

Projet SDCI

Oral de présentation

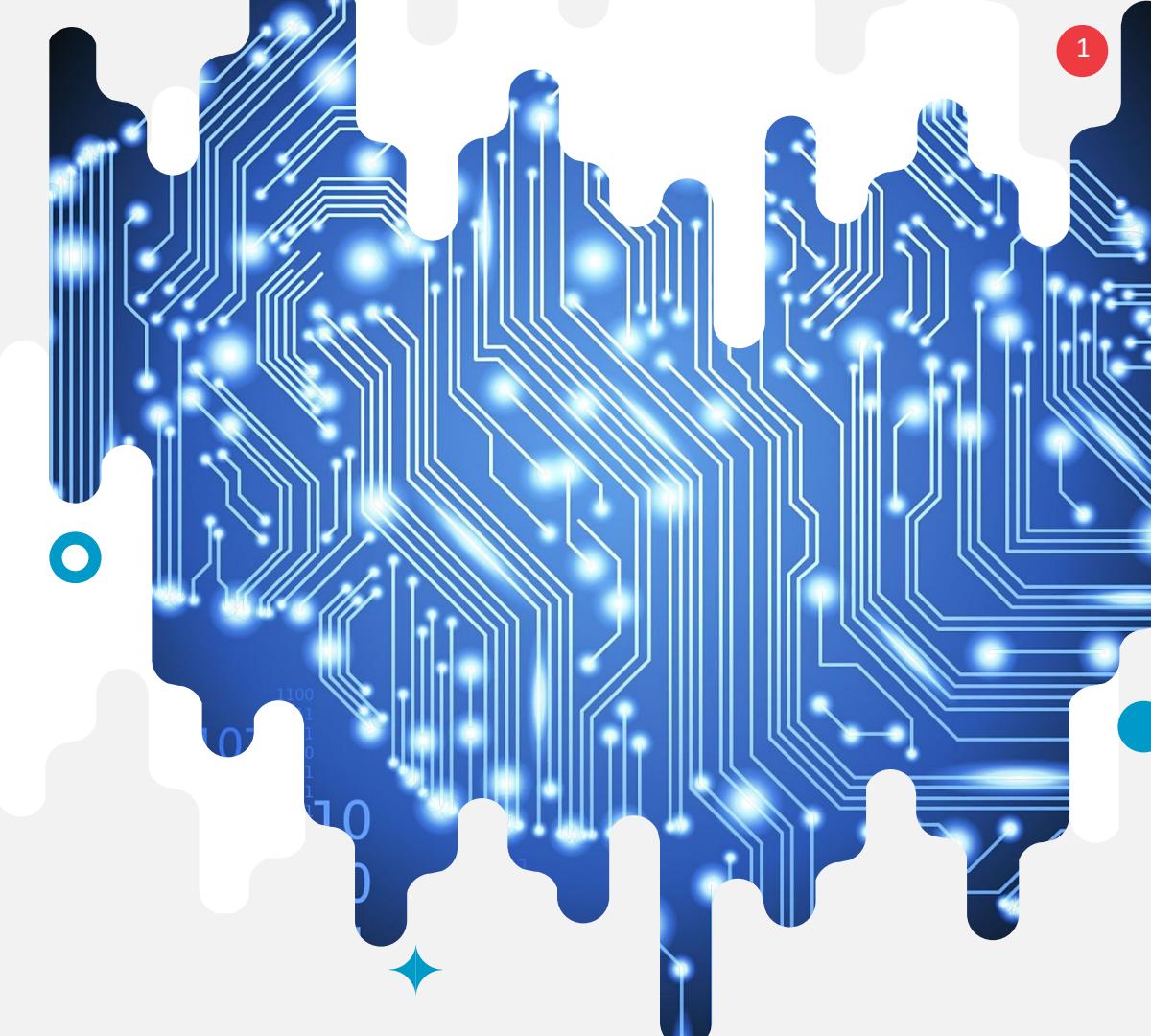
À l'attention de M. Chassot et M. Medjia

Travail réalisé par :

Florian CLANET

Rama DESPLATS

Yuxiao MAO

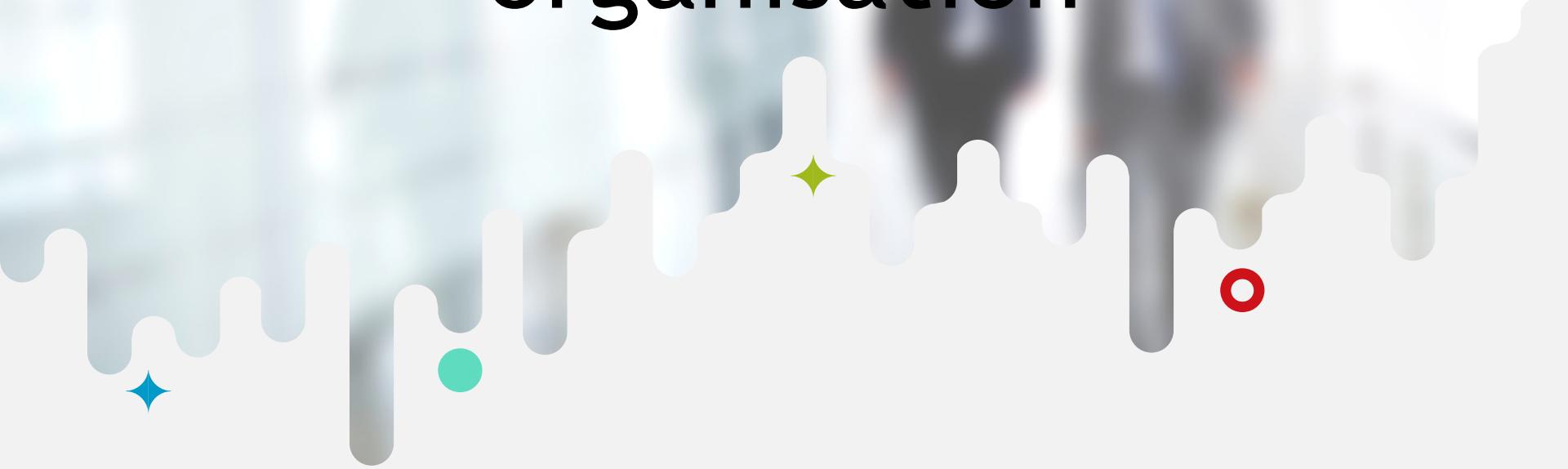




Sommaire

- 01 | Notre équipe et son organisation
- 02 | La conception du projet
- 03 | Nos choix d'implémentations

Notre équipe et son organisation



Rencontrez notre équipe



Rama DESPLATS

INSA-TSM-Contrat Pro



Florian CLANET

INSA-TBS



Yuxiao MAO

INSA-TSM

Notre organisation

Une organisation compliquée mais de qualité



Les rencontres virtuelles plutôt que physique

Au vu de nos emplois du temps jamais synchronisés, nous ne nous sommes retrouvés que **3 fois en vrai**



Se servir de nos doubles cursus

Afin de maximiser l'efficacité de notre groupe, nous nous sommes servis des **méthodes agiles** pour gérer le projet



S'autoformer pour monter en compétences

Avant même de commencer le projet, nous avons dû nous former pour acquérir les compétences des étudiants de la formation initiale



L'utilisation de gestionnaire de code en ligne

Afin de partager notre travail et de toujours rester synchronisé, nous nous sommes servis de **Git**



Favoriser l'entraide et la discussion

Nous avons choisi de réaliser des **bi-weekly meetings** pour toujours garder une vue d'ensemble de l'avancée du projet et de faire remonter les problèmes potentiels



Assister les autres dans leur formation

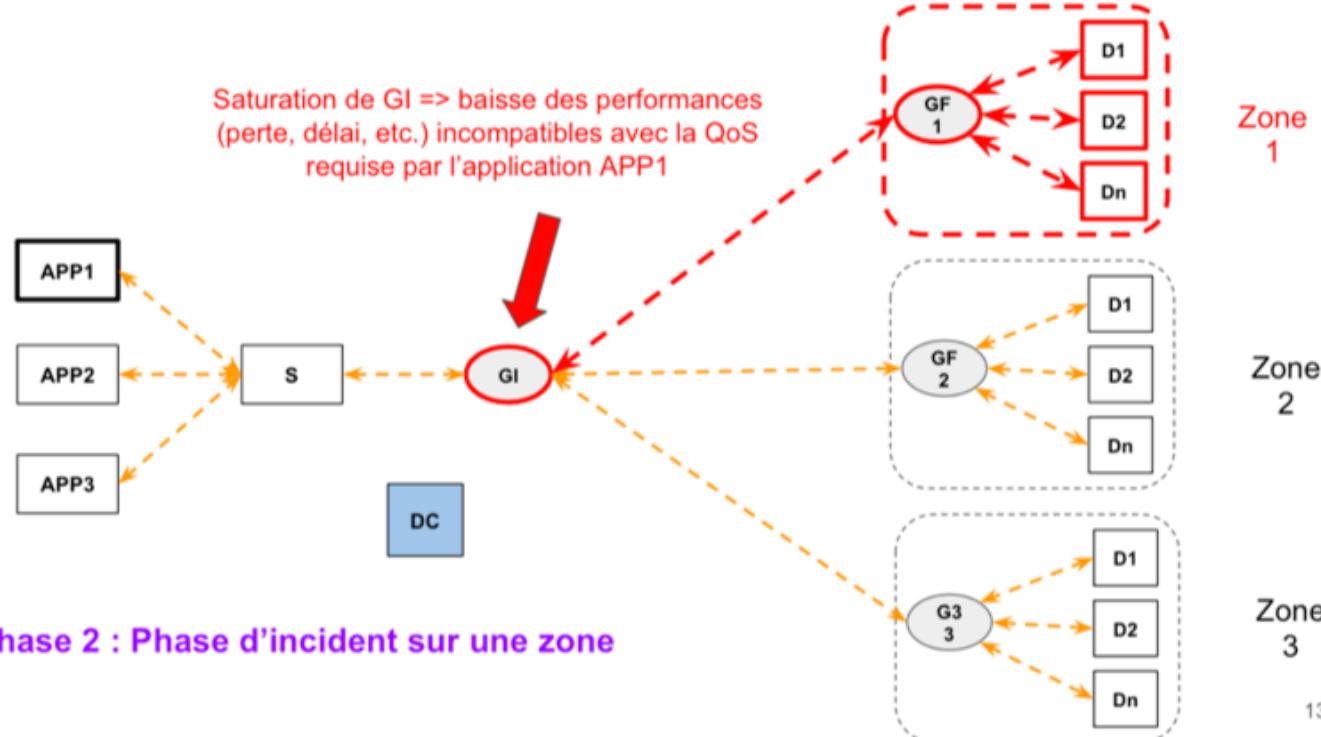
Certains d'entre nous avaient des acquis vis à vis de certains modules de cours, nous avons donc pu apporter notre expérience pour favoriser la montée en compétences des autres

La conception du projet



Remise en situation

Activité IoT ciblée : Activité de supervision/intervention à distance de \neq Incident sur la zone 1 => trafic zones dotées de capteurs / actionneurs (Di), par le biais d'une application supplémentaire générée par les Di (APP1)



Description des UC

Étape 1 - Gestion par l'administrateur



Déploiement d'une gateway intermédiaire

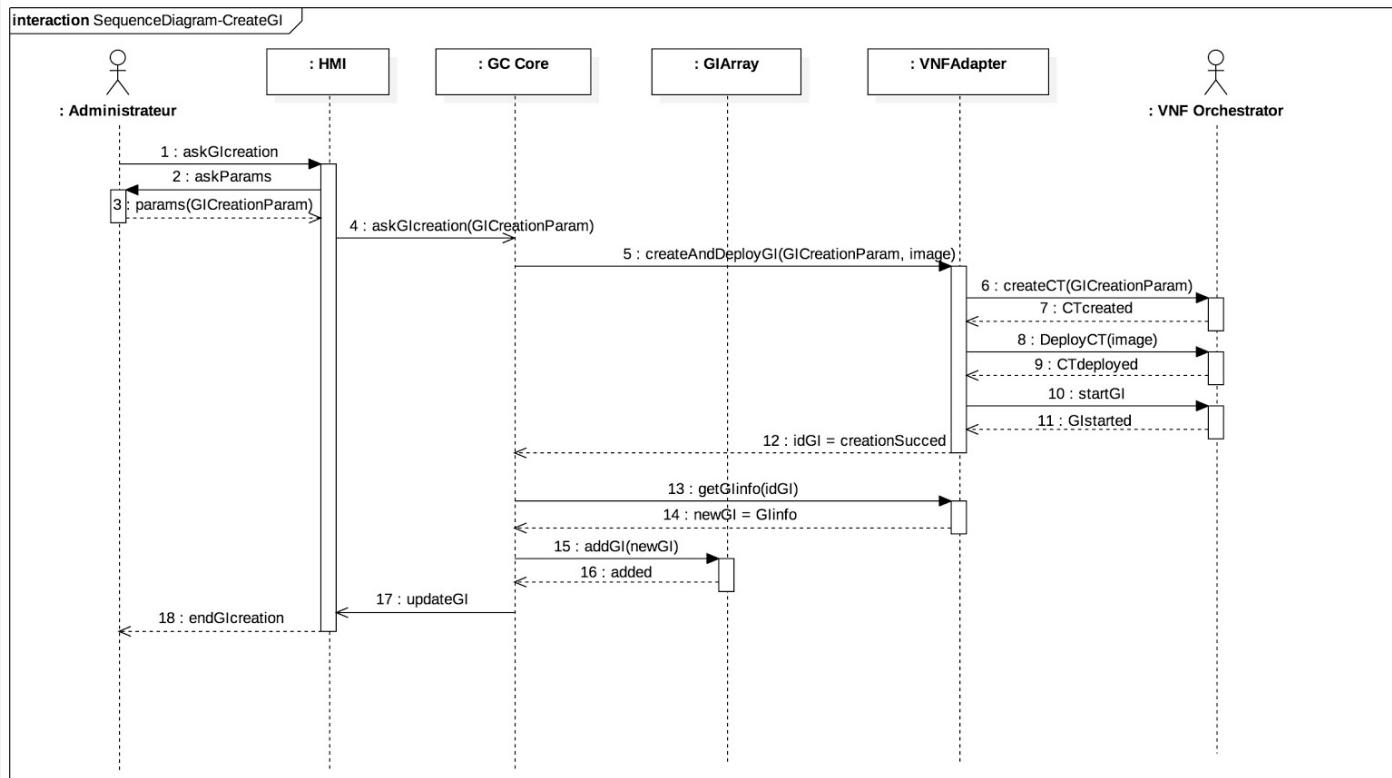
Lorsque l'administrateur constate une dépréciation des qualités de services, il peut déployer une gateway intermédiaire afin de rétablir les qualités de services initiales.



Suppression d'une gateway intermédiaire

Lorsque l'administrateur constate que les qualités de services sont revenues à la normale et que la gateway n'est plus nécessaire, il peut supprimer une gateway intermédiaire afin de réduire la dépense de ressources inutile par le datacenter.

Déploiement d'une gateway intermédiaire



Description des UC

Étape 1 - Gestion par l'administrateur



Créer une nouvelle règle de redirection



Editer une règle de redirection

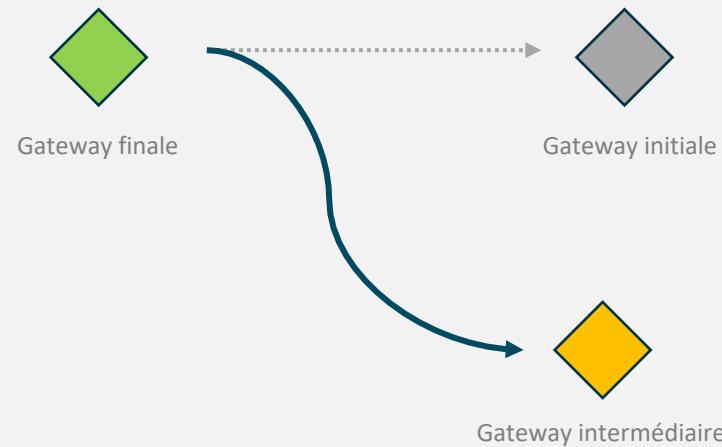


Supprimer une règle de redirection

Gestion des règles de redirection



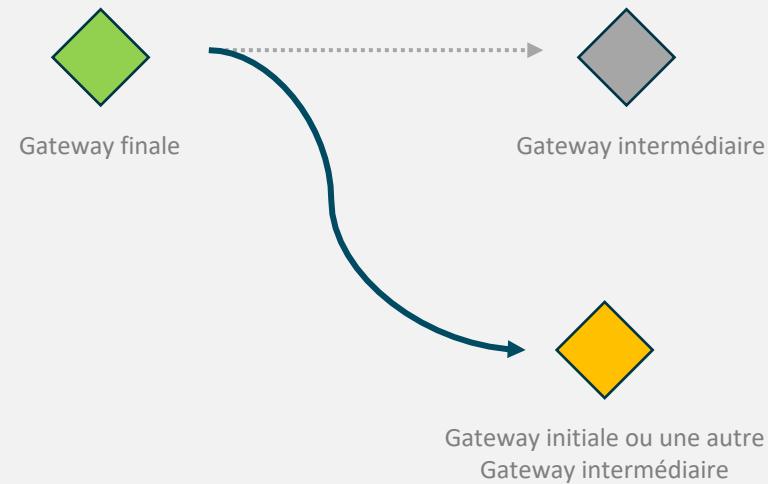
Créer une nouvelle règle de
redirection



Gestion des règles de redirection



[Editer une règle de redirection](#)



Gestion des règles de redirection



[Editer une règle de redirection](#)

Edit a link

Please select an intermediate gateway and a final gateway

Final Gateway : GF Zone 3

Intermediate Gateway : rz

rz
tzsd

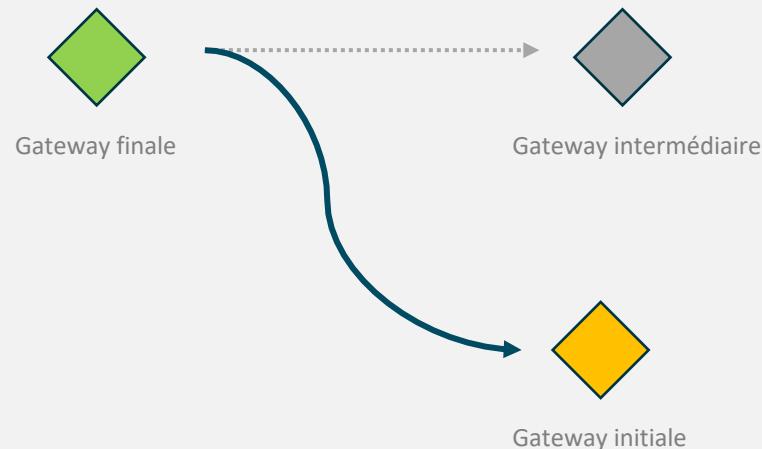
Cancel Edit

A modal dialog titled "Edit a link". It contains two dropdown menus. The first dropdown under "Final Gateway" is set to "GF Zone 3". The second dropdown under "Intermediate Gateway" has "rz" selected, with another option "tzsd" visible below it. At the bottom right of the dialog are "Cancel" and "Edit" buttons.

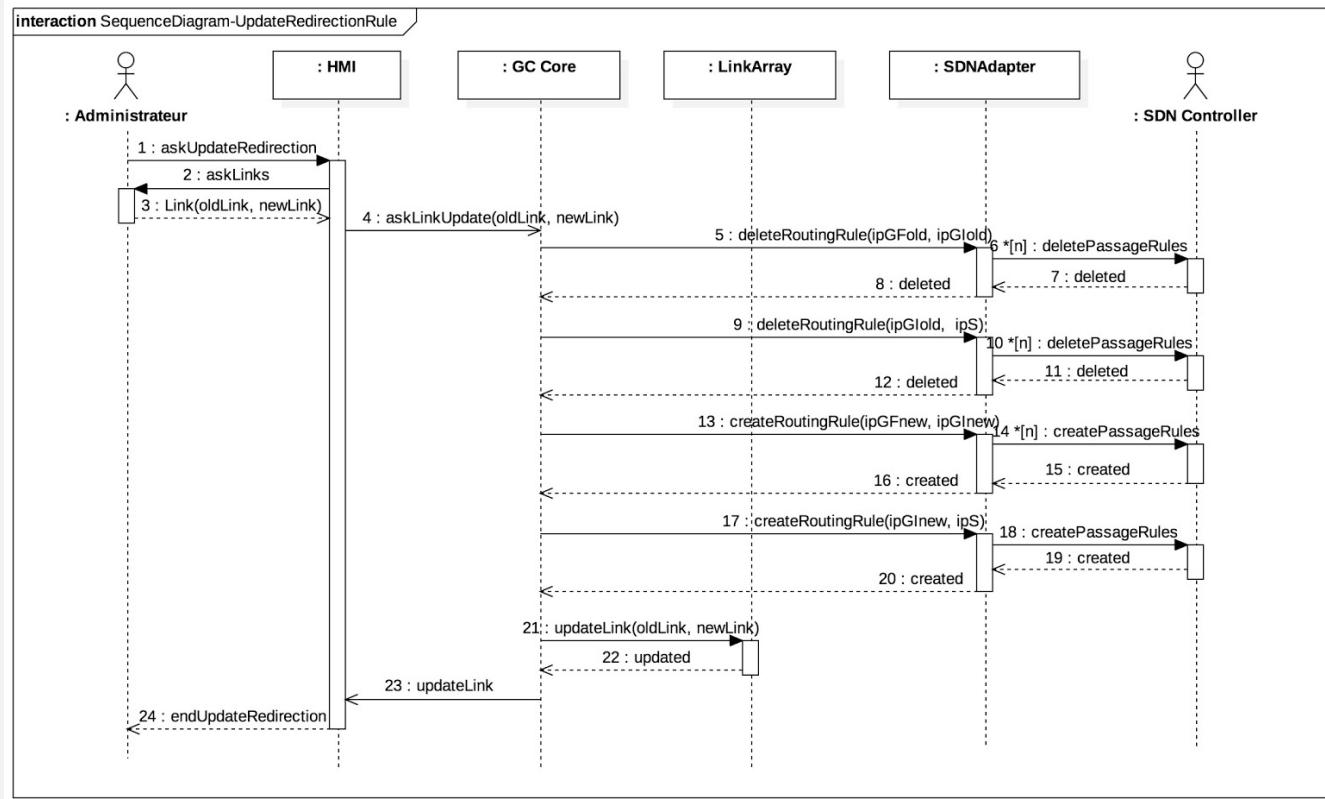
Gestion des règles de redirection



Supprimer une règle de
redirection



Gestion des règles de redirection



Description des UC

Étape 2 - Gestion automatique par le système



Initialisation des politiques par défaut du manager automatique

Le système mis en place doit être en mesure d'initialiser les politiques par défaut permettant au manager automatique de réguler le réseau. Cela afin de pouvoir analyser le réseau sans que l'administrateur n'ait à entrer ces politiques au préalable.

Initialisation des politiques par défaut



01 Période d'analyse de 3 min

02 Déduit les valeurs par défaut pour les métriques à analyser

03 Définition de la valeur acceptable et de la valeur maximum acceptable (valeur maximum = valeur acceptable + 20%)

Initialisation des politiques par défaut



01 Période d'analyse de 3 min

02 Déduit les valeurs par défaut pour les métriques à analyser

03 Définition de la valeur acceptable et de la valeur maximum acceptable (valeur maximum = valeur acceptable + 20%)

- Exemple -



Résultat de l'analyse:

Nombre de paquets sortant pour les GF : 200
Nombre de requêtes faites par le serveur : 150
Pourcentage d'utilisation de la CPU des GI : 70

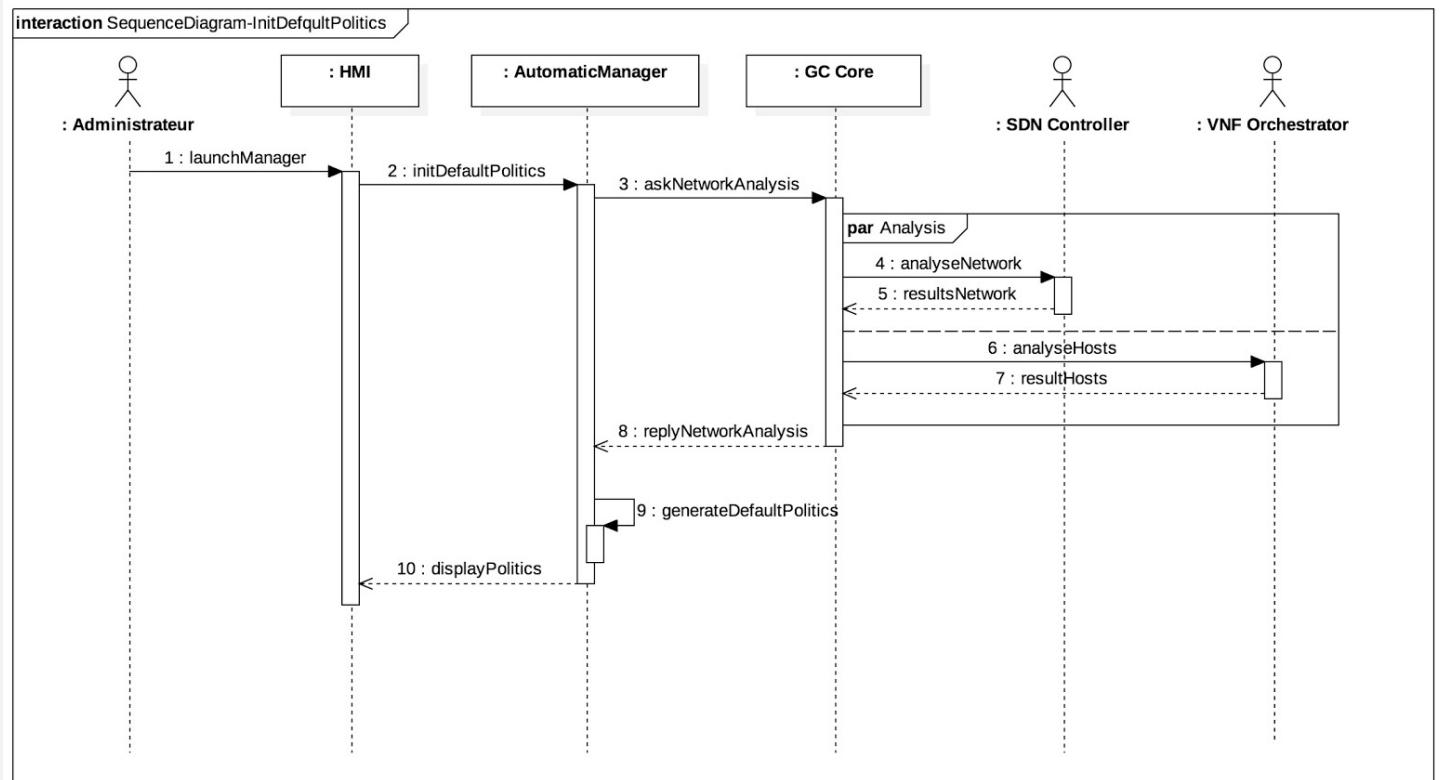
Période d'analyse de 3 min



Les limites sont donc, respectivement, 240, 180 et 84.

Lors de la prochaine analyse, si le nombre de paquets sortant pour la GF1 est de 242 alors une **alerte** sera levé et une **action corrective** sera prise

Initialisation des politiques par défaut



Description des UC

Étape 2 - Gestion automatique par le système

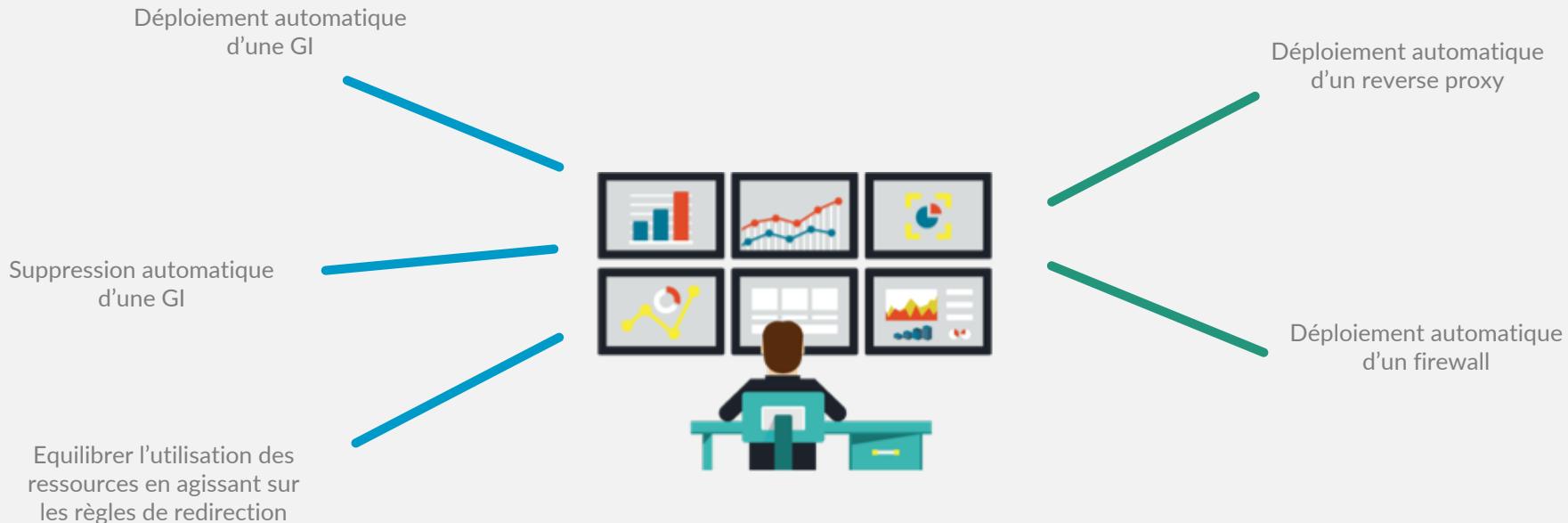


Monitoring automatique de l'état du système par le manager automatique

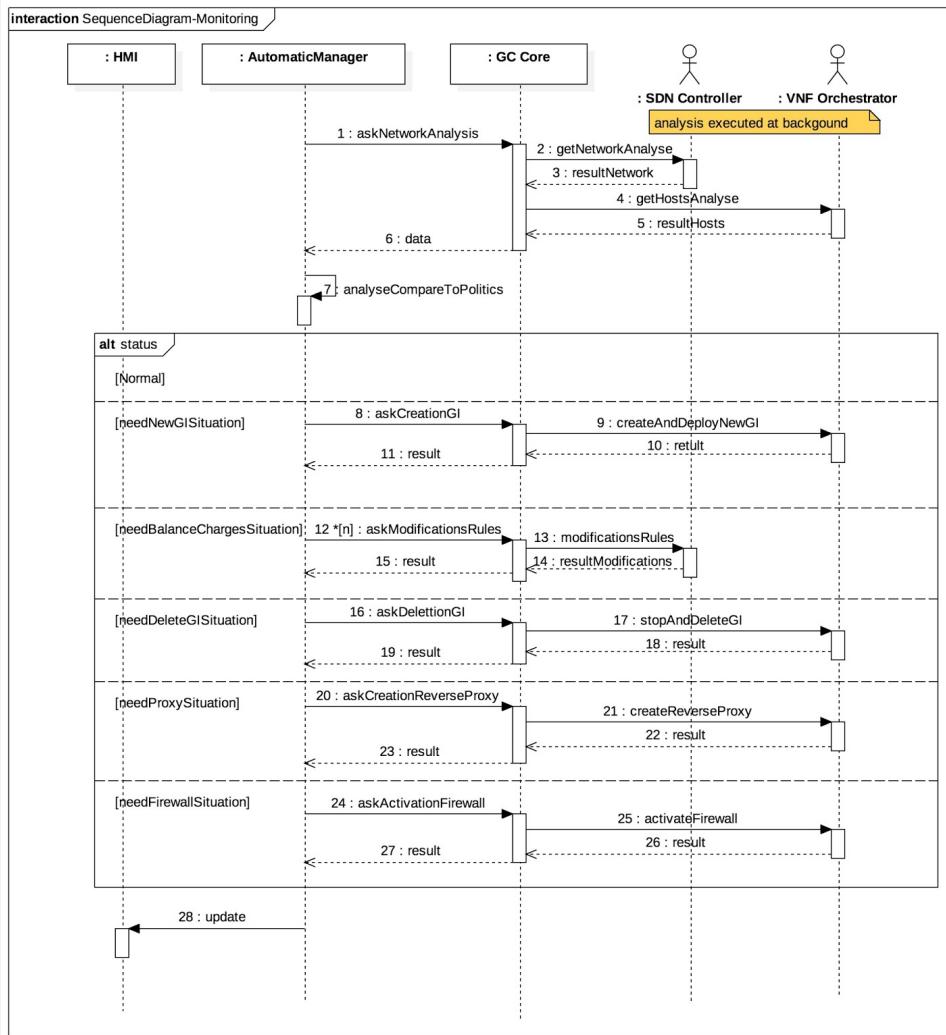
Si le manager automatique détecte une anomalie ou une amélioration possible vis-à-vis des politiques définies, le manager va demander au GC Core d'effectuer des actions.

Monitoring automatique du système par le manager automatique

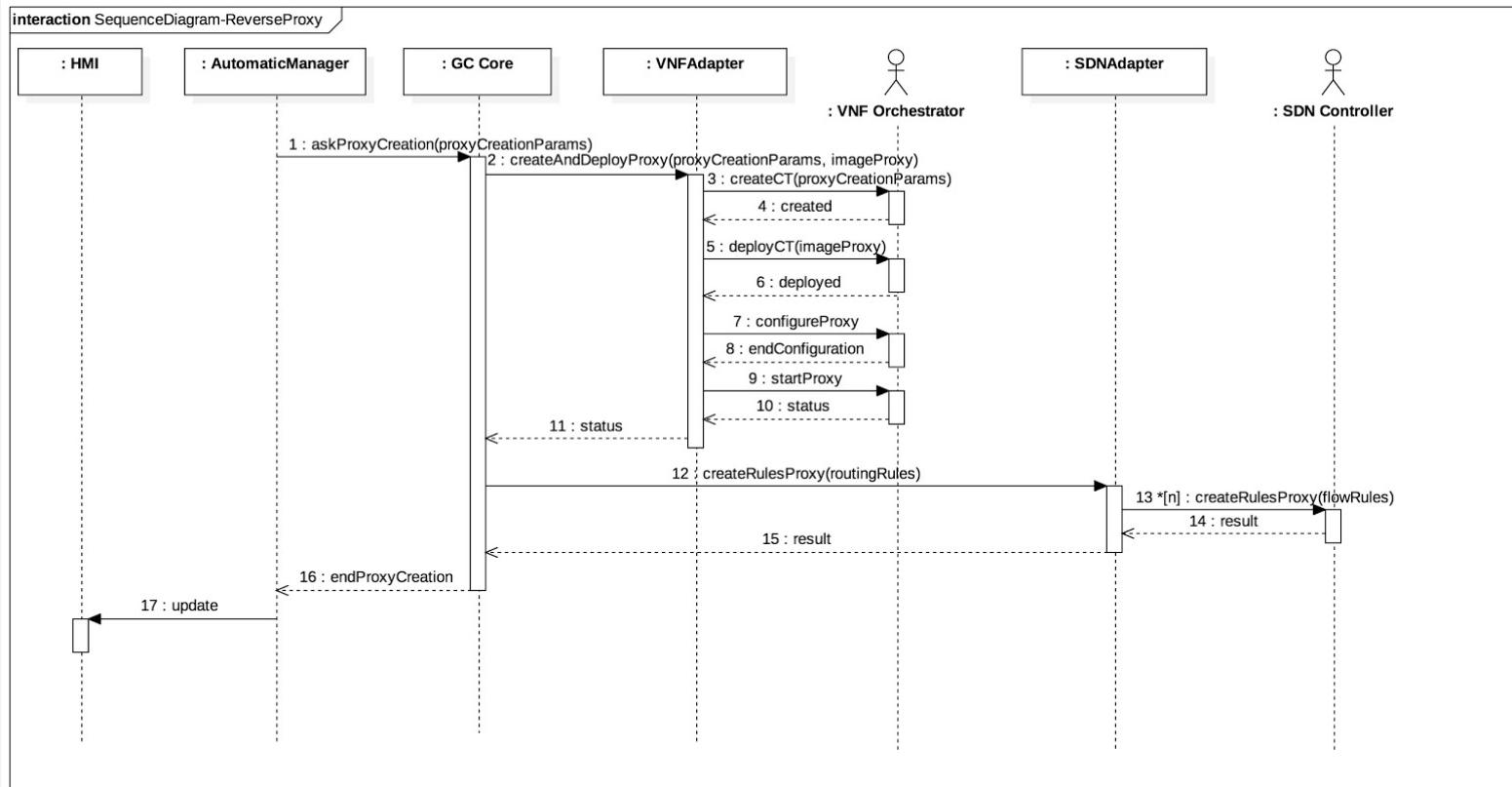
Des actions correctives peuvent être prises suite à ce monitoring



Monitoring automatique du système par le manager automatique



Déploiement d'un reverse proxy



Déploiement d'un firewall

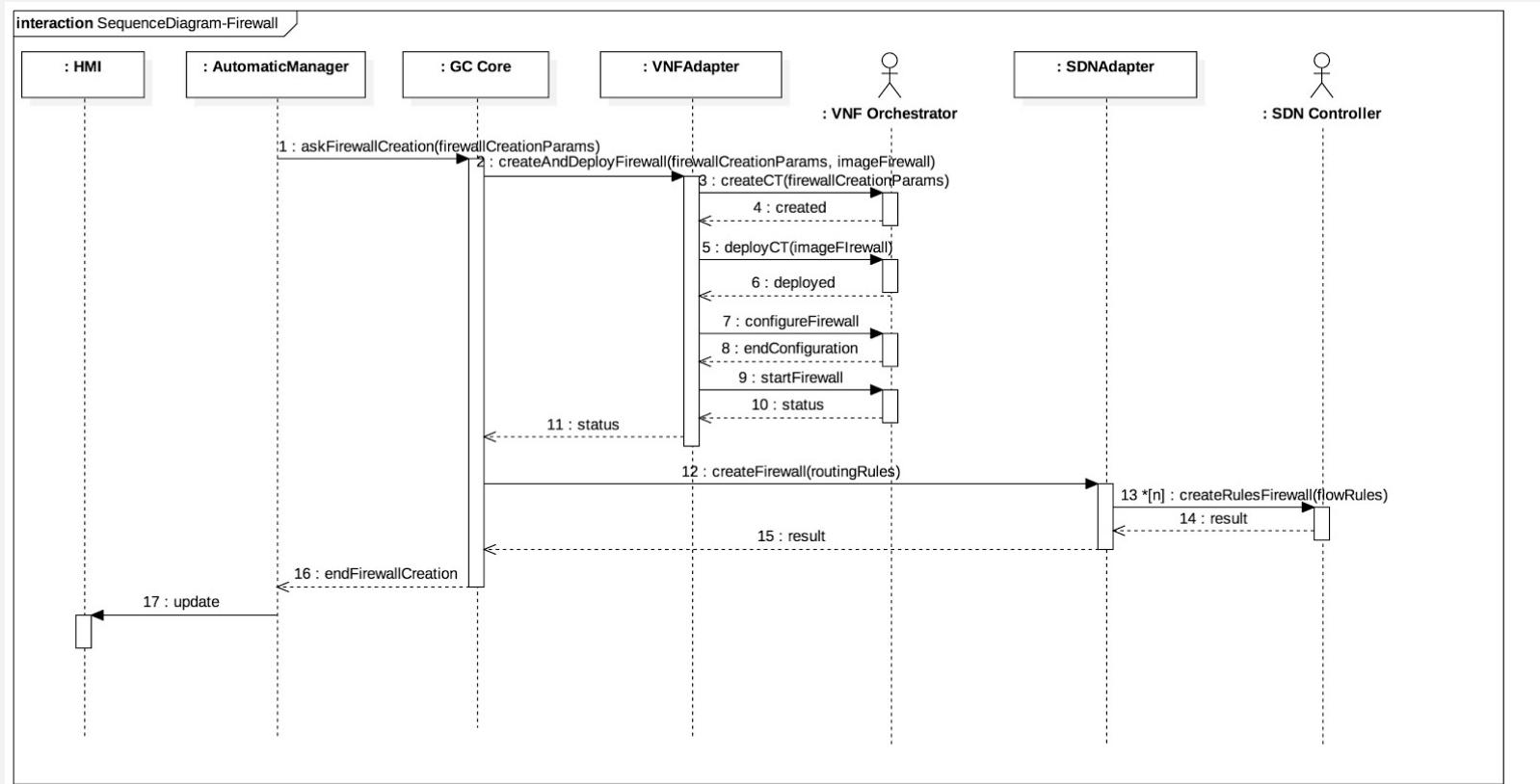


Diagramme composite

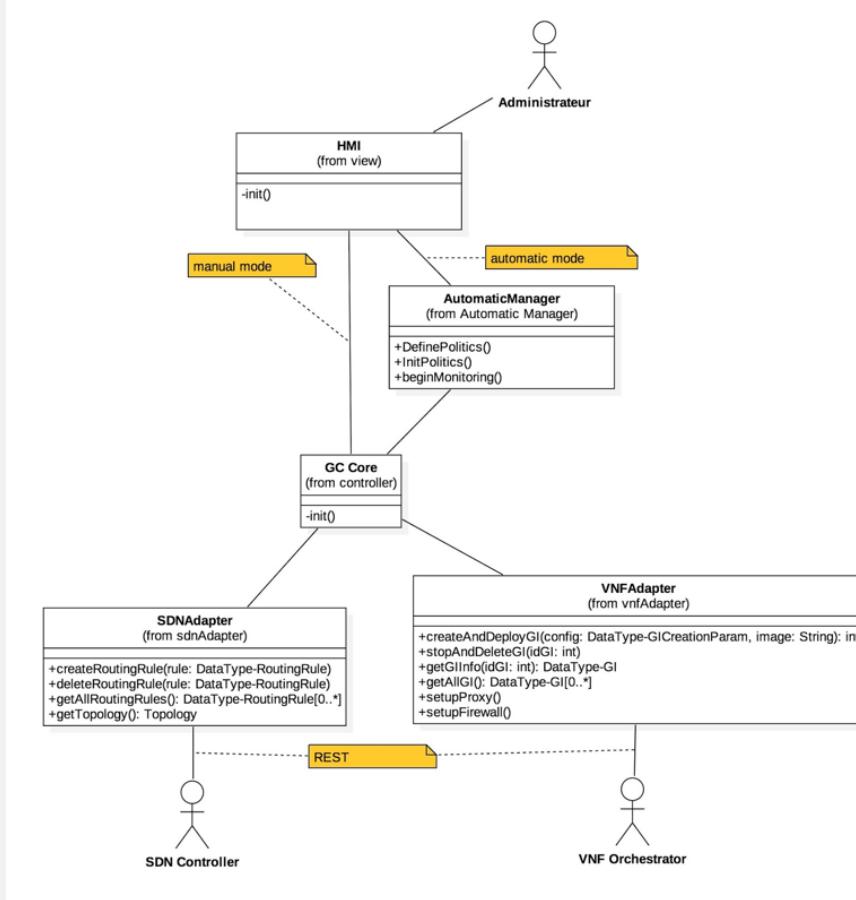
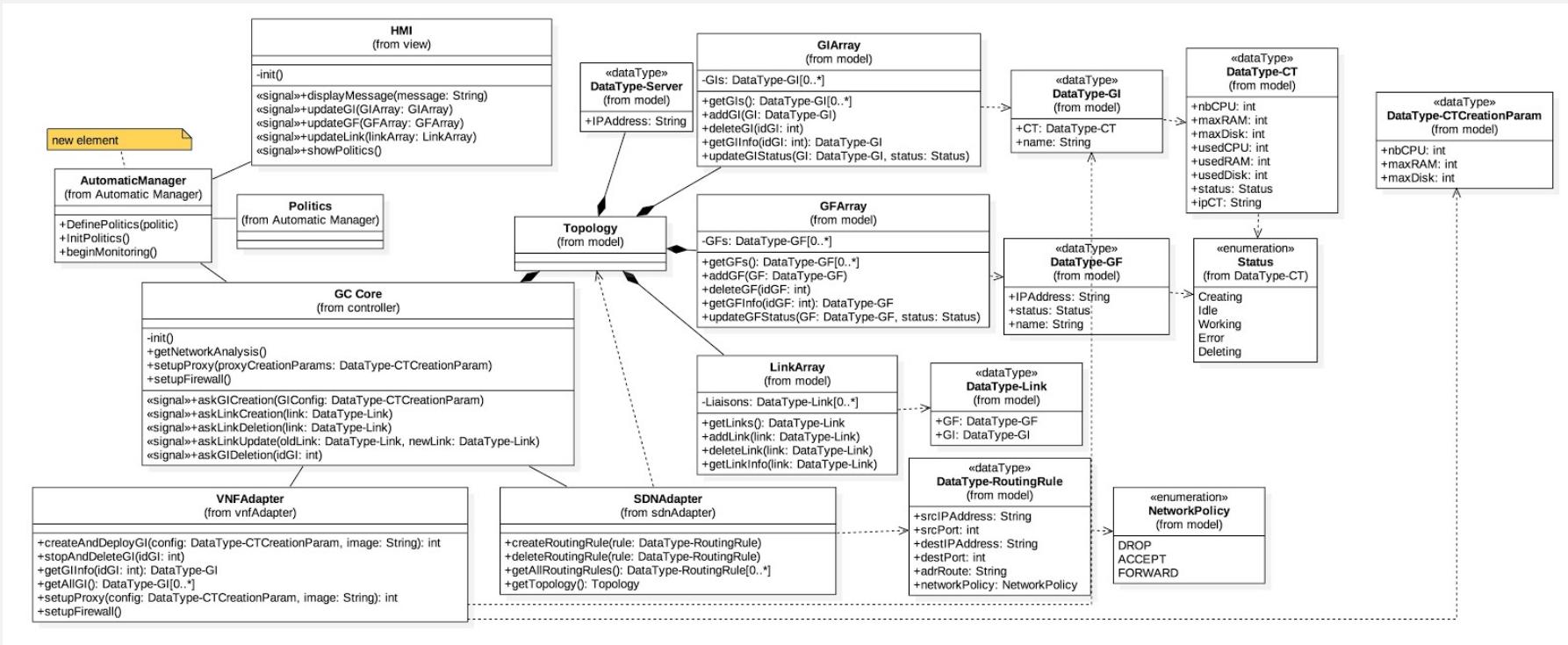


Diagramme de classe



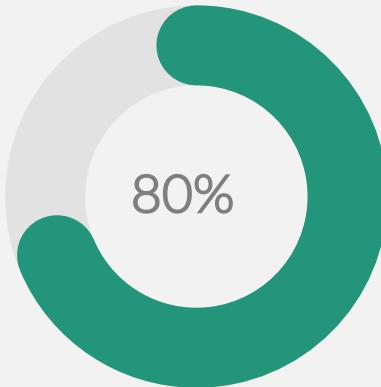
Et l'Automatic Computing

Où en est notre système dans la problématique d'Automatic Computing ?



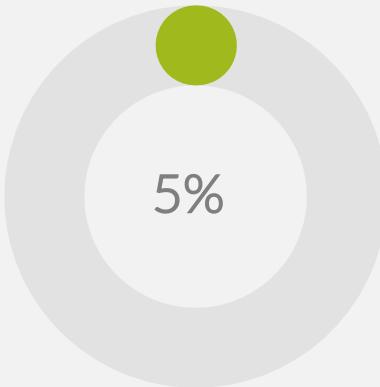
Self-configuring

Le système est en mesure de déployer, supprimer des GI pour s'adapter au changement dynamique d'environnement



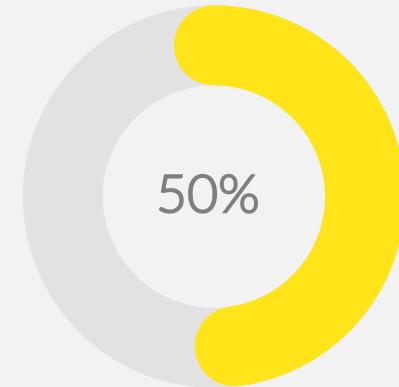
Self-optimizing

En plus du déploiement/suppression des GI, nous avons ajouté l'équilibrage de la charge des GI



Self-healing

Notre système actuel n'est pas en mesure de répondre à des perturbations internes (switch qui tombent, etc.)

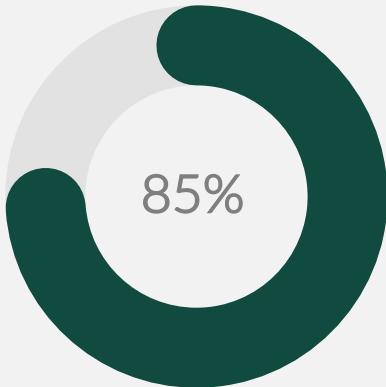


Self-protecting

Le système est en mesure d'anticiper, de détecter et de répondre à des attaques pré définies (Firewall et Reverse Proxy)

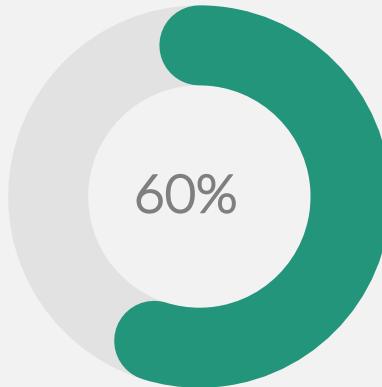
Et l'Automatic Computing

Où en est notre système dans la problématique d'Automatic Computing ?



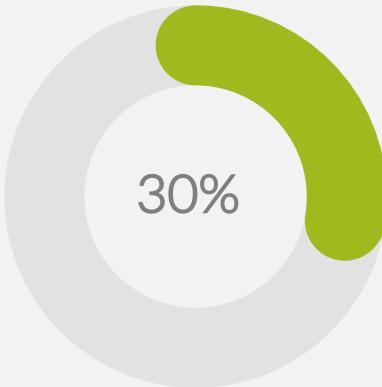
Monitoring

Le système est en mesure de récupérer des informations sur l'état du système, les filtrer et lever des symptômes en cas de non respect des objectifs



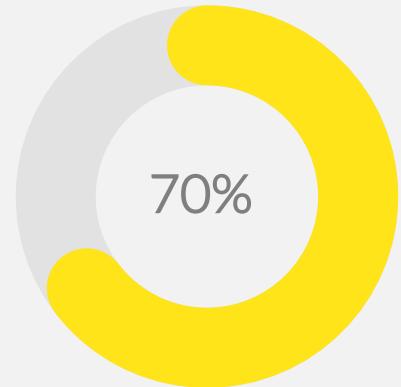
Analyzing

Le système est en mesure d'élaborer un diagnostic si les QoS dépassent des seuils d'exigences



Planning

Notre système ne réagit que vis à vis des stratégies déjà mises en place

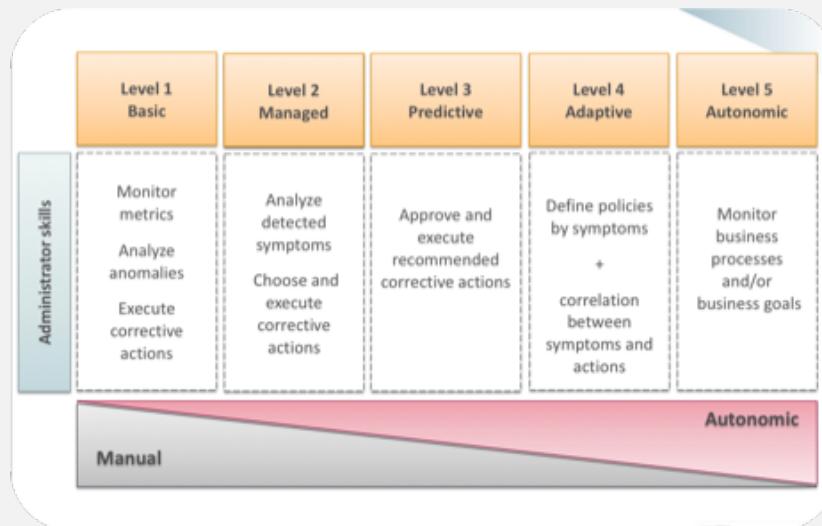


Executing

Le système déclenche une règle suite à l'analyse du système

Et l'Automatic Computing

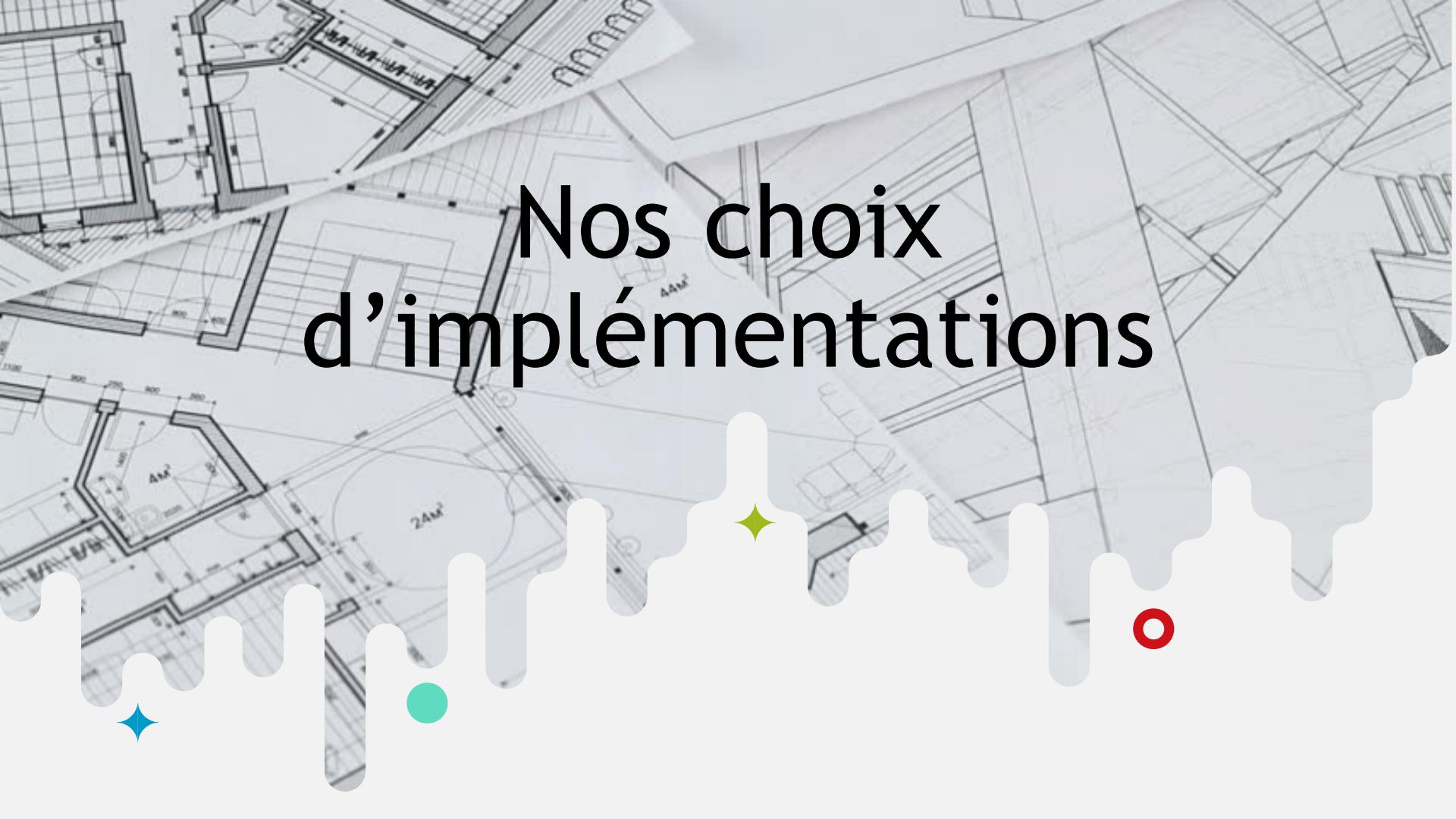
Son niveau de maturité



Niveau 4 - Adaptive Maturity Level

En effet, l'administrateur n'a pas la nécessité d'approuver les actions de corrections du système et se contente seulement de fixer des politiques de QoS qu'il souhaite respecter.

Des actions sont reliés aux symptômes et laisse le système décider de l'action corrective à effectuer en adéquation avec ses analyses de l'environnement et ce qu'il en déduit.



Nos choix d'implémentations



Des choix francs...

... pour apporter une réelle plus-value à l'administrateur du réseau



Suppression des gateways intermédiaires du DataCenter

Nous avons réduit le temps de déploiement d'une gateway à seulement 5 secondes. Ainsi, supprimer/réinstaller une gateway est un avantage conséquent vis-à-vis de problématiques d'espaces/d'utilisation du DataCenter



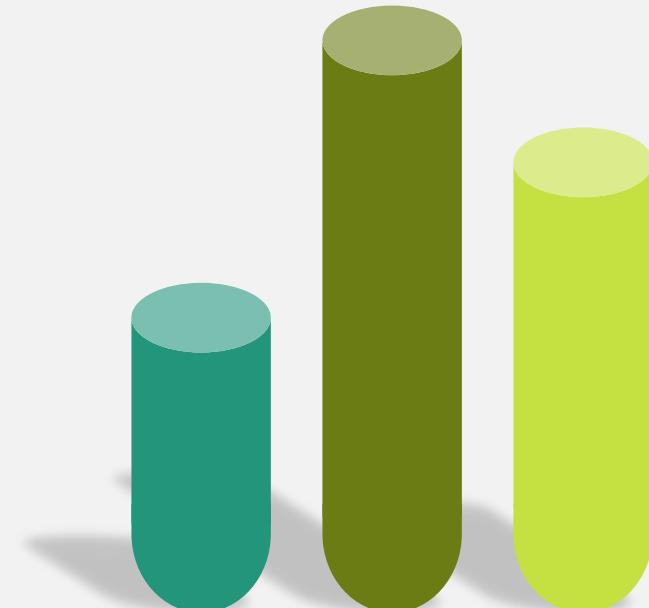
Afficher seulement les liens entre les GF et les GI

L'état standard des GF étant de transiter via la gateway initiale, nous avons choisi de seulement afficher les liens transitant via les GI pour permettre à l'administrateur de garder une vue d'ensemble claire de son système



Du point de vue de l'administrateur : 1 seul switch

L'administrateur et le GC core pensent communiquer avec un seul switch alors que dans les faits, c'est le SDN Adapter qui gère un ou plusieurs switchs (comme le serait une situation réelle)



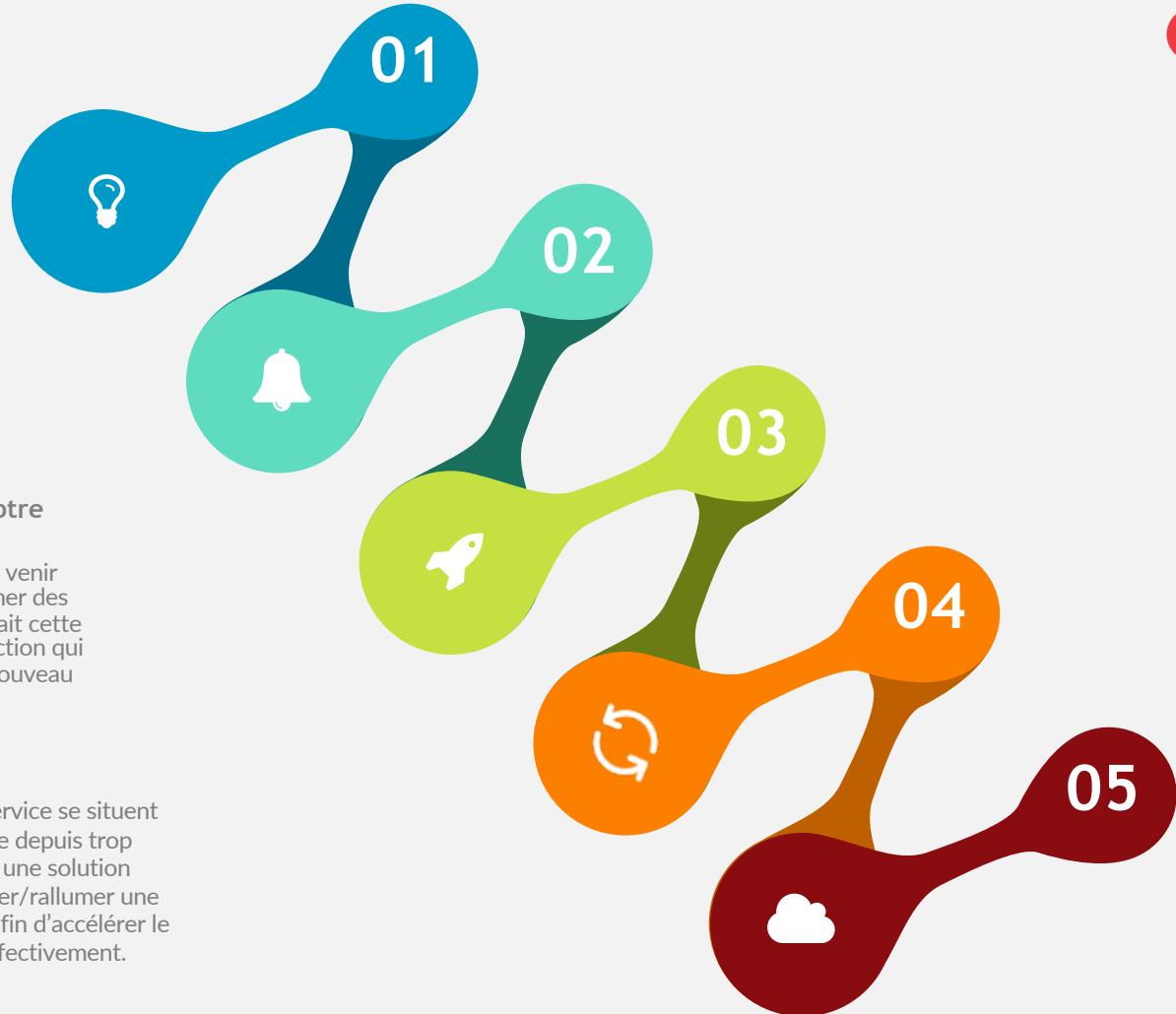
Améliorations possibles

Rajouter de l'apprentissage pour rendre notre système plus intelligent

Il faudrait ajouter la possibilité à l'administrateur de venir prendre la main sur le système et d'ajouter/supprimer des GI, firewall, etc. A chaque fois que le système subirait cette reprise en main, il analysera l'état du système et l'action qui a été faite pour apprendre et à terme, déduire un nouveau comportement.

Principe de surétude et de sécurité

Lorsque le système détectera que les qualités de service se situent dans une zone acceptable mais bientôt inacceptable depuis trop longtemps, il estimera que la nécessité de déployer une solution devient réelle. Cela se traduira par le fait de déployer/rallumer une GI (en fonction de la solution choisie) par sécurité afin d'accélérer le déploiement de la réponse si le besoin se traduit effectivement.



Démonstration



Merci de votre attention !

Avez-vous des questions ?

