres d'alerte se déclenche :

SRV-DHCP

Alerts

Key Metrics

Notifications

Les types d'alertes que nous allons créer pour la société MALO auront un coût mensuel de 0,60€⁵⁴ par serveur virtuel. Donc un coût total de 3.6€ par mois pour l'ensemble des serveurs virtuels.

Tarification pour la supervision

Puisque la société MALO ne souhaite pas appliquer une stratégie de rétention des données de type métrique, il n'y aura presque pas de coûts engendrés par cette partie. Le coût de 0,60€ par mois sera le seul montant que la société aura à payer. Ainsi, il s'élèvera à 3,6€ par mois pour l'ensemble de ses machines virtuelles.

⁵⁴ Coût des alertes dans Azure Monitor : [Pricing - Azure Monitor | Microsoft Azure](#)

Coût d'intégration et de migration

Nous avons listé précédemment les potentiels coûts de chaque solution. Nous allons maintenant déterminer le coût de la main d'œuvre pour le projet de migration de l'infrastructure MALO vers la nouvelle architecture cloud Azure.

Pour rappel, les coûts sont les suivants et sont exprimés en hors taxes & par journée :

- Chef de projet = 950 Euros.
- Ingénieur / Administrateur = 650 Euros.
- Technicien = 350 Euros.

Nous allons déterminer le coût de cette main d'œuvre par partie.

Coût de la main d'œuvre pour la solution *Infrastructure as Code*

Pour rappel, les coûts d'acquisition sont nuls dans cette partie, du fait de la gratuité de la solution. Concernant les coûts de la main d'œuvre, un ingénieur système sera mobilisé pour effectuer les tâches suivantes :

- Création du compte GitHub de l'entreprise et des répertoires par thématiques.
- Création des *Secrets* Azure dans GitHub.
- Installation de *Github Desktop* et sa configuration avec le compte GitHub de l'entreprise sur les ordinateurs des membres de l'équipe IT (suivant qui y travaillera sur cette partie d'IaC).
- Création des scripts en amont pour l'installation des différents serveurs virtuels et des sous-réseaux associés.

Le coût total sera de 1 300 Euros hors taxes, puisque l'ingénieur passera deux journées sur ces tâches. Les modalités envisagées pour rendre autonome l'équipe IT seront présentées après cette partie.

Coût de la main d'œuvre pour la solution *Servicenow*

Pour rappel, les coûts d'acquisition des licences sont de 60 000 Euros TTC. L'ingénieur système aura les tâches suivantes à accomplir :

- Acquisition des licences auprès de Servicenow (opération effectuée au préalable).
- Création du/des comptes administrateur(s) Servicenow et configuration du compte de l'entreprise (nom personnalisé du service avec l'instance, emplacement...).
- Configuration du SSO avec Azure.
- Configuration du processus de découverte d'équipements Servicenow (2 *MID Server* déployés sur les machines virtuelles SRV-VB365 & SRV-PRINT) en collaboration avec l'équipe commerciale de Servicenow.

Le coût total pour ces opérations sera de 2 600 Euros hors taxes, soit quatre journées de travail passées à configurer le nouvel outil de gestion du parc & des tickets. L'entreprise MALO n'ayant pas

d'outil de ticketing et de gestion du matériel, cette partie tiendra plus de l'installation que de la migration.

Coût de la main d'œuvre pour les solutions de gestion des logs *Azure Monitor Logs*

Pour rappel, il n'y a pas de coût d'acquisition de licence particulier, puisque l'outil est gratuit dès lors qu'un abonnement Azure est en place. Les tâches suivantes seront à effectuer pour la gestion des logs système :

- Création de l'espace de travail *Log Analytics* pour stocker les logs système & sécurité de l'infrastructure nouvellement créée.
- Configuration de la redirection des logs de l'Azure AD vers ce nouvel espace de travail.
- Création d'une règle de collecte des données pour les logs des machines virtuelles & clients légers. L'ingénieur système va définir quels types de données seront collectées pour commencer. L'équipe IT de l'entreprise MALO pourra à l'avenir modifier ces règles.
- Configuration des requêtes et autres règles associées mentionnées dans la partie dédiée.
- Enfin, modification de la stratégie de rétention sur l'espace de travail pour la définir à 6 mois glissants (donc 180 jours) pour les logs système.

Pour les logs sécurité, les tâches seront les suivantes :

- Configuration du lien entre l'espace de travail et l'outil SIEM, afin que ce dernier puisse y stocker les logs sécurité.
- Configuration du connecteur de données pour permettre à l'outil SIEM de savoir quels types de données il doit collecter (connecteur *Azure AD*).
- Configuration des outils mentionnés dans la partie dédiée.
- Modification de la stratégie de rétention sur l'espace de travail (365 jours).

Le temps que l'ingénieur passe sur ces tâches sera de 2 jours, soit 1 300 Euros de main d'œuvre hors taxes.

Coût de la main d'œuvre pour la solution de supervision *Azure Monitor*

La solution *Azure Monitor* est, pour rappel, l'outil centralisé qui permet la supervision et la gestion des logs du cloud Azure. L'ingénieur système mobilisé sur l'installation de cet outil devra effectuer les tâches suivantes :

- Création de la règle de collecte des données (même règle utilisée que pour les logs système) et de l'espace de travail dédié aux données de supervision si la société décide de stocker les données de type métrique. Sinon, la stratégie de rétention par défaut est de 31 jours sans frais supplémentaires.
- Création des règles et requêtes mentionnées dans la partie dédiée.

Le coût total pour cette partie sera de 650 Euros hors taxes, soit une journée passée sur l'installation de la solution.

Coût de la main d'œuvre pour la solution de gestion des logs de l'infrastructure On-Premise

La solution *FortiAnalyzer* permettra à la société MALO de gérer et analyser les logs de sa nouvelle infrastructure réseau physique pour le site de Paris uniquement. Pour rappel, le coût de cet outil est de 7 300€. Concernant le détail de la main d'œuvre, l'ingénieur réseau devra effectuer les tâches suivantes :

- Configuration réseau de l'outil via un ordinateur portable.
- Branchements des câbles aux firewalls.
- Configuration d'une règle d'alerte pour les botnets et génération d'un premier rapport pour s'assurer que l'outil fonctionne correctement.

Le coût total de la main d'œuvre sera de 650€, soit une journée de travail.

Le coût total de la main d'œuvre des 4 parties évoquées plus haut sera donc de 6 500 Euros hors taxes. Ce coût s'ajoute aux divers coûts présentés dans chaque partie. Nous arrivons donc à un total de 37 347,43€ euros annuels la première année avec les coûts d'intégration, ou 3 112,25€ mensuels pour la partie Gouvernance. A partir de la deuxième année, le coût sera de 23 547,43€ annuel ou 1 962,2859€ mensuels.

Le tableau Excel suivant récapitule tous les coûts associés aux différentes parties ainsi que les coûts de main d'œuvre par partie :

Nom	Coûts fixes	Coûts d'intégration	Coûts annuels	Total
Infrastructure as Code	0,00 €	2 600,00 €	0,00 €	2 600,00 €
Gestion du Parc & Tickets	0,00 €	1 300,00 €	20 000,00 €	21 300,00 €
Supervision & Logs Cloud	0,00 €	1 950,00 €	3 547,43 €	5 497,43 €
Logs On Premise (FortiAnalyzer)	7 300,00 €	650,00 €	0,00 €	7 950,00 €
Total	7 300,00 €	6 500,00 €	23 547,43 €	37 347,43 €

Les coûts fixes représentent les coûts liés à d'éventuels acquisition de licences et/ou de matériel. L'outil de gestion des tickets et du parc étant un contrat négocié spécialement pour la société MALO, il n'y a pas de coûts fixes à proprement parlé (coût sur 3 ans de 60 000€).

La partie Supervision & Logs Cloud regroupe la solution centralisée de monitoring et gestion des logs et métriques essentielles de l'infrastructure cloud de la société MALO.

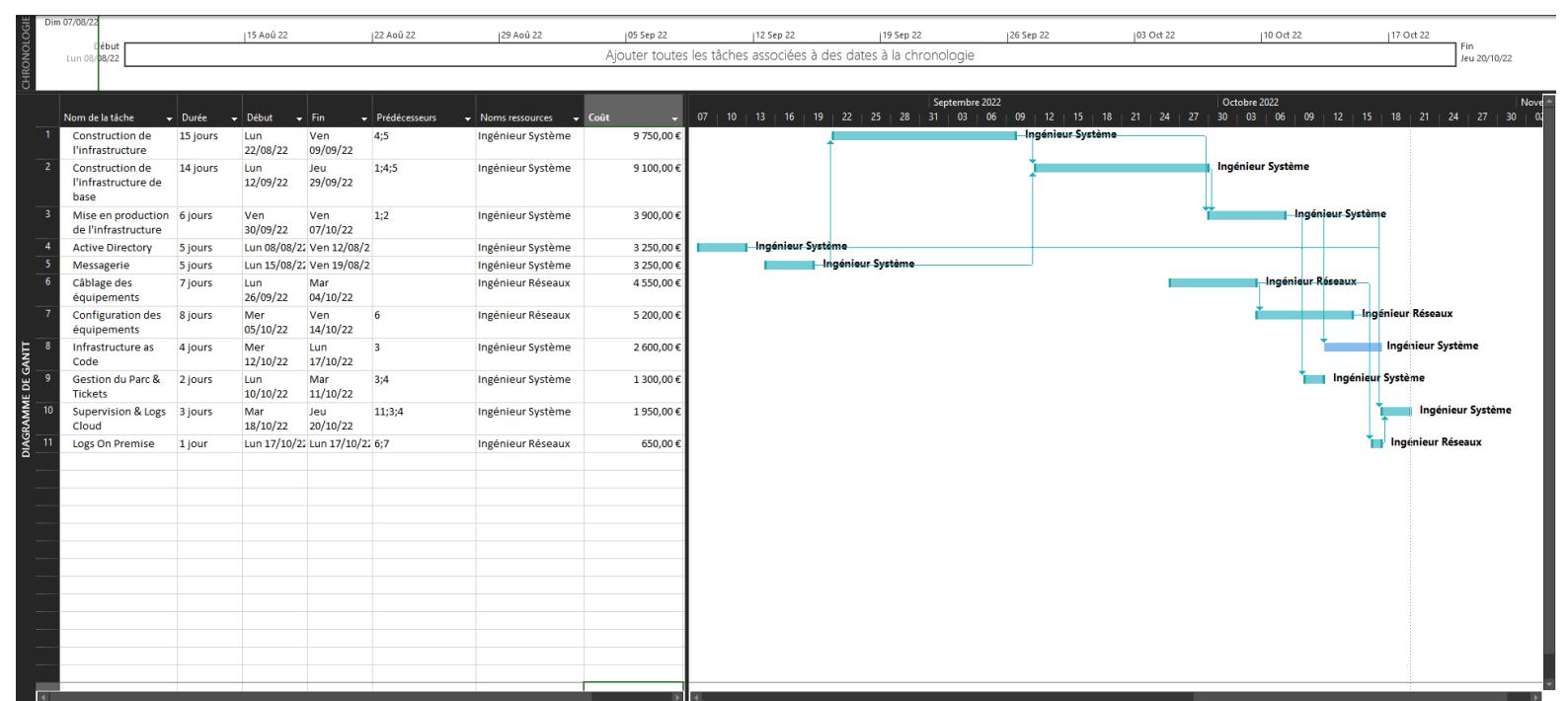
Planning de la migration

Nous avons réalisé deux diagrammes de GANTT pour planifier la migration de l'infrastructure MALO vers son nouveau parc informatique sur cloud Azure. Un diagramme de GANTT va préciser les tâches à effectuer et leurs coûts dans la globalité du projet, et un autre va quant à lui détailler la partie Gouvernance de la nouvelle infrastructure (*GANTT Gouvernance*).

Planning Gouvernance :

	Nom de la tâche	Durée	Début	Fin	Prédecesseurs	Noms ressources	Coût	19 Sep 22	L M M J V S D	26 Sep 22	L M M J V S D	03 Oct 22	L M M J V S D	10 Oct 22	L M M J V S D	17 Oct 22	L M M J V S D	24 Oct 22	L M M J V S D	31 Oct 22	L M M		
1	Infrastructure as Code	4 jours	Mer 12/10/22	Lun 17/10/22		Ingénieur Système	2 600,00 €																
2	Gestion du Parc & Tickets	2 jours	Lun 10/10/22	Mar 11/10/22		Ingénieur Système	1 300,00 €																
3	Supervision & Logs Cloud	3 jours	Mar 18/10/22	Jeu 20/10/22		Ingénieur Système	1 950,00 €																
4	Logs On Premise	1 jour	Lun 17/10/22	Lun 17/10/22		Ingénieur Réseaux	650,00 €																

Planning global :



Modalités pour rendre autonome l'équipe IT de la société MALO

Un SharePoint partagé sera mis en place pour permettre à l'ingénieur système d'alimenter le site avec des procédures pour la mise en œuvre d'actions concernant chacune des parties citées plus haut : [NetStack - Accueil \(sharepoint.com\)](#)

Les procédures de base décrites dans ce document seront stockées dans le SharePoint ainsi que d'autres procédures qui pourront être créées à la demande par l'ingénieur système (l'ensemble de ces procédures seront également facturées sur la même base de tarification que pour l'installation des différentes parties).

Sur ce même SharePoint, d'autres liens et documents de référence seront fournis pour aider l'équipe IT de la société MALO à monter en compétences sur les divers sujets de sa nouvelle infrastructure. Voici quelques exemples de liens de documentation :

- Pour la partie *Infrastructure as Code* :
 - GitHub : [GitHub Documentation](#)
 - VS Code : [Documentation for Visual Studio Code](#)
 - Modèle ARM : [Modèles de démarrage rapide Azure \(microsoft.com\)](#)

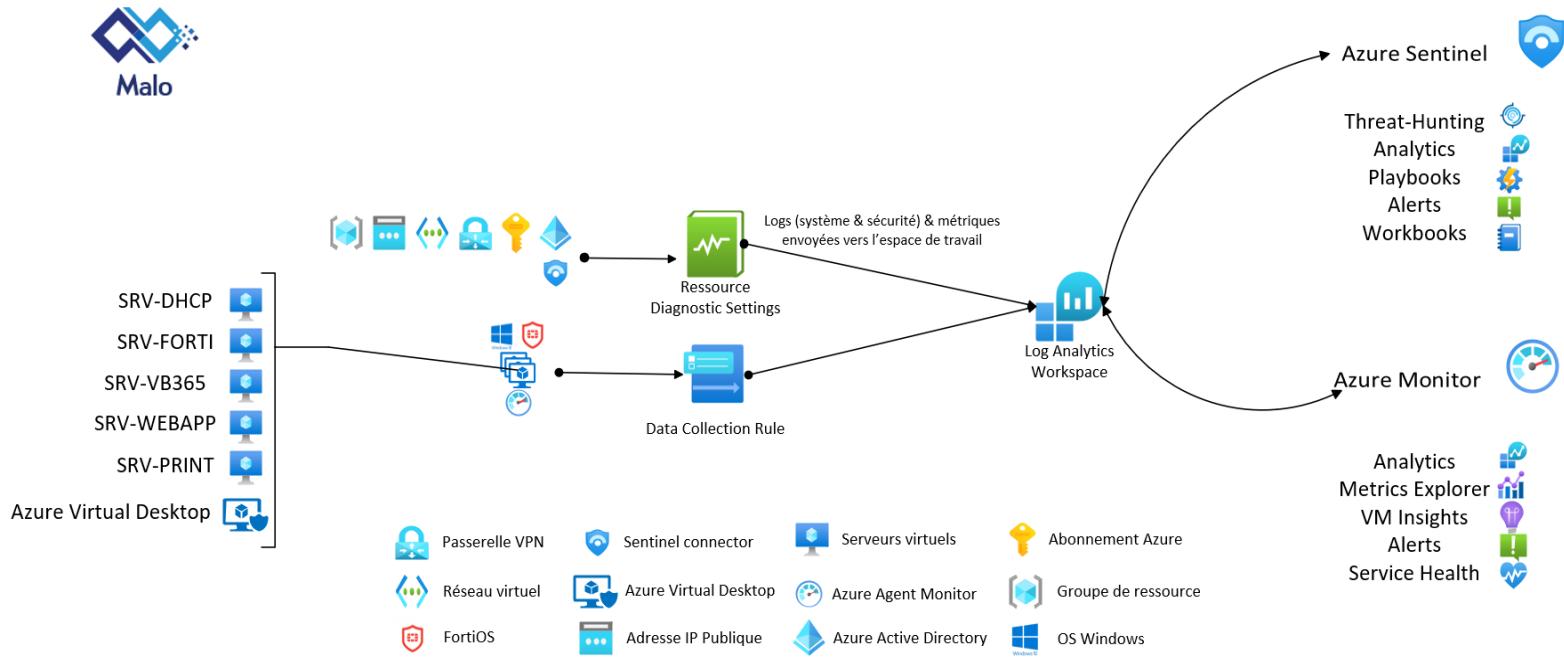
- Créer son premier modèle ARM : [Tutoriel - Créer et déployer un modèle - Azure Resource Manager | Microsoft Docs](#)
- FAQ pour les modèles ARM : [Forum aux questions sur le Modèle Resource Manager | Microsoft Docs](#)
- Pour la partie *Servicenow* (Ticketing & Asset Management) :
 - Documentation de Servicenow : [Product Documentation | ServiceNow](#)
 - Configuration du SSO avec Azure AD : [Tutoriel : Intégration de l'authentification unique Azure Active Directory à ServiceNow | Microsoft Docs](#)
 - Plus de détails sur le *MID Server* et son fonctionnement : [MID Server | ServiceNow Docs](#)
- Pour la partie *Gestion des logs et Supervision* :
 - Documentation générale de Azure : [Documentation Azure | Microsoft Docs](#)
 - Vue d'ensemble du fonctionnement des logs dans Azure : [Azure Monitor Logs - Azure Monitor | Microsoft Docs](#)
 - Documentation sur l'outil SIEM de Azure : [Documentation Microsoft Sentinel | Microsoft Docs](#)
 - Calculatrice de prix Azure : [Outil de calcul de tarification | Microsoft Azure](#)
- Pour la partie *Gestion des logs sécurité On-Premise* :
 - Fonctionnalités du modèle *FortiAnalyzer* : [FortiAnalyzer Data Sheet \(fortinet.com\)](#)
 - Documentation technique du produit : [FortiAnalyzer | Fortinet Documentation Library](#)
 - Guide complet des fonctionnalités de l'outil : [Administration Guide | FortiAnalyzer 7.0.3 | Fortinet Documentation Library](#)

En plus de ces liens, le présent document contient également des références aux documents utilisés pour détailler les solutions présentées ci-dessus.

Des cours théoriques pourront être dispensés par les ingénieurs système & réseaux pour mieux aider l'équipe IT de la société MALO à prendre en main cette nouvelle infrastructure. La tarification sera la même que pour la mise en place du projet.

Schéma récapitulatif

Dans le schéma ci-dessous, nous avons représenté les 3 grandes solutions qui constitueront la partie Gouvernance de l'infrastructure MALO :



Nous avons d'une part les machines virtuelles & nos clients légers (via *Azure Virtual Desktop*) qui vont être configurées via une DCR (*Data Collection Rule*) pour obtenir plus de logs sur non seulement le système hôte mais également le système invité via l'agent *Monitor*. Ces informations vont être envoyées sur l'espace de travail *Log Analytics*.

Concernant les paramètres de diagnostic, ils seront activés sur toutes les ressources sauf les machines virtuelles & clients légers, afin d'obtenir notamment les logs de l'Azure AD (logs de connexion des utilisateurs & activité de l'*Active Directory*). Le tout sera également envoyé vers l'espace de travail de la société MALO.

C'est donc dans notre espace de travail que se retrouvera toutes les données d'infrastructure. Et à partir de cet espace de travail, les deux outils *Azure Monitor* et *Azure Sentinel* vont pouvoir puiser dans ces données, nécessaires au bon fonctionnement des services tels que *Insights*, *Alerts* et *Playbook*.

Le connecteur Sentinel *Azure Active Directory* va permettre de récupérer tous les logs au niveau de l'AD, et donc des ressources de la société MALO. Un connecteur *Azure Activity* est également disponible pour obtenir des logs détaillés de l'activité Azure.

Il est important de rappeler que l'utilisation des deux outils cités précédemment est gratuite dès lors qu'un compte Azure est actif. Le coût sera déterminé en fonction de la quantité de données stockées sur notre espace de travail et de son utilisation par les deux services, ainsi que de sa stratégie de rétention.

Schéma global

