Quatrième période du 12-02-2024
au 08-03-2024 (4 semaines)

Rapport d'activités en entreprise

Alexis Déhu
a.dehu@aditu.fr

Responsable :

M. Éric Pierre-Sala
e.pierre-sala@aditu.fr

Tuteur :

M. Guillaume Devesa
g.devesa@aditu.fr

du 12 Février, au 8 Mars 2024

Alexis Déhu

Rapport d'activités en entreprise

Le présent document est le compte rendu de mes activités au sein de l'entreprise ADITU pour la quatrième période d'alternance allant du 12-02-2024 au 08-03-2024 (4 semaines) en tant qu'Apprenti Administrateur Systèmes et Réseaux.

du 12 Février, au 8 Mars 2024

Cet apprentissage en alternance a été réalisé dans le cadre de l'obtention d'un BUT en Réseaux & Télécommunications à l'Université de Pau et des Pays de l'Adour, IUT de Mont-de-Marsan. La période d'alternance d'une durée de 2 ans s'est établie du 1er Septembre 2023 au 31 Août 2025 dans les locaux d'ADITU, Technopole Izarbel Côte Basque, 64210 Bidart.

Aucune intelligence artificielle n'a été utilisée pour la rédaction ou l'aide à la production de ce document. Aucune information présente n'a été récupérée brute de forme depuis quelconque source, publique ou non. Ce document est le fruit d'un travail personnel et que je n'ai ni contrefait, ni falsifié, ni copié tout ou partie de l'œuvre d'autrui afin de la faire passer pour mienne.

Un immense merci à toutes les personnes m'ayant encadrées en entreprise.

M. Éric Pierre-Sala - Directeur

Mme. Marina Galant - Adjointe de direction

M. Guillaume Devesa - Directeur technique

M. Valentin Creton - Administrateur systèmes et réseau

M. David Alarcon - Administrateur systèmes et réseau

M. Charles-Henry Ploquin - Technicien informatique

M. Victor Dupas - Technicien informatique

du 12 Février, au 8 Mars 2024

Résumé de la période

J'ai pour cette quatrième période effectué la mise en production de la nouvelle solution de support client. Je me suis aussi vu attribuer l'assainissement d'une partie du réseau du data centre de Dax, le tout en continuant mes travaux d'études pour une nouvelle solution de supervision.

Cette quatrième période annonce l'aboutissement de mon travail sur la nouvelle solution de support client. La deuxième m'ayant permis d'en apprendre davantage sur le support d'une ESN et d'en choisir la solution qui correspondait au mieux à nos attentes et nos besoins. La troisième à préparer professionnellement celle-ci en y adaptant l'ensemble des attendus des clients et de mes collègues. Quant à cette quatrième période, elle marque son déploiement et l'utilisation par les clients, ainsi que le maintient de la solution dans un contexte de production.

Mon premier travail en réseau fut d'assainir l'infrastructure des VLANs du data centre de Dax. Son application étant différente des réseaux domestiques, je me suis formé à utiliser le protocole de gestion de VLANs VTP. J'ai été en charge de comprendre le fonctionnement actif de la structure, de proposer un plan d'assainissement, de l'implémenter une première fois en environnement virtualisé et de prochainement appliquer ces changements au data centre.

J'ai en parallèle continué mes travaux sur l'étude d'une nouvelle solution de supervision, en mettant à l'essai la solution retenue de l'étude comparative : Zabbix. J'y ai appliqué des principes fondamentaux et avancés de la supervision dans un environnement contrôlé, puis recherché à comprendre son fonctionnement et à découvrir des pistes d'amélioration pour notre infrastructure actuelle.

Compétences recherchées: autonomie; étude de solutions en activité; mise en production d'applicatifs; compréhension et virtualisation de réseaux avancés; documentation; rédaction; travaux de recherche; suivi de l'activité d'une solution

Table des matières

1

Lancement et suivi de la nouvelle interface de support client

Hormis des vérifications sur son fonctionnement à mon arrivée, je devais déployer la nouvelle solution de support la première semaine de cette quatrième période. La mise en production de l'application s'est déroulée en trois jours, avec un entretien quotidien qui a duré plus d'une semaine.

Les clients ont l'habitude de faire des retours sur les solutions qu'ils utilisent, et pendant les jours qui ont suivi la bascule; j'ai compris que la solution de support ne faisait pas exception à cette règle. Le plus grand inconvénient pour eux, de ce que j'ai compris à mon humble échelle, est de devoir s'en accoutumer pour travailler. Ainsi, je me suis rendu compte des erreurs que j'ai pu faire en voyant leurs retours.

1.1 Ouverture de l'interface

Les clients ont été averti du changement d'interface par des emails sur plusieurs semaines. Le mercredi de la semaine du déploiement, ils ont reçu un email avec leurs identifiants de connexion pour un lancement prévu le jeudi de la même semaine. L'interface était déjà disponible dès lors qu'ils avaient reçu leur email de connexion.

Pour qu'ils s'y connectent, nous avons dû modifier la redirection, dit enregistrement DNS, qui redirigait vers `support.aditu.fr` pour la nouvelle application. J'ai aussi effectué quelques modifications internes à l'application pour lui permettre d'être appelée depuis ce lien.

1.1.1 Envoi des identifiants aux clients

Un mail courtois fut envoyé à tous les contacts informatiques de nos clients pour leur annoncer leurs nouveaux identifiants de connexion et l'accessibilité à la nouvelle interface. Il était convenu un déploiement pour le jeudi 15 février, l'interface était disponible depuis le mercredi 12, date d'envoi des identifiants pour les plus impatients.

1.1.2 Changement du comportement de l'application

Des modifications au serveur hébergeant la solution ont été effectuées pour lui permettre d'être contacté depuis l'extérieur avec ce lien, différent de celui utilisé pour les essais. Pareil pour le passage du réseau local du serveur, dès lors utilisé, pour être accessible depuis Internet derrière un pare-feu. ESur celui-ci ont été configurées des règles dans le détécteur d'intrusions et de la translatation d'adresses pour l'accessibilité depuis l'extérieur.

1.1.3 Redirection du site support

Un serveur chez ADITU retranscrit les adresses des serveurs contactés pour nos services en `aditu.fr`. Ainsi, lorsque vous renseignez `www.aditu.fr`, vous atteignez notre serveur WEB sans avoir à connaitre son emplacement sur Internet car ce serveur spécifique vous indique son adresse, ici IP, à interroger pour y accéder.

Nous avons après la bascule modifié une entrée sur ce serveur pour modifier le serveur contacté lorsque vous renseignez `support.aditu.fr`, qui redirige désormais vers la nouvelle solution.

1.2 Vérifications après bascule

Le soir de la bascule, je faisais les dernières vérifications avant le jour J. Même si je les avais déjà faites en interne, il était pour moi impératif de les revérifier une fois l'application déployée.

Cette série de tests consistait à vérifier la redirection vers l'application, les informations qui y transitaient à travers les navigateurs des clients et à vérifier la connexion aux comptes clients et à la base de données.

Aussi à vérifier les fonctionnalités proposées aux clients, en simulant leur activité sur la plateforme.

1.3 Erreurs apprises

Grâce aux retours sur l'application, j'ai pu me rendre compte de mes erreurs; que je m'efforcerai de me rappeler et à ne pas reproduire pour d'autres déploiements et intéractions clients par la suite.

1.3.1 Mots de passe complexes

Ma première erreur fut dans le choix des mots de passe que j'ai attribué par défaut aux utilisateurs. J'ai préféré en générer un aléatoire et complexe pour leur première connexion, les clients ayant la possibilité de le changer par la suite dans l'interface.

Question sécurité, cela me paraissait être une bonne pratique. Par contre, question practicité c'était infâme pour les personnes novices en informatique. Les mots de passe alphanumériques avec des caractères spéciaux non communs (apostrophes inversées, symbole paragraphe, anti-slash...) ne les réussissait pas du tout.

Ils pouvaient bien-sûr le copier avec leur souris puis le coller dans le champ où leur mot de passe était demandé. Cependant ceci peut ne pas être un réflexe pour les novices en informatique.

Ainsi, j'ai appris qu'il faut vraiment réfléchir au plus simple quant à l'interfaçage utilisateur, en prenant parfois parti de négliger l'aspect sécuritaire. Des mots de passe trop complexes découragent les utilisateurs non avancés et leur fera préférer un retour à l'ancienne interface juste par ce jugement, préférant la simplicité et le bénéfice de savoir l'utiliser à l'inconvénient de devoir apprendre à utiliser la nouvelle sur leur temps de travail.

1.3.2 Cache des navigateurs clients

Ce problème ne m'est survenu qu'une fois et ne fut pas très embêtant à première augure, mais il mérite son attention, pouvant être source de nombreuses heures de malheurs si oublié.

Un client nous a appelé par téléphone pour nous informer qu'il n'arrivait pas à accéder à la page de connexion de l'interface de support. Il était au informé du changement de l'interface et en conséquent, celui-ci se questionnait sur le fait que celle-ci soit vraiment nécessaire, étant donné qu'il ne pouvait plus y accéder : il aurait continuer avec l'ancienne.

Or, je savais que celle-ci fonctionnait depuis une semaine ou plus. En l'assistant sur son poste par un contrôle à distance, je me suis rendu compte que son navigateur (Chrome) avait conservé les anciens cookies, informations mises en caches et celles de connexion de l'ancienne interface.

L'utilisateur avait pour habitude de laisser constamment son ordinateur allumé, et donc son navigateur, en conservant ses informations de connexion dedans. Au moment où il tentait d'accéder à l'interface de support, son navigateur essayait de rejouer les informations conservées de l'ancienne interface sans réussir retournant une erreur.

Il fallut fermer puis réouvrir son navigateur pour que celui-ci supprime certaines informations conservées, qui furent celles qui étaient rejouées et défaillantes.

1.3.3 Un lien n'est pas un mot de passe

Dans mon processus de distribution des identifiants, au lieu de transférer les mots de passe par email : j'indiquais que ceux-ci était accessibles en suivant un lien. Ce qui évite que si la boite mail d'un client soit compromise par un attaquant, que celui-ci puisse retrouver des identifiants de connexion pour les réutiliser ou les essayer sur d'autres services.

Cependant, certains clients comprennaient que leur mot de passe était ce lien, et le copiait dans le champ attendu de leur mot de passe. L'histoire du "lien vers le mot de passe" plutôt que le "mot de passe"...

La prochaine fois que je communiquerai des informations de connexion ou d'identification, je ferai en sorte d'attirer le regard du destinataire vers des lignes précisant le plus simplement possible comment accéder au lien pour récupérer les informations souhaitées.

1.3.4 Lexique technique envers les clients

Pour le renseignement de demandes utilisateurs ou d'incidents, les clients passent par une suite d'étiquettes pour leur faciliter l'accomodation à l'interface. Ainsi, ils ont premièrement deux choix : "Demande" ou "Incident", puis ils précisent un service impacté ("Messagerie", "Sauvegarde"...) avec à chaque fois une description.

Le problème n'a pas été remonté par un client mais par David : il faut utiliser les mots qui font le plus de sens aux clients lorsqu'ils veulent faire leur demande, plutôt que ceux les plus justes. Auquel cas, ceux-ci pourront prendre plus de temps à choisir dans quel "entonnoir" rentrer, ou renseigner un mauvais service etc.

Lorsque je communique avec les clients désormais, je m'efforce d'expliquer les choses avec leurs mots plutôt que les miens, même si ceux que j'utilise sont les mots justes ou adéquats.

2

Assainissement des VLANs du data centre de Dax

Le protocole VTP *VLAN Trunk Protocol* permet la déclaration de VLANs *Virtual LANs* sur plusieurs switchs en les renseignant qu'une seule fois sur un switch serveur. Les switchs clients apprennent du switch serveur les VLANs utilisés dans le réseau.

Ce protocole est propriétaire des équipements Cisco. Le data centre de Dax DATA3 incorpore le protocole VTP dans son réseau pour DATA3 et ses clients. Cependant, différentes personnes s'en sont servies pour des usages différents, celui-ci est désormais divisé en sections de réseaux (avec plusieurs switchs serveurs VTP).

L'objectif de cette mission est d'assainir l'implémentation du protocole VTP dans le data centre en laissant uniquement les switchs "coeur de réseaux" distribuer les VLANs. Ce sera aussi l'occasion de mettre à jour les versions du protocole VTP installés sur les équipements et de documenter l'intégration pour éviter d'à nouveau avoir différentes implémentations.

2.1 Fonctionnement du protocole VTP

VTP intervient dans un souci de répétition de la déclaration manuelle des VLANs sur les switchs d'un réseau. Dans un réseau de data centre, cela devient vite impossible de les déclarer ainsi sur chaque switch individuellement à grande échelle.

Le protocole fonctionne sur le principe client/serveur. Le serveur seul peut déclarer des VLANs sur un réseau, lui-même composé de switchs clients en écoute du serveur pour assimiler de nouveaux VLANs. Le serveur et ses clients VTP doivent être dans le même domaine VTP. Un

dernier mode "transparent" est adressable, permettant de laisser circuler les trâmes VTP sur le VLAN Default sans les assimiler.

Une des fonctionnalités avancées du protocole VTP est son *VTP Pruning* qui permet d'empêcher la diffusion de requêtes broadcast sur une partie du réseau si le VLAN n'y est pas utilisé (utile pour mitiger le traffic inutile).

Plusieurs versions de ce protocole existent et son inter-opératables : VTP-1, VTP-2 et VTP-3. La version 2 apportant du support pour l'architecture *Token ring*, des trâmes de vérification de configuration (pas juste d'assimilation) et quelques modifications dans son fonctionnement.

La version 3 apporte une configuration avec authentification : n'importe qui ne pourra pas joindre un domaine VTP sans y avoir été invité, il suffisait jusqu'à présent de regarder les trâmes passées et de se joindre au domaine pour récupérer les VLANs et communiquer avec les machines de ceux-ci. Elle permet aussi d'utiliser l'intégralité du nombre de VLANs de la norme 802.1q (4094) comparé à 1006 pour les versions précédentes.

À noter que les liens entre les switchs utilisant VTP doivent être en trunk, libre d'autoriser quels VLAN à circuler (le Default impérativement, 1 nativement, pour la circulation des messages VTP).

2.2 L'infrastructure VTP actuelle

L'infrastructure VTP était éclatée en deux domaines : un domaine pour le coeur de réseau et un autre pour le réseau de distribution/d'accès.

Dans ces deux réseaux, les serveurs VTP étaient empilés : un serveur VTP pouvait informer ses clients rattachés, mais pas ceux derrière le serveur VTP en dessous de lui (le tout sur le même domaine toujours).

L'infrastructure devait se débarrasser de l'empilement de serveurs VTP pour n'en permettre qu'à un seul uniquement de faire des annonces aux autres switchs et de pouvoir en créer.

2.2.1 Relevé et changement des syntaxes des VLANs

L'un des objectifs était donc d'unifier les deux domaines VTP présents en un seul.

Le problème étant qu'ils possédaient parfois les mêmes VLANs, avec ou sans même dénomination (e.g. "VLAN-0001" pour le coeur de réseau et "nom-du-client" pour le réseau d'accès).

J'ai donc répertorié les VLANs utilisés dans les deux domaines et en ai fait un tableur comparatif à montrer à Guillaume mon tuteur et Valentin mon superviseur pour cette tâche; afin qu'ils choisissent la dénomination à conserver pour les VLANs.

2.3 Essais en laboratoire

Les manipulations sur le réseau d'un data centre doivent être validés par des essais au préalable pour ne pas engendrer une discontinuité de services chez nos clients. En adoptant ce raisonnement, j'ai monté un réseau virtualisé d'équipements Cisco afin de simuler l'intervention et constater d'éventuels problèmes réfléchis ou imprévus sur la structure avant qu'ils ne le soient sur le data centre.

À l'aide des outils de simulation Cisco Packet Tracer et GNS3, j'ai simulé une partie du réseau du data centre et essayé mes manipulations. Je les ai simulées avec des équipements qui s'apparentaient le plus aux nôtres en respectant leur version de Cisco IOS utilisée (un des systèmes d'exploitation d'équipements Cisco).

Dans mes manipulations, j'ai répliqué les configurations de nos équipements physiques pour au mieux simuler les éventuelles pannes suites à mes manipulations et de m'assurer de l'implantation de la nouvelle structure avec les anciennes configurations des équipements.

J'ai documenté mon approche et mes manipulations pour les reproduire à l'identique et pour qu'elles puissent être compréhensibles rapidement par quelqu'un qui souhaiterait reprendre le projet.

2.4 Plan de modification

Une fois un plan de nomenclature validé, avec une démonstration faite et approbation reçu par la simulation. Je pourrai commencer à assainir le plan d'adressage des VLANs du data centre de Dax à mon retour.

Je n'oublierai pas de documenter mes actions et d'expliquer la nouvelle infrastructure textuellement et graphiquement. Je conserverai toutes mes démarches (fichiers temporaires, actifs...) pour que n'importe qui puisse revenir sur le projet et comprendre son fonctionnement, les tenants et les aboutissants de la structure.

3

Avancements sur l'étude d'une nouvelle solution pour la supervision

Concernant l'étude d'une nouvelle solution de supervision, ma dernière période s'etait terminée sur l'apprentissage de principes avancés fondamentaux de la supervision d'actifs en entreprise et par une vision d'ensemble des solutions existantes répondantes à nos besoins.

J'ai déjà manipulé une des solutions survolées pour un usage personnel et en laboratoire chez Aditu : Nagios. Outil extrêmement efficace pour de l'alerting mais ne proposant rien pour la métrologie dans son coeur.

Mon objectif pour cette période est de prendre en main un outil faisant de l'oeil à l'équipe plus que l'ancien Nagios parmis la sélection, et qu'une fois étudié je puisse leur montrer une étude comparative pour commencer mes travaux de migrations de la supervision avec la solution retenue.

3.1 Apprentissage et déploiement de Zabbix

Zabbix est une solution de supervision (monitoring, alerting et métrologie) d'ancienne génération qui essaye de regrouper tout au même endroit (comparé à la nouvelle génération : séparer un maximum les fonctionnalités pour permettre de pouvoir changer les briques qui composent sa solution quand on le souhaite par ce que l'on souhaite sans effort).

J'ai durant cette période fait une grande avancée sur l'étude de Zabbix, en apprenant toujours de nouvelles notions et de fonctionnalités en essayant de rechercher des liens entre eux et leur utilité potentielle... J'essayais de comprendre toujours un maximum de celles-ci. J'essaye aussi

de documenter au mieux mes efforts et de vouloir rechercher ce que je ne connais pas dans cette solution pour la comprendre au maximum.

Certains aspects ne sont pas beaucoup abordés en publique par l'équipe de Zabbix et sur les forums car généralement réservés aux clients du support. Certaines fonctionnalités cruciales pour un data centre ou une ESN se retrouvent alors dans les mains des équipes de Zabbix, qui attendent que l'on vienne leur demander de l'aide pour nous proposer une offre chiffrée de de support.

Ce service de support, au delà de l'appel la résolution de problèmes, est constitué de personnes expérimentées dans la supervision et l'administration de serveurs Zabbix pour nous conseiller sur des points importants de notre solution : le dimensionnement de la base de données, interopérabilité avec d'autres outils, développement pour applications métiers, haute disponibilité de l'ensemble...

Pour ne pas avoir à souscrire à ce service, je me suis lancé dans la compréhension du fonctionnement de Zabbix avec et sans ces aspects, puis d'essayer de les incorporer d'une manière la plus saine et stable possible.

3.1.1 Prise en main

L'installation d'une infrastructure Zabbix couverte, je me suis tourné vers la prise en main vers des premiers équipements en laboratoire. Sans commencer à voir comment nos équipements actuels pourraient être amenés ou agencés par Zabbix, je souhaitais faire le tour des possibilités d'options à apporter à un équipement dans Zabbix.

Une des fonctionnalités les plus intéressantes que j'ai relevé est l'utilisation de l'agent Zabbix sur un hôte dès que possible. Zabbix propose des modèles de gestion pour différents appareils (routeurs Cisco, parefeu PfSense...) en utilisant des protocoles standards, mais il est possible parfois d'installer leur agent pour plus de fonctionnalités.

Cet agent permet notamment de lancer des commandes de vérification à distance et d'en récupérer la sortie pour en définir l'état d'un service personnalisé. C'est aussi par cet agent que nous pouvons exécuter une suite de commande à distance si nous connaissons la source d'un problème et sa résolution (pour ne pas devoir intervenir manuellement).

La notion de proxy est aussi importante, celle-ci permet d'avoir un réseau de supervision Zabbix dispersé à différents endroits. Plusieurs serveurs Zabbix effectuent les tâches sur leur région seul et partagent uniquement les remontés au serveur Zabbix principal (extrêmement utile pour

la répartition de charge).

3.1.2 Haute disponibilité

La haute disponibilité regroupe l'ensemble des pratiques permettant la continuité d'un service pour un ensemble de risques et d'aléas donnés. La haute disponibilité intervient après une étude des risques/aléas d'un système d'informations, proposant un plan d'action pour la mitigation des problèmes engendrés par les éléments de l'étude (malfonctionnement du service, perte de communication, défaillance matérielle ou d'alimentation...).

Dans le câdre de notre supervision, nous voulions implémenter de la haute disponibilité pour permettre une redondance du service, une réplication quasi-temps réelle de son fonctionnement et une tolérance à l'erreur accrue.

Une grande partie de mon temps lors de cette période a été consacré au montage d'un cluster pour implémenter les fonctionnalités précédemment citées à Zabbix, sans support. Celui-ci est opérationnel mais encore non stable et non mise à l'épreuve. Toute mon avancée a été documentée et répliquée plusieurs fois.

Pour ce faire, je me suis servi des outils Corosync et Pacemaker, faisant parfois appel à Heartbeat. Le principe est qu'un service est exécuté en simultané sur plusieurs hôtes (plus de deux) - en exemple, un serveur primaire et un serveur secondaire; base de données, serveur Zabbix...

Les serveurs sont vus de l'extérieur comme un seul, ils se partagent une adresse IP flottante d'accès. Par défaut, l'adresse flottante est attribuée au serveur primaire. Si le service n'est plus en fonctionnement sur le serveur primaire : le serveur secondaire prend immédiatement l'adresse flottante pour toujours distribuer le service.

Les causes de la bascule peuvent être multiples : panne de courant, plantage du service ou d'un système... Leurs fichiers de configuration pour ces services sont aussi synchronisés entre eux : aucune configuration n'est perdue.