

ROYAUME DU MAROC
UNIVERSITE CADI AYYAD
ECOLE NATIONAL DES SCIENCES
APPLIQUES

Département : Informatique Réseaux et Telecom

Niveau : 5^{ème} année GTR

Rapport D'avancement Du Stage PFE

Sous thème :

L'automatisation D'un Réseau Data Center



Stage du 14/02/2019 au 31/05/2019

Préparé par :

BADRE Hamza

Encadré par :

Mr. MAAMORI Nour-eddine (OCP)

Mr. BENLAMKADEM Abdellatif (ENSA)

Table des matières

| | |
|--|-----------|
| Le contexte du Projet : | 5 |
| Chapitre 1 : Présentation du réseau défini par logiciel | 6 |
| 1 Introduction : | 6 |
| 2 Comprendre le SDN : | 6 |
| 3 Où étions-nous avant SDN? | 7 |
| 4 Où SDN nous emmène-t-il? | 8 |
| 4.1 SDN facilite la virtualisation des serveurs et réseaux en nuage (Cloud)..... | 9 |
| 4.2 SDN concerne principalement l'automatisation basée sur des règles | 10 |
| Chapitre 2 : Comprendre les composants et la structure ACI..... | 11 |
| 1 Introduction : | 11 |
| 2 Un aperçu du Fabric ACI..... | 12 |
| 2.1 Matériel ACI | 12 |
| 2.2 Les Composants d'ACI..... | 13 |
| 3 Terminologie ACI..... | 15 |
| 3.1 Locataires ACI..... | 15 |
| 3.2 Locataire "commun" | 15 |
| 3.3 Mise en réseau des locataires..... | 16 |
| 3.4 Locataire des politiques | 18 |
| 4 Compréhension de la third-party intégration : | 19 |
| 5 La plateforme Cisco Devnet et Sandbox | 20 |
| 5.1 Qu'est-ce que Devnet Sandbox? | 20 |
| 6 Une introduction à l'interface graphique du contrôleur APIC : | 21 |
| 6.1 Menu système..... | 22 |
| 6.2 Menu des locataires..... | 24 |
| 6.3 Menu de Fabric | 25 |
| 6.4 VM Networking..... | 27 |
| 6.5 Services L4-L7 | 27 |
| 6.6 Admin | 28 |
| 6.7 Opérations | 29 |

Chapitre 3: Configuration des stratégies et Le locataires.....30

| | |
|---|----|
| 1 Introduction : | 30 |
| 2 Créer des locataires : | 31 |
| 3 Configuration des domaines du pont : | 33 |
| 4 Configuration des contextes : | 35 |
| 5 Création de profils de réseau d'application | 37 |
| 6 Création de groupes de terminaux (EPGs): | 38 |
| 7 Utilisation de contrats entre locataires : | 39 |
| 8 Création de filtres | 43 |

Table des Figures

| | |
|--|----|
| Figure 1 : L'architecture d'ACI | 13 |
| Figure 2 : Le fonctionnement d'APIC | 14 |
| Figure 3 : Locataire ACI | 15 |
| Figure 4 : Locataire réseau | 16 |
| Figure 5 : L'infrastructure d'ACI | 17 |
| Figure 6 : Locataire des politiques | 18 |
| Figure 7 : Profile d'application | 19 |
| Figure 8 : Devnet Labs | 20 |
| Figure 9 : Devnet ACI simulator | 21 |
| Figure 10 : Login au Plateforme APIC | 21 |
| Figure 11 : APIC : Menu système | 22 |
| Figure 12 : APIC : sous-menu Controllers | 23 |
| Figure 13 : Les Interfaces du contrôleur APIC | 23 |
| Figure 14 : le stockage d'APIC | 24 |
| Figure 15 : APIC : Menu Locataire | 24 |
| Figure 16 : APIC : Menu Fabric | 25 |
| Figure 17 : APIC : nœud spine et leaf | 25 |
| Figure 18 : Le menu des interfaces spine et leaf | 26 |
| Figure 19 : Les informations sur les nœuds spine et leaf | 26 |
| Figure 20 : APIC : menu VM Networking | 27 |
| Figure 21 : APIC : menu Services L4-L7 | 27 |
| Figure 22 : APIC : menu Admin | 28 |
| Figure 23 : arbre d'information de gestion MIT | 30 |

| | |
|--|----|
| Figure 24 : Interface de login au contrôleur APIC..... | 31 |
| Figure 25 : Les informations d'accès au simulateur APIC | 31 |
| Figure 26 : Le MIT du locataire | 32 |
| Figure 27 : Création d'un locataire..... | 33 |
| Figure 28 : création d'un VRF associé à un domaine du pont | 34 |
| Figure 29 : création d'un sous réseau | 34 |
| Figure 30 : les domaines de pont à créer..... | 35 |
| Figure 31 : création d'un VRF 1 | 36 |
| Figure 32 : création d'un VRF 2 | 36 |
| Figure 33 : association des domaines de pont ave les EPGs..... | 37 |
| Figure 34 : Création d'un Profile d'application | 37 |
| Figure 35 : Création d'un EPG | 38 |
| Figure 36 : création du deuxième Locataire | 40 |
| Figure 37 : création du deuxième sous réseau | 40 |
| Figure 38 : Création d'une Contrat | 41 |
| Figure 39 : Création d'un filter | 41 |
| Figure 40 : création d'un contrat fourni | 41 |
| Figure 41 : création d'un contrat consommé | 42 |
| Figure 42 : contrat exporte | 42 |
| Figure 43 : le contrat exporté a l'autre locataire | 43 |
| Figure 44 : affichage du contrat crée | 43 |
| Figure 45 : création d'un filtre pour le protocole https | 43 |
| Figure 46 : attaché le filtre au contrat déjà crée | 44 |
| Figure 47 : affichage des filtres créés | 44 |

Le contexte du Projet :

Mon projet consiste à étudier l'automatisation d'un réseau data center, pour cela je travaille sur la solution SDN de Cisco : Cisco ACI (Application Centric Infrastructure) et plus précisément sur le contrôleur SDN qui s'appelle APIC (Application Policy Infrastructure Controller).

Donc mon projet sera divisé en plusieurs parties :

1-Introduction sur la technologie SDN et Cisco ACI en particulier.

2-l' étude de la solution Cisco ACI sa terminologie, topologies et ses composants.

3-Introduction de l'interface graphique du contrôleur APIC.

4-la réalisation d'un exemple de configuration du contrôleur APIC.

5-autres configurations sur le contrôleur APIC (routage, sécurité,...).

6- automatiser ces configurations à travers des scripts en python ou avec l'outil d'automatisation Ansible.

Les parties 1 à 4 sont déjà présentées dans ce rapport d'avancement.

Chapitre 1 : Présentation du réseau défini par logiciel

1 *Introduction :*

Les réseaux sont devenus un élément absolument essentiel dans le climat moderne des affaires. Que le réseau soit complètement sur site, sur le Cloud ou hybride, les réseaux fournissent les liaisons de communication vitales qui organisations le besoin pour exécuter leurs applications, fournir services, et être compétitif. Réseau défini par logiciel (SDN) représente une toute nouvelle façon de voir comment les réseaux sont configurés, contrôlés et exploités.

Ce chapitre fournit une introduction à SDN, explique pourquoi SDN est nécessaire et vous montre pourquoi les gens sont si enthousiasmés par l'arrivée des solutions SDN.

2 *Comprendre le SDN :*

Beaucoup de gens ont différentes définitions de SDN. Probablement SDN évolue à mesure que la technologie évolue et que des solutions sont introduites. En général, SDN signifie le plus souvent

que les réseaux sont contrôlés par des applications logicielles et des contrôleurs SDN plutôt que par la gestion de réseau traditionnelle des consoles et des commandes qui nécessitaient de travail administratifs et pouvaient être fastidieuses à gérer à grande échelle.

À l'origine, le réseau SDN suscitait beaucoup d'enthousiasme, tout simplement parce que le contrôle logiciel était beaucoup plus souple que les anciennes consoles de gestion rigides et les interfaces de ligne de commande (CLI). Cette capacité à contrôler rapidement les réseaux via un logiciel on s'est rendu compte que de nombreuses tâches informatiques complexes devant être mises en œuvre à l'aide d'outils de gestion peu pratiques pouvaient maintenant être remplies. Automatisé et fait beaucoup plus efficacement. La rapidité et l'automatisation sont des conditions essentielles pour les réseaux émergents en nuage et les réseaux multi-locataires, qui ont besoin de plus d'échelle et qui ne peuvent pas s'embourber dans des tâches

administratives fastidieuses. En fait, l'automatisation du Cloud (sous ses nombreuses formes) est rapidement devenue l'un des principaux cas d'utilisation de la technologie SDN. Aujourd'hui, de nombreuses solutions SDN sont en réalité des plates-formes d'hébergement de solutions d'automatisation dans le Cloud. Lorsque le SDN a fait son apparition dans le paysage technologique, il existait des idées plus rigides sur la manière dont les architectures SDN devaient être conçues et sur ce qui définissait une solution SDN. Aujourd'hui, les clients ont une vision plus large du type de solution SDN qui leur convient. Le cas d'utilisation principal de SDN ayant évolué vers l'automatisation en nuage, les clients considèrent ce qu'ils recherchent dans une solution d'automatisation basée sur des règles plutôt que seulement les détails de la technologie SDN sous-jacente.

3 *Où étions-nous avant SDN?*

Pour mieux comprendre pourquoi le SDN est devenu si important, vous devez regarder ce qui existait avant le SDN. Les architectures de réseau traditionnelles ont d'importantes limites à surmonter pour répondre aux exigences informatiques modernes. Le réseau d'aujourd'hui doit évoluer pour faire face à des charges de travail accrues avec une plus grande agilité, tout en maintenant les coûts au minimum. Mais l'approche traditionnelle présente des limites importantes:

- Complexité : l'abondance de protocoles de réseau et de fonctionnalités pour des cas d'utilisation spécifiques a considérablement accru la complexité du réseau. Les anciennes technologies étaient souvent recyclées comme solutions rapides pour répondre aux nouvelles exigences de l'entreprise. Les fonctionnalités avaient tendance à être spécifiques au fournisseur ou à être mises en œuvre au moyen de commandes propriétaires.
- Des politiques incohérentes: sécurité et les stratégies de qualité de service (QoS) dans les réseaux actuels doivent être configurées manuellement ou par script sur des centaines, voire des milliers, de périphériques réseau. Cette exigence rend les modifications de stratégie extrêmement compliquées à mettre en œuvre par les organisations sans investissement important dans des compétences en langage de script ou des outils pouvant automatiser les

- modifications de configuration. La configuration manuelle est sujette aux erreurs et peut entraîner de nombreuses heures de dépannage pour déterminer quelle ligne d'une stratégie de sécurité ou d'une liste de contrôle d'accès (ACL) a été entrée de manière incorrecte sur un périphérique donné. De plus, lorsque les applications étaient supprimées, il était presque impossible de supprimer toutes les stratégies associées de tous les périphériques, ce qui augmentait encore la complexité.
- Incapacité à évoluer: à mesure que la charge de travail des applications évolue et que la demande de bande passante réseau augmente, le service informatique doit soit se satisfaire d'un réseau statique sursouscrit, soit s'adapter aux besoins de l'entreprise. Malheureusement, la majorité des réseaux traditionnels sont configurés de manière statique de manière à augmenter le nombre de points de terminaison, de services ou de bande passante nécessite une planification et une refonte substantielles du réseau.

4 Où SDN nous emmène-t-il?

Au début, il y avait beaucoup de battage publicitaire autour du SDN avant de comprendre les cas d'utilisation réels des clients. Cependant, ce qui émerge lentement et qui motive tous les investissements, projets pilotes et conceptions de produits, constitue un moyen bien plus efficace de gérer le réseau étendu (WAN) d'entreprise, les data centers et les réseaux en nuage - et d'automatiser les tâches informatiques afin que l'infrastructure puisse réagir de manière dynamique aux changements rapides et les exigences. L'intelligence nécessaire pour que tout cela se produise passe des périphériques réseau et des consoles de gestion de périphériques aux contrôleurs de gestion de stratégie centralisés basés sur SDN. La principale évolution de SDN est la prise de conscience du fait que très peu d'organisations ont réellement le désir, les compétences et les incitations nécessaires pour écrire une nouvelle classe d'applications pour la programmation du réseau. La grande majorité des entreprises cherchent simplement à automatiser leurs tâches informatiques, à accélérer le déploiement d'applications, à assouplir leurs réseaux dans le Cloud et à mieux aligner leur infrastructure informatique sur les besoins de l'entreprise. SDN est désormais une plate-forme capable d'héberger une multitude de

solutions d'automatisation de flux de travail informatique et d'orchestration qui permettent aux clients d'atteindre leur objectif final. Les administrateurs réseau n'écriront donc pas nécessairement de nouvelles applications, mais ils achèteront de nouvelles solutions d'automatisation clé en main reposant sur des plates-formes et des technologies SDN.

Voir pourquoi il y a tant d'excitation

SDN a déjà suscité beaucoup d'intérêt et d'enthousiasme dans la communauté informatique. Les sections suivantes examinent rapidement certaines des raisons pour lesquelles cela se produit.

4.1 SDN facilite la virtualisation des serveurs et réseaux en nuage (Cloud)

Traditionnellement, les entreprises avaient une réponse simple à la demande croissante de capacité de données et aux besoins croissants en bande passante - une capacité matérielle supplémentaire (et coûteuse). Malheureusement, la plupart des entreprises ne peuvent plus se permettre un tel système. L'approche coûteuse, surtout face à la croissance exponentielle en demande. Les marchés extrêmement concurrentiels signifient que vous ne pouvez pas vous permettre de vous en sortir. SDN a notamment pour avantage de tirer parti de la virtualisation des serveurs pour accroître l'efficacité des ressources, réduire la complexité du réseau et simplifier les processus informatiques manuels pour déployer, gérer et adapter les applications et les réseaux. L'une des raisons pour lesquelles l'approche traditionnelle visant à résoudre le besoin de ressources informatiques supplémentaires était si coûteuse est que le modèle traditionnel a assigné une unité informatique complète à une tâche unique. Par exemple, chaque utilisateur avait son propre PC dédié et chaque serveur de réseau consistait en un ordinateur physique situé quelque part dans un rack dans un data center. L'approche plus moderne utilise la virtualisation des serveurs pour faire fonctionner un seul serveur physique comme s'il s'agissait de plusieurs serveurs, chacun effectuant des tâches différentes et exploitant toute la capacité du serveur. SDN utilise la virtualisation pour accroître considérablement l'efficacité du réseau et

ainsi apporter des solutions au besoin de capacité accrue sans casser la banque et simplifier la gestion de ces ressources consolidées.

4.2 *SDN concerne principalement l'automatisation basée sur des règles*

À mesure que la taille des réseaux augmente, leur gestion et leur maintenance deviennent beaucoup plus complexes. Dans le modèle traditionnel, cette complexité signifie que de plus en plus de ressources informatiques sont nécessaires pour gérer des processus tels que le provisionnement, la configuration et la correction. Il s'agissait tout simplement de processus manuels. Par conséquent, si votre réseau passait de dix à cent nœuds, il était nécessaire de manipuler et de configurer manuellement dix fois plus de périphériques. SDN modifie cette équation de manière fondamentale: il automatise des processus tels que le provisionnement, configuration et correction via un logiciel. Plutôt que de demander à un informaticien de configurer physiquement chaque élément matériel, SDN vous permet de déployer les modifications apportées au réseau en envoyant des mises à jour logicielles. Toutes les implémentations SDN ne sont pas égales. Par exemple, la structure ACI (Application Centric Infrastructure) de Cisco englobe les périphériques réseau intelligents qui facilitent beaucoup l'automatisation des processus réseau, car il n'est pas nécessaire de s'adresser spécifiquement à chaque périphérique pour propager correctement les processus là où ils doivent être appliqués. Vous voudrez vous assurer que la solution SDN que vous choisissez prend pleinement en charge les fonctions d'automatisation dont vous avez besoin afin de tirer pleinement parti du passage à la technologie SDN. ACI, la solution SDN la plus complète de Cisco, accélère considérablement les délais de livraison des applications grâce à des processus informatiques simplifiés et automatisés.

Chapitre 2 : Comprendre les composants et la structure ACI

1 Introduction :

Cisco Application Centric Infrastructure (ACI) est une étape importante dans l'évolution des data centers. la mise en réseau. Non pas parce que cela ajoute de la programmabilité au réseau, cela a été une hausse tendance au cours des dernières années, mais en raison de la compatibilité accrue entre les fournisseurs. C'est là que sont les avantages réels.

Alors, qu'en est-il des réseaux où un fournisseur peut fournir tous les équipements, de la mise en réseau au stockage, en passant par les éléments de calcul? Il est en fait assez rare de trouver un environnement composé d'un seul fournisseur dans le monde réel, la plupart des réseaux (et j'inclus les plates-formes de virtualisation et de stockage dans ce terme) ont des équipements de plus d'un fournisseur, car lorsque vous recherchez les meilleures performances, vous allez avec les grands noms (VMware pour la virtualisation, NetApp pour le stockage, etc.), car ils ont la longévité de l'industrie, les connaissances et les options de support nécessaires. Le réseau devient hétérogène, car il doit l'être pour répondre aux besoins des utilisateurs, des applications et des entreprises.

ACI permet à l'administrateur réseau et aux développeurs d'applications de collaborer plus étroitement. Les applications changent, les réseaux changent. Les deux ont des cycles de vie de durée variable et ACI permet à ces cycles de coexister les uns avec les autres et de se compléter. Les deux équipes peuvent travailler ensemble pour atteindre un objectif commun. ACI réduit la complexité du réseau en ce qui concerne le déploiement, la gestion et la surveillance, et ce, grâce à un cadre de règles commun. Les applications peuvent être déployées rapidement et les frais administratifs sur le réseau sont considérablement réduits. Il est donc centré sur les applications et peut faciliter les services des couches 4 à 7 pour améliorer le cycle de vie des applications.

Grâce à ACI, nous pouvons automatiser et programmer le réseau. Nous disposons d'une plate-forme unique pour approvisionner le réseau. Nous pouvons facilement intégrer des services

tels que la virtualisation (VMware et Hyper-V), des pare-feu, des équilibreurs de charge et toute une gamme d'infrastructures qui nécessiteraient auparavant de nombreuses heures de configuration et de reconfiguration, à la demande du marché. Changement d'application.

Cette automatisation est effectuée via des stratégies. Les stratégies sont configurées de manière centralisée sur les APIC (Application Policy Infrastructure Controller), qui sont (généralement) en cluster. L'APIC est l'endroit où nous allons commencer.

2 *Un aperçu du Fabric ACI*

Le fabric est un terme sophistiqué pour la manière dont les composants informatiques, réseau et logiciels d'une data center sont disposés. Le nom lui-même vient du croisement du réseau, un peu comme un vêtement tissé. La structure de l'ACI est relativement simpliste. Il emploie un double niveau conception faite des commutateurs spines et leaves, mais des commutateurs très particuliers.

2.1 *Matériel ACI*

Dans la figure, nous pouvons voir un déploiement typique avec deux spines et trois leaves. Le Nexus 9500 commutateurs modulaires sont déployés au sommet de la topologie et agissent comme des spines qui, dans la conception de réseau classique à trois niveaux serait l'agrégation ou les commutateurs centraux. Les cartes de ligne sont utilisées pour fournir les ASIC (circuits intégrés à application spécifique) requis pour l'ACI. Différentes cartes de ligne sont disponibles. Le composant suivant est le commutateur leaf. Ce sont les commutateurs de la série Nexus 9300. Les spines se connectent aux leaves via 40 ports GE(GigaEthernet), mais les spines et les leaves ne sont jamais connectées (spine à spine, ou leaf à leaf).

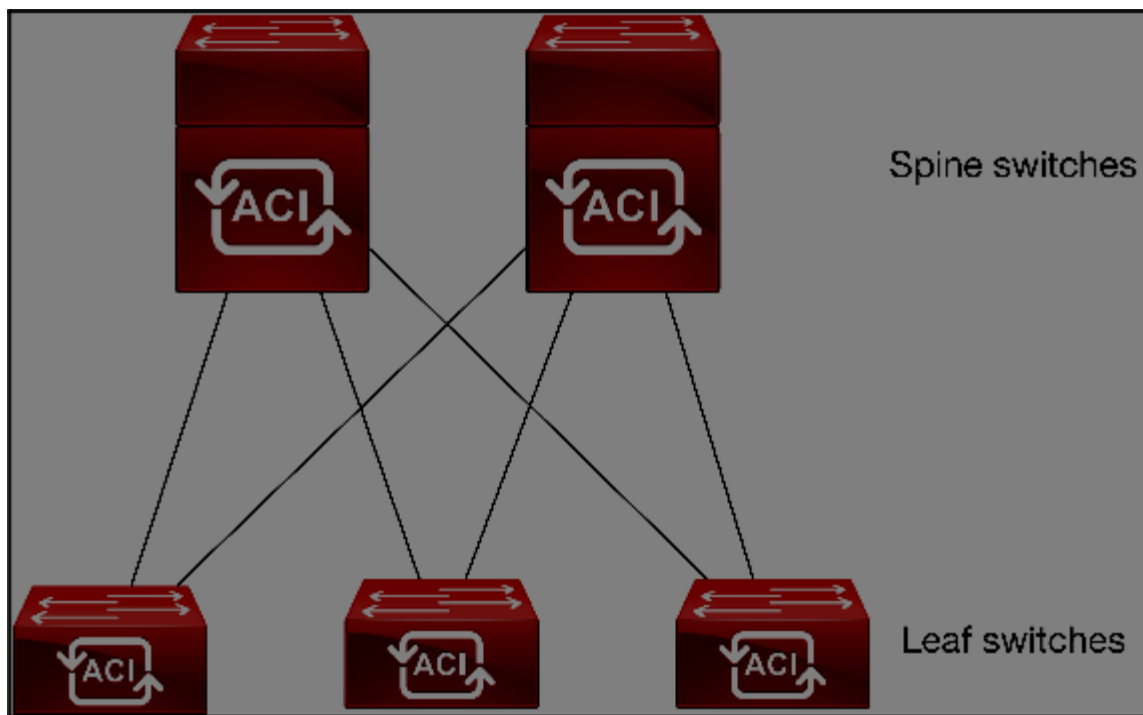


Figure 1 : L'architecture d'ACI

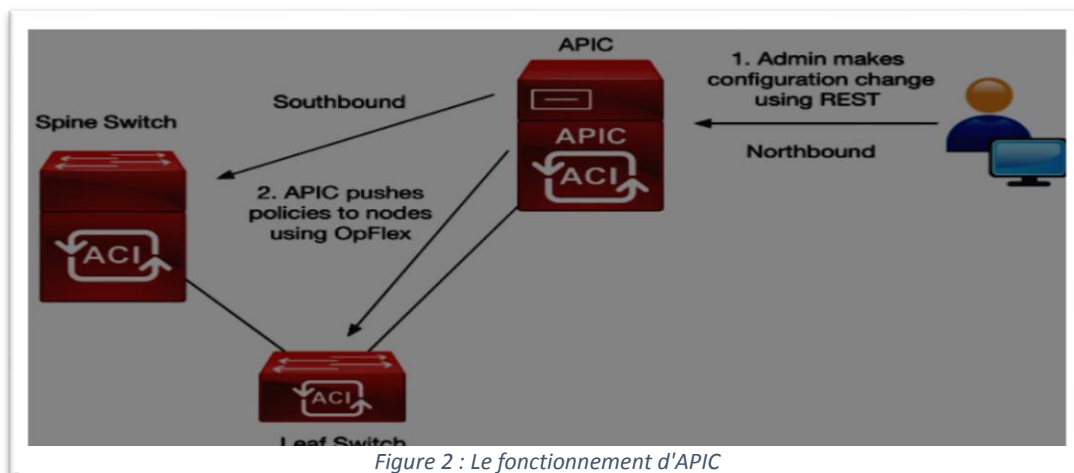
2.2 Les Composants d'ACI

Les principaux composants d'un déploiement d'ACI sont les suivants:

- **Les commutateurs feuilles (Leaves)** : fournissent une connectivité à la structure au niveau du ToR ou de l'EoR. Ils servent de passerelles distribuées de couche 3, de points d'application des règles et de passerelles vers des réseaux externes.
- **Les commutateurs feuille frontière (Border Leaf Switches)** : sont tous les nœuds feuille qui se connectent à un périphérique réseau externe à la structure ACI, tels que les pare-feu, les équilibreurs de charge, les routeurs ou les commutateurs non ACI; permettant une migration en douceur vers un réseau ACI.
- **Les Spines Switches** : constituent une structure non bloquante permettant une détection rapide des défaillances et un réacheminement. Ceux-ci sont utilisés pour transférer le trafic entre deux commutateurs de feuille. À compter de la version

logicielle 2.0 (2), ACI prend en charge les connexions de couche 3 avec EVPN aux commutateurs spine.

- Les contrôleurs APIC** fournissent le point de gestion centralisé pour la configuration de la structure et l'observation de l'état opérationnel récapitulatif. Du point de vue des politiques, l'APIC est le principal point de contact pour la configuration et fait référentiel de politique. L'APIC est notre frontend. Grâce à cela, nous pouvons créer et gérer nos politiques, gérer le fabric, créer des locataires (Tenant) et résoudre les problèmes. Plus important encore, l'APIC n'est pas associé au chemin de données. Si nous perdons l'APIC pour quelque raison que ce soit, le fabric continuera à transmettre le trafic. ACI utilise plusieurs API (Application Programming Interfaces) tels que REST (Representational State Transfer) en utilisant des langues comme JSON (JavaScript Object Notation) et XML (eXtensible Markup Language), ainsi que CLI et l'interface graphique, pour gérer le fabric et d'autres protocoles, tels qu'OpFlex, pour politiques aux périphériques réseau. Le premier ensemble (ceux qui gèrent le fabric) est appelé Protocoles «northbound». Les protocoles Northbound permettent aux composants réseau de bas niveau de parler à ceux de niveau supérieur. OpFlex est un «southbound».protocole. Les southbound protocoles (tels que OpFlex et OpenFlow) permettent aux contrôleurs de pousser les politiques vers les nœuds(les commutateurs).



3 Terminologie ACI

Les APIC fonctionnaient à l'aide d'un moteur de règles basé sur les objets. Cela permet à l'administrateur réseau de définir les états souhaités de la structure, tout en laissant l'implémentation au contrôleur (APIC). À mesure que les charges de travail sont déplacées, le contrôleur reconfigure l'infrastructure sous-jacente afin de garantir que les stratégies nécessaires sont toujours en place pour les hôtes finaux. La branche du modèle d'objet dans laquelle ces stratégies sont définies est l'objet **Tenant**. C'est là que se trouvent la plupart des opérations quotidiennes.

3.1 Locataires ACI

Les locataires sont un objet de niveau supérieur qui aide à identifier et à séparer le contrôle administratif, les domaines de réseau / de défaillance et les stratégies d'application. Les objets de sous-niveau d'un client peuvent être regroupés en deux catégories de base: le locataire Mise en réseau et le locataire des politiques (Policies). Ces deux catégories ont des relations inhérentes, mais il peut être utile d'en discuter séparément.

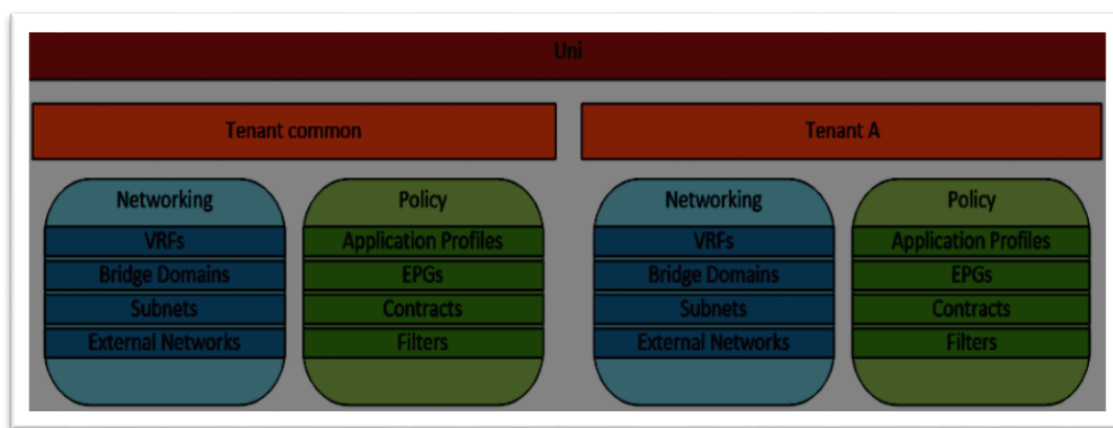


Figure 3 : Locataire ACI

3.2 Locataire "commun"

ACI a un locataire spécial nommé "commun" qui a la capacité unique de partager facilement ses ressources avec d'autres locataires. Le locataire "commun" est conçu pour fournir des ressources partagées à l'ensemble de la structure de l'ACI, telles que

le DNS, les services d'authentification, les outils de sécurité, etc. Vous pouvez également définir tous les objets, contrats et filtres de mise en réseau de locataire dans le locataire "commun" et les associer à des applications d'autres locataires.

3.3 Mise en réseau des locataires

Les objets Mise en réseau client sont similaires aux structures réseau que les ingénieurs connaissent déjà et fournissent la connectivité de couche 2 et de couche 3 entre les hôtes le locataire Mise en réseau comprend des fichiers VRF, des domaines de pont, des sous-réseaux et des réseaux externes.

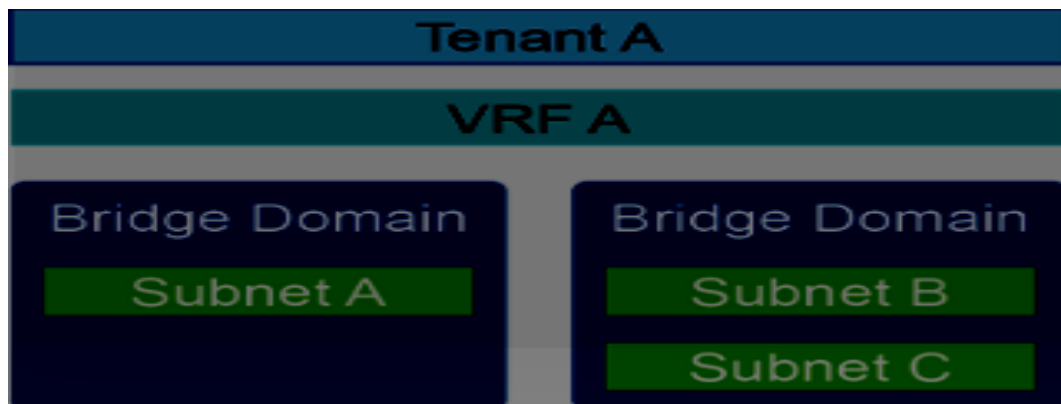


Figure 4 : Locataire réseau

- **Les VRF** : également appelés contextes et réseaux privés, sont des tables de routage isolées pour le locataire. Un locataire peut avoir un ou plusieurs VRF, ou peut utiliser un VRF du locataire "commun". Dans le diagramme ci-dessous, l'infrarouge est situé dans la zone grise. Tous les VRF supplémentaires existent sur toute Leaf commutateur ayant un hôte attribué au VRF.
- **Les domaines de pont** : sont les domaines de transmission de couche 2 au sein de la structure et définissent l'espace d'adressage MAC unique et le domaine d'inondation (diffusion, monodiffusion inconnue et multidiffusion). Chaque domaine de pont est associé à un seul fichier VRF. Toutefois, un fichier VRF peut être associé à de nombreux domaines de pont. Contrairement au mode de

déploiement traditionnel des VLAN, chaque domaine de pont peut contenir plusieurs sous-réseaux.

- **Sous - réseaux** : sont la couche 3 réseaux qui fournissent des services spatiaux et de passerelle IP pour les hôtes de se connecter au réseau. Chaque sous-réseau est associé à un seul domaine de pont.
- **Les réseaux pontés externes** : connectent un réseau de couche 2 Spanning-Tree à la structure ACI. Ceci est couramment utilisé dans les environnements de friches industrielles pour permettre une migration en douceur d'une infrastructure réseau traditionnelle vers un réseau ACI. Le diagramme suivant présente également des réseaux externes de couche 2 pour les périphériques de couche 4 à 7 (L4-L7).
- **Les réseaux routés externes** : créent une adjacence de couche 3 avec un réseau situé en dehors de la structure ACI. Couche 3 Les réseaux externes prennent en charge les adjacences à l'aide d'itinéraires statiques ou de BGP, OSPF et EIGRP. Les connexions de couche 3 ont également des réseaux définis, qui

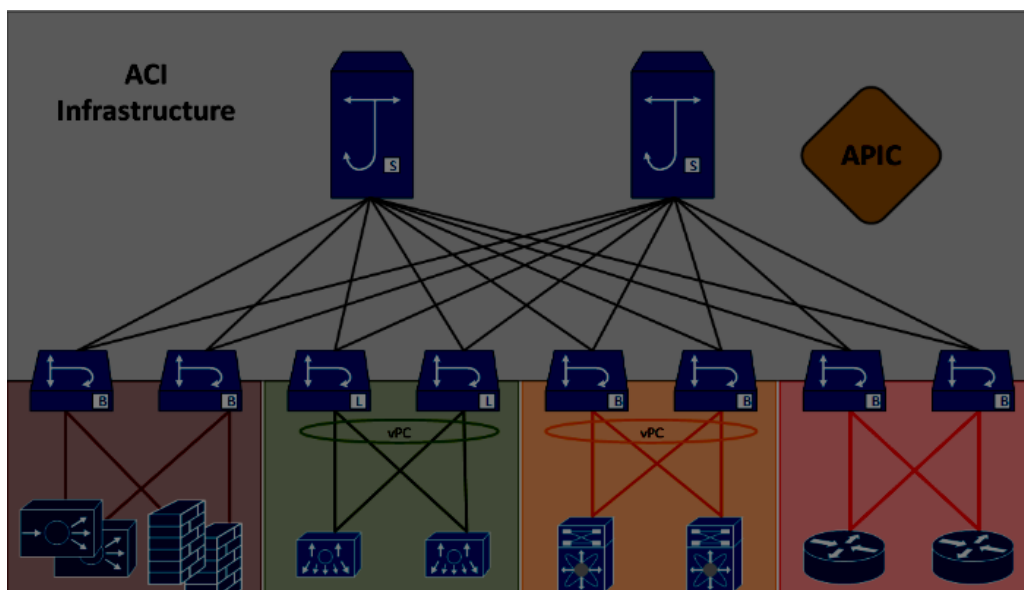


Figure 5 : L'infrastructure d'ACI

fournissent et consomment des contrats (traités plus en détail dans la politique du locataire).

3.4 Locataire des politiques

Les objets de locataire de politique sont liés aux objets réseau, mais les objets de locataire de politique sont davantage centrés sur les politiques et les services reçus par les ordinateurs d'extrémité. Le locataire de politique comprend des profils d'application, des groupes des points de terminaison, des contrats et des filtres. Ce sont tous des termes nouveaux et spécifiques à ACI.

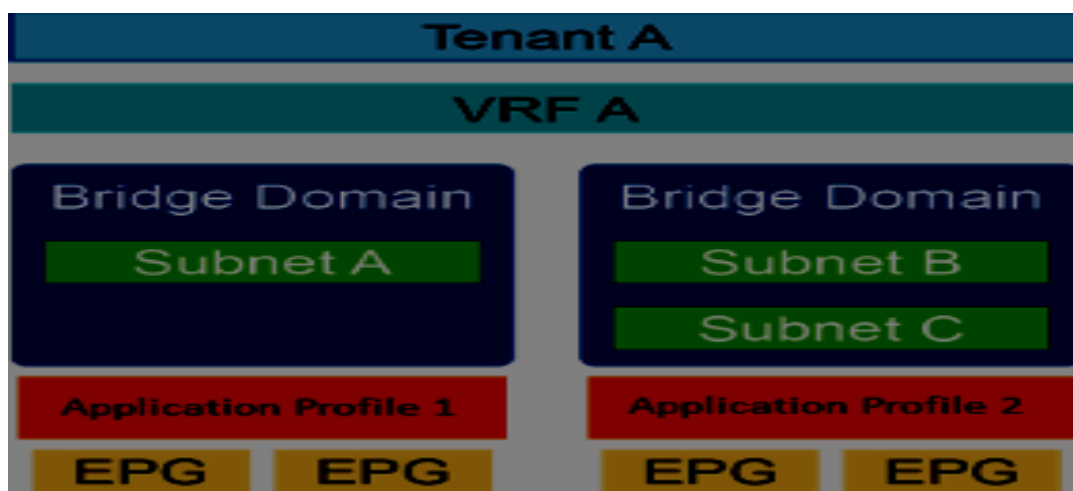


Figure 6 : Locataire des politiques

- **Un profil d'application** : est un conteneur pour les groupes des équipements d'extrémité (EPG). Le profil d'application est utilisé comme identifiant pour les applications et permet la séparation des privilèges d'administrateur.
- **Un groupe des équipements d'extrémité(EPG)** est un ensemble des équipements d'extrémité auxquels les mêmes services et stratégies sont appliqués. Les EPG définissent les ports de commutation, les commutateurs virtuels et les encapsulations de couche 2 associés à un service d'application. Chaque EPG ne peut être associé qu'à un seul domaine de pont.

- **Les contrats** : définissent les services et les politiques appliqués aux équipements d'extrémité dans un EPG. Les contrats peuvent être utilisés pour la redirection de service vers un périphérique L4-L7, l'attribution de valeurs de QoS et l'application de règles ACL. L'EPG qui offre les services fournit le contrat et les EPG qui doivent utiliser le service utilisent le contrat.
- **Les filtres** : sont les objets qui définissent les protocoles (TCP, UDP, ICMP, etc.) et les ports. Les objets de filtre peuvent contenir plusieurs protocoles et ports, et les contrats peuvent utiliser plusieurs filtres.

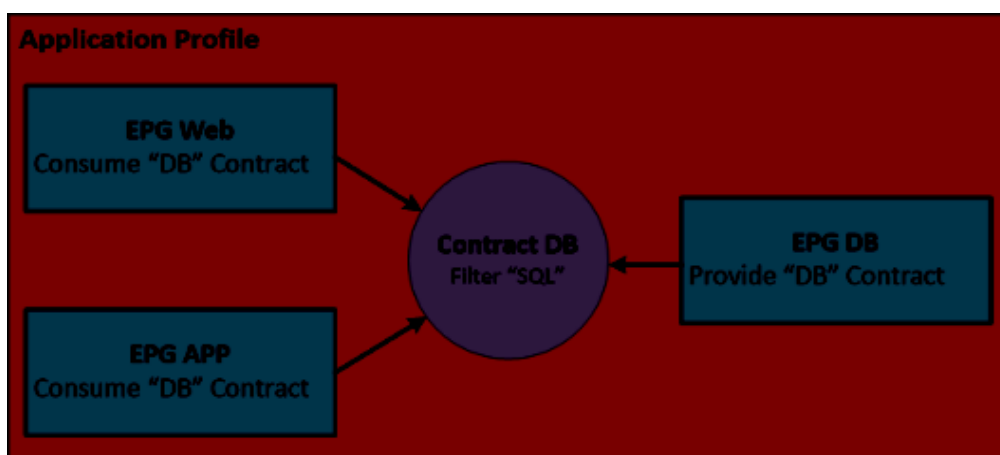


Figure 7 : Profile d'application

4 Compréhension de la third-party intégration :

L'une des raisons les plus intéressantes de déployer ACI est la facilité d'intégration avec d'autres logiciels produits (tels que le pare-feu ASA) et les systèmes tiers. Cette intégration est effectuée via OpFlex. OpFlex est un protocole southbound, basé sur des normes ouvertes, conçu pour faciliter l'intégration multifournisseurs dans les réseaux de centres de données et dans le Cloud. OpFlex est important car il différencie ACI des autres modèles SDN, qui intègrent mais ne prennent pas en charge l'ensemble des fonctionnalités.

5 La plateforme Cisco Devnet et Sandbox

Cisco offre une plateforme de test s'appelle devnet en collaboration avec sandbox, cette plateforme contient plusieurs labs et des simulations :

5.1 Qu'est-ce que Devnet Sandbox?

Devnet Sandbox permet aux développeurs et aux ingénieurs d'accéder **gratuitement** à la technologie Cisco aux laboratoires en proposant des laboratoires prêts à l'emploi que nous appelons des Sandbox. C'est vrai, totalement gratuit! Il existe deux types de Sandbox, **Toujours** actif et **Réservation**. Chaque sandbox met généralement en évidence un produit Cisco (think, CallManager, APIC, etc.). Sandbox peuvent être utilisés pour le développement, le test des API, l'apprentissage de la configuration d'un produit, la formation, les hackathons et bien plus encore!

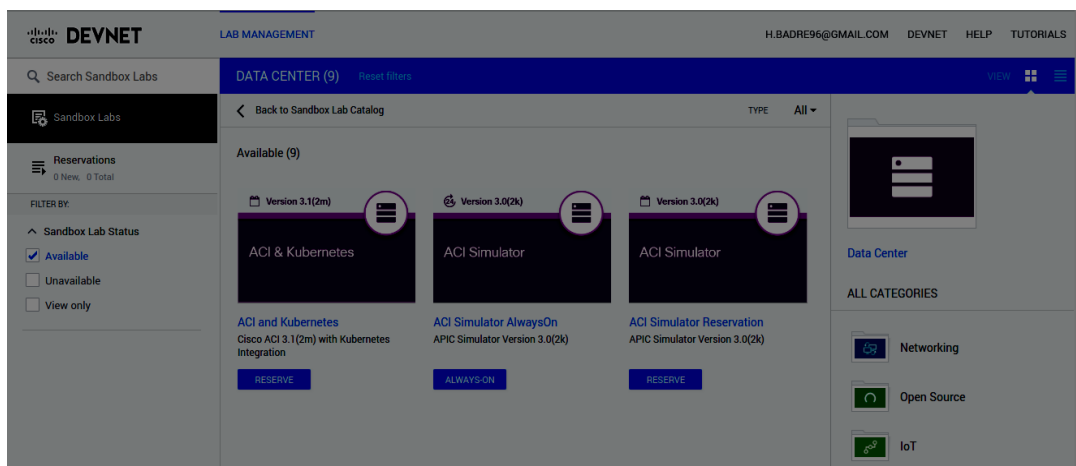


Figure 8 : Devnet Labs

parmi ces simulations, Cisco offre un simulator de la solution Cisco ACI AlwaysOn contient deux switch leaf et une spine avec un contrôleur SDN de la solution Cisco ACI, le contrôleur APIC.

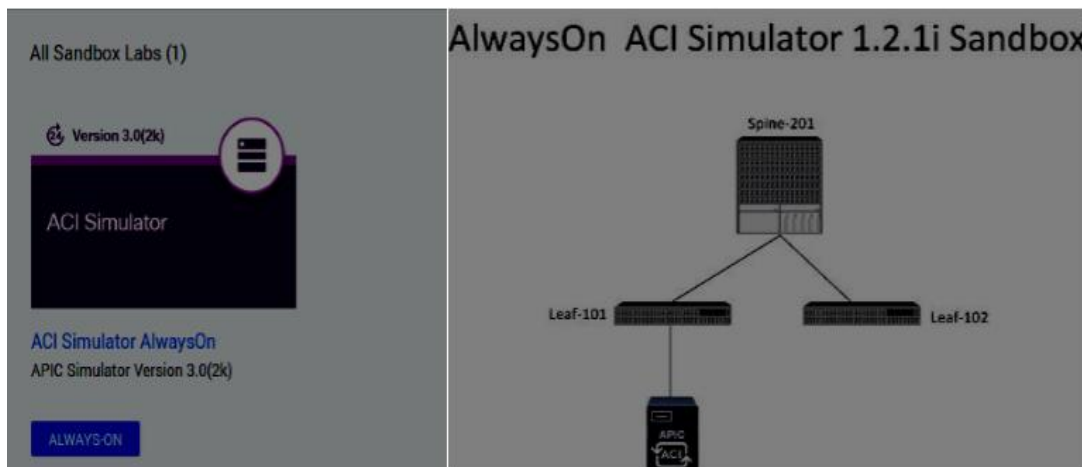


Figure 9 : Devnet ACI simulator

sur cette plateforme où je travaille durant ce projet :

6 Une introduction à l'interface graphique du contrôleur APIC :

Lors de l'accès à l'APIC de la plateforme Devnet, la page de connexion s'affiche. Cela peut prendre quelques minutes au système pour s'initialiser complètement avant que nous puissions nous connecter.

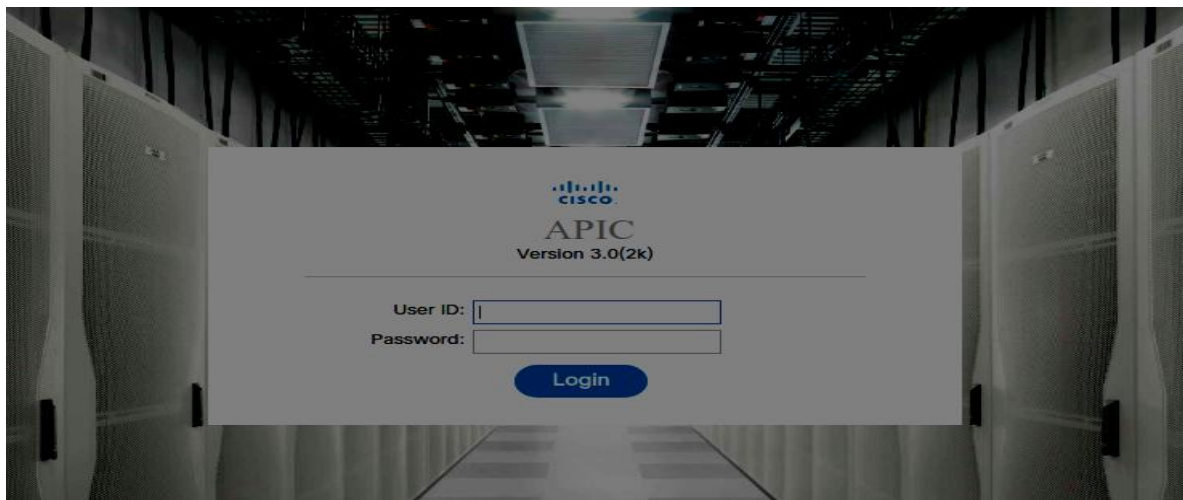


Figure 10 : Login au Plateforme APIC

User Id : admin

Password : ciscopsdt

Une fois que nous nous sommes connectés avec succès, la page Système s'affiche. Nous avons le menu principal en haut et chaque élément de menu a un sous-menu. Ici, nous pouvons voir le menu Système, avec son sous-menu affichant Démarrage rapide, Tableau de bord, Contrôleurs, Défauts, Paramètres par défaut, Zones de configuration, Événements et Journal d'audit:

6.1 Menu système

La page système nous montre la santé du système, répartie entre la santé globale du système et les nœuds et les locataires avec une santé inférieure à 99%. Le nombre de défauts est indiqué à droite, par domaine et par type. Nous pouvons voir l'état du contrôleur dans le coin inférieur droit.

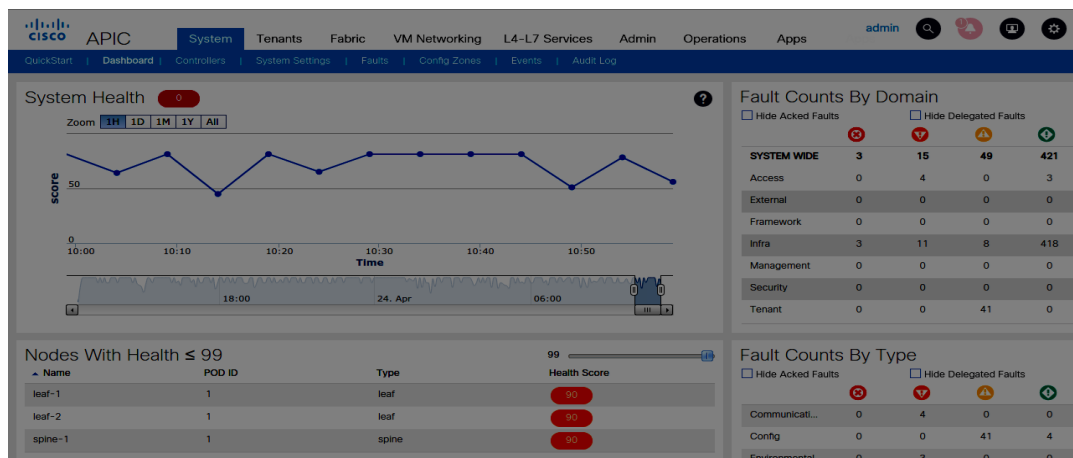


Figure 11 : APIC : Menu système

En passant au sous-menu Controllers, nous pouvons voir l'écran de la section précédente.

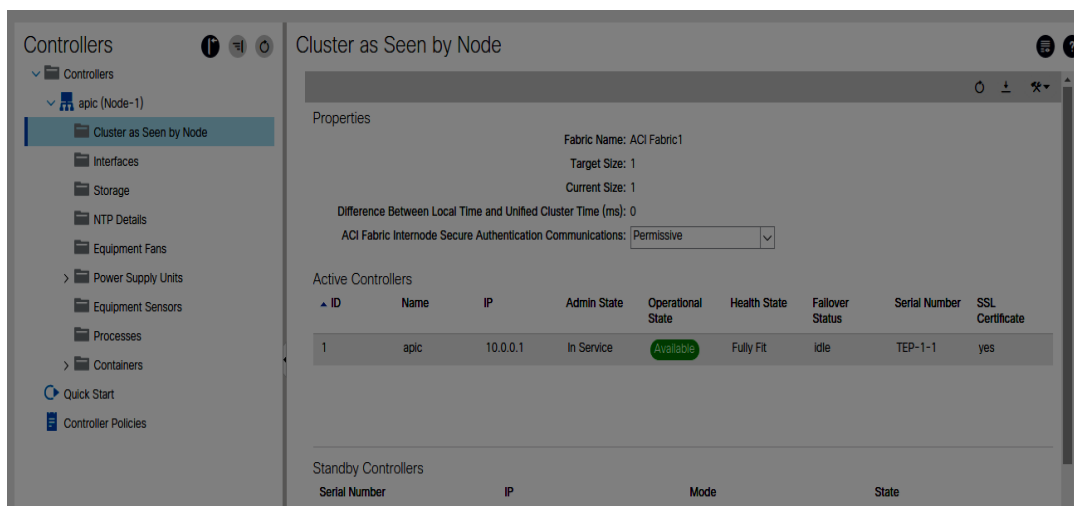


Figure 12 : APIC : sous-menu Controllers

Nous avons un contrôleur (apic1), son adresse IP est 10.0.0.1, il est en service, disponible et l'état d'intégrité est «Fully Fit».

Nous pouvons voir les interfaces présentes sur notre contrôleur (apic1) à partir du menu Interfaces à gauche:

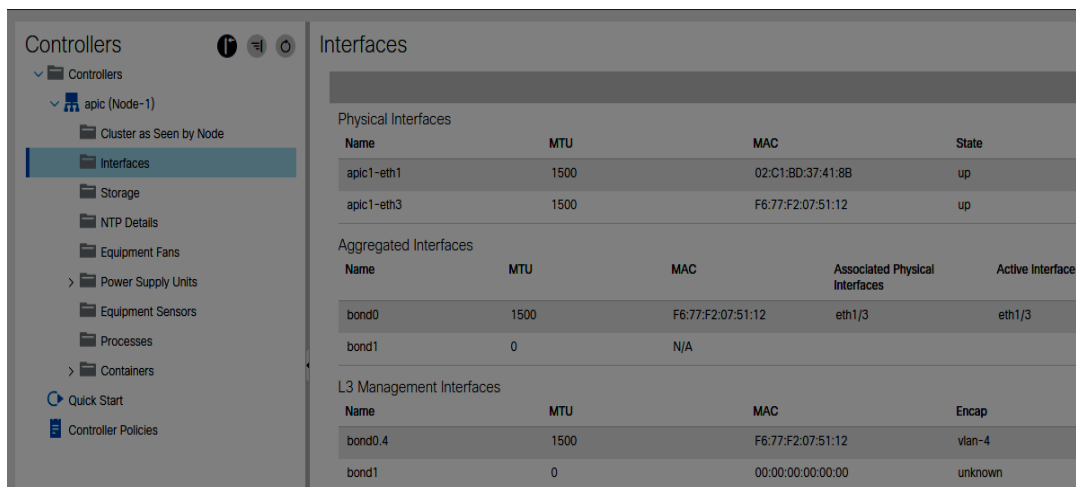
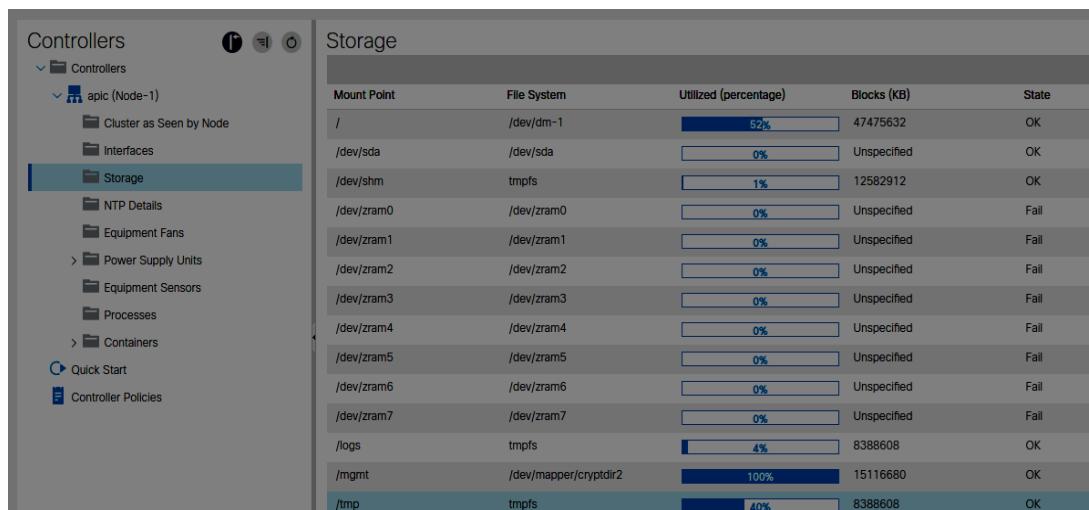


Figure 13 : Les Interfaces du contrôleur APIC

Nous pouvons suivre la quantité de stockage que nous avons utilisée à partir de l'option de menu Stockage.



| Mount Point | File System | Utilized (percentage) | Blocks (KB) | State |
|-------------|-----------------------|-----------------------|-------------|-------|
| / | /dev/dm-1 | 52% | 47475632 | OK |
| /dev/sda | /dev/sda | 0% | Unspecified | OK |
| /dev/shm | tmpfs | 1% | 12582912 | OK |
| /dev/zram0 | /dev/zram0 | 0% | Unspecified | Fail |
| /dev/zram1 | /dev/zram1 | 0% | Unspecified | Fail |
| /dev/zram2 | /dev/zram2 | 0% | Unspecified | Fail |
| /dev/zram3 | /dev/zram3 | 0% | Unspecified | Fail |
| /dev/zram4 | /dev/zram4 | 0% | Unspecified | Fail |
| /dev/zram5 | /dev/zram5 | 0% | Unspecified | Fail |
| /dev/zram6 | /dev/zram6 | 0% | Unspecified | Fail |
| /dev/zram7 | /dev/zram7 | 0% | Unspecified | Fail |
| /logs | tmpfs | 4% | 8388608 | OK |
| /mgmt | /dev/mapper/cryptdir2 | 100% | 15116680 | OK |
| /tmp | tmpfs | 40% | 8388608 | OK |

Figure 14 : le stockage d'APIC

6.2 Menu des locataires

L'onglet Locataires nous montre tous nos locataires. Nous avons trois préconfigurés (commun, infra et mgmt.):



| Name | Description | Bridge Domains | VRFs | EPGs | Health Score |
|--------|-------------|----------------|------|------|--------------|
| common | | 1 | 2 | 0 | 100 |
| infra | | 1 | 1 | 1 | 100 |
| mgmt | | 1 | 2 | 0 | 100 |

Figure 15 : APIC : Menu Locataire

Si nous sélectionnons un locataire et que nous parcourons les options, nous pouvons voir les profils d'application qui lui sont attribués, la configuration de la mise en réseau, les paramètres de service Layer4-Layer7 et toutes les stratégies. Nous verrons cela plus en détail dans le prochain chapitre lorsque nous établirons des locataires. C'est là que nous créerions de nouveaux locataires.

6.3 Menu de Fabric

Dans le menu Fabric et le sous-menu Inventory, vous pouvez voir notre topologie:

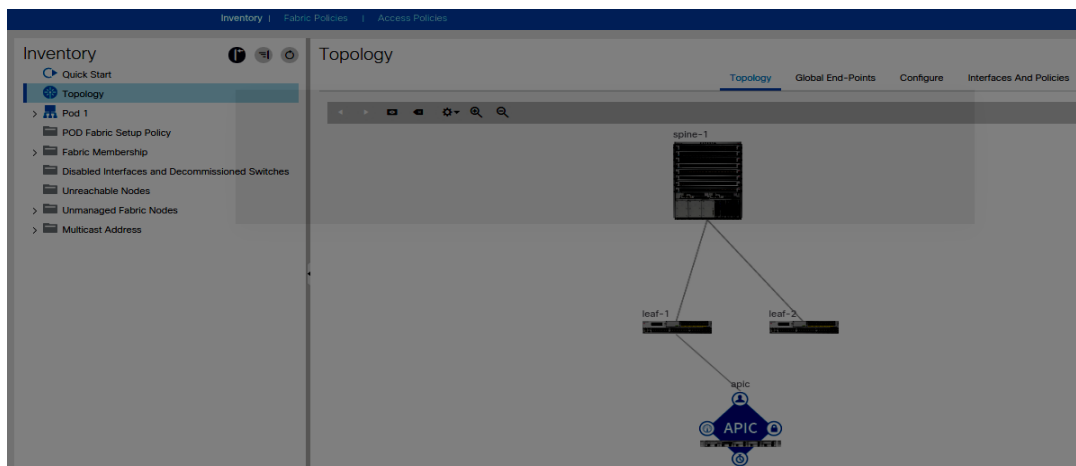


Figure 16 : APIC : Menu Fabric

Si nous parcourons le Pod, nous pouvons voir tous nos nœuds de leaves et spines

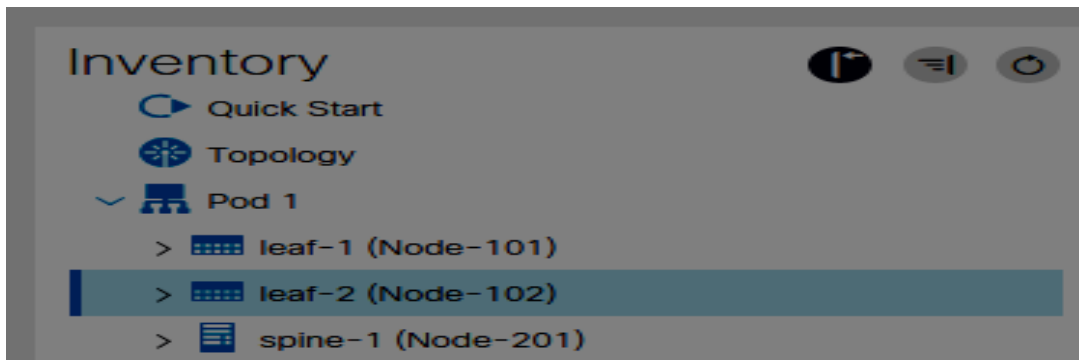


Figure 17 : APIC : nœud spine et leaf

En les parcourant, nous pouvons voir nos interfaces, nos tables de routage, nos processus, nos pools et nos règles. Une chose à noter ici est que nous avons beaucoup plus d'options de routage avec un nœud leaf que nous ne faisons un nœud spine:

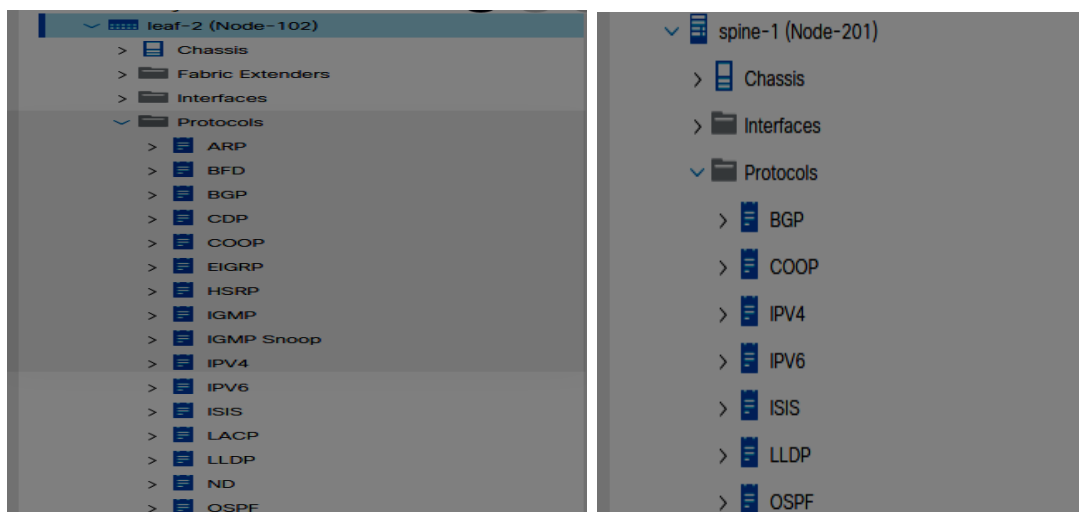


Figure 18 : Le menu des interfaces spine et leaf

Sous l'option Fabric Membership, nous avons une liste de nos nœuds leaf et spine, qui nous indique les numéros de série, l'ID, le nom, le modèle, le rôle et l'adresse IP attribuée. Il nous fournit également les informations de certificat.

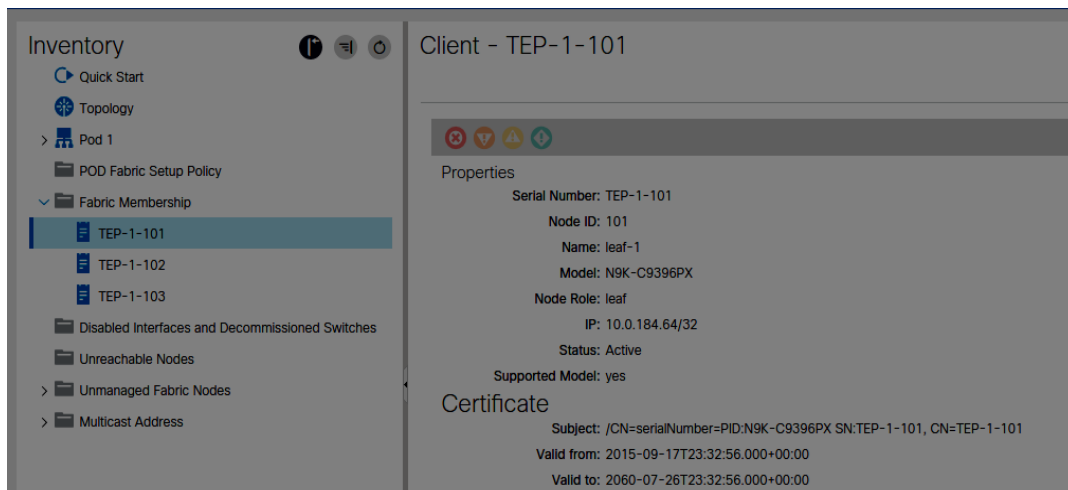


Figure 19 : Les informations sur les nœuds spine et leaf

6.4 VM Networking

Dans le menu VM Networking, vous pouvez commencer à connecter ACI à nos third-party fournisseurs. Les options par défaut sont kubernetes, Microsoft, OpenStack et VMware.

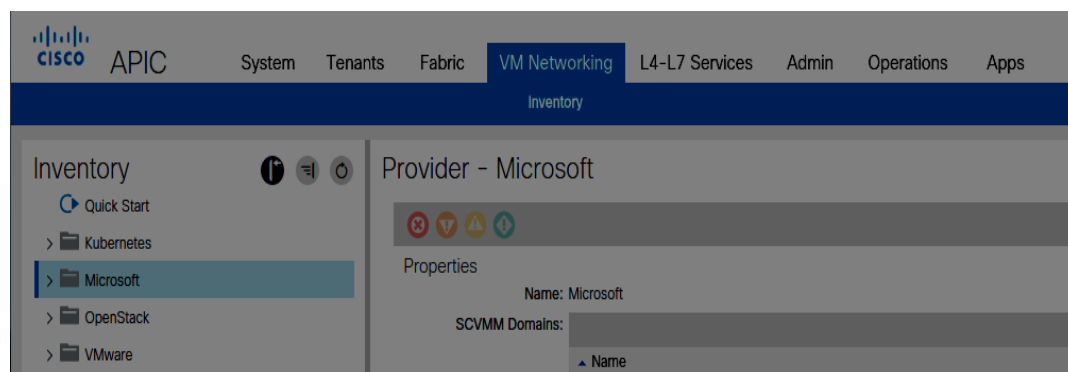


Figure 20 : APIC : menu VM Networking

6.5 Services L4-L7

Les services L4-L7 nous permettent d'élargir davantage notre ACI fabric avec des third-party solutions supplémentaires. Ceci est effectué via l'ajout de packages, que nous pouvons importer à partir du sous-menu Packages.

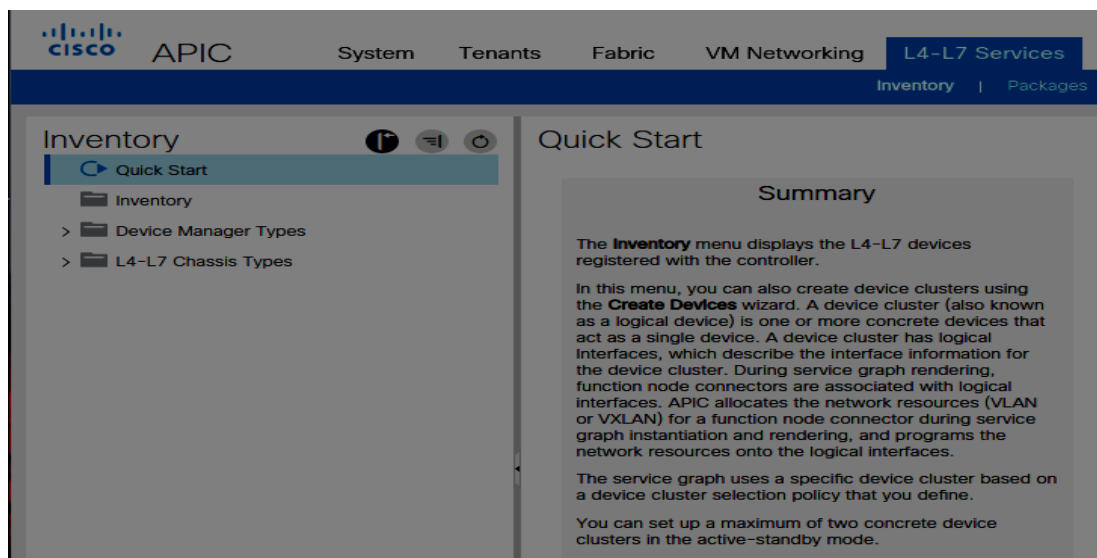


Figure 21 : APIC : menu Services L4-L7

6.6 Admin

Dans le menu Admin, nous configurons AAA (authentification, autorisation et comptabilité). Ici, nous pouvons configurer RBAC et également vous connecter à des fournisseurs d'authentification, tels que LDAP, tels que Microsoft Active Directory, RADIUS ou TACACS +. Nous pouvons également configurer PKI pour utiliser des chaînes de certificats.

Nous pouvons créer des calendriers de maintenance, qu'ils soient ponctuels ou réguliers. Nous pouvons configurer nos stratégies de conservation des journaux, mettre à niveau notre microprogramme et configurer Callhome (après avoir configuré les stratégies dans le menu Fabric), SNMP et Syslog.

Le menu Admin est également celui où nous effectuerions des restaurations de configuration, l'importation de fichiers de configuration et l'exportation de fichiers de support technique.

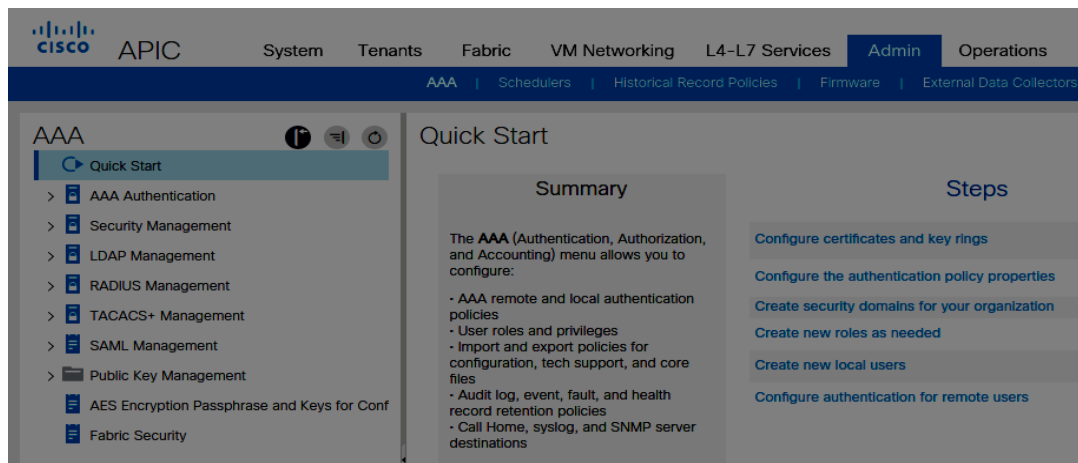


Figure 22 : APIC : menu Admin

6.7 *Opérations*

La dernière option du menu est Opérations. C'est là que nous pourrions effectuer la plupart de nos dépannages, le cas échéant. À partir de là, nous trouvons des points d'extrémité et examinons le chemin du trafic, ainsi que les éventuelles failles le long du chemin. Nous pouvons également effectuer un traceroute pour vérifier le plan de données.

Nous pouvons également vérifier l'utilisation avec Capacity Dashboard, créer des modèles de configuration optimisée

Chapitre 3: Configuration des stratégies et Le locataires

1 Introduction :

Nous allons commencer à configurer l'ACI fabric en créant des règles et quelques locataires. Le modèle de stratégie ACI concerne uniquement la mise en correspondance des exigences d'application et des stratégies. Nous avons besoin du locataire A pour parler à un serveur SQL; nous créons une politique pour cela. Nous avons également besoin du locataire A pour parler au système de stockage; nous créons une politique pour cela.

L'APIC gère les politiques. Lorsque nous apportons une modification à un objet du fabric, il appartient à l'APIC d'appliquer cette modification au modèle de stratégie, qui effectue ensuite la modification sur le nœud final affecté. Un tel exemple serait d'ajouter un nouveau périphérique au fabric.

La communication avec le nouveau périphérique est interdite jusqu'à ce que le modèle de stratégie soit mis à jour pour inclure le nouveau périphérique.

Il existe différentes politiques, mais elles peuvent être divisées en groupes assez distincts. celles qui régissent l'ensemble du fabric d'ACI et celles qui concernent les locataires. Toutes les stratégies sont enregistrées dans le MIT (Management Information Tree), ou arbre d'informations de gestion.

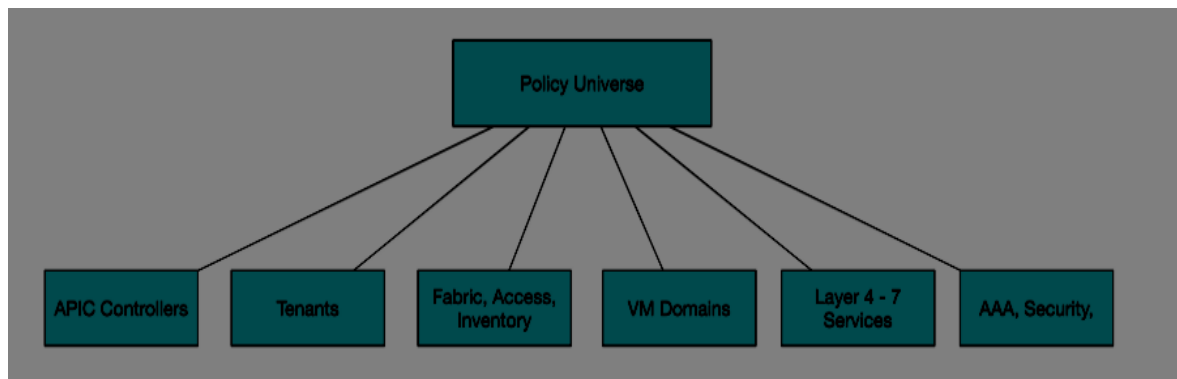


Figure 23 : arbre d'information de gestion MIT

Exercice:

Pour commencer, nous devons parcourir et connecter à l'interface du contrôleur APIC comme suit :

```
URL: https://sandboxapicdc.cisco.com
User: admin
Password: ciscopsdt
```

Figure 25 : Les informations d'accès au simulateur APIC

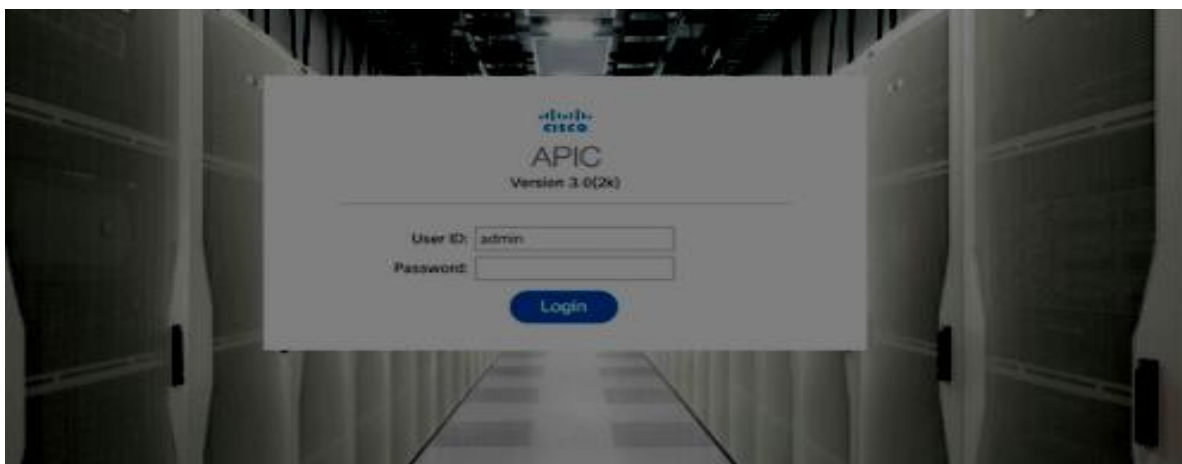


Figure 24 : Interface de login au contrôleur APIC

2 Créer des locataires :

Les locataires peuvent être ce que nous voulons (dans des limites raisonnables), ils peuvent être un client ou une unité commerciale au sein d'une entreprise ou un groupe de règles. Le terme «locataire» est flexible, mais chaque locataire est (par défaut) une unité isolée au sein de la structure. Il s'agit d'un conteneur logique, qui peut rester autonome ou, au moyen de contrats, partager des ressources avec d'autres locataires.

Le MIT pour le locataire est présenté ci-dessous.

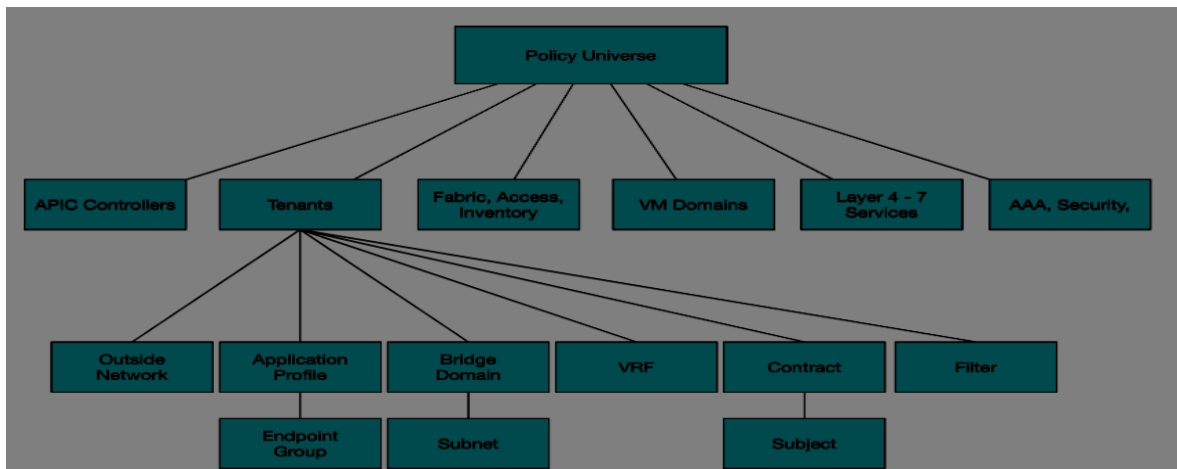


Figure 26 : Le MIT du locataire

Comme on peut le voir sur le diagramme ci-dessus, les locataires contiennent différents composants, notamment des profils d'application, des domaines de pont, des VRF (également appelés «contextes») et des contrats. Certains de ces composants, tels que les domaines de pont, ont leurs propres composants, tels que les sous-réseaux.

Nous avons quelques locataires préconfigurés. Il s'agit du locataire «commun», qui contient les stratégies des services partagés, tels que les pare-feu, les paramètres DNS, le locataire «Infrastructure», qui contient les stratégies et les pools VXLAN, et du locataire «Mgmt», ou du client de gestion. Qui est utilisé pour l'accès hors bande, la découverte de matrice. Les locataires que nous configurons entrent dans la catégorie des locataires «utilisateurs». Dans cette recette, nous allons créer notre premier locataire.

Nous avons créé un locataire qui s'appelle ENSAS_Tenant



Figure 27 : Création d'un locataire

Nous n'avons pas encore de composants, commençons donc par configurer un domaine de pont.

3 Configuration des domaines du pont :

Les domaines de pont (BD) fournissent des transferts de couche 2 au sein du fabric, ainsi qu'une limite de couche 2. Un BD doit être lié à VRF (également appelé contexte) et doit avoir au moins un sous-réseau associé. Les BD définissent l'espace d'adressage MAC unique de la couche 2 ainsi que le domaine flood (si flooding est activée).

Les domaines de pont peuvent être publics, privés ou partagés. Les domaines de pont publics sont les endroits où le sous-réseau peut être exporté vers une connexion routée, tandis que les domaines privés s'appliquent uniquement dans la location. Les domaines de pont partagés peuvent être exportés vers plusieurs VRF au sein du même client hébergé ou entre les hébergés lorsqu'ils font partie d'un service partagé.

Dans cette étape, nous allons créer un domaine de pont ENSAS_BD et définir avec lui un VRF ENSAS_VRF et un sous-réseau 10.0.0.0/24 pour la communication au sein de la location.

Nous choisissons de créer un VRF associé à ce domaine du pont à partir de son menu.

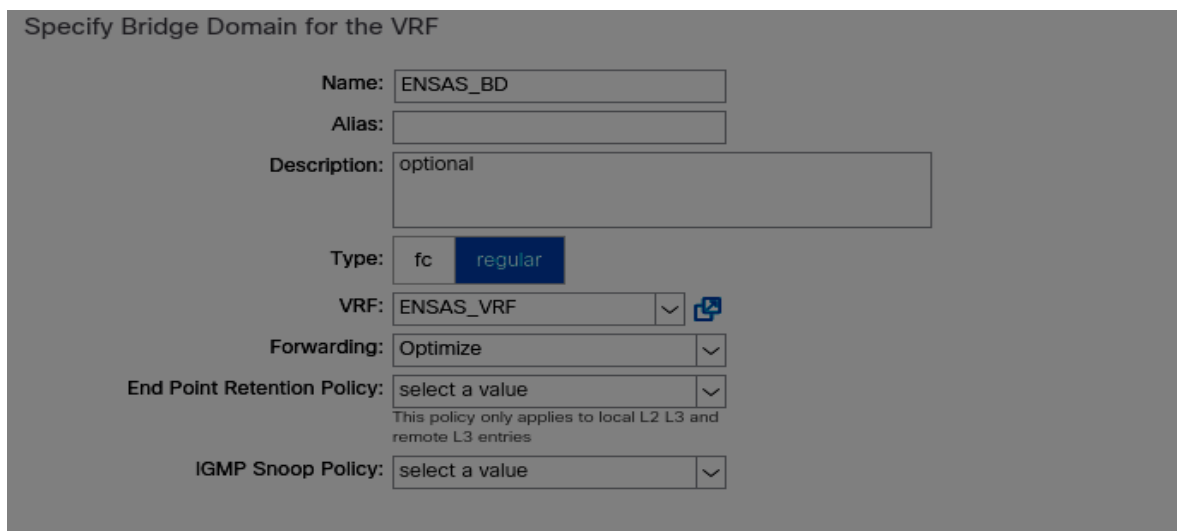


Figure 28 : création d'un VRF associé à un domaine du pont

Puis nous créons un sous réseau associe à ce domaine du pont.

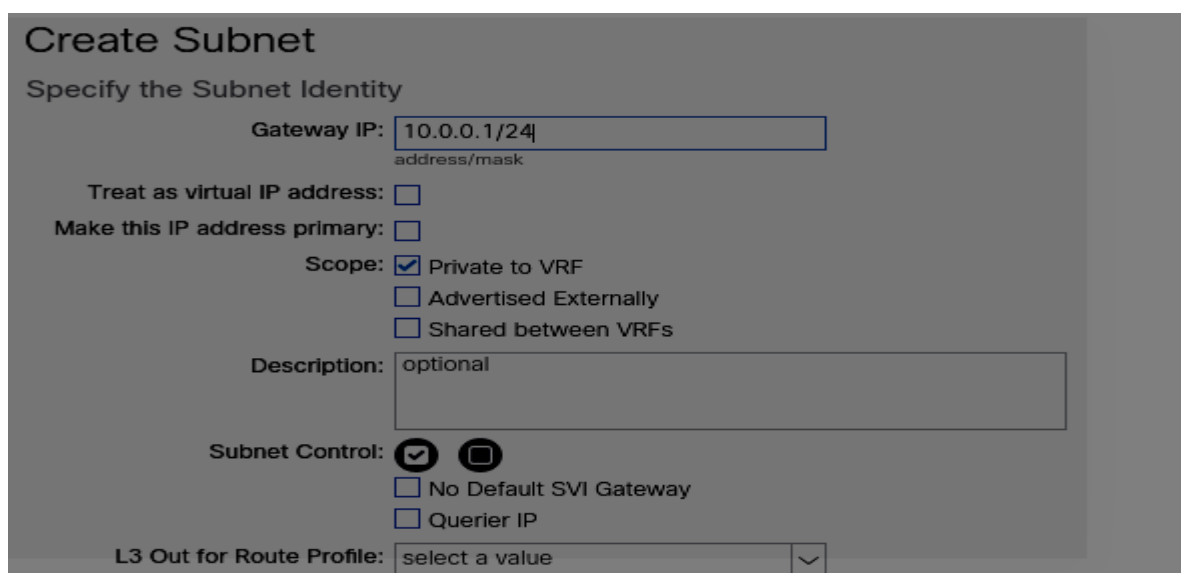


Figure 29 : création d'un sous réseau

Private to VRF signifie que le sous-réseau ne sera pas annoncé à l'extérieur (en dehors du VRF). Annoncé en externe signifie juste cela, et sera marqué pour l'annonce via un protocole de routage à un périphérique externe. Le partage entre les VRF est similaire à l'annonce à l'externe, mais reste dans le fabric.

Parce que nous nous concentrons uniquement sur ENSAS_Tenant, à ce stade, nous allons utiliser l'option Private to VRF.

4 *Configuration des contextes :*

Jusqu'à présent, nous avons configuré un locataire et créé un domaine de pont et un contexte pour celui-ci. Les contextes, également appelés VRF (Virtual Routing and Forwarding), sont des domaines de transfert de couche 3 uniques. Vous pouvez avoir plusieurs VRF au sein d'un locataire et ces derniers peuvent être associés à plusieurs domaines de pont (mais nous ne pouvons pas associer un domaine de pont à plusieurs VRF).

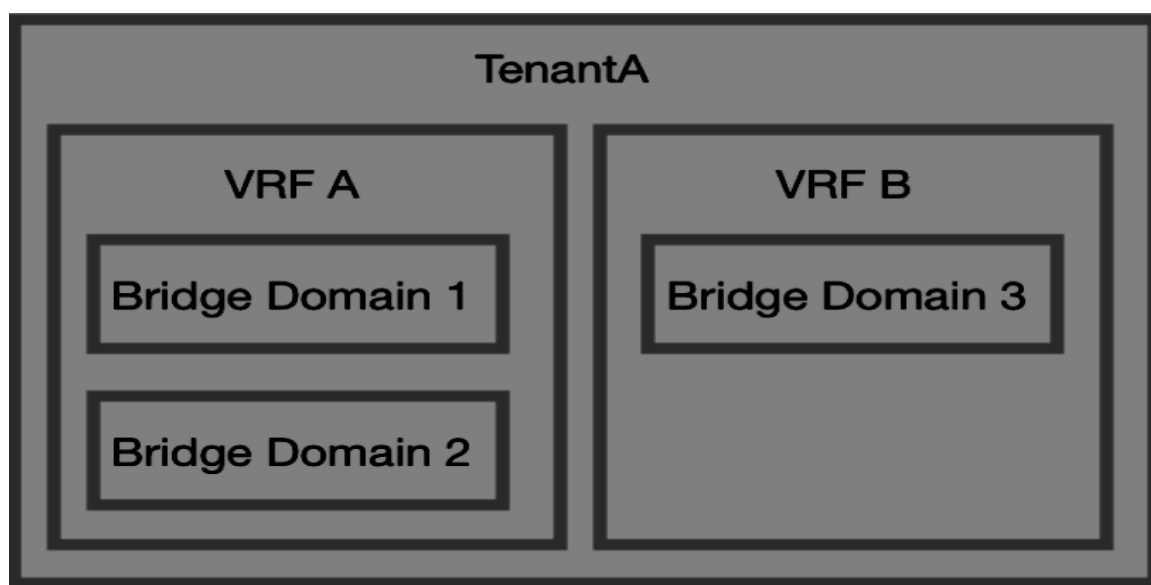


Figure 30 : les domaines de pont à créer

Dans cette étape, nous allons créer un deuxième VRF ENSAS_VRF2 sous ENSAS_Tenant et un nouveau domaine de pont ENSAS_BD2.

Create VRF

STEP 1 > VRF

Specify Tenant VRF

Name:

Alias:

Description:

Policy Control Enforcement Preference: ☒ Enforced ☐ Unenforced

Policy Control Enforcement Direction: ☐ Egress ☒ Ingress

BD Enforcement Status: ☐

End Point Retention Policy:
This policy only applies to remote L3 entries

Monitoring Policy:

DNS Labels:
enter names separated by comma

Route Tag Policy:

Create A Bridge Domain: ☒

Configure BGP Policies: ☐

Configure OSPF Policies: ☐

Configure EIGRP Policies: ☐

Figure 31 : création d'un VRF 1

Create VRF

STEP 2 > Bridge Domain

Specify Bridge Domain for the VRF

Name:

Alias:

Description:

Type: ☐ fc ☒ regular

Forwarding:

IGMP Snoop Policy:

Monitoring Policy:

ND policy:

ARP Flooding: ☐ Enabled

Endpoint Dataplane Learning: ☒

Limit IP Learning To Subnet: ☒

Config BD MAC Address: ☒

MAC Address:

Figure 32 : création d'un VRF 2

5 Création de profils de réseau d'application

Les profils d'application (AP) sont des conteneurs pour le regroupement un groupe des points de terminaison, (EPGs). Nous pouvons avoir plus d'un EPG avec un AP. Par exemple, un AP peut regrouper un serveur Web avec la base de données principale, avec le stockage, etc. Les EPG sont attribués à différents domaines de pont.

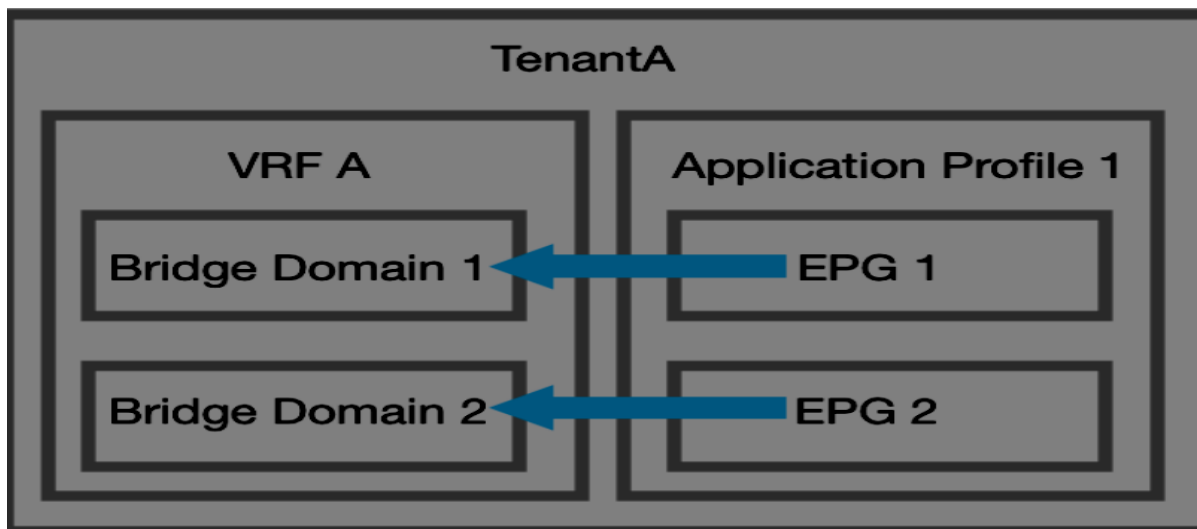
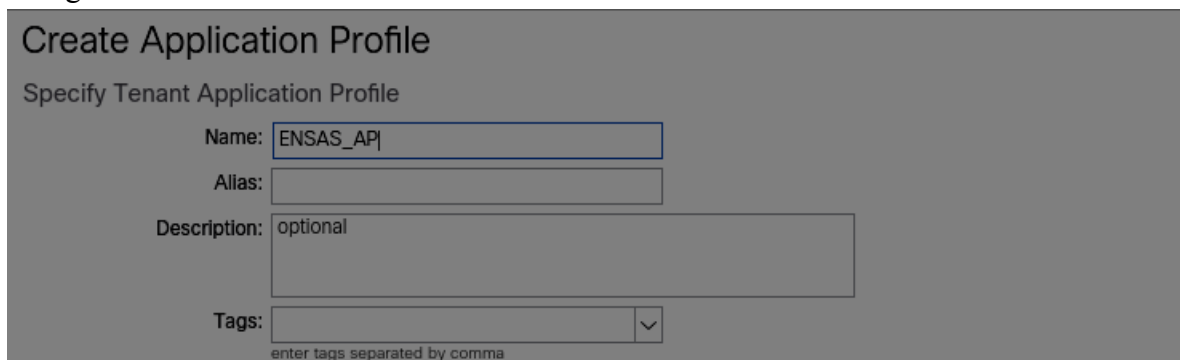


Figure 33 : association des domaines de pont avec les EPGs

Les profils d'application définissent différents aspects de la location, de la sécurité, de la qualité de service, des accords de niveau de service (Service Level Agreements (SLAs)) et des services de la couche 4 à la couche 7. Les AP sont tellement intrinsèquement liés aux EPG (et contractuels dans une moindre mesure) qu'il est plus difficile de les créer séparément.

Pour cette raison, nous les créons dans une seule étape. Comme vous pouvez le voir sur l'image ci-dessous.



The screenshot shows a web form titled 'Create Application Profile'. Below the title is the instruction 'Specify Tenant Application Profile'. The form contains the following fields:

- Name:** A text input field containing 'ENSAS_API'.
- Alias:** An empty text input field.
- Description:** A text input field containing 'optional'.
- Tags:** A text input field with a dropdown arrow on the right. Below it, a small note says 'enter tags separated by comma'.

Figure 34 : Création d'un Profile d'application

Nous devons également créer un groupe de points de terminaison associé à ce dernier profil d'application puis nous allons associer le domaine de pont ENSAS_BD avec cet EPG.

6 Création de groupes de terminaux (EPGs):

Les groupes de points de terminaison sont des objets gérés qui contiennent (sans surprise) des points de terminaison. Les points finaux sont des périphériques connectés au réseau, directement ou indirectement. Les points finaux ont certains attributs, tels qu'une adresse, un emplacement; ils peuvent être physiques ou virtuels. Les groupes de points de terminaison sont un groupe logique de ceux-ci, basés sur des facteurs communs. Les facteurs sont davantage liés aux entreprises, tels que des exigences de sécurité communes, que les ordinateurs d'extrémité nécessitent une mobilité de machine virtuelle, aient les mêmes paramètres de qualité de service ou utilisent les mêmes services L4-L7. Par conséquent, il est logique de les configurer en tant que groupe.

Les EPG peuvent s'étendre sur plusieurs commutateurs et sont associés à un domaine de pont. Il n'existe pas de mappage un-à-un entre un EPG et des sous-réseaux particuliers, et l'un des avantages intéressants de l'appartenance à un EPG est qu'il peut être statique pour un équipement physique ou dynamique lorsque nous utilisons l'APIC avec les contrôleurs de machine virtuelle.

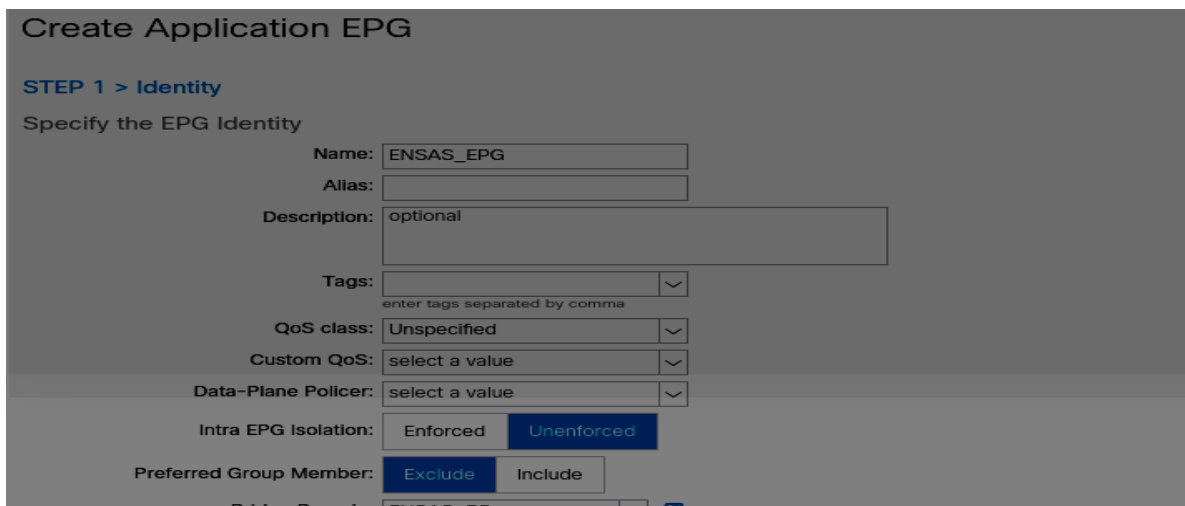


Figure 35 : Création d'un EPG

Nous pouvons commencer à voir les différents composants du fabric ACI commencer à fusionner ensemble maintenant, nous permettant de comprendre comment ils se lient tous ensemble. Une machine virtuelle (point de terminaison) peut être affectée à un groupe de points de terminaison lié à un profil d'application. Le groupe de points de terminaison est associé à un domaine de pont, qui contient le sous-réseau (ou les sous-réseaux) et, à son tour, le domaine de pont est lié à une instance de VRF. Le VRF contrôle notre routage et tous ces composants constituent le locataire.

Le locataire est pour le moment très isolé. Si nous devons ajouter un autre locataire dans le fabric, les deux ne pourraient pas communiquer. Nous pouvons permettre la communication entre locataires en utilisant des contrats. C'est ce que nous allons commencer à mettre en place ensuite.

7 Utilisation de contrats entre locataires :

Les contrats permettent aux EPG de communiquer les uns avec les autres, conformément aux règles que nous avons définies. Les contrats peuvent être très détaillés, notamment le protocole, le port et la direction du trafic. Nous n'avons pas besoin d'un contrat pour le trafic intra-EPG, cela est implicitement autorisé, mais un contrat est essentiel pour le trafic inter-EPG.

Un EPG peut être un fournisseur de contrat, un consommateur de contrat ou peut remplir les deux fonctions; fournir et consommer en même temps. Nous pouvons également fournir ou utiliser plusieurs contrats simultanément. Les contrats sont (pour les simplifier) des listes d'accès. Cependant, ils ne sont pas liés par les mêmes limitations que les listes d'accès. Pour essayer de simplifier la définition de fournisseur et de consommateur, nous avons deux contrats. L'un ouvre l'accès HTTP à une destination particulière (il fournit), l'autre autorise l'accès de l'autre EPG au serveur HTTP (consommateur). Nous pouvons également être moins stricts et disposer d'un accès TCP et UDP complet entre deux EPG. Par conséquent, nous aurons deux contrats et les deux EPG consomment l'un et fournissent l'autre, permettant ainsi une connectivité bidirectionnelle complète.

1. Nous devons créer un autre locataire pour cette étape. Nous répétons les étapes précédentes en utilisant les paramètres suivants:

Locataire: ENSAS_2_Tenant, Domaine du pont: ENSAS_2_BD, VRF: ENSAS_2_VRF

Sous-réseau: 10.0.1.1/24 Profil d'application: ENSAS_2_AP EPG: ENSAS_2_EPG

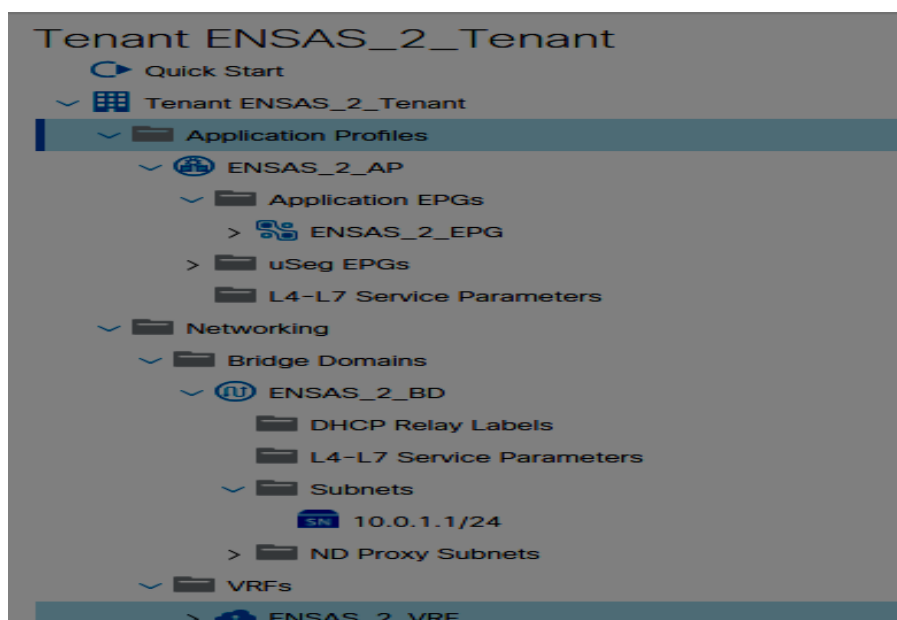


Figure 36 : création du deuxième Locataire

2. nous avons créé un autre locataire, mais pour le moment, les deux ne seront pas en mesure de communiquer. Nous devons modifier les sous-réseaux que nous avons créés et les définir sur «Shared between VRFs» pour les deux sous-réseaux (10.0.0.0/24 et 10.0.1.0/24) du locataire « ENSAS_2_Tenant ».



Figure 37 : création du deuxième sous réseau

3. Nous allons créer un contrat très basique. ENSAS_Tenant sera le fournisseur et ENSAS_2_Tenant sera le consommateur du contrat.

Security Policies - Contracts

| Name | Alias | Scope | QoS Class | Target DSCP | Subjects |
|----------------|-------|-------|-------------|-------------|---------------|
| ENSAS_Contract | | VRF | Unspecified | Unspecified | ENSAS_Subject |

Figure 38 : Création d'une Contrat

Create Filter

Specify the Filter Identity

Name: ENSAS_HTTP_Filter

Alias:

Description: optional

Entries:

| Name | Alias | EtherType | ARP Flag | IP Protocol | Match Only Fragments | Stateful | Source Port / Range | | Destination Port / Range | | TCP Session Rules |
|------|-------|-----------|----------|-------------|----------------------|----------|---------------------|-------------|--------------------------|------|-------------------|
| | | | | | | | From | To | From | To | |
| HTTP | | IP | | tcp | False | False | unspecified | unspecified | http | http | Unspecified |

Figure 39 : Création d'un filter

L'étape suivante consiste à l'attacher à l'EPG. Nous le faisons à partir de l'option Contrats sous le profil d'application du locataire.

Add Provided Contract

Select a contract

Contract: ENSAS_Contract

QoS: Unspecified

Contract Label:

Subject Label:

Figure 40 : création d'un contrat fourni

Nous devons faire la même chose avec ENSAS_2_Tenant, cette fois en le définissant comme un contrat consommé, mais avant nous devons changer la portée du contrat car la portée est définie sur «VRF». Nous avons besoin que la portée soit définie sur «Global» afin que les autres locataires puissent la voir.

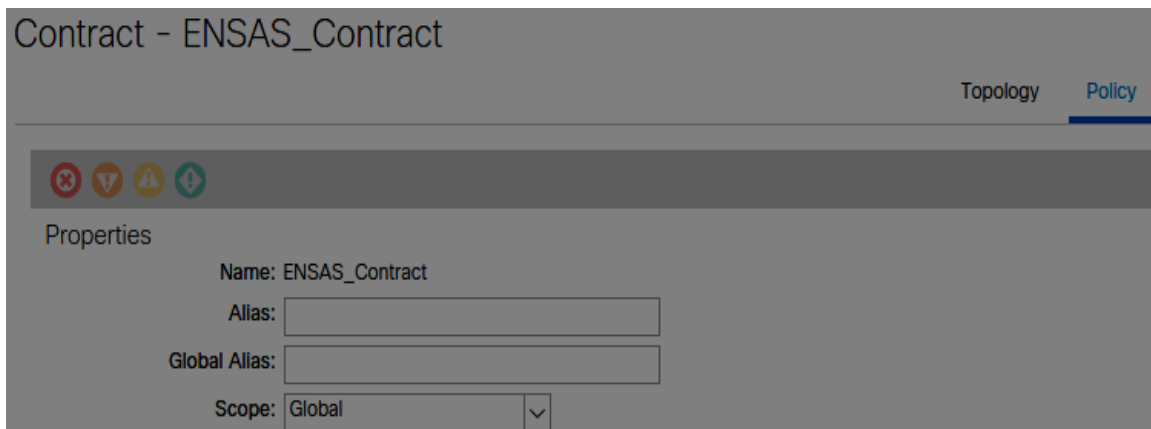


Figure 41 : création d'un contrat consommé

Nous devons exporter le contrat maintenant. De ENSAS_Tenant> Règles de sécurité, définissons le nom de l'exportation, sélectionnons le contrat créé précédemment et sélectionnez ENSAS_2_Tenant.



Figure 42 : contrat exporte

Nous devrions maintenant pouvoir voir le contrat exporté être importé dans ENSAS_Tenant.

Add Consumed Contract Interface

Select a contract interface

Contract Interface:

QoS:

Figure 43 : le contrat exporté a l'autre locataire

Nous pouvons maintenant voir le contrat énuméré.

Contracts

[Contracts](#)

| Tenant Name | Tenant Alias | Contract Name | Contract Type | Provided / Consumed | QoS Class |
|-----------------------------------|--------------|-------------------------|--------------------|---------------------|-------------|
| Contract Type: Contract Interface | | | | | |
| ENSAS_2_Tenant | | ENSAS_Exported_Contract | Contract Interface | Consumed | Unspecified |

Figure 44 : affichage du contrat crée

8 Création de filtres

Dans cette étape, nous allons créer un filtre et l'appliquer au contrat que nous avons créé précédemment.

1. créer un filtre pour le protocole https.

Create Filter

Specify the Filter Identity

Name:

Alias:

Description: optional

Entries:

| Name | Alias | EtherType | ARP Flag | IP Protocol | Match Only Fragments | Stateful | Source Port / Range | | Destination Port / Range | | TCP Session Rules |
|-------|-------|-----------|----------|-------------|----------------------|----------|---------------------|-------------|--------------------------|-------|-------------------|
| | | | | | | | From | To | From | To | |
| HTTPS | | IP | | tcp | False | False | unspecified | unspecified | https | https | Unspecified |

Figure 45 : création d'un filtre pour le protocole https

2-Pour attacher ce filtre au contrat, nous devons sélectionner le contrat que nous avons créé précédemment.

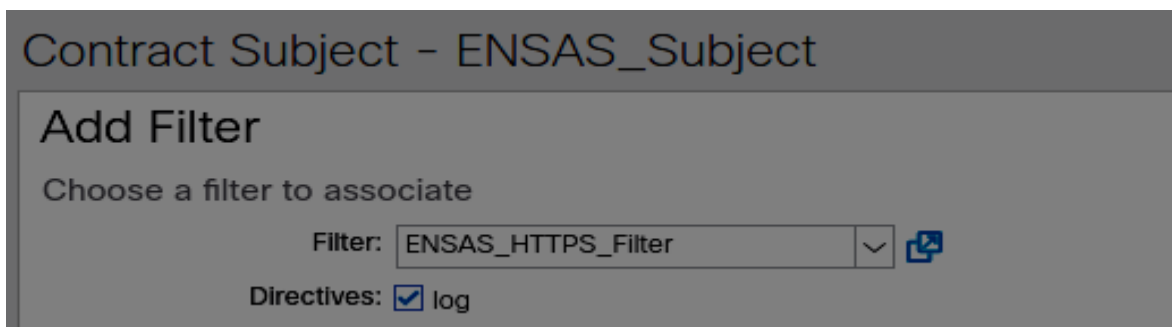


Figure 46 : attaché le filtre au contrat déjà crée

3-Enfin, nous voyons notre filtre assis à côté du filtre par défaut de l'étape précédente.

| Filters: | | | | |
|--------------------|--------------|------------|--------|--|
| Name | Tenant | Directives | State | |
| ENSAS_HTTP_Filter | ENSAS_Tenant | | formed | |
| ENSAS_HTTPS_Filter | ENSAS_Tenant | log | formed | |

Figure 47 : affichage des filtres créés

La configuration des contrats entre différents locataires est la plus difficile des options.