Agents Azure

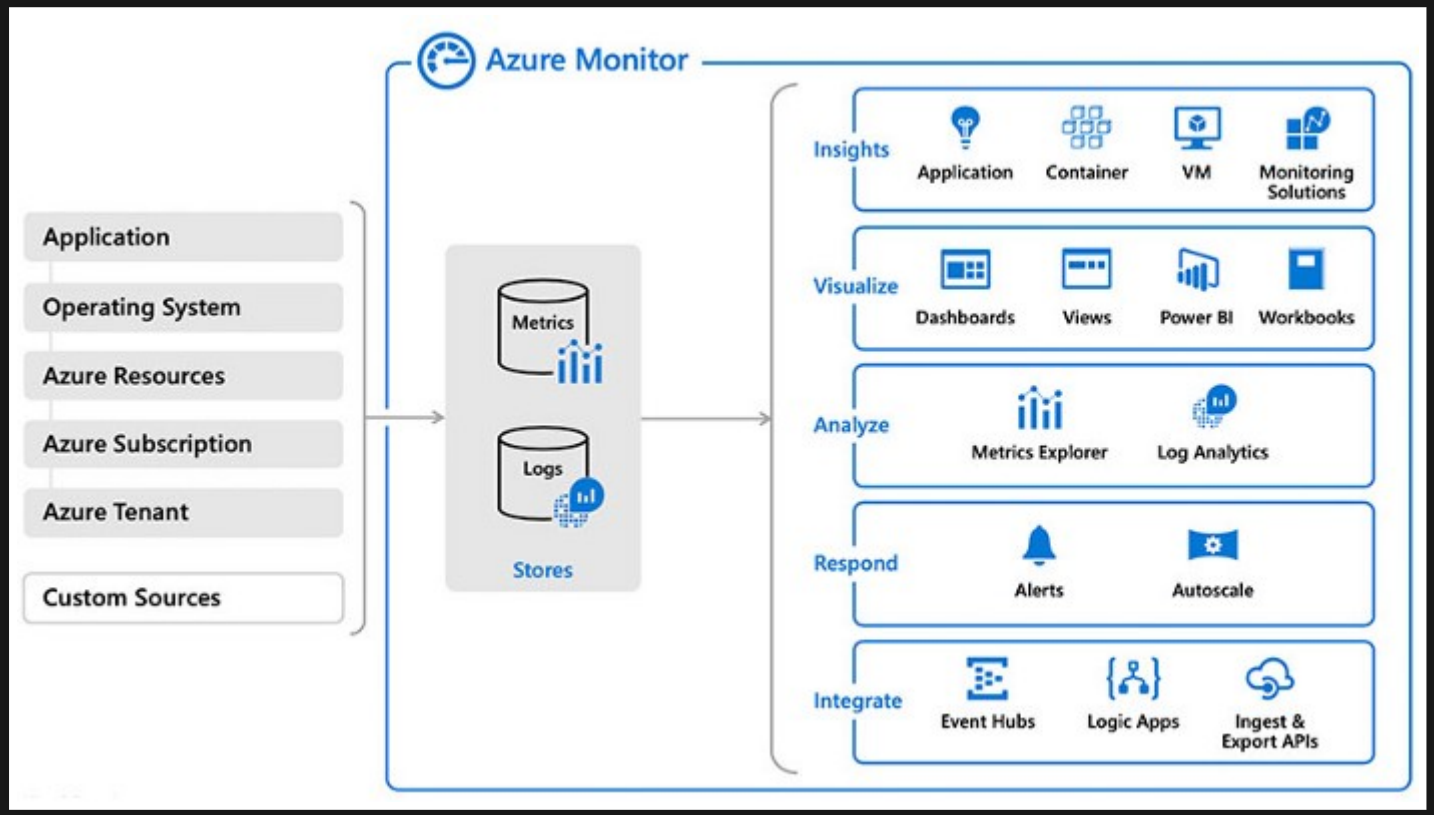
Objectifs

- Etudier les différents agents que propose Azure pour la collecte des métriques et logs customs des VMs afin de répondre à un besoin spécifique d’analyse et d’alerting via **Azure monitor**
- Tester un agent recommandé par le cloud provider

Azure monitor

Azure monitor offre une solution pour collecter, analyser et exploiter les données…

Azure monitor overview



Azure monitor permet ? (1/2)

Métriques:

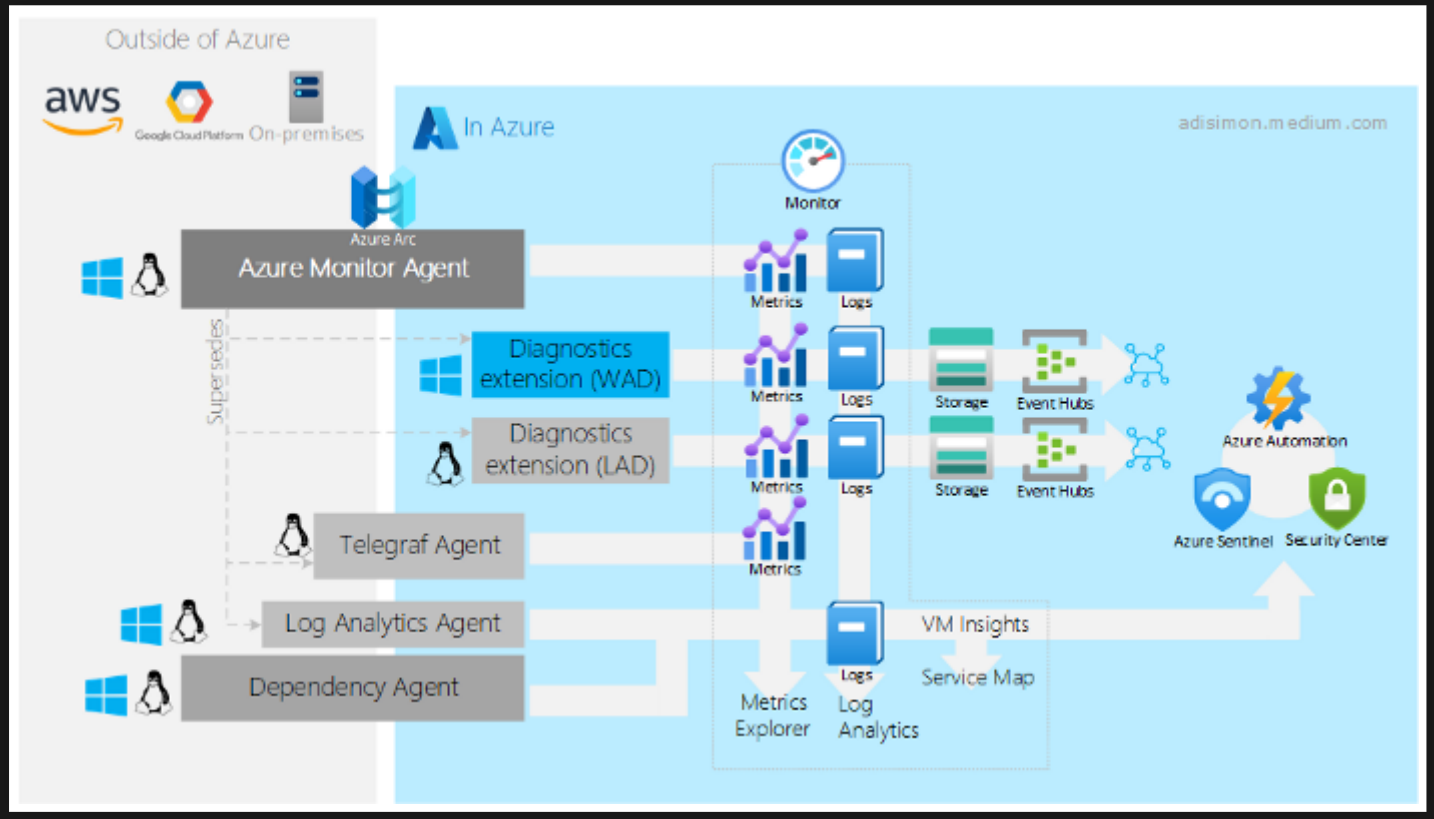
- Stockées dans une base de données de série chronologique
- Rétention : 93 jours
- Visualisation/Analyse dans Metrics Explorer

Azure monitor permet ? (2/2)

Logs :

- Stockés dans Log Analytics Workspace
- Rétention : Au miminum 30 jours, au maximum 730 jours (configurable dans Log Analytics Workspace)
- Visualisation/Analyse dans Log Analytics

Agents Overview: In Azure / Outside of Azure



Les différents agents

- Agent Azure Monitor
- Extension Diagnostics Azure
- Agent Log Analytics
- Agent Telegraf

Agent Azure Monitor (AMA)

Agent Azure Monitor (AMA)

- Nouvel agent unifié : prévu pour remplacer les autres agents
- Collecte des données de supervision auprès de la VM de Azure et les délivre à Azure Monitor
- Il peut envoyer des données aux Journaux Azure Monitor et aux Métriques Azure Monitor

Installation & Configurations requises

- Règles de collecte de données (DCR=Data Collection Rules)
- Une DCR est constituée de :
  - resource(s)
  - source(s) de données (performances, logs)
  - destination(s)

Resources

- VMs pour lesquelles on veut collecter les données

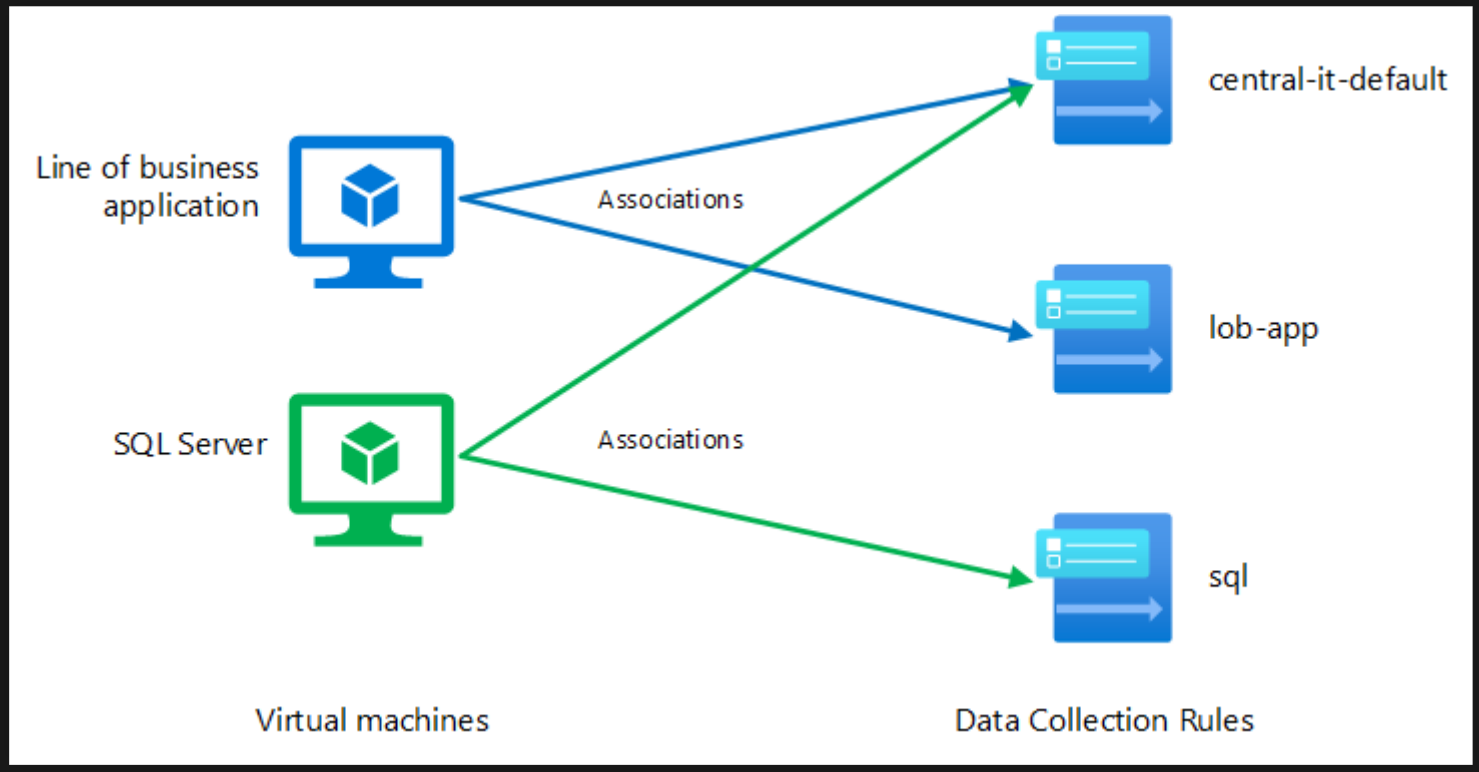
Sources de données

- performances :
  - CPU
  - Memory
  - Disk
  - Network
- logs : syslog (Linux) et event log (Windows)

Destination

- performances : dans log analytics workspace ou/et métriques
- logs : dans log analytics workspace

- Affectation des DCR aux différentes machines :



Installation & Configurations requises

Différentes solutions pour créer la DCR :

- Utilisation du portail
- Utilisation de PowerShell
- Utilisation de la CLI azure
- Utilisation de Azure policy (permet de faire du déploiement de masse)

Une fois que la DCR est crée avec l’association à la VM, l’agent Azure Monitor est automatiquement installé et une identité managée est créée pour la VM

Fonctionnalités

- fonctionne pour Windows et Linux
- possibilité de filtrer les données collectées (performances et logs)
- peut collecter des données sur des VMs en dehors d'Azure (avec l'aide d'Azure Arc)
- multi-homing : les logs et compteurs de performances peuvent être envoyés à plusieurs workspaces Log Analytics

Limitations

- Logs : pas de collecte des logs basés sur les fichiers, uniquement syslog ou event windows (actuellement uniquement en préversion privée)
- Pas de métriques applicatives collectées
- Pas encore de prise en charge des Event Hubs et des comptes de stockage en tant que destinations.

Empreinte Mémoire/CPU

Linux :

- Plusieurs processus lancés
- Mémoire : 200MB
- CPU : 2% pour 1CPU

Windows :

- Plusieurs processus lancés
- Mémoire : 100MB
- CPU : 0

Extension Diagnostics Azure

Fonctionnalités

- fonctionne pour Windows et Linux
- capacité d’envoyer les logs et les métriques au stockage azure : permet de conserver les logs pendant plus longtemps (azure monitor : 730 max, azure storage indéfiniment)
- capacité d’envoyer les données à Event hubs (service d’ingestion de données en temps réel)

Liste des données collectées

- Compteurs de performance
- Logs :
  - Syslog (linux)
  - Events (windows)
  - Fichiers de logs

Limitations

- Impossibilité de collecter des données sur des VMs en dehors d’Azure
- Configuration pour chaque machine virtuelle : difficile de gérer les configurations de façon centralisée

Agent Log Analytics

- Les agents Log Analytics sont en voie de dépréciation et ne seront plus pris en charge à partir du 31 août 2024. 😿

Fonctionnalités

- fonctionne pour Windows et Linux
- peut collecter des données sur des VMs en dehors d'Azure
- plus de sources de données possibles en faisant des confs particulières : données de CollectD, donnés JSON personnalisées

Liste des données collectées

- Compteurs de performance
- Logs :
  - Syslog (linux)
  - Events (windows)
  - Fichiers de logs

Limitations

- Facilité à configurer de manière centralisée mais difficulté d’établir des définitions indépendantes pour différentes machines virtuelles
- Dépréciation

Agent Telegraf

Fonctionnalités

- Peut collecter des données sur des VMs en dehors d'Azure
- Plusieurs plugins input → permet de récupérer des métriques OS ainsi que des métriques applicatives
- Envoie des métriques à l'aide du plug-in de sortie Azure Monitor

Liste des données collectées

- Métriques OS
- Métriques applicatives

Limitations

- Peut être installé seulement sur Linux ?? (d’après la doc Azure) 😕

Tableau récapitulatif

https://confluence.corp.cloudwatt.com/display/CAAS/Agents+A

Recommandations globales

- Utiliser l’agent Azure monitor si les limitations ne sont pas bloquantes
- Si les limitations sont bloquantes, combiner avec un autre agent
- Faire attention à la duplication des données si on combine plusieurs agents